Intégration des moyens de paiement non bancaires sur Internet

Refka Abdellaoui

UNIVERSITÉ de CAEN BASSE-NORMANDIE

U.F.R. de Sciences
École doctorale S.I.M.E.M

THESE

présentée par

Refka ABDELLAOUI

et soutenue

le 4 juillet 2012

en vue de l'obtention du

Doctorat de l'Université de Caen Basse-Normandie
Spécialité : spécialité

Arrêté du 7 août 2006

Intégration des moyens de paiement non bancaires sur Internet

MEMBRE du JURY

M. Pascal Urien	Professeur à TELECOM ParisTech	(Rapporteur)
M. Pascal Berthomé	Professeur à ENSI-Bourges	(Rapporteur)
M. Nicolas Benady	Ingénieur (co-fondateur) à LIMONETIK	(Invité)
M. Olivier Berthelier	Ingénieur (co-fondateur) à LIMONETIK	
M. Christophe Rosenberger	Professeur à l'ENSICAEN	
Mme. Maryline Laurent	Professeur à TELECOM et Management SudParis	
M. Marc Pasquet	Professeur à l'ENSICAEN	(Directeur de thèse)

Remerciements

Résumé

Le commerce électronique ou E-commerce peut être défini comme l'ensemble des échanges électroniques liés aux activités commerciales. Il recouvre toute opération de vente de biens et de services via un canal électronique. Internet n'est donc qu'un support parmi d'autres du E-commerce avec, entre autres, l'EDI (échanges des données informatisées), le Minitel (en France) voire le téléphone ou la télévision. Cependant, si le commerce électronique n'est pas un phénomène nouveau, le développement très rapide d'Internet lui apporte une nouvelle dimension. Dans cette étude, le terme commerce électronique (ou E-commerce) est alors restreint aux opérations dont le support est Internet.

Tout comme dans le commerce physique (appelé également commerce de proximité), plusieurs acteurs sont impliqués dans le commerce électronique. Afin de vendre ses services/biens, l'E-commerçant doit se munir d'un terminal de paiement électronique « virtuel ». Ce terminal permet à l'E-commerçant, d'un côté, d'acquérir les paiements électroniques, il fait dans ce cas partie d'un système d'acquisition, et d'un autre côté, d'accepter les **moyens de paiement** du client et dans ce cas, il fait partie d'un système d'acceptation. Un moyen de paiement étant un instrument de paiement permettant à un client donné de réaliser une opération de paiement, c'est-à-dire tout instrument qui permet à son utilisateur de réaliser un transfert de fonds monétaires. Cependant, l'**intégration** d'un terminal de paiement électronique pose des problèmes différents selon qu'il s'agit du monde physique « réel » ou du monde « virtuel ».

Dans notre travail, nous optons pour une approche orientée marchand (« Merchant-Centric ») où nous nous plaçons dans le système d'acceptation. En d'autres termes, nous nous intéressons à l'intégration des terminaux de paiements électroniques virtuels dans les E-boutiques afin de permettre aux E-commerçants d'accepter des moyens de paiement. D'autant plus qu'avec l'apparition de nouvelles technologies et l'évolution des règlementations, on voit émerger progressivement de nouveaux

usages dans le commerce électronique sur Internet. Ainsi, ces dernières années, le paiement électronique a pu vivre plusieurs évolutions importantes tant au niveau des équipements qu'au niveau des architectures. Ces évolutions ont facilité l'émergence de nouveaux acteurs qui ont contribué à développer de nouvelles fonctionnalités des paiements sur Internet. Cependant, de nombreux moyens de paiement ne sont pas encore acceptés dans l'E-commerce. De plus, les systèmes de paiement actuels ne permettent pas plusieurs fonctionnalités comme : l'intégration flexible et transparente d'un nouveau moyen de paiement et l'agrégation de plusieurs moyens de paiement alternatifs à la carte bancaire (comme les cartes cadeaux, les cartes de fidélité, etc.). Dans ce document, le terme « moyens de paiement alternatifs » désigne les moyens de paiement émergents.

L'objectif global de cette thèse est d'analyser les différentes procédures d'intégration de ces nouveaux moyens de paiement « alternatifs » afin de déterminer dans quelle mesure cette intégration est coûteuse en termes de temps, de ressources et de prix pour l'E-commerçant. Le but de notre travail est de proposer un nouveau système de paiement facile à intégrer dans l'E-commerce, sécurisé et qui propose de nouvelles fonctionnalités, tout en respectant les exigences d'un système de paiement sur Internet.

Afin de résoudre le problème d'intégration des moyens de paiement non bancaires sur Internet, nous proposons une nouvelle architecture de paiement permettant de convertir les paiements non bancaires en paiements bancaires à l'aide des cartes virtuelles dynamiques. Cette architecture permet d'appréhender facilement des échanges complexes entre les différents acteurs du système de paiement afin de diminuer la complexité de l'intégration des moyens de paiement alternatifs pour l'E-commerçant. Nous proposons par la suite une approche d'intégration de cette architecture dans le site E-commerce qui consiste à rendre possible l'acceptation de plusieurs moyens de paiement alternatifs sur Internet sans aucune intégration technique chez l'E-commerçant. Il s'agit de concevoir un Proxy Web qui joue le rôle d'intermédiaire entre le navigateur du client et le serveur du site marchand.

Malgré la facilité d'intégration de cette solution pour l'E-marchand, cette solution présente quelques inconvénients à cause de la nécessité de passer par un portail afin d'utiliser le nouveau moyen de paiement sur le site marchand et de maintenir continuellement des configurations Proxy des sites E-commerce. Pour parer à ces inconvénients, une deuxième approche est proposée. Il s'agit d'une approche qui permet de ne pas altérer l'expérience utilisateur sur le site E-commerce tout en facilitant l'intégration des nouveaux moyens de paiement et qui consiste à intégrer un Plugin JavaScript dans la page de choix de moyens de paiement du site E-commerce.

Summary

Table des matières

Introduction générale

Présentation du contexte

Le Commerce électronique (ou E-commerce) concerne l'ensemble des échanges électroniques liés à la vente de biens et de services sur les réseaux informatiques. Dans notre travail, nous nous sommes intéressés au réseau Internet. La diffusion rapide d'Internet a fait du commerce électronique un nouvel outil efficace pour des transactions monétaires. Le E-commerce est en train de vivre une mutation importante, tant de ses équipements que ses architectures et son organisation, depuis l'utilisation de la carte bancaire sur Internet à l'aide des terminaux de paiement électroniques « virtuels » par extension aux terminaux de paiement électroniques « physiques » dans le commerce physique. Dans notre travail, nous nous plaçons dans un contexte français qui peut être étendu au contexte européen surtout après l'avènement de l'espace unique de paiement en euro SEPA (Single Euro Payment Area).

Le nombre de paiement lié à la vente sur Internet est en constante progression depuis plusieurs années. Certes, la migration vers le commerce électronique sur le Web rencontre plusieurs freins, mais il est important de préciser que les principaux indicateurs sont à la hausse : le nombre d'internautes, qu'ils soient domestiques ou professionnels, est en augmentation (d'après le rapport publié par le « Forum des droits d'Internet », l'année 2008 confirme la place de l'Internet dans le quotidien des Français et leur rattachement croissant à la toile) et le nombre de sites marchands qui continue à augmenter remarquablement. Selon une étude effectuée par ADN'co pour la société Limonetik (le partenaire industriel de cette thèse), le commerce électronique poursuit son développement avec une croissance annuelle de 20% des chiffres d'affaires en Europe dans les prochaines années.

Le commerce électronique actuel en Europe est essentiellement bancaire et s'articule autour des moyens de paiement traditionnels : carte bancaire, chèque, pré-

lèvement, virement, etc. Cependant, avec l'apparition de nouvelles technologies et l'évolution des règlementations, on a vu émerger progressivement de nouveaux moyens de paiement ainsi que le développement de plusieurs canaux de paiement sur Internet, en particulier le M-commerce (mobile) et le S-commerce (social). Plusieurs nouveaux acteurs se sont positionnés sur la chaîne de valeur de paiement créant ainsi de nouvelles fonctionnalités de paiement et de nouveaux besoins.

Positionnement de la problématique

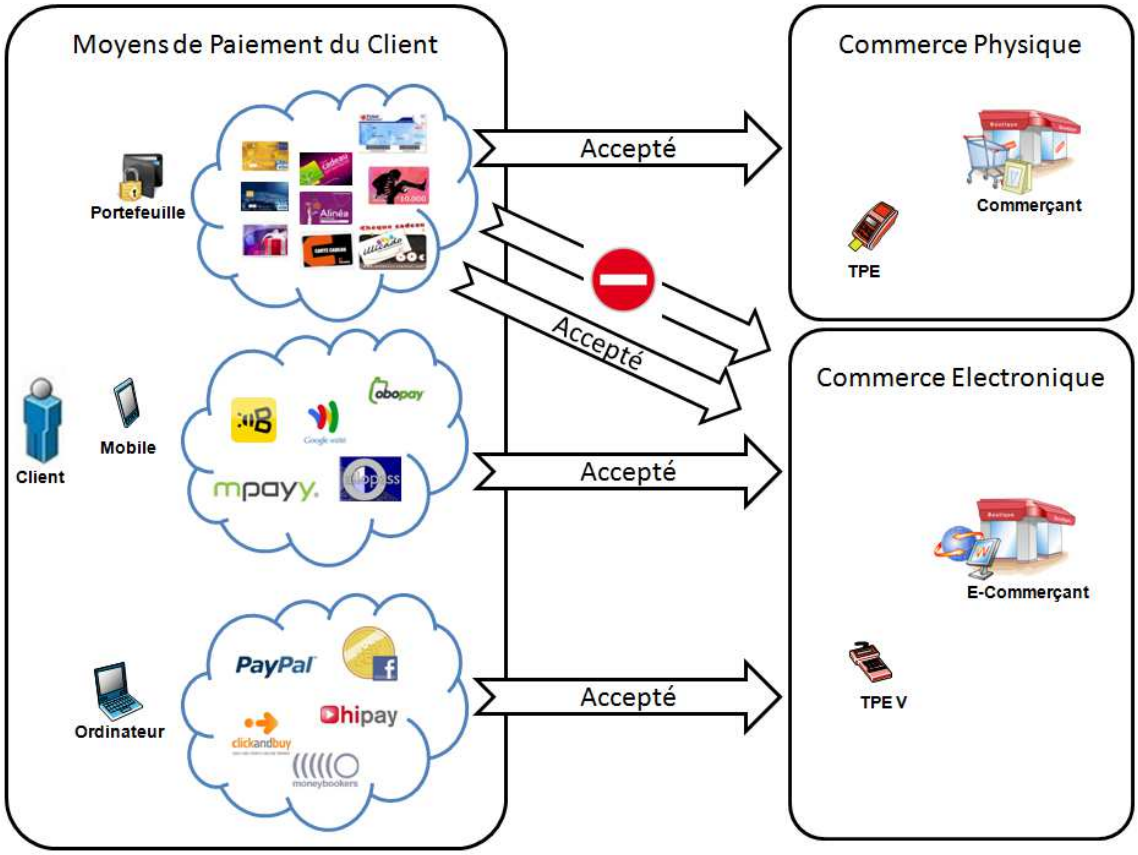


FIGURE 0.1 – Le problème d'intégration des moyens de paiement non bancaires sur Internet

Un client qui dispose de plusieurs moyens de paiement et qui a l'habitude de les utiliser dans le commerce physique (citons par exemple : les tickets restaurants, les cartes cadeaux, les listes de mariage, etc.), a tendance généralement à vouloir les utiliser également sur Internet. Cependant, les E-commerçants n'acceptent pas, actuellement, tous les moyens de paiement utilisés dans le commerce de proximité. Seuls les moyens de paiement classiques (bancaires) sont communément acceptés dans

le commerce électronique sur Internet (comme dans l'exemple décrit dans la figure 0.1). En plus, le client peut potentiellement avoir à disposition de nouveaux moyens de paiement propre au Web (Paypal, Buyster, Facebook Crédits, etc.), qu'il veut également utiliser pour payer ses achats sur Internet. Même ces nouveaux moyens de paiement ne sont pas tous acceptés par les marchands sur Internet. Nous constatons également que, malgré les évolutions technologiques, le commerce électronique sur Internet est encore très restreint en fonctionnalités comparé à celui de proximité. En effet, un commerçant dans une boutique physique, propose plusieurs moyens de paiement en plus des moyens de paiement classiques, il offre également au client la possibilité de payer son panier avec plusieurs moyens de paiement à la fois. En revanche, ces fonctionnalités sont peu ou pas encore proposées sur Internet.

En nous plaçant dans le cadre de l'E-commerce sur Internet, nous proposons d'analyser les raisons de ces différents écarts afin d'apporter une réponse permettant de faciliter l'accès pour les clients et les E-commerçants aux moyens de paiement non bancaires sur la toile. Cette problématique peut être traitée sous plusieurs angles : technique, commercial, contractuel, financier, etc. Dans le cadre de cette thèse nous nous intéressons à l'aspect technique de la problématique, l'objectif global étant de proposer une nouvelle plateforme de paiement qui permet l'intégration des moyens de paiement non bancaires dans les E-boutiques sur Internet. La nouvelle architecture qui en découle permet de pallier les différentes contraintes techniques d'intégration d'un système de paiement sur Internet et d'être conforme aux critères d'évaluation d'un système de paiement sur le Web. Le problème d'acceptation des nouveaux moyens de paiement sur Internet, est, selon nous, fortement lié aux problèmes d'intégration dans le site Web du marchand et à la gestion de la commande E-commerce.

Le besoin de nouvelles architectures

Malgré la croissance rapide de l'E-commerce, les systèmes de paiement actuels présentent quelques limites empêchant l'acceptation des nouveaux moyens de paiements non bancaires sur Internet :

- Le manque d'applicabilité : la grande majorité des sites marchands n'acceptent pas des moyens de paiement particuliers ce qui limite la capacité de paiement.
- Le manque d'éligibilité : n'importe quel client avec de l'argent et l'intention de payer, n'est pas toujours en mesure d'effectuer un paiement sur Internet.
- Le manque d'efficacité : certains paiements sur Internet sont de petits montants. Les frais de gestions des cartes bancaires sont, dans ce cas, assez chers ce qui rend les paiements de petits montants impossibles.

- Des coûts élevés : des frais d'usage élevés pour les clients et les marchands. Les systèmes de paiements actuels ont une infrastructure coûteuse afin de sécuriser le processus de paiement.

La nécessité de proposer une nouvelle architecture de paiement émerge donc clairement de la situation actuelle. Dans ce contexte, nous proposons une nouvelle architecture de paiement, tout en optant pour une approche orientée marchand « Merchant-Centric ». Il existe deux façons classiques d'aborder un processus de conception d'une architecture, qu'il soit appliqué au bâtiment ou au logiciel. La première est qu'un concepteur parte de zéro (avec une feuille blanche, un tableau blanc...) et construise petit à petit une architecture à base de composants connus jusqu'à ce que cette architecture satisfasse les besoins du système envisagé. La seconde approche consiste à commencer par les besoins du système dans son ensemble, sans contrainte. Puis, de façon incrémentale, les contraintes sont identifiées et appliquées aux éléments du système afin de différencier l'espace de conception et de permettre aux forces qui influencent son comportement de s'arranger naturellement, en harmonie avec le système. Le premier procédé met en avant la créativité et une imagination sans limite. Le second met l'accent sur les contraintes et la compréhension du contexte du système. L'architecture proposée dans le cadre de cette thèse a été conçue en utilisant le second processus.

Ce manuscrit de thèse est organisé en cinq chapitres. Le premier chapitre décrit l'évolution du commerce électronique sur Internet, les caractéristiques et les exigences d'un système de paiement et définit les nouveaux moyens de paiement « alternatifs » objet de notre travail. Le deuxième chapitre présente un état de l'art des principaux modes d'intégration des systèmes de paiement sur Internet. Cette étude définit les besoins et les caractéristiques des systèmes de paiement existants. Elle nous permet de situer notre démarche dans le cadre des travaux menés jusqu'à présent et de dégager les limites et les faiblesses des architectures existantes. Le troisième chapitre décrit nos propositions pour étendre les solutions de paiement existantes afin de permettre l'acceptation des nouveaux moyens de paiement. Nous développons dans le chapitre quatre une approche d'intégration via Proxy Web des nouveaux moyens de paiement sur Internet. Cependant, cette approche présente quelques inconvénients, raison pour laquelle, nous proposons dans le dernier chapitre une deuxième approche d'intégration via Plugin JavaScript. Ces approches sont suffisamment flexibles pour prendre en compte les exigences et les contraintes d'intégration d'un système de paiement sur Internet. Nous terminons nos propos par une conclusion dans laquelle nous réalisons un bilan de nos contributions et nous y présentons les voies de recherches ouvertes par notre travail.

Chapitre 1

Emergence de nouveaux moyens de paiement sur Internet

Ce chapitre introduit les principaux concepts du commerce électronique sur Internet afin de définir un référentiel terminologique nécessaire pour la suite de ce document. Nous présentons l'influence de l'évolution d'Internet sur l'E-commerce (section 1.2). Bien qu'il existe plusieurs classifications des moyens de paiements sur Internet, nous présentons dans ce chapitre une classification sommaire qui consiste à définir deux catégories : les moyens de paiement classiques et les moyens de paiement « alternatifs » (section 1.3). Puis nous présentons le système de paiement sur Internet ainsi que ses principaux acteurs et typologies (section 1.4). Enfin, nous nous intéressons aux exigences d'un système de paiement afin d'en déduire les critères importants à prendre en compte lors de la conception d'un système de paiement sur Internet (section 1.5). Ces critères nous serviront, par la suite, d'outils d'évaluation.

Sommaire

1.1 Introduction

Il est difficile d'aborder le commerce électronique sans évoquer l'essor extraordinaire de l'Internet et la croissance constante du nombre d'utilisateurs du réseau. En effet, le développement d'Internet à un niveau mondial favorise les échanges et les contacts entre la demande des consommateurs et l'offre des commerçants. L'évolution progressive de l'E-commerce favorise l'apparition de nouveaux moyens de paiement et de nouveaux besoins sur Internet. Cependant, nous constatons que certains nouveaux moyens de paiement ne sont pas encore disponibles sur Internet, ce qui va à l'encontre de l'expansion des technologies sur Internet. Nous proposons, dans le cadre de ce chapitre, d'analyser cette évolution, de présenter les nouveaux moyens de paiement objet de notre problématique. Nous en profitons également pour créer un référentiel terminologique commun en définissant ce qu'est un système de paiement sur Internet et ses principaux critères d'évaluation.

1.2 Situation actuelle complexe et contrastée

Nous décrivons, dans cette section, la situation actuelle de l'E-commerce sur Internet. Il s'agit d'une situation complexe et constatée dans laquelle les principaux indicateurs sont en évolution.

1.2.1 Internet et l'évolution du Web

Internet, dit réseau des réseaux, est considéré comme le support de toute l'information scientifique [Mennis A., 1999] : information « publiée », données, fichiers, images ou de sons, etc. Selon Richard J. SMITH, « *Le terme Internet est difficile à cerner, car il fait référence à d'innombrables services et possibilités ouvrant autant d'horizons jusque-là inconnus* ». Internet s'est imposé au grand public et est devenu beaucoup plus accessible et convivial grâce au système de consultation World Wide Web (WWW). Au début de l'apparition du Web, l'internaute n'avait pas un rôle central dans la navigation sur Internet, ce n'est plus le cas après l'émergence du Web 2.0. D'après une étude de Jean-François Gervais, intitulée *« Web 2.0, les internautes au pouvoir »* [Gervais J F., 2007], les concepts Web 2.0 ont créé de nouvelles relations avec l'internaute fondées sur un mode collaboratif permettant à chacun de s'exprimer, d'échanger et de personnaliser sa navigation. Le Web ne cesse d'évoluer tous les jours,

dans la recherche d'un « Web Intelligent » où les informations ne sont plus stockées, mais comprises par les ordinateurs afin d'apporter à l'utilisateur ce qu'il recherche véritablement [Floridi L., 2005].

L'usage d'Internet a également beaucoup évolué au cours des dernières années : il est passé d'un simple moyen convenable et pratique d'envoyer du courrier électronique à d'autres utilisateurs, à un réseau de commerce électronique, s'articulant par rapport au commerce « traditionnel ». Il crée des formes hybrides de distribution et encourage le recours à la « multi-modalité » dans le processus de consommation. Ce qui rend les frontières floues entre commerce « réel » et « virtuel ». En effet, le bouleversement apporté aujourd'hui par Internet aux processus d'achat des cyber-consommateurs joue un rôle primordial dans l'expansion de l'E-commerce [Lehuédé F, 2006].

1.2.2 Evolution de l'E-commerce

A l'ère des développements des réseaux informatiques, l'E-commerce est loin de se limiter de l'achat et à la vente à distance. Il englobe tout le processus de développement, de commercialisation, de vente, de livraison et de paiement des produits achetés par des communautés virtuelles de clients sur Internet [O'Brien T., 2000]. D'après l'Organisation de Coopération et Développement Economique OCDE, le commerce électronique peut être défini comme le processus de publicité, de vente, d'assurance et de paiement de produits sur des réseaux informatiques. Et selon ACSEL (Association pour le Commerce et les Service en Ligne), l'E-commerce a une définition restreinte et une définition plus extensive ; « Dans sa définition restreinte, l'E-commerce désigne l'ensemble des échanges commerciaux dans lesquels l'achat s'effectue sur un réseau de télécommunication. L'E-commerce recouvre aussi bien la simple prise de commande que l'achat avec paiement, et concerne autant les achats de biens que les achats de services, qu'ils soient eux-mêmes en ligne ou non [Lorentz F., 1998]. Dans une définition plus extensive, on peut inclure dans l'E-commerce, l'ensemble des usages commerciaux des réseaux. Il est bien entendu que l'E-commerce est avant tout du commerce et qu'Internet n'est qu'un moyen ou support de communication [Commission Commerce Electronique, 2012], comme entre autres, l'EDI (échanges des données informatisés), le minitel, la téléphonie, etc. Il recouvre toute opération de vente de biens et de services via un canal électronique ». Dans la suite du document, le terme E-commerce sera utilisé pour désigner le commerce électronique sur Internet.

Une façon d'aborder les usages de l'E-commerce consiste à identifier ses différentes typologies [Brousseau E., 2001] :

- Le B to B ou B2B (Business to Business) qui correspond à des transactions inter-entreprises [Macarez N. et Lesle F., 2001].

- Le B to C ou B2C (Business to Consumer) qui fait référence au commerce entre une entreprise et une personne privée [Macarez N. et Lesle F., 2001]. [Brousseau E., 1999].

A côté de ces deux grands ensembles commerciaux, on peut identifier d'autres types de relations moins médiatisées, car elles ne génèrent pas des revenus élevés :

- Le C to B ou C2B (Consumers to Business) qui représente une tentative de renversement de la logique des rapports entre demande et offre. Son principe de base est de s'appuyer sur les réseaux électroniques pour consolider la demande des particuliers et mettre en concurrence les offreurs [Brousseau E., 1999].
- C To C ou C2C (Consumer to Consumer) qui concerne des services d'intermédiation entre les particuliers.
- Le B to G ou B2G (Business to Government) qui concerne les transactions électroniques entre une entreprise et une administration gouvernementale [Mennis A., 2003] [Peressini C., 2001]. Cependant, il faut noter que les échanges commerciaux générés par le B2G sont en pratique souvent assimilables à du B2B stratégique [Le Crosnier H., 1997].
- le G to C ou G2C (Government to Consumer) qui touche les transactions électroniques entre une personne privée et une administration gouvernementale [Le Crosnier H., 1997] [Lorentz F., 1998].
- le E to E ou E2E (Employe to Employe) qui concerne les échanges électroniques entre au moins deux employés d'une même organisation.

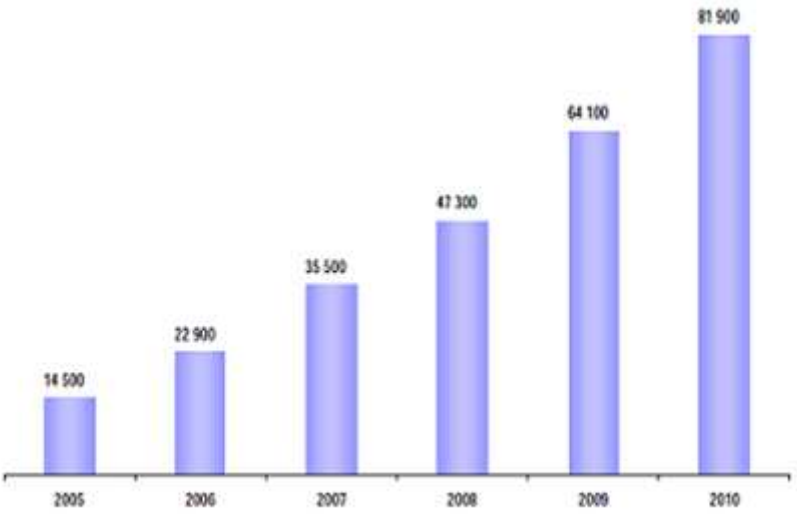


FIGURE 1.1 – Evolution du nombre de sites marchands actifs [Fevad, 2010b]

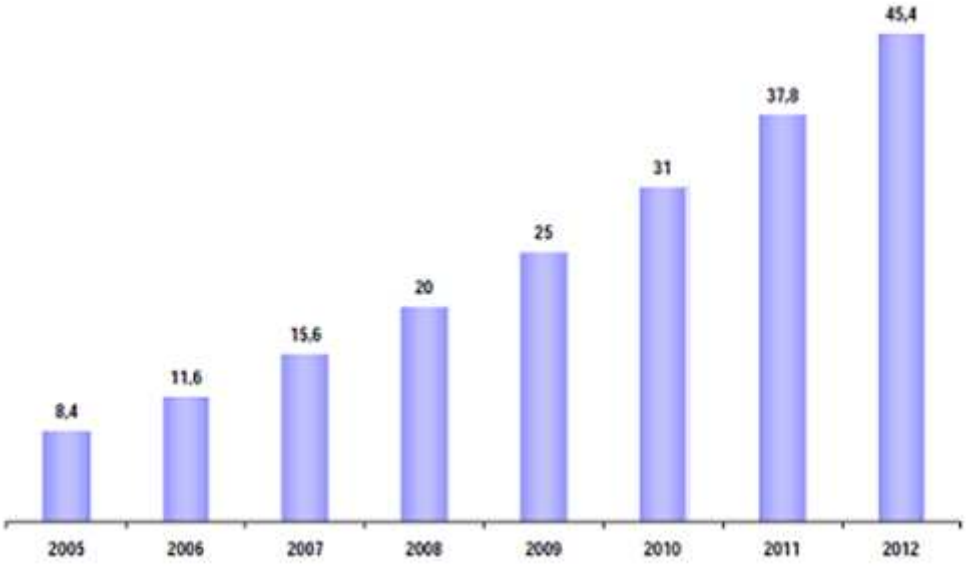


FIGURE 1.2 – Evolution du chiffre d'affaires de l'E-commerce [Fevad, 2010b]

Nous nous intéressons ici, plus particulièrement, au commerce B to C. La diffusion rapide d'Internet a fait du commerce électronique un nouvel outil efficace pour des transactions monétaires [Association Française de la Télématique, 1997]. Il a atteint 31 milliards d'euros en 2010, contre 8,4 milliards d'euros en 2005, soit une multiplication par 4 en 5 ans [Credoc-Institut Français de la Mode, 2011]. En cinq ans, le nombre de sites marchands actifs du E-commerce a été également multiplié par 5,6 : il est passé de 14 500 en 2005 à 81 900 en 2010 [CREDOC-FEVAD, 2010]. 17 800 sites ont été créés en 2010. Ce nombre de sites double tous les 2 ans environ. En 2010, 58% des personnes âgées de 18 ans et plus ont commandé des produits ou services par Internet, contre 51% 2 ans plus tôt [Fevad, 2010a] [CREDOC-FEVAD, 2008]. Les figures 1.1 et 1.2 montrent l'évolution remarquable d'E-commerce en nombre de sites marchands et nombre d'internautes.

La complexité des transactions du commerce électronique a également augmenté rapidement au cours des dernières années et plusieurs systèmes de paiement sont apparus. Il existe de nombreuses approches essayant de diviser la transaction E-commerce en plusieurs étapes. Parmi ces approches, on trouve celle de l'Observatoire de Systèmes de Paiement Electronique (ePSO) qui propose un modèle de transaction de commerce électronique en ligne basé sur la notion d'entrée-sortie [Lelieveldt Consultancy, 2001] [Bohle K., 2002] où le marchand et le client échangent une valeur monétaire contre des marchandises ou des services donnés et un institut financier intermédiaire qui garantit la validité de ces échanges monétaires.

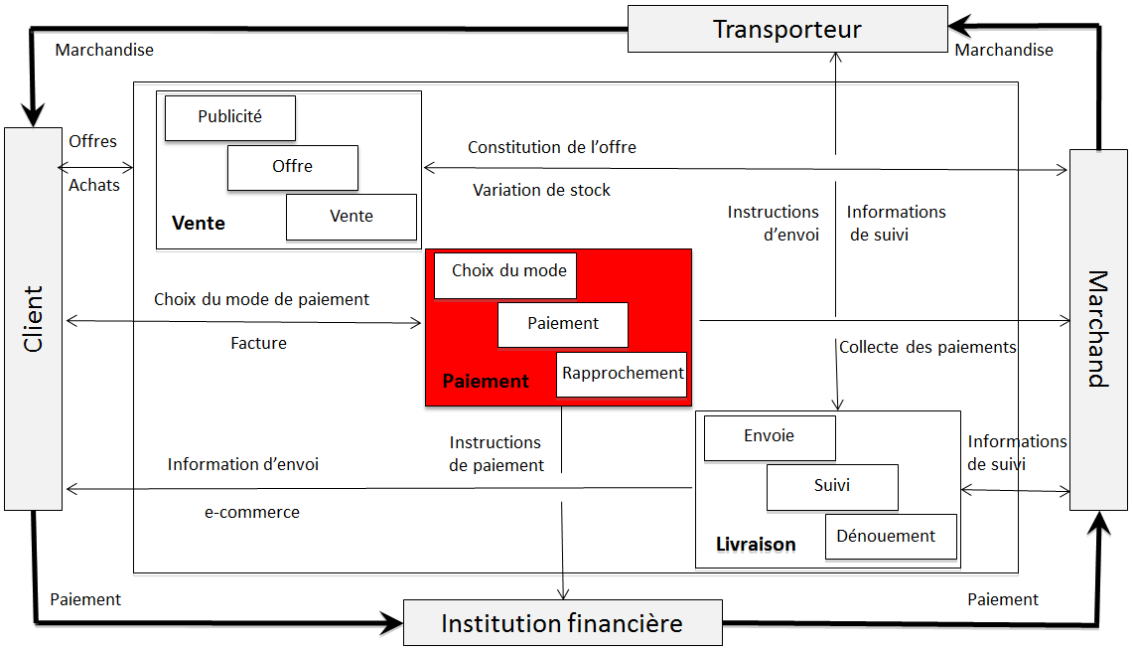


FIGURE 1.3 – Processus d'une transaction électronique sur Internet [Bohle K., 2002]

Cette approche, présentée dans la figure 1.3 et qui a été légèrement modifiée afin de l'adapter à notre vision de l'E-commerce d'aujourd'hui, montre qu'une transaction de commerce électronique comporte trois fonctions principales : vente, paiement et livraison. A gauche, la phase de vente comporte la publicité des produits et services vendus. A droite, la phase de livraison comporte la validation de paiement et la livraison de la commande. La phase de paiement est vue comme une partie centrale de la transaction en ligne pendant laquelle l'acheteur paye le vendeur. La page de choix de moyen de paiement ainsi que le rapprochement des transactions constituent une partie majeure de la phase de paiement.

1.2.3 Evolution de la monnaie électronique

Qui dit paiement électronique dit monnaie électronique. Mais avant de définir la monnaie électronique, il est intéressant de définir le terme monnaie : il s'agit d'un intermédiaire indispensable aux échanges. Elle est transmise entre les agents économiques à travers des instruments de paiement (appelés également moyens de paiement). Ainsi, un instrument de paiement correspond à « tout instrument qui permet à son utilisateur de transférer des fonds ». Il offre donc la possibilité de réaliser des opérations de paiement c'est-à-dire des versements, des transferts ou des retraits d'actifs monétaires. Dans les économies monétaires contemporaines, la monnaie peut être définie comme une créance sur un institut d'émission inscrite soit

sur du papier (monnaie fiduciaire) soit sur des livres (monnaie scripturale). Depuis des siècles, la monnaie a pris plusieurs formes qui sont présentées dans la figure 1.4, de la monnaie marchandise à la monnaie électronique en passant par la monnaie métallique et fiduciaire.

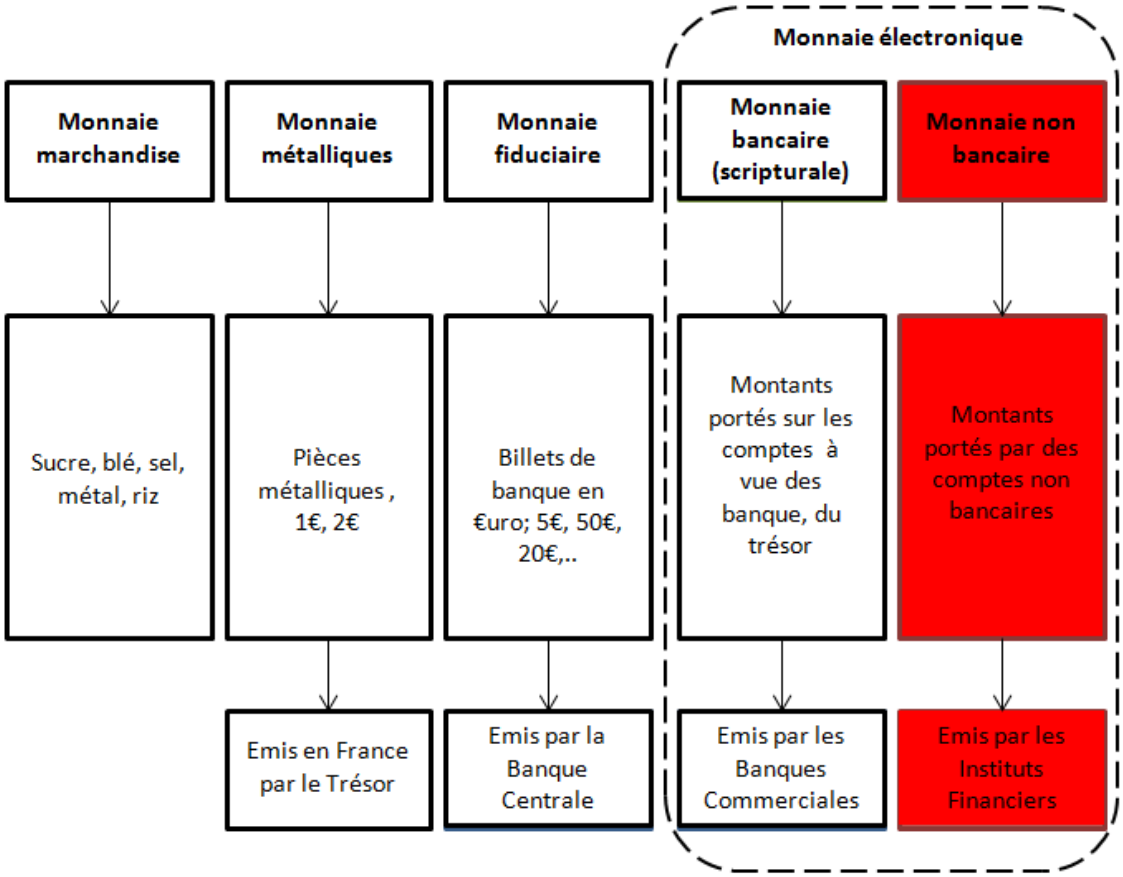


FIGURE 1.4 – Les différentes formes de la monnaie

La monnaie remplit les fonctions suivantes : unité de compte, réserve de valeur, intermédiaire des échanges et instrument de paiement. En tant qu'unité de compte, la monnaie sert à égaliser différentes quantités de biens hétérogènes. En tant que réserve de valeur, la monnaie garantit une valeur en terme nominal. La monnaie constitue également un intermédiaire nécessaire dans les relations marchandes. Enfin, la monnaie a une fonction de paiement. Cette dernière fonction requiert, en particulier, la création de moyens de paiement ou de moyens d'échange pour permettre la circulation des monnaies comme les pièces et les billets pour la monnaie fiduciaire. Il se trouve que les banques se sont engagées depuis longtemps sur le chemin de la dématérialisation de la monnaie. Des réseaux bancaires ont été conçus pour réduire, d'une part, les coûts des paiements et assurer d'autre part, leur sécurité.

L'idée de départ lors de la création de la monnaie électronique était de transposer la monnaie réelle au monde virtuel. L'argent électronique se veut donc aussi simple et anonyme que l'argent liquide [Polanyi K., 1968]. Afin de comprendre les enjeux de la monnaie électronique et son influence sur un système de paiement, nous commencerons par essayer de définir ce type de monnaie qui ne constitue pas une nouveauté. En effet, depuis la fin des années 1990, un vif débat s'est développé dans le monde des économistes sur les implications de cette innovation monétaire, notamment en matière de sécurité des paiements. La monnaie électronique est passée par deux générations différentes [Financial Crimes Enforcement Network, 2000] : elle a été considérée pendant plusieurs années comme une monnaie bancaire (monnaie scripturale) jusqu'à son émission par des institutions financières non bancaires ce qui a permis de la rendre « non bancaire » elle aussi. Nous estimons que pour comprendre la signification de la monnaie électronique, il faut distinguer ces deux générations. Seule la plus récente (non bancaire) suscite des interrogations et des craintes.

La monnaie bancaire couvre la monnaie émise par les banques commerciales. Il s'agit de la première génération de monnaie électronique qui s'insère dans des circuits fermés et sécurisés par les banques (monnaie scripturale). Ainsi en est-il des paiements par carte bancaire, des retraits de billets dans les guichets automatiques et de la plupart des paiements et prélèvements réguliers. Cette première génération de monnaie électronique n'a pas suscité beaucoup d'interrogations car les banques commerciales contrôlent l'émission et la dépense de cette monnaie. La monnaie électronique bancaire ou scripturale, par opposition à la monnaie fiduciaire (pièces) qui est émise par la banque centrale et qui ne peut être utilisée que dans le commerce physique, se traduit par l'existence d'un support qui représente l'écriture de sommes d'argent sur des comptes financiers. Comme la monnaie scripturale est un support monétaire dématérialisé, pour circuler, elle doit utiliser des instruments de paiement dont l'unique fonction est de faire circuler les unités de paiement contenues dans cette monnaie d'un compte bancaire à un autre. On les appelle parfois moyens de paiement scripturaux en raison de leur lien indissociable à la monnaie scripturale.

Après les différentes évolutions techniques de ces dernières années, plusieurs établissements non bancaires ont acquis la possibilité d'émettre de la monnaie électronique et des moyens de paiements qui se basent sur ce nouveau type de monnaie sont devenus très répandus. Des formes non bancaires de monnaies sont apparues dans les années 80, suite à l'utilisation des cartes prépayées et à l'essor du minitel en France [Petit B., 1999]. La monnaie non bancaire est alors comprise comme toute monnaie émise par un établissement non bancaire, non autorisé à recevoir l'épargne du public et à l'utiliser en crédit [Tarazi, M. et Breloff, P., 2010].

Elle n'a longtemps pas été considérée comme une monnaie, mais plutôt perçue comme un instrument très automatisé de mobilisation de la monnaie scripturale. Cette vision a changé avec la publication de la directive du Parlement Européen et du Conseil 2000/46/CE, qui a permis de donner une définition légale et définitive de l'activité des établissements de monnaie électronique ainsi que la surveillance prudentielle de ces établissements. Il s'agit maintenant d'« *une valeur monétaire stockée sur un support électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement (...) et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique* ». Ce type de monnaie suscite plus d'intérêt, car les émetteurs de ce type de monnaie sont rarement soumis à des réglementations prudentielles très strictes comme celles qui s'appliquent aux banques.

Par souci de simplification, le terme « monnaie électronique » désigne dans la suite de ce document la monnaie électronique non bancaire. Nous utilisons le terme « monnaie scripturale » pour désigner la monnaie électronique non bancaire.

1.3 Emergence de nouveaux moyens de paiement

Comme nous venons de le constater, l'évolution majeure d'Internet ces dernières années a permis l'expansion de l'E-commerce et des paiements sur Internet, ramenant ainsi plusieurs clients du commerce de proximité sur le Web. D'où le besoin d'intégrer de nouveaux moyens de paiement dans les sites marchands [Bounie D., 2000]. Ces nouveaux moyens de paiement électroniques se composent des anciens moyens de paiement qui existent depuis longtemps dans le commerce physique et de nouveaux moyens de paiement qui sont apparus après les innovations technologiques. Ces derniers recouvrent des centaines de systèmes désignés de manières multiples et variées, traduisant le caractère nouveau, imagé et virtuel des innovations en cours : « carte virtuelle dynamique », « argent virtuel », « jetons numériques », « e-cash », « protocoles de paiement électronique », etc. Cependant, face à l'inflation des dénominations, une clarification s'impose. Nous proposons une typologie sommaire des principales classes génériques des différents moyens de paiement en s'inspirant de notre typologie de la monnaie électronique présentée dans la section précédente (figure 1.4) : l'ensemble des moyens de paiement sur Internet peut alors être divisé en deux classes génériques : la première classe, baptisée moyens de paiement classiques (bancaires) et la seconde, baptisée moyens de paiement alternatifs (non bancaires).

1.3.1 Moyens de paiement classiques

La première classe générique des moyens de paiement bancaires classiques est exclusivement composée de systèmes scripturaux. Il s'agit des instruments de paiement les plus répandus sur Internet. En effet, avec plus de 83% des paiements [Fevad, 2010c], la carte bancaire demeure l'outil le plus utilisé sur la toile en matière d'achats en ligne. Tout comme dans le commerce de proximité, où le client entre sa carte bancaire dans un terminal de paiement électronique, l'acheteur sur Internet saisit le numéro de sa carte bancaire dans un terminal de paiement « virtuel » sur le site marchand. La solution prédominante de paiement en ligne par carte de paiement s'appuie sur le protocole Transport Layer Security (TLS), anciennement nommé Secure Socket Layer (SSL), qui est très bien décrit dans la littérature [Zhao L., Srihari M., Laxmi B., 2005] et [Wagner D. et Schneier B., 1996]. Lors du paiement, l'acheteur communique son numéro de carte de paiement ainsi que la date de validité de cette dernière au commerçant via le protocole de communication SSL qui permet d'établir un canal sécurisé pour la transmission des données. Le commerçant a ensuite la charge de gérer la transaction avec sa banque acquéreuse.

1.3.2 Moyens de paiement alternatifs

Une étude a été effectuée par ADN'co récemment pour le compte de la société Limonetik (partenaire industriel des travaux de recherche effectués dans le cadre de cette thèse) afin de définir la deuxième classe de MPEs (non bancaires ou « alternatifs ») et essayer d'estimer le potentiel de ces nouveaux moyens de paiement électroniques pour l'E-commerce. Cette étude [ADN'co, 2011] publiée en fin 2011 a montré que les moyens de paiements alternatifs devraient représenter près d'1/4 des transactions en ligne réalisées en France, d'ici 2015. Un marché qui pèserait donc près de 13,8 milliards d'euros. Les moyens de paiement alternatifs sont tous les moyens de paiement qui existent en dehors des traditionnels cartes bancaires, chèques ou espèces. Nous distinguons ainsi deux sous-catégories des moyens de paiement alternatifs : les « transfuges » et les « pure players » présentés dans la figure 1.5.

Les « transfuges » sont les moyens de paiement qui existent depuis longtemps dans le commerce physique sous la forme de titres prépayés (tickets restaurant, cartes cadeaux, etc.), de cartes de fidélité, de listes de mariage, de facilités de paiement en magasin (paiement en trois fois sans frais...), etc. Ces moyens paiement, jusqu'à présent réservés aux boutiques physiques, commencent à se déployer sur le Web sous forme dématérialisée. Ces « transfuges » pourraient représenter jusqu'à 4,8 milliards d'euros en 2015, soit 8,6% des transactions en ligne.

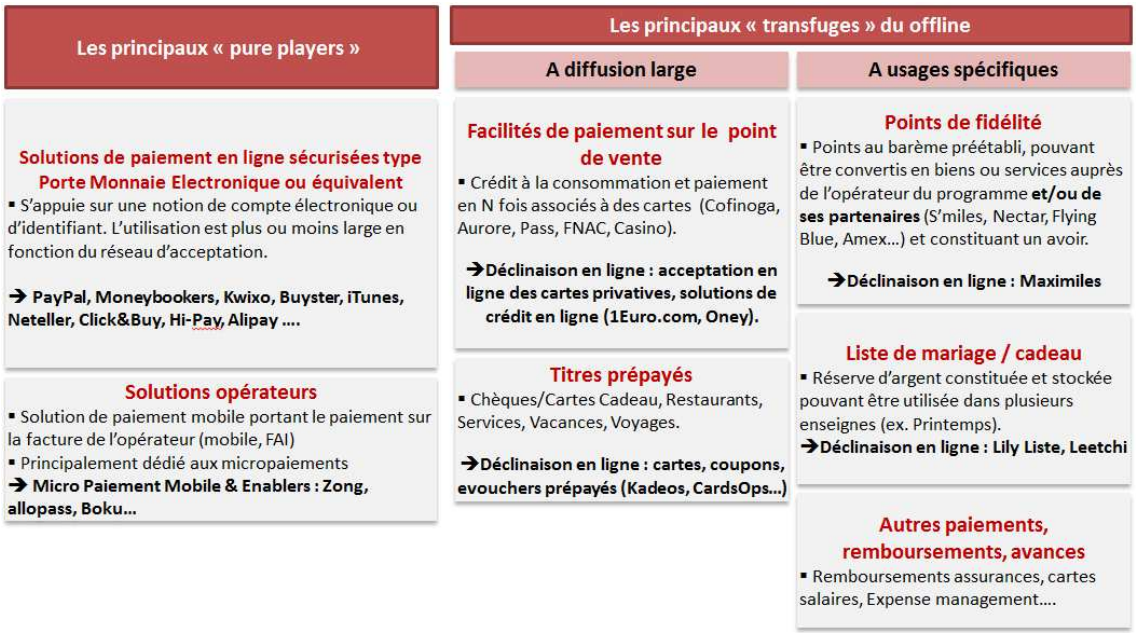


FIGURE 1.5 – Moyens de paiement alternatifs (MPA) sur Internet [ADN'co, 2011]

Les « pure players » sont des moyens de paiement propres au Web, comme le porte-monnaie électronique (Paypal, Buyster...) ou le m-paiement (le paiement par mobile) facturé sur le relevé opérateur. On y trouve également les moyens de paiement du s-commerce (s pour « social »). Certains réseaux communautaires comme Facebook utilisent leur propre monnaie virtuelle (les Facebook Crédits par exemple) permettant ainsi aux internautes d'acheter des « biens virtuels » sur les plateformes de jeux. Les pure players pourraient représenter 16% des transactions sur les sites marchands d'ici à trois ans, soit 9 milliards d'euros en volume.

Malgré l'éventuel grand potentiel de ce type de moyens de paiement électroniques, ces derniers ne sont pas encore acceptés dans le commerce électronique sur Internet. La première contribution de cette thèse consiste à étudier les différentes contraintes d'intégration de ces moyens de paiement sur Internet. Cependant, avant de présenter cette partie de l'étude, nous proposons d'analyser les différentes caractéristiques d'un système de paiement de paiement sur Internet.

1.4 Système de paiement sur Internet

Dans l'économie, pour qu'une opération de paiement soit finalisée, il faut que le bénéficiaire ait totalement reçu la somme d'argent qui lui est associée. Le mécanisme qui permet cette action est le système de paiement. Ce dernier peut simplement être manuel et, dans ce cas, le paiement est immédiat car la monnaie passe de

main en main. Cependant, il devient plus complexe lorsque des instruments de paiement dématérialisés sont utilisés. Des comptes bancaires sont alors mobilisés et le paiement implique des mouvements de fonds dans les comptabilités des banques [Chanel-Reynaud, G. et Chabert, D., 2004]. Un système de paiement est donc un système d'échange et de règlement. Plus précisément, il correspond à un ensemble d'instruments, d'intermédiaires, de règles, de procédures, de processus et de systèmes interbancaires de transfert de fonds, destiné à assurer la circulation de la monnaie [Banque Centrale Européenne, 2010].

L'expression « système de paiement » est également utilisée pour qualifier un « système de transfert de fonds (Funds Transfer System) » qui est un dispositif qui implique de multiples participants et qui est régi par des procédures formelles standardisées et des règles communes pour l'autorisation, la transmission, la compensation et/ou le règlement d'opérations de paiement. L'importance du système de paiement devient plus élevée dans le cadre de l'E-commerce car les relations entre les acteurs dans la transaction sont purement virtuelles. C'est pour cette raison que le choix du système de paiement et l'assurance de la sécurité font partie de l'analyse stratégique d'un projet E-commerce [Mennis A., 2005]. En effet, le marchand est amené à effectuer de nombreuses analyses entre l'idée du site et la prise de décision de lancement du site E-commerce. Ces analyses commencent par des analyses stratégiques du projet qui consistent à réfléchir aux aspects de marketing, de logistique, de paiement et de sécurité jusqu'à l'analyse de l'exploitation du site Web qui consiste en l'analyse des données de mesure de la fréquentation, la maintenance et l'entretien du site Web. En passant par l'analyse de la conception et de la technologie à utiliser et la mise en oeuvre du site (publicité, formation des employés...). A ce titre, et vu le niveau de fraude sur Internet, la notion de sécurisation de paiement est un élément important dans le « business plan » commerçant.

1.4.1 Principaux acteurs d'un système de paiement

Connaître l'ensemble des acteurs qui interviennent dans l'environnement des paiements sur Internet est essentiel pour bien comprendre le fonctionnement des systèmes de paiement. Cette section présente donc une approche descriptive de tous les acteurs de l'environnement du paiement qui sont :

- Le porteur : la personne physique qui détient le moyen de paiement et qui a l'intention d'acheter sur Internet.
- L'accepteur : la personne physique ou morale qui accepte le moyen de paiement grâce à un système accepteur. Dans une transaction électronique, l'accepteur est

assimilé au commerçant équipé d'un terminal de paiement électronique (TPE). Sur Internet, l'accepteur est le commerçant qui possède une boutique sur le Web, qui propose un terminal de paiement électronique virtuel pour gérer ses paiements et qui accepte le moyen de paiement du porteur comme instrument de paiement (soit directement soit par l'intermédiaire d'un prestataire de paiement).

- L'émetteur : l'entité financière qui émet le moyen de paiement du client. Dans une transaction bancaire, par exemple, l'émetteur est la banque du client. Il établit généralement un contrat porteur avec le client, où il définit les différentes règles de gestion du moyen de paiement. Il est le responsable de la sécurité du moyen de paiement et de l'authentification du client.
- L'acquéreur : l'organisme financier qui va acquérir les données de la transaction. Dans une transaction bancaire, par exemple, il s'agit de la banque du commerçant. Il établit généralement un contrat accepteur avec le commerçant, où il définit les différentes règles de gestion du terminal de paiement. Il est le responsable de la sécurité des terminaux de paiement fournis à l'accepteur.
- Le Prestataire de Service de Paiement (PSP) : introduit par la directive européenne sur les services de paiement 2007/64/CE. Il s'agit d'une entreprise agréée pour offrir des services de paiement [Parlement Européen et du Conseil, 2007]. Il peut s'agir alors soit des établissements de crédit (dont les banques) traditionnellement engagés dans ces activités puisque la loi leur conférait jusqu'à présent l'exclusivité de la mise à disposition et gestion des moyens de paiement, soit des « établissements de paiement » nouvellement créés, qui ne sont pas des établissements de crédit, mais peuvent désormais également offrir des services de paiement. Un PSP peut également être un intermédiaire entre l'accepteur et les différents autres acteurs du système monétaire [Kannen M., Leischner M., Stein T., 2003].
- Le prestataire de paiement : l'intermédiaire technique qui propose d'intégrer des terminaux de paiement virtuels dans les sites E-commerce (par exemple : Paybox, Ogone, Payline, Atos...).
- Les associations financières : des associations de banques et/ou des organismes financiers, qui contrôlent les échanges entre les acquéreurs et les émetteurs. Ces associations gèrent également les communications interbancaires et garantissent l'interopérabilité entre les différents organismes financiers. Dans le cas du système bancaire, elles sont appelées « Card Schemes », par exemple : Visa, Mastercard, CB...).

1.4.2 Typologies d'un système de paiement

Selon le nombre des acteurs qui participent à la transaction électronique, les systèmes de paiement sur Internet peuvent être divisés en deux catégories [Sitruk H, 2009].

Système quatre coins

FIGURE 1.6 – Système de paiement quatre coins

Un système est dit à « quatre coins » (ou « quatre parties ») quand un institut financier intervient pour l'émission de la carte et un autre pour l'acquisition des opérations chez le commerçant, conformément au fonctionnement des instruments scripturaux, évoqués ci-dessus. Des intermédiaires financiers s'occupent d'assurer les fonctions d'autorisation et/ou de compensation des transactions. Ce type de système de paiement est largement accepté par les consommateurs et les commerçants dans le monde entier et peut être considéré comme le système de paiement le plus populaire. Dans le cadre de ce type de système de paiement, un institut financier émet des cartes de paiement, maintient les comptes des titulaires des cartes et gère les utilisations frauduleuses de ces cartes. D'autre part, les marchands se sont mis d'accord avec les acquéreurs pour recevoir des paiements en leur nom. Ce type de système de paiement permet de sécuriser la transmission des ordres de paiement réalisés à partir

de la carte de paiement (généralement bancaire). Il s'agit d'un système qualifié de quadripartite (ouvert), car il implique 4 acteurs ; le client, le marchand, l'émetteur et l'acquéreur.

Il s'agit d'un système composé de quatre sous-systèmes (figure 1.6) :

1. Le système d'émission composé du porteur et de l'émetteur. Il permet d'émettre le moyen de paiement.
2. Le système d'acceptation composé du porteur et du marchand. Il permet d'accepter le moyen de paiement du client.
3. Le système d'acquisition composé de l'accepteur et de l'acquéreur. Il permet d'acquérir les paiements au nom du marchand.
4. Le système interbancaire composé des différents instituts financiers. Il permet le transfert sécurisé des fonds depuis le compte du client au compte du marchand.

Le système quatre coins est généralement un système bancaire dont la transaction comporte deux étapes :

1. La demande d'autorisation : l'acquéreur interroge la banque du client sur le solde de ce dernier et s'il autorise un prélèvement du montant de la transaction.
2. La compensation et le règlement : une fois que l'émetteur a approuvé l'autorisation de la transaction, l'acquéreur se charge de la gestion des flux de compensation en passant par les infrastructures bancaires et crédite le compte du commerçant.

Système trois coins

Suite à l'évolution de l'E-commerce, plusieurs systèmes de paiement sont apparus, il s'agit généralement des systèmes dits « trois coins ». Dans ce cas, un seul institut financier assure les fonctions d'émission des moyens de paiement électroniques et d'acquisition des paiements.

Généralement, un système de paiement « trois coins » est un système qui implique trois entités : le client, le marchand et l'établissement financier qui émet des cartes de paiement (figure 1.7). Ce système peut être appelé aussi système tripartite (ou système fermé), car l'émetteur et l'acquéreur sont confondus. Dans ce système, la même société contracte aussi bien avec les clients que les marchands, traite les transactions et la gestion du réseau de paiement. Ce type de système de paiement permet de sécuriser la transmission des ordres de paiement réalisés à partir des comptes non bancaires (ou de monnaie électronique).

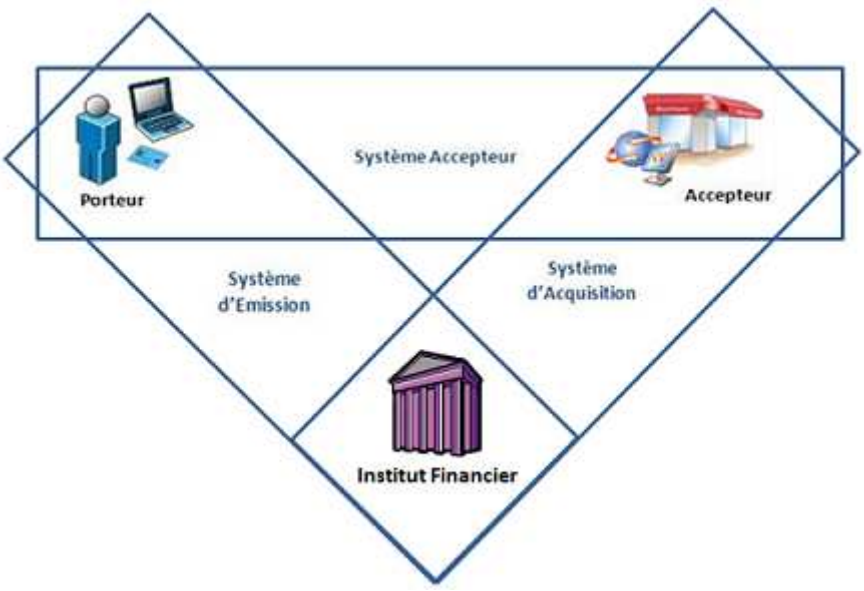


FIGURE 1.7 – Système de paiement trois coins

1.5 Exigences d'un système de paiement

Après avoir présenté le système de paiement sur Internet et afin de comprendre les raisons pour lesquelles les nouveaux moyens de paiement ne sont pas encore acceptés sur Internet, nous allons étudier les facteurs qui déterminent le succès ou l'échec d'un système de paiement. Autrement dit, les exigences auxquelles doit répondre un système de paiement.

1.5.1 Revue de la littérature

Notre état de l'art a permis d'identifier plusieurs recherches qui ont essayé de développer et d'introduire les exigences d'un système de paiement sur Internet. Schmidt et Muller [Schmidt, C. et Müller, R., 1999] ont affirmé avoir identifié plus que 30 critères dans la littérature. La plupart des recherches effectuées concernant ce sujet se sont focalisées sur les critères technologiques d'un système de paiement, citons, dans ce contexte : [Neuman, C. and Medvinsky, G., 1995], [Furche, A. et Wrightson, G., 1996] et [Jeffrey K. MacKie M, et Kimberly W, 1997]. Nous avons recensé également, d'autres travaux de recherches qui se sont intéressés à d'autres exigences d'un système de paiement, citons, par exemple, les travaux suivants : [Abrazhevich D., 2001], [Havinga M., Smit M., Helme A., 1996], [Asokan N., Janson A., Steiner M, 1997] et [Sahut J M., 2008]. Pour notre part, partant de ces différentes analyses, nous avons choisi de classifier ces exigences selon

quatre catégories majeures présentées dans le tableau 1.1 qui sont : exigences technologiques, exigences économiques, exigences sociales et exigences juridiques.

	Critères d'évaluation	**Source dans la littérature**
Exigences Technologiques	– Sécurité – Interopérabilité – Traçabilité – Commodité/Ergonomie – Confiance – Durabilité – Liquidité/convertibilité – Anonymat – Complexité	– Bellare and Alii (2000) – Abrazhevich D. (2001) – Sahut (2001) – Wright (2002) – Peffers and Ma (2003) – Tsiakis and Stephanides (2005) – Hadidi et Siripaiboon (1999) – Abrazhevich (2001) – Kannen et Alii (2003)
Exigences Economiques	– Coûts – Echange atomique – Accessibilité du système – Risque financier – Retour sur investissement	– Schmidt et Müller (1999) – Hadidi et Siripaiboon (1999) – Wright (2002) – Chou, Lee, et Chung (2004)
Exigences Sociales	– Installation/souscription – Protection de la vie privée – Accessibilité	– Wright (2002) – Lee et Tsang (2003) – Chou, Lee, et Chung (2004)
Exigences Légales	– Légalité du Paiement – Contrat E-commerce – Standards techniques – Transactions internationales – Protection de la propriété intellectuelle	– Banque des règlements internationaux (2001) – Banque centrale européenne (2003)

TABLE 1.1: Les exigences d'un système de paiement électronique

Exigences technologiques

Lors de la conception d'un système de paiement sur Internet, plusieurs critères technologiques doivent être pris en compte, le critère le plus important étant la sécurité de toutes les transactions électroniques générées par ce système. L'essor du commerce électronique a fait naître la nécessité d'avoir de nouveaux moyens de

paiement numériques, adaptés au monde virtuel de l'Internet. Ce type de communications nécessite également un niveau minimal de confiance, tant de la part des consommateurs que de la part des vendeurs : d'un côté, les acheteurs veulent que leurs cartes bancaires ou portefeuilles virtuels ne puissent tomber entre les mains d'un tiers mal intentionné, et que les biens et les services achetés « en ligne » soient livrés. D'un autre côté, les fournisseurs de biens et de services veulent la garantie qu'ils recevront les fonds qui correspondent aux marchandises vendues. Le système doit garantir également un degré élevé de sécurité et de fiabilité opérationnelle. Il doit être interopérable avec les autres systèmes de paiement et doit permettre de tracer les différents mouvements financiers effectués suite au paiement.

Exigences économiques

Les exigences économiques incluent les différents échanges atomiques qui garantissent que le consommateur payera avec de l'argent ou quelque chose d'équivalent en valeur. Un système de paiement électronique doit aussi être accessible dans le monde entier. Les exigences économiques sont liées également aux risques financiers et à la notion du retour sur investissement (ROI) qui est une mesure de performance permettant d'évaluer l'efficacité d'un investissement et le coût de transaction ; par exemple dans le choix du système de paiement électronique pour de petits paiements, le coût de la transaction pourrait être un facteur déterminant dans le choix du système de paiement.

Exigences sociales

En plus de la satisfaction des besoins techniques et économiques, le système de paiement électronique doit toujours adresser les besoins sociaux. Le système de paiement doit empêcher les sociétés ou les institutions financières de tracer des informations d'utilisateur et doit être simple, convivial et facilement accessible.

Exigences légales

Le système de paiement électronique doit se soumettre à la loi et aux règlements gouvernementaux. Il doit pouvoir aussi garantir toutes les preuves nécessaires (la signature numérique, contrats...) afin de protéger les utilisateurs (clients et E-commerçants) réalisant des transactions domestiques ou internationales. Les systèmes de paiement de masse en euros reconnus comme présentant une grande importance économique doivent disposer d'une base juridique solide. Les participants pourraient encourir des risques financiers si les règles et les procédures du système n'étaient pas claires et pré-

cises. Le système doit être doté de règles et procédures permettant aux participants d'appréhender correctement l'incidence du système sur chacun des risques financiers découlant de leur participation [Banque des Règlements Internationaux, 2001] [Banque Centrale Européenne, 2003].

1.5.2 Nos objectifs de recherche

Comme nous l'avons dit au début de ce chapitre, l'évolution perpétuelle de l'E-commerce a créé de nouveaux besoins auxquels celle-ci ne répond pas encore en totalité. Surtout suite à l'émergence de nouveaux moyens de paiement qui ne sont pas encore communément acceptés sur la toile. Les cartes bancaires sont les moyens de paiement les plus utilisés pour le paiement des marchandises et l'achat des services en ligne. En termes de transactions, l'ACSEL (L'Association pour le Commerce et les Service En Ligne) a annoncé qu'en 2009, 85 % les achats sur Internet sont réalisés en utilisant la carte bancaire CB. Et selon TNS Sofres et Gartner Data, la carte de crédit est le moyen le plus utilisé sur Internet en Europe et aux États-Unis. Pour analyser cette situation, nous proposons d'étudier les différents facteurs liés à la conception d'un système de paiement pour le commerce B2C. Et pour ce faire, nous avons choisi de nous focaliser sur certains critères d'évaluation parmi ceux trouvés dans la littérature. Il s'agit, selon nous, des critères qui peuvent expliquer la réticence des commerçants à intégrer les nouveaux moyens de paiement « alternatifs » sur Internet.

Sachant que nous proposons, dans le cadre de cette thèse, une nouvelle plateforme de paiement qui permet de faciliter l'intégration des nouveaux moyens de paiement, les critères retenus nous serviront par la suite de critères d'évaluation de cette plateforme.

1.5.3 Exigences et critères retenus

Les critères présentés dans cette section font, pour la plupart des sites marchands, partie des indicateurs utilisés pour l'évaluation de l'intégration d'un système de paiement. Nous allons nous intéresser aux exigences technologiques présentées précédemment, car nous considérons qu'ils contiennent des critères qui peuvent freiner l'intégration d'un système de paiement sur Internet. Parmi les critères d'évaluation présentés dans le tableau 1.1, nous nous restreindrons aux critères suivants : la sécurité, l'ergonomie et la complexité.

Sécurité

La sécurité dans le domaine de l'E-commerce sur Internet concerne plusieurs aspects [Solange G H., 2000]. En effet, sécuriser les transactions sur Internet consiste à prendre en compte les différents aspects techniques, opérationnels, humain économiques et réglementaires. Pour que le client ait l'assurance que ses informations de paiement sont à l'abri de toute utilisation frauduleuse et que le marchand soit sûr d'être payé après la livraison de la commande. Malgré les grands efforts de sécurisation des plateformes de paiement bancaires qui représentent un des premiers systèmes de paiement sur Internet et donc bénéficient d'une grande expérience dans le domaine de paiement en ligne, le risque de fraude de la carte bancaire est réel. En effet, selon l'Observatoire de la sécurité des cartes de paiement en France [Observatoire de la Sécurité des Cartes de Paiement, 2010], le taux de fraude sur les paiements Internet continue d'augmenter. Les paiements à distance, qui représentent 8,6% de la valeur des transactions nationales, comptent ainsi pour 62% du montant de la fraude (contre 57% en 2009), dans un contexte de croissance toujours soutenue du volume et de la valeur de ces paiements (+ 23,8% entre 2009 et 2010 en valeur), malgré la mise en oeuvre de mesures nécessaires permettant de lutter contre cette tendance en la généralisation progressive de l'authentification du porteur.

Dans le cadre de notre travail, nous nous plaçons dans le contexte du commerce électronique sur Internet qui est très différent de celui du commerce de proximité. Lors d'un paiement de proximité par carte bancaire, le client est authentifié d'une manière forte, ce qui permet un contrôle plus sécurisé des usages du moyen de paiement électronique. Le client tape son code secret dans le terminal de paiement électronique du marchand ce qui réduit considérablement la fraude de type usurpation d'identité et la répudiation des paiements. Cependant, dans le cas des paiements sur Internet, le client est absent et tous les échanges entre ce dernier et l'E-commerçant sont « virtuels ». Pour sécuriser ces échanges, plusieurs types de systèmes de paiement sont apparus : le système SSL sans intermédiaire, le système SSL avec intermédiaire et le système avec signature numérique (3D-Secure, SET...) [Bounie D. et Bourreau M. , 2004] décrits en annexe A.

Ergonomie

L'ergonomie est un facteur important de succès pour n'importe quel site Web. Il l'est surtout pour les sites commerçants où l'on vise une meilleure expérience client et une fidélisation des acheteurs. Une étude menée par la FEVAD - Médiamétrie/NetRatings, montre que 14% des cyberacheteurs qui abandonnent leur panier d'achat, le font car le service de paiement proposé ne le satisfait pas [Fevad, 2008]. Il

s'agit donc d'un critère très important à prendre en compte lors de la conception d'un système de paiement. Cependant, avant d'aborder la question de l'ergonomie des sites de E-commerce, il est nécessaire de préciser les spécificités du comportement d'achat sur Internet. Celles-ci permettront de mettre en évidence l'importance des enjeux associés à la fidélisation. Le processus d'achat sur Internet suppose tout d'abord que l'individu ait accès à une interface homme-machine dont il doit maîtriser le fonctionnement. Ainsi, être familier du réseau Internet semble être un paramètre non négligeable pour expliquer les achats sur Internet. Sans doute, faut-il y voir la nécessité d'une appropriation cognitive et opérationnelle indispensable pour s'adapter à la situation d'achat qu'offre Internet. Cette appropriation passe de plus par un phénomène cumulatif d'expériences. En ce sens, il a pu être vérifié que la fréquence d'utilisation d'Internet est liée à l'antériorité de l'accès à Internet et au fait d'avoir un usage professionnel du réseau [Christos E., Hammond K., 2000].

Le design des pages Web d'un site E-commerce constitue la base de l'ergonomie du site marchand. En effet un site E-commerce mal conçu ne permet pas de fidéliser les clients et de les motiver pour payer leurs commandes. Le premier facteur à privilégier lors du design des pages Web d'un site marchand est la prise en compte de l'équipement des internautes, car tous les utilisateurs ne disposent pas du même équipement et il existe une forte hétérogénéité tant en ce qui concerne l'équipement matériel, qu'en ce qui concerne l'équipement logiciel. Ce paramètre a des incidences considérables sur la visualisation des pages Web et les temps de téléchargement. Il faut également tenir compte de la vitesse de connexion des modems des utilisateurs. Ainsi, il faut faire attention au poids de la page Web. Il est indispensable également que les pages appelées puissent être téléchargées rapidement, surtout lorsque le client s'apprête à valider sa commande et payer. Car si le temps de chargement de la page est trop long, les visiteurs ont tendance à se lasser et à abandonner leur panier. Un bon design permet de trouver un compromis entre la qualité graphique de la page et le potentiel d'affichage dont disposent les visiteurs [Ladwein R, 2000]. L'identification des liens est également un facteur à prendre en compte lors du design des pages de paiement. Ce facteur est particulièrement important dans le processus d'achat. En effet, le client a besoin de pouvoir bien identifier les liens des différents choix de moyens de paiement (et donc différentes pages de paiement).

Nous nous intéressons dans cette section à l'ergonomie du « tunnel de paiement » du site marchand., c'est-à-dire l'ergonomie des pages comprises entre la page de choix de moyen de paiement jusqu'à la page de résultat de paiement. L'ergonomie de ces pages et de leur contenu renvoie à la nécessité de travailler sur la lisibilité générale de la page Web. En effet, une page difficilement lisible est susceptible d'empêcher le

visiteur d'accéder aisément aux informations les plus importantes ou de contrarier, voire rendre complexe, l'accès à la page de paiement. Assurer la lisibilité d'une page Web, c'est permettre au visiteur d'accéder aux informations disponibles de façon claire pour qu'il puisse décider s'il continue le processus d'achat ou s'il met un terme à sa commande. Il apparaît alors indispensable de structurer les informations de telle sorte que le visiteur puisse aisément distinguer le principal de l'accessoire [Ladwein R, 2000].

Complexité

Lors de la conception d'un système de paiement, le marchand doit prendre en compte plusieurs facteurs car un système de paiement compte plusieurs fonctionnalités qui dépassent la gestion du paiement. En plus, un système de paiement doit être facile à mettre en place pour le marchand (table 1.1).

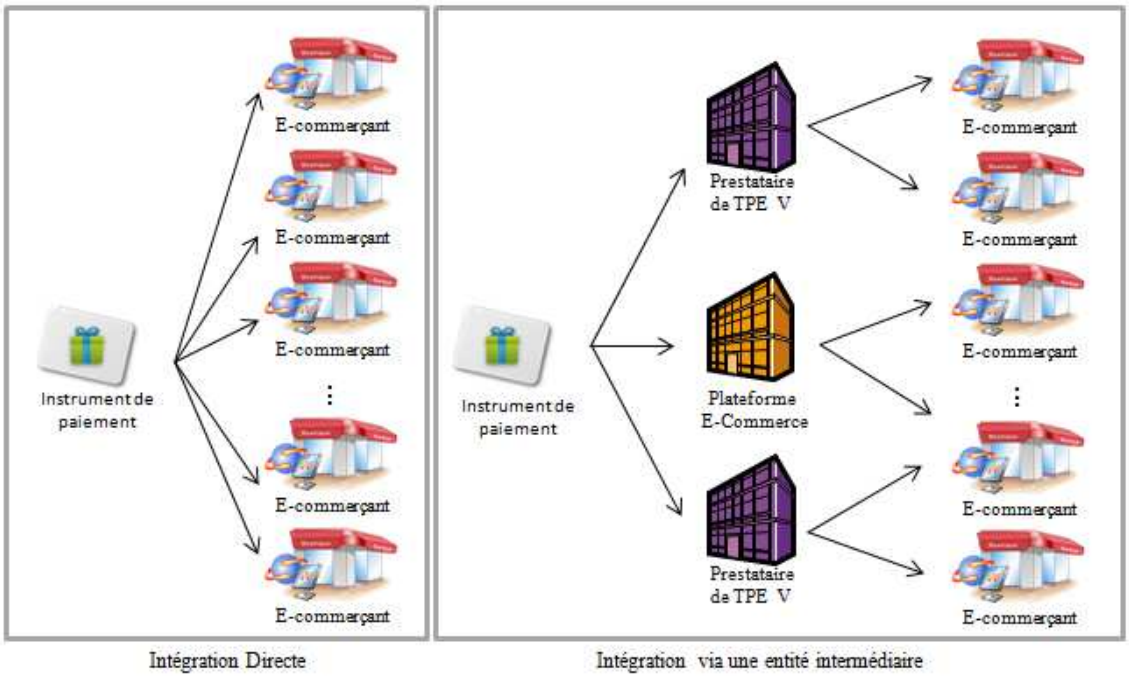


FIGURE 1.8 – Les différentes méthodes d'intégration d'un système de paiement

Sachant que nous nous intéressons à l'intégration des nouveaux moyens de paiement sur Internet, nous proposons d'étudier la complexité de l'intégration technique d'un système de paiement dans un site marchand. Les moyens de paiement non bancaires (alternatifs) sont rarement proposés dans les sites d'E-commerce car ils impliquent de lourdes contraintes d'organisation et d'intégration. En effet, afin d'accepter un nouveau moyen de paiement sur son site, l'E-commerçant doit gérer

plusieurs opérations : le développement informatique à entreprendre, le rapprochement comptable à gérer dû à l'intégration de ce moyen de paiement, la modification des procédures de back-office, la prise du risque d'un retour sur investissement non garanti, les négociations juridiques et commerciales nécessaires, la motivation de tous les décideurs en interne, etc.

Il existe deux possibilités afin d'intégrer les moyens de paiement sur la toile (figure 1.8). La première consiste en l'intégration du moyen de paiement directement dans les sites marchands, ce qui peut prendre beaucoup de temps car chaque site marchand est différent des autres. La deuxième possibilité est l'intégration du moyen de paiement dans les plateformes des prestataires techniques à qui les marchands délèguent généralement leurs systèmes de paiement. Cette deuxième solution concerne également les sites marchands qui sont hébergés par une plateforme E-commerce et qui s'appuient sur les modules de paiement déjà intégrés par la plateforme.

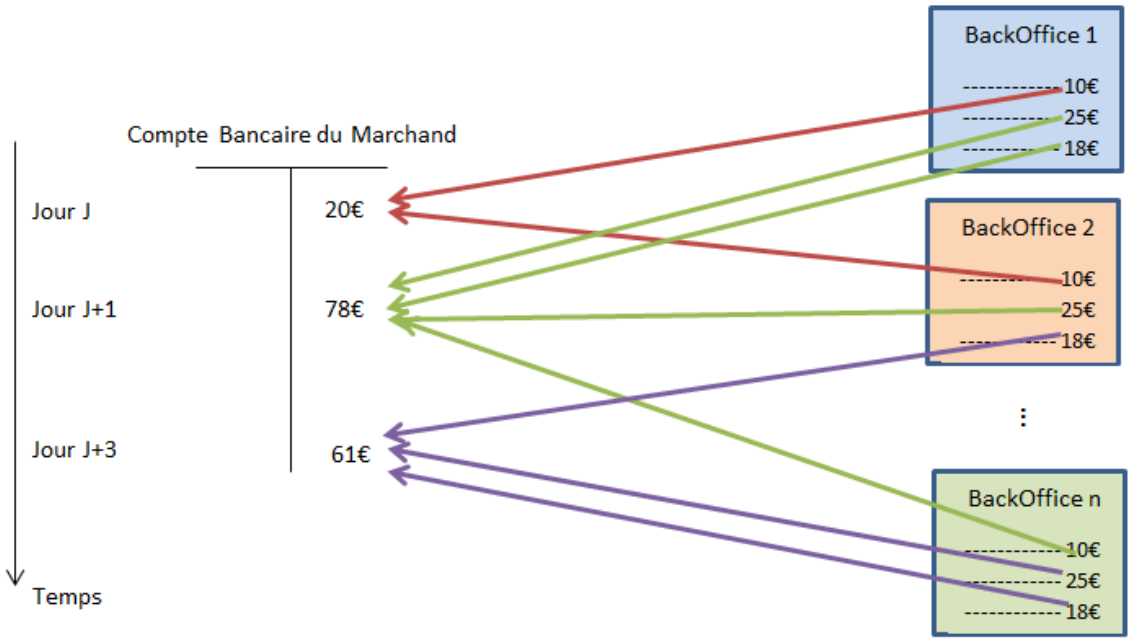


FIGURE 1.9 – Rapprochement comptable de plusieurs flux financiers

En plus de la complexité technique de l'intégration d'un nouveau moyen de paiement, le marchand sera amené à réaliser plusieurs rapprochements comptables des nouveaux flux financiers. Le marchand aura alors autant de back-office que de nouveaux moyens de paiement et sera obligé de les consulter afin de rapprocher les transactions qui sont affichées dans son relevé bancaire avec les transactions affichées dans les différents back-offices (figure 1.9).

Sachant qu'il s'agit des moyens de paiement qui ne sont pas forcément liés à

un compte bancaire, le montant que le client peut payer à l'aide de ces moyens de paiement est généralement limité à une somme donnée, ce qui nécessite de proposer un paiement complémentaire et d'orchestrer plusieurs paiements. La littérature montre que l'agrégation de plusieurs moyens de paiement est une fonctionnalité qui n'est pas très présente dans l'E-commerce. En effet, les pages de paiement sont majoritairement mono-paiement ; chaque choix de moyen de paiement redirige le client vers une page de paiement différente. L'agrégation de plusieurs moyens de paiement consiste à avoir une seule page de paiement qui permet au client de payer avec plusieurs moyens de paiement à la fois (tel qu'il est illustré dans la figure 1.10).

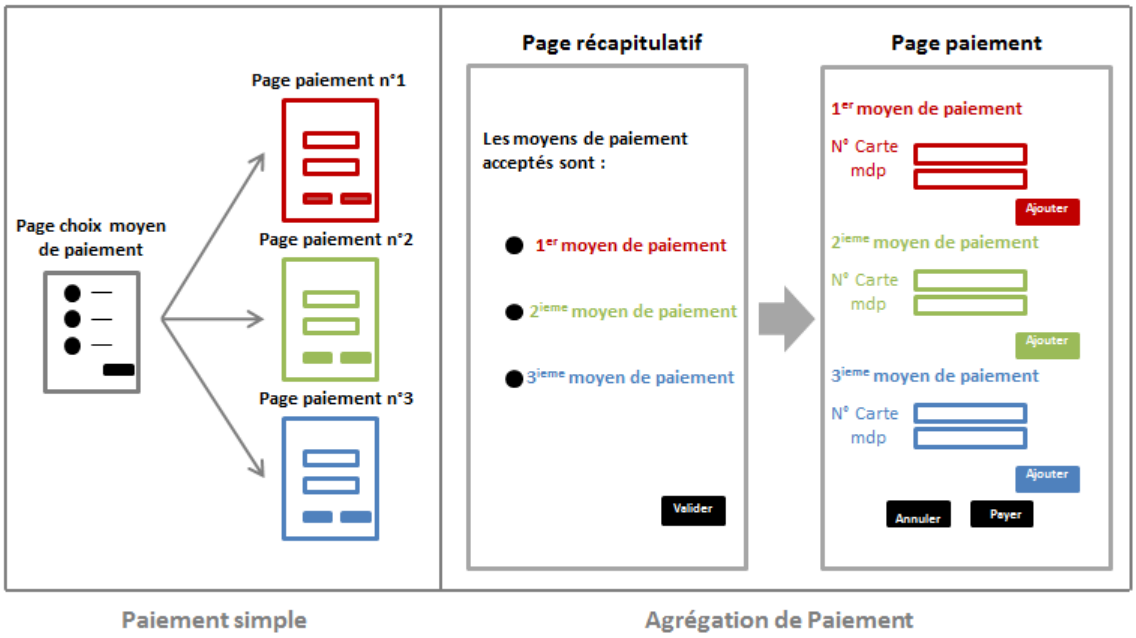


FIGURE 1.10 – Représentation des différents types de pages de paiement dans le cas d'un paiement simple ou d'une agrégation de plusieurs paiements

En effet, la particularité des nouveaux moyens de paiement alternatifs est qu'ils ne sont pas liés directement à un compte bancaire. La plupart de ces moyens de paiement ont des soldes limités (cartes prépayées, cartes cadeaux...). La fédération de l'E-commerce et de la vente à distance (Fevad) a estimé le montant moyen du panier en France en 2010 à 92€ [Fevad, 2010b], ce qui explique le besoin de proposer un paiement complémentaire (généralement avec la carte bancaire) lors de l'utilisation d'un moyen de paiement non bancaire.

L'agrégation de plusieurs moyens de paiement implique une orchestration des différentes demandes d'autorisation, une gestion des opérations financières effectuées après le paiement et leur transposition sur les moyens de paiement utilisés afin de prendre en compte les caractéristiques de chaque moyen de paiement, ce qui peut

s'avérer complexe pour le marchand. L'objectif de notre travail est alors de diminuer cette complexité pour l'E-commerçant afin de lui faciliter l'intégration des nouveaux moyens de paiement

1.6 Conclusion

Nous avons présenté dans ce chapitre le vocabulaire du commerce électronique sur Internet, nécessaire pour la suite de notre étude. Nous avons défini le système de paiement sur Internet et étudié les différents types des monnaies manipulées ainsi que les différentes typologies des systèmes existants. Néanmoins, il s'agit d'un système qui évolue tous les jours afin de s'adapter aux nouvelles technologies et aux nouvelles approches de l'E-commerce. Nous avons aussi défini les nouveaux moyens de paiement « alternatifs » objet de nos travaux de recherche. En effet, plusieurs nouveaux moyens de paiement ne sont pas encore communément acceptés par les sites marchands sur Internet. Afin d'étudier ce problème d'acceptation des nouveaux moyens de paiement, nous avons cherché, dans la littérature, les exigences d'un système de paiement sur Internet, ce qui nous a permis de déduire les différentes contraintes d'intégration d'un système de paiement sur Internet que nous avons résumées dans les trois critères suivants : la sécurité, l'ergonomie et la complexité.

Maintenant qu'est présenté et défini le système de paiement sur Internet, nous allons nous intéresser, aux différents enjeux d'un système de paiement sur Internet, et surtout à la possibilité d'intégrer facilement et rapidement un nouvel instrument de paiement et d'agréger plusieurs moyens de paiement. Le prochain chapitre présentera des éléments de l'état de l'art de cette problématique afin de montrer les limites de l'existant et les contributions de cette thèse.

Chapitre 2

Analyse des approches d'intégration existantes

Dans ce chapitre, nous proposons une étude détaillée de la problématique d'intégration d'un moyen de paiement dans une boutique E-commerce sur Internet en présentant les étapes du procédé d'intégration. Nous présentons également les outils d'évaluation de cette intégration en nous basant sur les critères retenus dans le chapitre précédent (section 2.2). Puis, nous proposons une étude bibliographique qui présente un panorama des différents modes d'intégration des systèmes de paiement existant sur Internet de nos jours (section 2.3, section 2.4, section 2.5 et section 2.6). Enfin, nous présentons une étude comparative des différents modes décrits afin d'identifier les besoins non couverts par les solutions existantes (section 2.7).

Sommaire

2.1 Introduction

Plusieurs architectures de paiement électroniques sont apparues depuis 1960 et ont évolué rapidement, ce qui a augmenté leur complexité. L'Observatoire des Systèmes de Paiement électroniques (ePSO) recense ainsi environ 80 méthodes de paiement pour le B2C, dont les caractéristiques sont assez différentes les unes des autres. Dans ce chapitre, nous allons analyser plus en détail l'intégration des systèmes de paiement sur Internet afin de comprendre les limites de l'existant et l'intérêt des travaux effectués dans le cadre de cette thèse.

D'une manière générale, il existe deux moyens d'intégrer un système de paiement sur Internet : la première méthode consiste à héberger la page de paiement directement dans le site marchand. Il s'agit dans ce cas d'un système de paiement « intégré ». La seconde méthode consiste à rediriger le client vers une page de paiement externe. Il s'agit dans ce cas d'un système de paiement « déporté ». Ces deux modes d'intégration sont décrits dans la figure 2.1. Nous allons étudier en détail la différence entre ces deux modes, en nous basant sur les critères d'évaluation définis dans le chapitre précédent.

Figure 2.1 – Les modes d'intégration d'un système de paiement sur Internet

Nous étudions également les différents modes de redirection de client vers la page de paiement déportée chez le « prestataire de paiement » qui est un prestataire technique qui offre au marchand la possibilité d'avoir un terminal de paiement électronique virtuel pour encaisser les paiements des clients. Il s'agit de l'équivalent des fournisseurs de terminaux de paiement électroniques dans le commerce physique (exemple : Ingenico, Xiring, etc.) . Nous présentons, dans ce chapitre, une liste non exhaustive des systèmes de paiement les plus utilisés, en étudiant, à chaque fois, leur méthode d'intégration dans le site marchand. En effet, dans ce cas, l'E-commerçant

peut envoyer les données de la commande, au serveur de son prestataire de paiement, selon trois manières :

1. Via un service Web : le marchand effectue un appel aux services Web du prestataire de paiement afin de récupérer l'url de la page de paiement et rediriger le client.
2. Via une redirection HTTP chiffrée : le marchand installe un logiciel sur son serveur Web qui lui permet de rediriger le client vers la page de paiement du prestataire de paiement avec des données de commande chiffrées.
3. Via une redirection HTTP signée : le marchand génère un formulaire HTML contenant plusieurs champs cachés avec les détails de la transaction (identifiant unique de la transaction, montant, identifiant du marchand, etc.) et l'envoi au serveur du prestataire de paiement via le navigateur du client.

2.2 Intégration d'un système de paiement

Généralement, il y a trois manières d'intégrer un nouveau moyen de paiement sur Internet (figure 2.2) : la première consiste à l'intégrer dans toutes les plateformes d'E-commerce, la deuxième consiste à l'intégrer chez tous les prestataires de paiement, et la troisième consiste à l'intégrer directement dans tous les sites marchands. Cependant, aucune de ces solutions n'est facilement réalisable parce que chacune impose l'intégration du moyen de paiement dans toutes les plateformes concernées. Dans notre travail, nous nous intéressons aux marchands qui ont déjà intégré le moyen de paiement bancaire et qui souhaitent intégrer un nouveau moyen de paiement non bancaire, soit parce que ce moyen de paiement n'est pas proposé par la plateforme E-commerce qui héberge leur site marchand, soit parce que leur prestataire de paiement ne propose pas ce nouveau moyen de paiement.

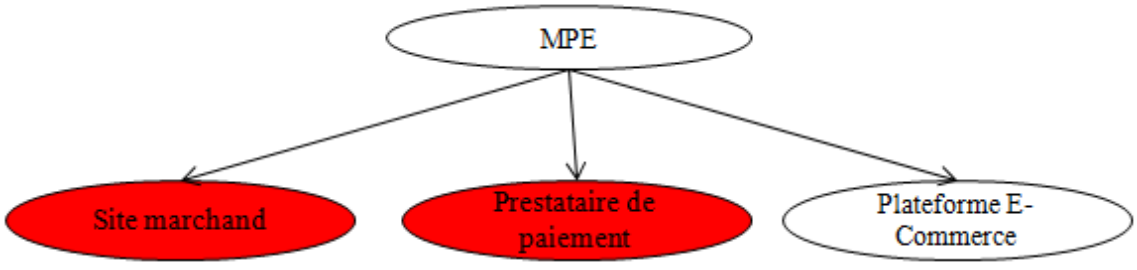


FIGURE 2.2 – Les différentes approches d'intégration d'un moyen de paiement électronique (MPE) sur Internet

2.2.1 Etapes de l'intégration

Avant de détailler les différentes étapes d'intégration d'un système de paiement, nous proposons d'analyser le processus d'une transaction E-commerce présenté dans le chapitre précédent. Pour ce faire, nous avons repris la figure 1.3 en détaillant les étapes de la phase de paiement. Nous divisons le processus d'achat en trois phases : l'avant-paiement, le paiement et l'après-paiement. La première phase concerne l'ajout du moyen de paiement dans la page de choix des instruments de paiement et la redirection du client vers le terminal de paiement virtuel. La deuxième phase concerne le paiement et comporte essentiellement la page de paiement et l'orchestration de plusieurs paiements (en cas de besoin). La dernière phase concerne la communication du résultat de paiement (appelé également le ticket de paiement) au client et le rapprochement entre le paiement effectué et la commande en cours.

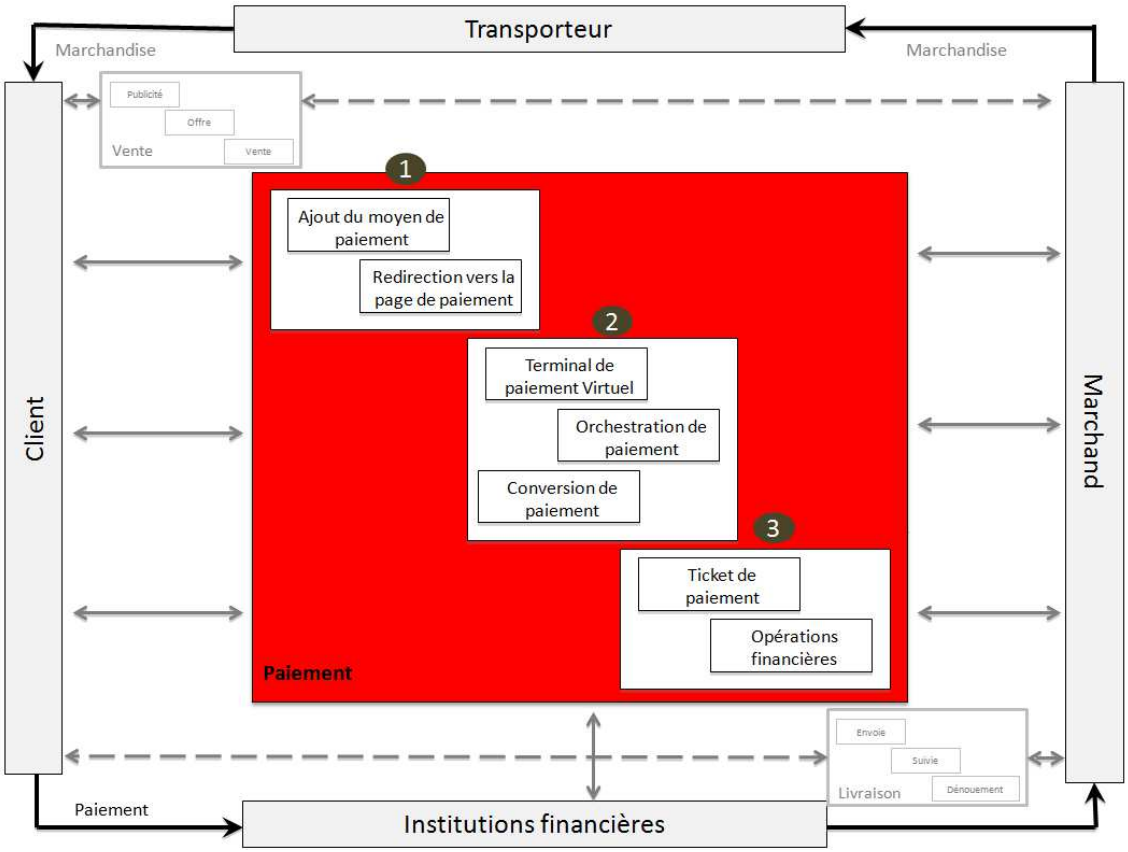


FIGURE 2.3 – Les étapes d'intégration d'un système de paiement

Ajout du moyen de paiement

Dans le commerce électronique B2C, le site Web est central pour le marchand car il permet de guider le client et l'inciter à acheter les produits proposés. D'où l'importance du design du site marchand et plus particulièrement de la page de choix de moyens de paiement afin d'éviter le risque d'abandon de l'achat. Le marchand doit bien réfléchir à l'ordre d'affichage des moyens de paiement acceptés, selon leur importance. Il doit également garantir une bonne ergonomie pour ne pas embrouiller le client et ne pas le démotiver pour valider sa commande.

Paiement

Il s'agit de la phase pendant laquelle le client communique ses coordonnées de paiement, puis le système de paiement contacte l'émetteur afin d'obtenir l'autorisation de paiement et la garantie du paiement. Cette page doit rappeler au client le montant qu'il doit payer et le numéro de la commande en cours (et le nom du marchand dans le cas du paiement déporté chez un prestataire de paiement). La plupart des pages de paiement actuelles sont des pages mono-paiement où on ne gère qu'un seul moyen de paiement. Parmi les contributions de cette thèse, on trouve la proposition d'un système de paiement qui agrège plusieurs instruments de paiement pour un même achat et qui gère l'orchestration des différents flux financiers.

Rapprochement

Le processus de transaction en ligne ne s'arrête pas au paiement ; il reste d'autres opérations à accomplir après la confirmation de paiement au client. Ces opérations sont accessibles depuis le back-office marchand qui permet le rapprochement entre des paiements et des commandes (le débit, l'annulation d'autorisation, le remboursement...). En effet, le marchand a besoin de lier les paiements effectués aux paniers validés afin de pouvoir livrer les produits/services et gérer les différentes opérations financières tout au long de la vie de la commande depuis sa validation jusqu'à sa clôture.

2.2.2 Evaluation de l'intégration

Maintenant que nous avons décrit les étapes d'intégration d'un système de paiement, nous nous intéressons aux outils d'évaluation de l'intégration d'un système de paiement sur Internet. Pour ce faire, nous allons reprendre les exigences retenues dans le chapitre précédent afin de définir les outils de mesure de chacune.

Evaluation de la sécurité d'un système de paiement

Il existe, dans la littérature, plusieurs éléments de mesure et d'évaluation de la sécurité d'un système de paiement sur Internet [Sahut J M., 2008]. Dans notre étude d'intégration des nouveaux moyens de paiement nous nous intéressons aux quatre critères suivants : la confidentialité, l'authentification, l'intégrité et la non-répudiation.

- La confidentialité : elle consiste à assurer que seules les personnes autorisées peuvent prendre connaissance des données. Pour obtenir ce service, on utilise généralement le chiffrement des données concernées à l'aide d'un algorithme cryptographique. Un système de paiement doit garantir la confidentialité des échanges entre le marchand et le client et protéger les données de paiement du client.
- L'authentification : elle permet d'assurer qu'une communication est authentique. On peut distinguer deux types d'authentification : l'authentification d'un tiers consiste à prouver son identité et l'authentification de la source des données qui sert à prouver que les données reçues proviennent bien de l'émetteur déclaré. L'authentification nécessite de fournir un élément d'identification et de prouver sa validité. Sur la plupart des réseaux, le mécanisme d'authentification utilise une paire code d'identification/mot de passe. Cependant, en raison de la vulnérabilité constamment associée à l'utilisation des mots de passe, il est souvent recommandé de recourir à des mécanismes plus robustes tels que l'authentification par des certificats, des clés publiques ou à travers des centres de distribution des clés. Dans le cas du système de paiement, le client et le marchand doivent être bien authentifiés afin de s'assurer que les données reçues lors d'une transaction électronique proviennent bien de l'entité déclarée.
- L'intégrité : elle se rapporte à la protection contre les changements. L'intégrité est garantie si les données émises sont identiques à celles reçues. Les techniques utilisées pour empêcher les modifications des données échangées sont, les bits de parité, les checksums ou encore les fonctions de hachage à sens unique [Preneel B., Bosselaers A., Govaerts R. et Vandewalle J., 1990]. Mais il ne s'agit pas des mécanismes les plus sûrs car il est possible qu'un attaquant modifie les données et recalcule le résultat de la fonction de hachage (empreinte). Pour que seul l'expéditeur soit capable de modifier l'empreinte, on utilise des fonctions de hachage avec clé secrète ou privée. Dans ce cas, on garantit à la fois l'intégrité et l'authentification.
- La non-répudiation : elle empêche tant l'expéditeur que le destinataire de nier avoir transmis un message. Dans le cadre de la cryptographie à clé publique

(asymétrique), chaque utilisateur est le seul et unique détenteur de la clé privée. Ainsi, tout message accompagné par la signature électronique d'un utilisateur ne pourra pas être répudié par celui-ci. En revanche, la non-répudiation n'est pas directement acquise dans les systèmes utilisant des clés secrètes (cryptographie symétrique). La clé de chiffrement étant distribuée par le serveur de distribution de clés aux deux parties, un utilisateur peut nier avoir envoyé le message en question en alléguant que la clé secrète partagée a été divulguée soit par une compromission du destinataire, soit par une attaque réussie contre le serveur de distribution de clés. Dans le cadre des paiements électroniques, le risque est qu'un client nie avoir payé une commande en ligne ou un marchand nie avoir reçu le paiement d'une commande.

Afin de mesurer le niveau de sécurité des systèmes de paiement sur Internet, nous allons procéder de deux manières : la première méthode consiste à vérifier que le nouveau système garantit les critères de sécurité décrits auparavant tout en prenant comme système de référence le système de paiement bancaire qui est le plus utilisé sur Internet. Pour ce faire, nous présentons le niveau de sécurité du système bancaire dans le tableau 2.1. PP étant l'acronyme de Prestataire de Paiement).

Type du système	Critères							
	Confidentialité	Authentification			Intégrité	Non-répudiation		
		Client	Marchand	PP		Client	Marchand	PP
CB classique	x	-	x	x	x	-	x	x
CB avec 3D-Secure	x	x	x	x	x	x	x	x

TABLE 2.1: Niveau de sécurité du système bancaire sur Internet

Nous constatons alors qu'un système de paiement bancaire classique ne permet pas de garantir l'authentification et la non-répudiation du client, contrairement à un système bancaire doté d'une authentification 3D-secure. Nous prenons alors comme référence le système bancaire avec authentification 3D-secure, même s'il ne s'agit pas aujourd'hui du système le plus utilisé sur Internet.

La deuxième méthode consiste à montrer que le système proposé résiste aux différentes attaques standards d'un système informatique sur Internet. Dans la littérature, plusieurs attaques ont été présentées [Mookhey K., 2011], [Wilson C., 2005] et [Dubois J. et Jreije P., 2006]. Ces attaques peuvent être divisées en quatre catégories principales [Gill S., 2003] :

- Attaque d'accès : il s'agit d'une tentative d'accès à d'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information.

- Attaque de modification : elle consiste, pour un attaquant, à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information
- Attaque par saturation (déni de service) : il s'agit d'une attaque informatique qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes. Cette technique de piratage assez simple à réaliser est jugée comme de la pure malveillance. Elle ne fait que bloquer l'accès aux sites, sans en altérer le contenu.
- Attaque de répudiation : il s'agit d'une attaque contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se sont réellement passés.

Dans notre travail, nous allons montrer que les solutions que nous proposons résistent aux différents types d'attaque en prenant à chaque fois un exemple d'attaque dans chaque catégorie tel qu'il est décrit dans le tableau 2.2.

Types Attaque	Exemple
Attaque d'accès	Attaque homme au milieu
Attaque de modification	Modification du montant
	Modification du résultat de paiement
Attaque par saturation	Flooding
Attaque de répudiation	Répudiation du paiement par le client

TABLE 2.2: Quelques exemples d'attaques d'un système de paiement sur Internet

Ci-après un descriptif des différentes attaques choisies :

- Attaque de l'homme au milieu (Man-In-The-Middle). Il s'agit d'une attaque d'accès : ce type d'attaque vise à intercepter les communications entre deux parties sans que ni l'une, ni l'autre ne puisse s'en apercevoir. Il s'agit ici d'une attaque par interception. Lorsqu'un pirate réussit à se placer au milieu d'une communication, il peut écouter ou modifier celle-ci. Ce type d'attaque peut être dangereux dans le cas d'un système de paiement. En effet, un attaquant interceptant la communication entre le client et le serveur du marchand (ou son prestataire de paiement) peut récupérer les données de paiement du client (numéro de carte bancaire...) et les utiliser afin de payer sur d'autres sites marchands.
- Attaque de modification du montant de la commande par un client malveillant afin de payer moins cher (voire ne rien payer) pour sa commande. Il existe également une deuxième attaque de modification très connue dans le domaine

des paiements sur Internet, qui consiste à modifier le résultat de paiement envoyé par le prestataire de paiement au marchand après le paiement afin de simuler une confirmation de paiement.

- Attaque par Flooding : il s'agit d'une attaque de déni de service qui consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.
- Attaque de répudiation de paiement et demande de remboursement. Dans le cas des paiements sur Internet, les paiements se font d'une manière virtuelle sans la présence physique du client (contrairement au cas du commerce de proximité). Un client malveillant peut alors répudier son paiement afin de récupérer la somme qui a été payée après avoir reçu la commande.

Evaluation de l'ergonomie d'un système de paiement

Parmi les trois critères d'ergonomie que nous avons étudiés dans le chapitre précédent (la lisibilité des pages, le design des pages et l'enchaînement des pages), nous allons nous arrêter sur les deux critères design et enchaînement des pages du tunnel de paiement du site marchand, car il s'agit des critères qui peuvent être altéré lors de l'intégration d'un système de paiement externe. Cependant, la lisibilité des pages Web du site marchand est un critère qui n'est pas forcement modifié suite à l'intégration d'un système de paiement. Nous pensons ici, à la redirection du client vers le terminal de paiement virtuel et aux conséquences de cette redirection sur l'expérience utilisateur.

Evaluation de la complexité d'intégration

Pour étudier la complexité d'intégration d'un système de paiement, nous avons deux possibilités : la première consiste à définir les différentes étapes à suivre afin d'accomplir l'intégration du système de paiement. Il s'agit alors de définir une « procédure » d'intégration d'un système de paiement. Il existe dans la littérature différents modes de présentation d'une procédure. Les procédures les plus connues et utilisées sont les procédures visuelles [KONZ S., JOHNSON S., 2000] présentées sous forme écrite (texte et nombre) ou schématique (graphe, organigramme...). Au fil des ans, plusieurs auteurs ont développé des plans de rédaction pour structurer la création d'une procédure et ont proposé une démarche complète de conception afin d'écrire des procédures de qualité. Il existe des métriques permettant de mesurer les différents facteurs affectant la complexité d'une procédure, ce qui permet également de quantifier

la complexité [Denis M E., 2010]. Pour obtenir un score du niveau de complexité d'une procédure, il faut une équation globale intégrant certains facteurs. Il existe deux outils d'évaluation de la complexité d'une procédure. L'outil d'évaluation TACOM [Park J., 2009](pour TAsk COMplexity), qui est le seul outil qui a tenté d'intégrer le maximum de facteurs afin d'obtenir un score global du niveau de complexité d'une procédure et qui ait été validé et accepté par la communauté scientifique. Bien que ce modèle a été validé, il reste très peu employé par les entreprises, car il est extrêmement difficile à utiliser. L'utilisateur voulant quantifier le niveau de complexité d'une procédure avec TACOM doit transformer celle-ci en quatre différents graphiques permettant de calculer, dans un premier temps, l'entropie et, dans un deuxième temps, le score global de complexité. Lors de cette transformation, une partie de l'information contenue dans la procédure est modifiée ou tout simplement perdue. Le deuxième outil de mesure de la complexité d'une procédure est l'outil SPARK LITE [Denis M E., 2010] conçu par la compagnie Systèmes Humains-Machines (Shumac), qui, contrairement à TACOM, est un outil entièrement informatisé et automatisé, ce qui facilite grandement son utilisation. Cependant, il ne considère pas tous les facteurs affectant la complexité d'une procédure, ce qui le rend ainsi moins efficace. Nous avons alors choisi de nous baser sur un autre critère d'évaluation afin de déterminer la complexité de l'intégration d'un système de paiement.

La deuxième méthode consiste à mesurer le coût d'installation du système de paiement afin de mesurer la complexité de la procédure d'intégration. Nous partons du principe qu'un système de paiement difficile à installer est un système cher à mettre en place. Sur Internet, les coûts d'entrée sont à première vue plus faibles que sur un marché physique. Un site de commerce électronique peut rapidement avoir une présence nationale sans disposer d'un réseau de magasins sur l'ensemble de territoire. Néanmoins, les coûts de sécurisation des flux financiers transitant via un site E-commerce peuvent facilement augmenter, surtout lorsque le marchand décide d'héberger sa propre page de paiement. En général, les choix de l'E-commerce sont poussés par une grande motivation de minimiser les coûts et de diminuer les prix, ce qui exige une adaptation des stratégies utilisées et une mûre réflexion des choix stratégiques [Amami M., Rowe F., 2000]. Généralement, les coûts d'un projet E-commerce sont calculés afin d'avoir un bon retour sur investissement ce qui garantit une bonne rentabilité financière [Albouy M., Schatt A., 2004] [Battini P., 2000] [Hassairi A F., 2001]. Un marchand doit bien estimer le retour sur investissement lié à l'intégration d'un système de paiement et bien estimer le coût des développements techniques par rapport au nombre de clients utilisant ce moyen de paiement. Cependant, nous nous sommes heurtés à un problème d'accès à ce type d'information. En

effet, le coût d'intégration d'une plateforme de paiement dans un site E-commerce semble différer d'un site marchand à un autre. Les coûts sont également très variables car ils comportent trois catégories [Amami M., Rowe F., 2000] : les coûts d'accès à la technologie, les coûts d'erreur et les coûts des délais. Il s'agit parfois des données confidentielles que certains E-commerçants ne souhaitent pas communiquer. A notre connaissance, il n'existe aucune étude comparant les systèmes de paiement selon ce critère de coûts d'intégration technique du système. Généralement, les études comparent les frais d'installation facturés par les établissements financiers et/ou les prestataires de paiement. Pour notre part, une enquête a été réalisée auprès de quelques E-commerçants, afin de mesurer le coût d'intégration de leur système de paiement. Il s'agit d'une mesure externe, mais indéniablement liée à la complexité. La valeur mesurée, ici, est à titre indicatif, elle sert seulement pour comparer les différents modes d'intégration entre eux.

Avant de présenter les différents modes d'intégration d'un système de paiement, nous présentons dans le tableau 2.3 un récapitulatif des étapes et des outils de mesure/évaluation de l'intégration d'un système de paiement sur Internet.

Critère d'évaluation	Eléments de mesure
Sécurité	Confidentialité Authentification Intégrité Non-répudiation Résistance à certaines attaques
Ergonomie	Enchaînement des pages
Complexité	Coût/Développement technique

TABLE 2.3: Evolution de l'intégration d'un système de paiement sur Internet

2.3 Intégration directe dans le site E-commerce

Certains marchands (généralement les grands sites marchands) préfèrent héberger leur propre page de paiement afin de gérer par eux-mêmes le paiement et sauvegarder les données de leurs clients et leurs proposer des facilités de paiement (paiement en un clic) afin de les fidéliser. Dans ce cas, le marchand est le seul responsable de la sécurité des paiements et du bon usage des données des clients. C'est pour cette raison que ce type marchand, doit être conforme au standard Payment Card Industry Data Security Standard (PCI DSS). Il s'agit d'un ensemble de prescriptions établies par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa International en vue d'améliorer la sécurité des données de paiement sur Internet. Ce standard a été développé pour favoriser l'adoption à vaste échelle de mesures

consistantes de sécurité des données dans le monde entier. Tous les marchands qui traitent, stockent ou transmettent des informations de cartes de paiement bancaires sont alors tenus de se conformer au standard PCI DSS. Néanmoins, la satisfaction des exigences peut être coûteuse en temps et en argent [Clusif, 2011]. C'est pour cette raison que, généralement, seuls les grands sites marchands prennent la décision de gérer leurs propres pages de paiement (Fnac.com, Amazon.com...), en partenariat avec leurs banques « acquéreuses ». Par contre, les moyens et petits sites marchands préfèrent déporter leur page de paiement, afin d'éviter le coût et la complexité de la conformité PCI-DSS et déléguer le paiement électronique à un prestataire de paiement.

Généralement, dans le cas de cette intégration, le marchand héberge le formulaire de paiement, mais il passe par un prestataire de paiement afin d'acheminer les demandes d'autorisations de paiement auprès des instituts financiers. La communication avec le prestataire de paiement dans ce cas est effectuée via des services Web (section suivante). Cependant, le marchand doit gérer l'affichage de la page de paiement et sécuriser le paiement, comme nous l'avons dit auparavant.

2.4 Intégration via Service Web

Afin d'éviter de véhiculer des données sensibles (le montant, numéro de commande...) par le navigateur du client, le marchand peut choisir de communiquer en services Web (serveur à serveur) avec le prestataire de paiement et récupérer toutes les données nécessaires pour rediriger le client vers la page de paiement d'une manière sécurisée. Il existe plusieurs définitions pour les services Web mais la plus simple pourrait être « *fonctionnalité utilisable au travers du réseau en mettant en oeuvre un format standard, généralement XML* ». Les services Web permettent l'invocation de fonctions distantes, présentes sur des systèmes distribués et hétérogènes, grâce au protocole HTTP et à XML. « *Un service Web est un composant applicatif mis à la disposition sur un réseau et disposant de méthodes que l'on peut invoquer à distance via l'emploi de protocoles standards. Les services Web présentent l'avantage d'être faiblement couplés et indépendants des plateformes et réutilisables* » [Bardet S., 2003]. Le groupe W3C qui travaille sur les services Web a utilisé, dans un document appelé « Web Services Architecture », la définition de service Web suivante [World Wide Web Consortium W3C, 2004] : « un service Web est un système logiciel destiné à supporter l'interaction ordinateur-ordinateur sur le réseau ».

L'historique des services Web est assez simple à retracer. Cela a commencé avec des applications Web et des analyseurs syntaxiques de code HTML, puis un

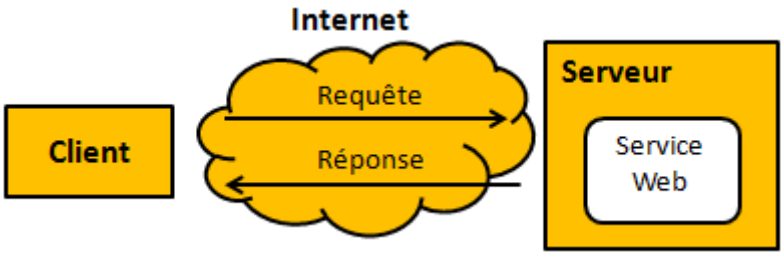


FIGURE 2.4 – Service Web

encodage spécifique pour des appels de procédures distantes (RPC), XML-RPC et son évolution SOAP (1998). L'écosystème autour de SOAP est rapidement devenu touffu [Gambarotto P., 2009], le nombre et la complexité des spécifications WS-* étant là pour en attester : WSDL pour la description des services Web, SOAP et ses nombreuses extensions pour la définition des messages, WS-Security pour l'aspect sécurité, UDDI pour le référencement de services Web, pour n'en citer qu'une infime partie. L'objectif ambitieux étant de définir des architectures orientées autour de services logiciels interconnectés [Borzmeyer S., 2003]. Or, vu la complexité des premiers modèles de services Web proposés, une nouvelle architecture plus simple orientée ressource a été proposée en 2000. Le grand succès de la technologie des services Web sur Internet, s'explique en partie par le fait qu'ils sont basés sur la technologie standard XML.

2.4.1 XML : eXtensible Markup Language

XML est un format texte simple, très flexible, tiré du SGML (l'ISO 8879) recommandé par W3C depuis 1998 en tant que standard de description de données. Il s'agit d'un méta langage permettant d'identifier la structure d'un document. La structure d'un document XML est souvent représentée graphiquement comme un arbre. La racine du document constitue le sujet du document, et les feuilles sont les éléments de ce sujet. De ce fait, XML est alors flexible et extensible, et est devenu rapidement le standard d'échange de données sur le Web [World Wide Web Consortium W3C, 2003]. Un exemple de la hiérarchie d'un document XML est présenté dans 2.4.

Les services Web reprennent la plupart des idées et des principes du Web (HTTP, XML), et les appliquent à des interactions entre machines. Comme pour le World Wide Web, les services Web communiquent via un ensemble de technologies fondamentales qui partagent une architecture commune. Ils ont été conçus pour être réalisés sur de nombreux systèmes développés et déployés de façon indépendante. Sur Internet, il existe plusieurs méthodes pour implémenter des services Web parmi lesquels : RPC,

```
<?xml version="1.0" encoding="utf-8" ?>
    <ShoppingCart>
        <Items>
            <ShoppingCartItem>
                <Label>Ipod Nano 5Go</Label>
                <UnitPrice>7000</UnitPrice>
                <Quantity>1</Quantity>
                <Category1>568</Category1>
                <Category2>Hifi/Baladeurs</Category2>
                <Brand>Apple</Brand>
                <MerchantItemId>R49203</MerchantItemId>
            </ShoppingCartItem>
            <ShoppingCartItem>
                <Label>Clef USB 8Go</Label>
                <UnitPrice>2000</UnitPrice>
                <Quantity>1</Quantity>
                <Category1>782</Category1>
                <Category2>Informatique/Accessoires</Category2>
                <Brand>Asus</Brand>
                <MerchantItemId>R49210</MerchantItemId>
            </ShoppingCartItem>
        </Items>
    </ShoppingCart>
```

TABLE 2.4: Extrait de code Fichier XML : ShoppingCard.xml

SOAP, REST, etc.

2.4.2 SOAP : Simple Object Access Protocol

SOAP est un protocole standard de communication décrit en XML et standardisé par le W3C. Il se présente comme une enveloppe pouvant être signée et pouvant contenir des données ou des pièces jointes. Un exemple de message SOAP est présenté dans la figure 2.5.

```
<env :Envelope xmlns :env="http ://www.w3.org/2003/05/soapenvelope">
<env :Header>
<n :alertcontrol xmlns :n="http ://example.org/alertcontrol">
<n :priority>1</n :priority>
<n :expires>2005-01-26T10 :30 :00-11 :00</n :expires> </n :alert control>
</env :Header>
<env :Body>
<m :alert xmlns :m="http ://example.org/alert">
<m :msg>Il s'agit d'un message SOAP </m :msg>
</m :alert>
</env :Body>
</env :Envelope>
```

TABLE 2.5: Exemple de message SOAP

Comme nous pouvons le constater, un message SOAP est composé essentiellement de trois parties : une enveloppe (qui permet de spécifier la version de SOAP et les règles d'encodage des messages), un en-tête (qui contient des éléments spécifiques et optionnels à l'application), un corps de message (contient les données de la requête SOAP). Mais, vu la complexité de la mise en place de ce protocole, une nouvelle architecture a été proposée en 2000, baptisée REST qui se distingue largement d'un service SOAP ou XML-RPC en se reposant uniquement sur l'utilisation du protocole HTTP, des URIs et d'XML, là où les deux autres protocoles se compliquent la tâche en utilisant des API RPC (Remote Procedure Call). SOAP et XML-RPC ne suivent pas la spécification HTTP, car ils ajoutent une nouvelle couche d'abstraction par-dessus le protocole, plutôt que de l'utiliser tel qu'il a été conçu.

2.4.3 REST : REpresentational State Transfer

REST est une architecture de services Web, élaborée en l'an 2000 par Roy Fielding [Fielding R T., 2000], l'un des créateurs du protocole HTTP, du serveur Apache HTTP et d'autres travaux fondamentaux. Cette architecture part du principe selon lequel Internet est composé de ressources accessibles à partir d'une URL. REST fait usage des standards Web, des verbes GET, PUT, POST, DELETE, prévu déjà par le protocole HTTP, afin de manipuler les ressources de manière simple. Lorsqu'un client Web récupère une URL, il sait qu'il peut récupérer une représentation de cette ressource en utilisant la méthode GET. Un exemple des échanges REST est présenté dans la table 2.6.

URI	Sémantique	Code réponse
GET http ://server/users	Récupère la liste des utilisateurs	200 OK
POST http ://server/users	Création d'un nouvel utilisateur	201 Created
GET http ://server/user/idUser	Récupère la représentation de l'utilisateur identifié par idUser	200 OK, 404 resource not found
PUT http ://server/user/idUser	Modifie un utilisateur	200 OK, 404 ressource not found
DELETE http ://server/user/idUser	Efface un utilisateur	200 OK, 404 ressource not found

TABLE 2.6: Exemple d'échange REST

Le principe de REST est d'utiliser HTTP pour l'implémentation d'un service Web , non seulement comme simple protocole de transport, mais également pour définir l'API de chaque service, c'est-à-dire la définition même des messages entre clients et serveurs. Paradoxalement, c'est donc un retour aux sources sachant que la spécification de HTTP 1.1 est légèrement antérieure (1997) aux premiers services Web basés sur les RPC (1998). Tout ceci présente plusieurs avantages : utiliser HTTP

comme un protocole applicatif et non pas seulement comme un protocole de transport et avoir des interfaces uniformes basées sur les messages HTTP.

2.4.4 Exemple

Il existe plusieurs systèmes de paiement sur Internet qui se basent sur l'architecture des services Web (Amazon Flexible Payment Service, Paypal Express Chekout, Google Checkout, Payline...). A titre d'exemple, nous allons décrire l'intégration de la plateforme de paiement Paypal Express Checkout. Il s'agit d'un service de paiement en ligne qui permet de payer des achats, de recevoir des paiements, ou d'envoyer et de recevoir de l'argent. Paypal a été conçu au début pour répondre à un manque de système de paiement entre des particuliers. Vu le succès de ce système de paiement, plusieurs sites marchands l'ont intégré afin d'acquérir de nouveaux clients. Paypal propose plusieurs API de paiement : DoDirectPayment API, DoNonReferencedCredit API, Express Checkout API, GetBalance API, GetPalDetails API, GetTransactionDetails API, RefundTransaction API, MassPay API [Paypal, 2009]. Dans le cadre de cette section nous allons décrire le service Web Express Checkout de Paypal présenté dans la figure 2.5. Nous décrivons ci-après les étapes du paiement :

1. Après la validation de la commande par le client, le marchand appelle l'API SetExpressCheckout avec les données de la transaction (ReturnURL, CancelURL, Amount...)
2. Paypal renvoie un jeton cryptographique permettant l'identification de la transaction d'une manière unique.
3. Le marchand ajoute le jeton cryptographique de la réponse SetExpressCheckout sous forme de paire nom/valeur à l'URL de la page de paiement Paypal, et redirige le navigateur de l'utilisateur vers l'adresse de la page de paiement (https ://www.paypal.fr/cgi-bin/Webscr ?cmd=_express-checkout&token=value)
4. Le client se connecte à son compte PayPal, approuve l'utilisation de PayPal comme moyen de paiement et confirme ses coordonnées et les informations de livraison. Puis Paypal redirige le navigateur de l'utilisateur vers le ReturnURL du marchand en y ajoutant le token en paramètre.
5. Le marchand appelle l'API GetExpressCheckoutDetails avec le jeton cryptographique pour récupérer les informations du client. Paypal renvoie une réponse avec le PayerID, l'adresse email, l'adresse de livraison, l'état de cette adresse (confirmée ou non confirmée) et d'autres détails.
6. Le marchand affiche une page de confirmation de paiement au client. Lorsque le client valide son paiement, le marchand appelle DoExpressCheckoutPayment

API avec les paramètres nécessaires (Token, OrderTotal, PaymentAction et PayerID) afin de confirmer le paiement.

7. Paypal renvoie les informations sur le paiement avec l'identifiant unique de la transaction et d'autres détails concernant la commande. Et le marchand affiche la page de résultat de paiement.

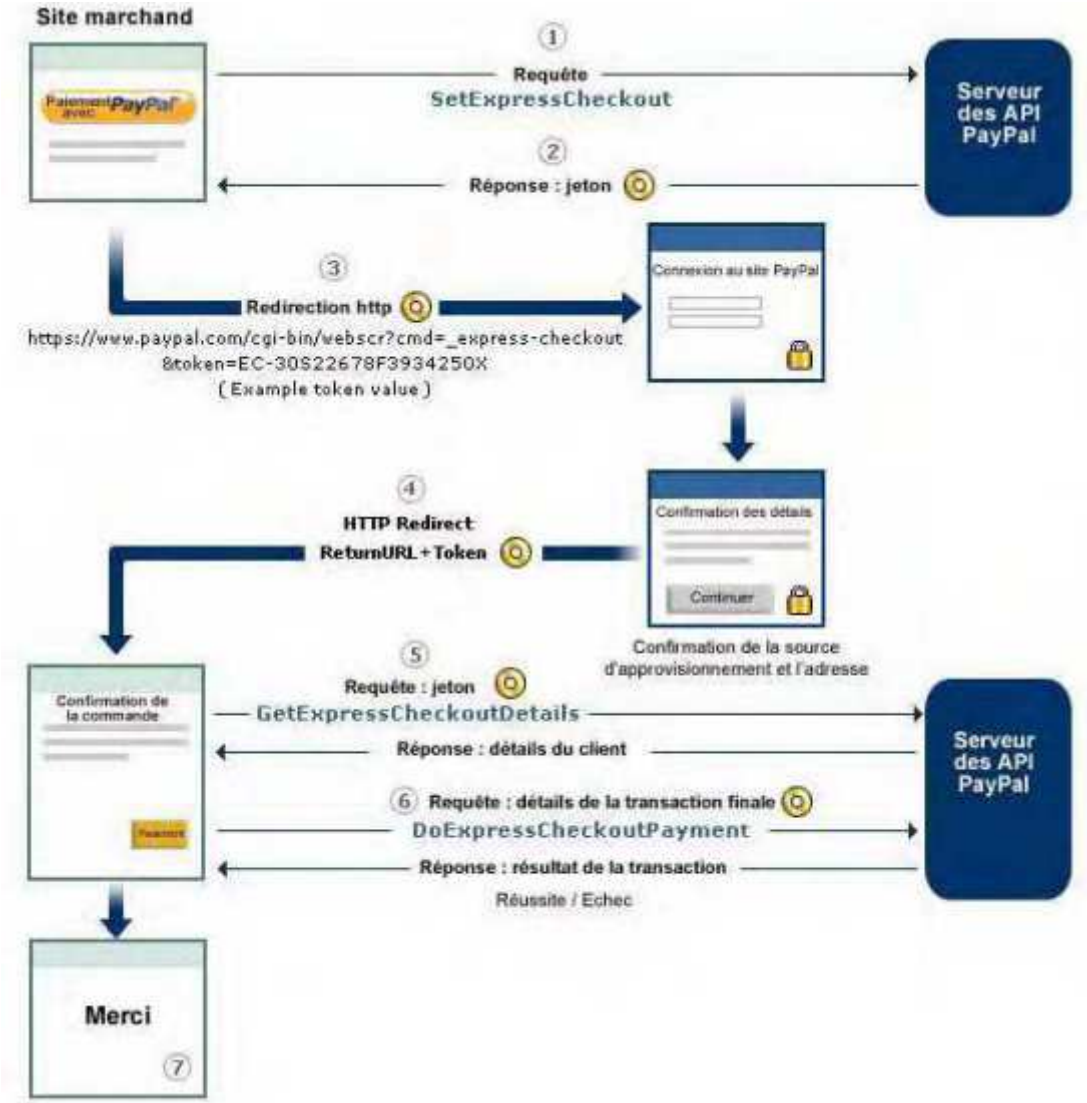


FIGURE 2.5 – Paypal Express Checkout [Paypal, 2009]

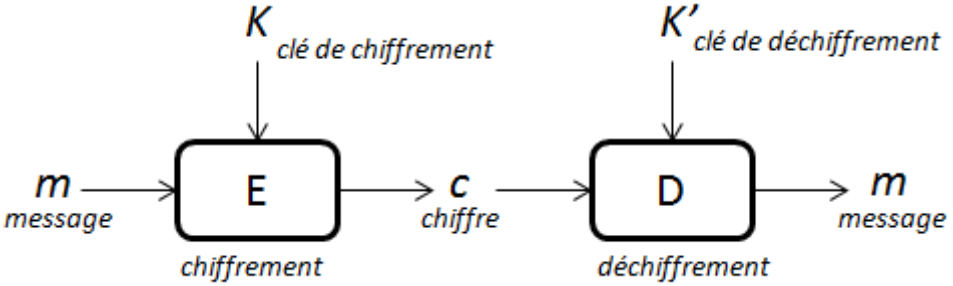
2.5 Intégration via redirection HTTP chiffrée

Contrairement au mode d'intégration via des services Web où les données de la commande ne transitent pas via le navigateur du client, le mode d'intégration via une

redirection HTTP chiffrée permet au client d'accéder aux données échangées entre l'E-commerçant et le prestataire de paiement. Afin d'éviter qu'un client malveillant puisse modifier les données de la commande, certains prestataires de service de paiement ont choisi de chiffrer les données de la commande transmises via le navigateur du client, ce qui assure la confidentialité, l'intégrité et l'authentification des données échangées entre le marchand et le prestataire de paiement. Cependant, il existe deux méthodes de chiffrement des données sur Internet : le chiffrement symétrique et le chiffrement asymétrique. Nous allons alors étudier la différence entre ces deux méthodes afin de justifier les choix effectués par les prestataires de paiement.

2.5.1 Chiffrement symétrique vs asymétrique

Le chiffrement est un processus basé sur une fonction qui permet de changer le message d'origine afin de cacher les informations contenues dans ce message. Ce qui permet de garantir la confidentialité et l'intégrité des données.



Le chiffrement symétrique (ou à clé secrète) consiste à partager une seule clé secrète entre l'émetteur et le récepteur du message ($K = K'$) [Stinson D, 1995]. Cette clé secrète est connue seulement par ces deux entités et dans ce cas, ils sont les seuls à pouvoir chiffrer et déchiffrer le message (figure 2.6). Cette méthode permet le chiffrement de n'importe quel type de message et ne dépend pas de la longueur du message à chiffrer, ce qui présente un grand avantage, en plus de la rapidité du processus de chiffrement. Parmi les algorithmes de chiffrement, citons : AES, DES, etc. Cependant, ce type de chiffrement souffre d'un problème de gestion des clés, car, à chaque fois qu'une entité souhaite échanger un message avec une autre entité, elles doivent, tout d'abord, créer un canal sécurisé afin d'échanger la clé secrète, puis utiliser cette clé pour chiffrer la communication, ce qui peut multiplier les clés à gérer car à chaque fois qu'on change d'interlocuteur on doit changer de clé secrète.

La deuxième méthode de chiffrement est le chiffrement asymétrique (ou à clé publique), basée sur des fonctions à sens unique, faciles à appliquer à un message, mais qui rendent le retour à ce message d'origine extrêmement complexe à partir

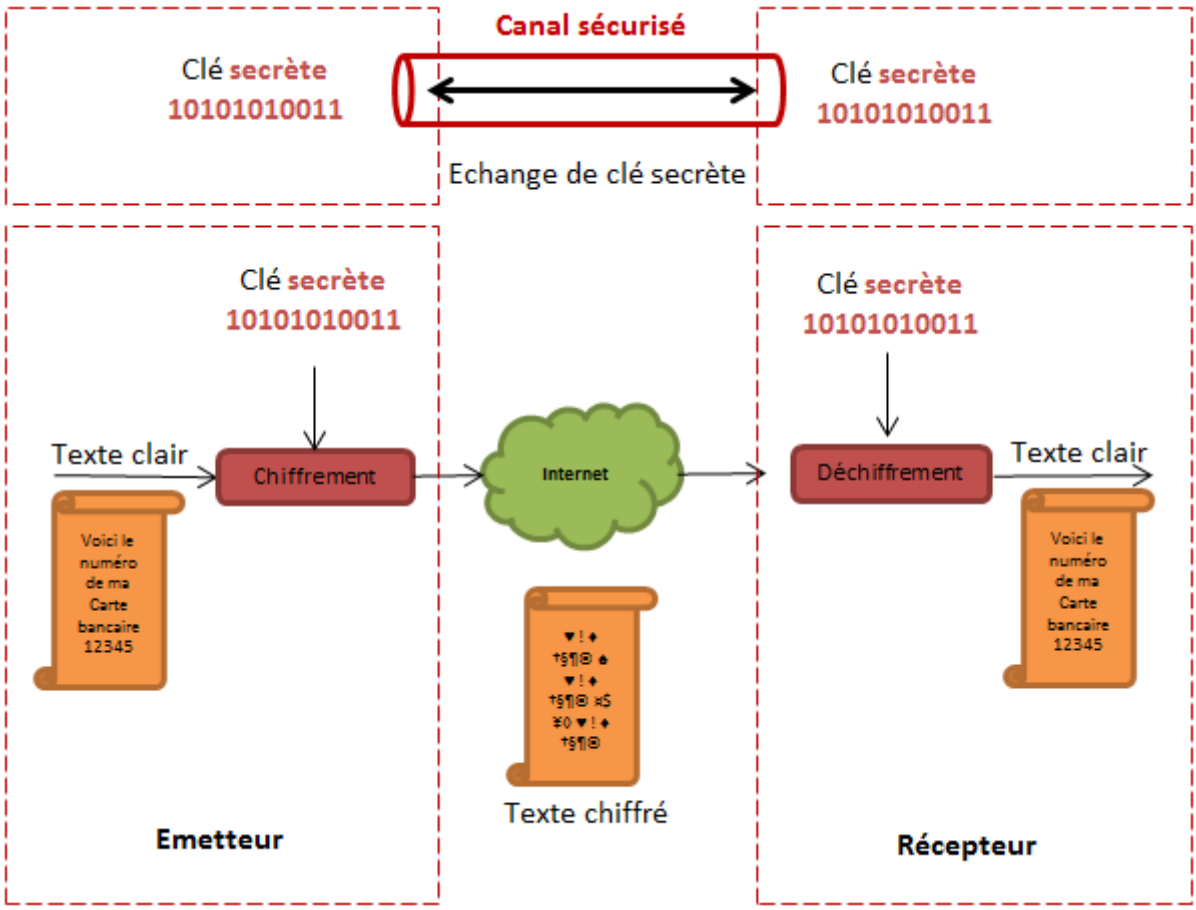


FIGURE 2.6 – Principe du chiffrement symétrique

du moment ou une fonction de ce type lui a été appliquée. En fait, cette technique de chiffrement utilise des fonctions non seulement à sens unique mais également connues comme basées sur des problèmes reconnus difficiles (exemple : problème de logarithme discret, problème de factorisation...). Contrairement au chiffrement symétrique où il faut s'échanger une clé secrète afin de chiffrer le message échangé, dans le cas du chiffrement asymétrique, chaque entité possède une paire de clé (privée, publique). Une illustration du principe de ce mécanisme est présentée dans la figure 2.7. L'émetteur du message utilise la clé publique du récepteur afin de chiffrer le message. Ainsi, seul le récepteur est capable de retrouver le message d'origine car il est le seul en possession de la clé privée correspondante à la clé publique de chiffrement (K est la clé publique du récepteur et K' est sa clé privée). Le grand avantage du chiffrement asymétrique est alors qu'il n'est pas limité par le problème de distribution des clés. Cependant, ce type de chiffrement s'avère très lent et il ne permet pas de chiffrer des grands volumes de données.

Pour pallier le problème de distribution des clés dans le cas de la cryptographie

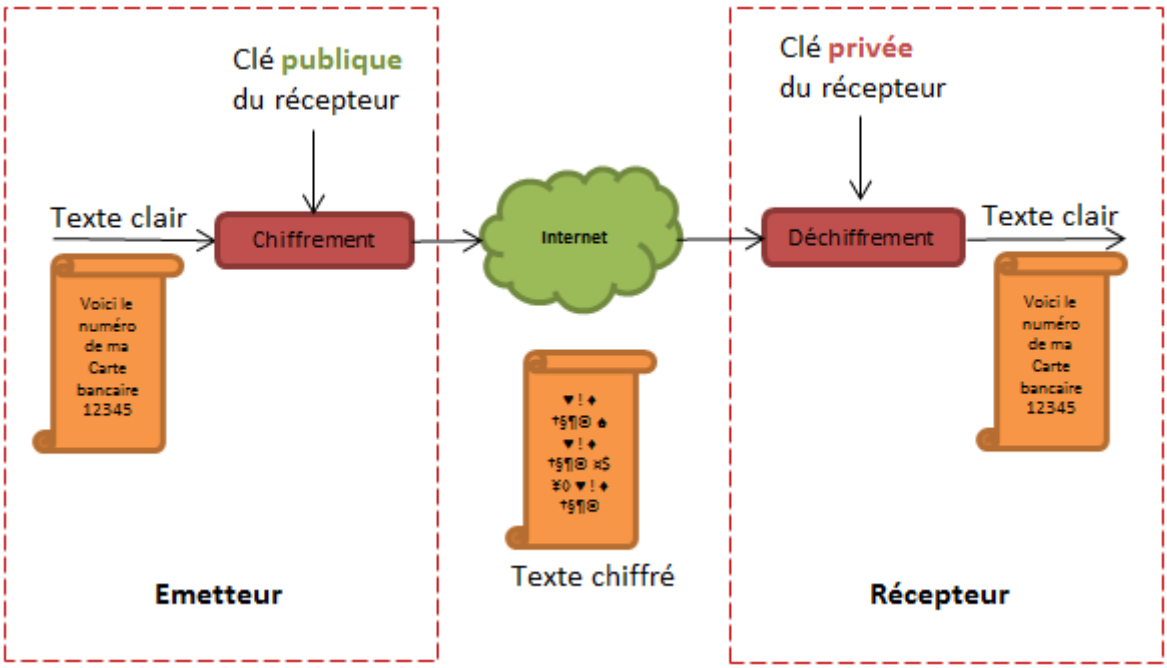


FIGURE 2.7 – Principe du chiffrement asymétrique

symétrique, la cryptographie asymétrique est toujours utilisée au début de la communication afin de convenir d'une clé de session qui servira de clé secrète pour la suite de la communication (le cas du protocole SSL par exemple).

2.5.2 Module CGI (Common Gateway Interface)

Comme nous venons de le voir dans la section précédente, afin d'utiliser le chiffrement asymétrique, les interlocuteurs doivent avoir une paire de clés (privée, publique). En revanche, la plupart des marchands qui délèguent leur terminal de paiement électronique virtuel à un prestataire de paiement, le font pour éviter d'effectuer les opérations cryptographiques pour sécuriser la page de paiement. Il se trouve que la majorité des sites marchands à paiement déporté ne possèdent pas de certificat SSL et du coup ne proposent pas des services sécurisés. C'est pour cette raison, en plus des différents inconvénients du chiffrement asymétrique, que les prestataires de paiement ont choisi le chiffrement symétrique afin de sécuriser la redirection du client vers leurs serveurs de paiement.

En effet, afin de faciliter l'intégration du système de paiement chez le site marchand, certains prestataires ont choisi de communiquer un module CGI (Common Gateway Interface) aux marchands. Ce module cryptographique est un exécutable qui permet à partir de certaines données (telles que l'identifiant du commerçant, la

référence de la commande, le montant de la transaction, etc.) de générer une donnée chiffrée et de rediriger le client vers la page de paiement. Dans ce cas, le prestataire de paiement communique au marchand une clé secrète (ou un certificat) via un canal sécurisé. Cette clé est par la suite prise en compte par le module cryptographique lors du chiffrement.

2.5.3 Exemple

Citons, comme exemple dans cette catégorie d'intégration, la solution technique Sips qui est une solution de paiement commercialisée par la société Atos en direct, ainsi que par de nombreux partenaires bancaires : banque populaire (CyberPlus), société générale (Sogenactif), crédit lyonnais (Sherlock's), crédit du nord (Webaffaires), CCF (Elysnet), etc. Pour intégrer la page de paiement Sips, le marchand doit installer un module CGI.

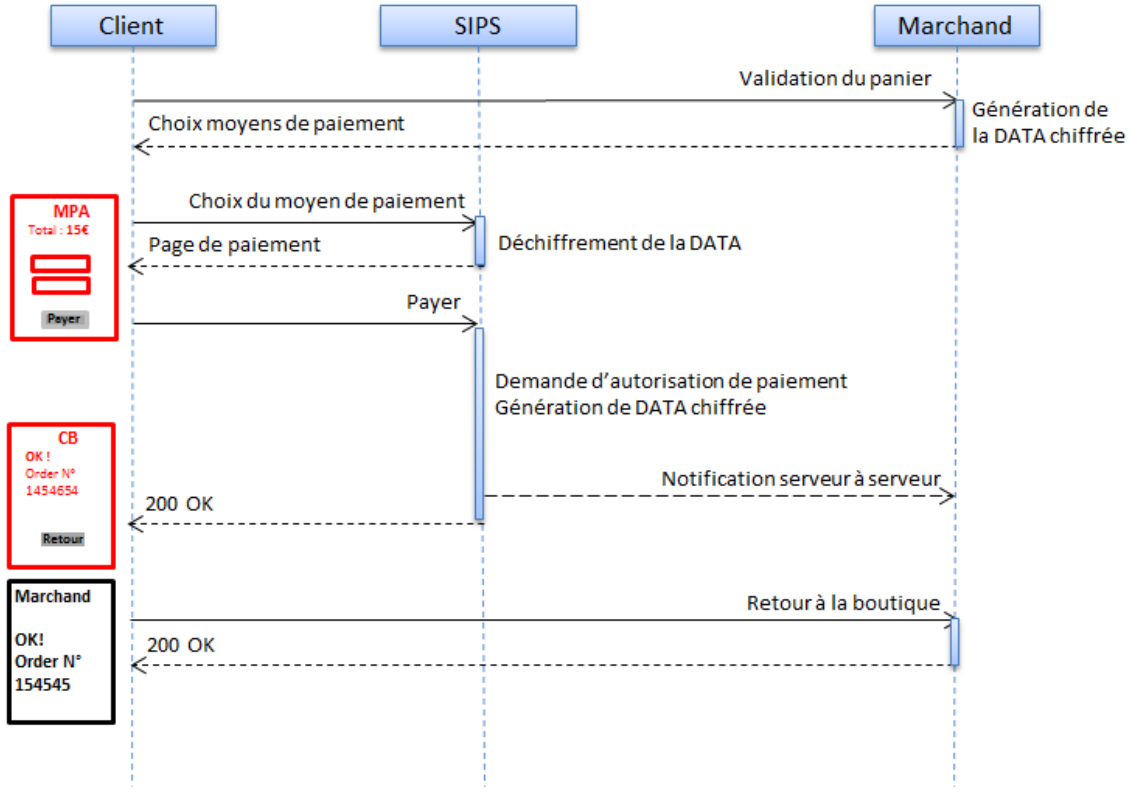


FIGURE 2.8 – Transaction Sips

Le déroulement d'une transaction Sips est décrit dans la figure 2.8 et correspond aux étapes suivantes :

1. Le client navigue sur le site marchand et valide sa commande.

2. Le marchand appelle le module CGI installé sur son serveur qui génère une data chiffrée à partir des informations du panier (montant, article...)
3. Le marchand redirige le client vers la page de paiement du prestataire de paiement avec les données chiffrées.
4. A la réception de la requête du client, Sips déchiffre la data chiffrée et affiche la page de paiement avec l'information de la commande (montant, référence de la commande...).
5. Le client paie sa commande en communiquant ses coordonnées bancaires au prestataire de paiement et validant son paiement.
6. Le prestataire de paiement demande alors l'autorisation de paiement à la banque du client, en passant par le front-office de la banque du marchand.
7. Une fois la réponse à la demande d'autorisation reçue, le partenaire de paiement envoie une notification automatique (serveur à serveur) au site marchand pour lui communiquer le résultat de paiement et redirige le client vers le site marchand (en envoyant aussi le résultat de paiement dans une data chiffrée)
8. Grâce au module CGI installé sur son serveur, le marchand peut déchiffrer le résultat de paiement et afficher une page de résultat de paiement au client.

2.6 Intégration via redirection HTTP signée

Une autre méthode de sécurisation de la redirection HTTP du client vers la page de paiement déportée consiste à « signer » les données envoyées via le navigateur du client, ce qui permet de garantir l'intégrité et l'authenticité des données échangées. Il ne s'agit pas d'une vraie signature numérique (avec une clé privée), mais plutôt d'envoyer un MAC (Message Authentication Code) avec les données de la commande.

2.6.1 Hachage

Rappelons qu'une fonction de hachage est une fonction à sens unique très utilisée en cryptographie, principalement dans le but de réduire la taille des données à traiter par les fonctions cryptographiques. En effet, la caractéristique principale d'une fonction de hachage est de produire un haché des données, c'est-à-dire un condensé de ces données. Ce condensé est de taille fixe, dont la valeur diffère suivant la fonction utilisée. Cependant, il ne suffit pas d'appliquer le principe de hachage sans clé, appelé également MDC (Modification Detection Code), tel qu'il est décrit dans la figure 2.9, car un client malveillant peut facilement changer les données de la commande,

générer un nouveau hash et l'envoyer au prestataire de paiement. Dans ce cas, le prestataire de paiement ne peut pas détecter la modification des données reçues car la vérification du hash sera validée (figure 2.10). D'où l'intérêt d'authentifier les données en plus de garantir leur intégrité. Pour ce faire, il faut utiliser les fonctions de hachage avec clé appelées aussi Message Authentification Code (MAC). Dans ce cas, un client malveillant ne peut pas générer le même hash que le marchand car il ne détient pas la clé secrète connue seulement par le marchand et le prestataire de paiement (figure 2.11).

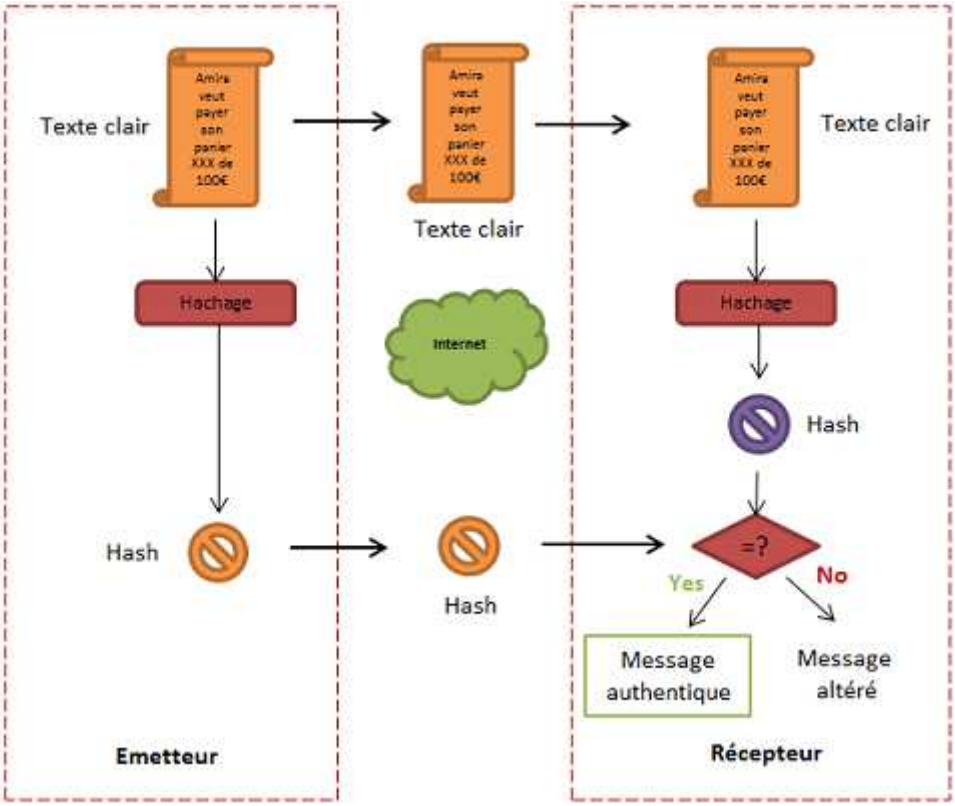


FIGURE 2.9 – Principe du Modification Detection Code (MDC)

Dans ce cas, le marchand et le prestataire de paiement partagent une même clé secrète d'une manière sécurisée (générée via le back-office marchand ou un autre canal sécurisé). Lors de la redirection du client vers la page de paiement du prestataire de paiement, le marchand calcule le MAC avec la clé secrète et l'envoie avec les données de la commande via le navigateur du client. Ainsi, à la réception de la requête du client, le prestataire de paiement peut vérifier l'intégrité et l'authenticité du message avant d'afficher la page de paiement correspondante. Parmi les prestataires qui utilisent cette technique, nous trouvons : Ogone, Cybermut, etc. Nous allons étudier dans la section suivante, plus en détail, l'exemple d'Ogone.

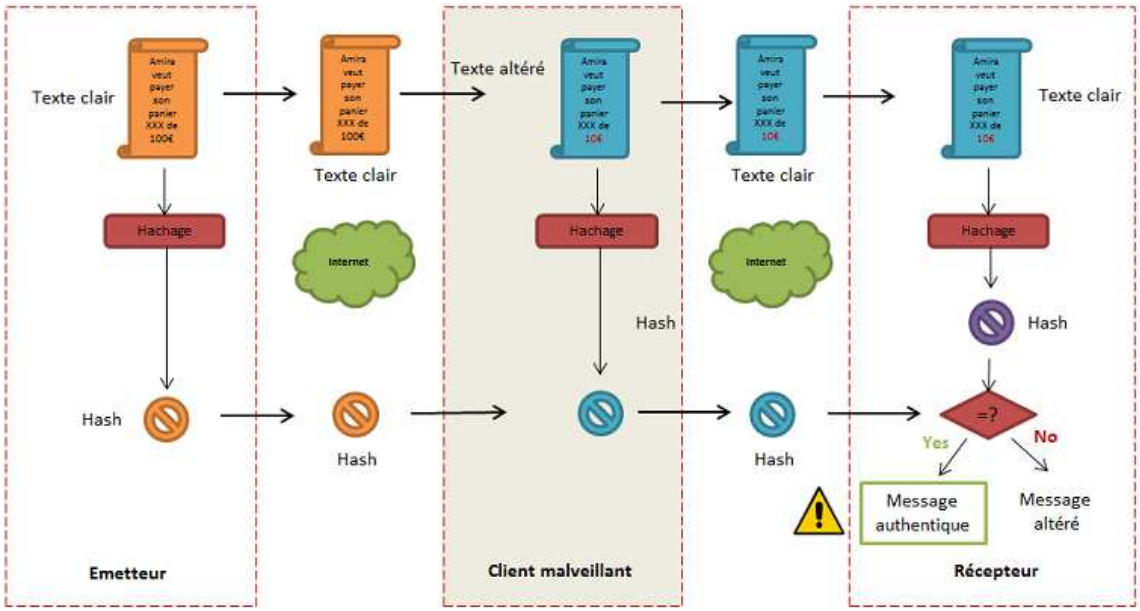


FIGURE 2.10 – Exemple de fraude appliquée au Modification Detection Code (MDC)

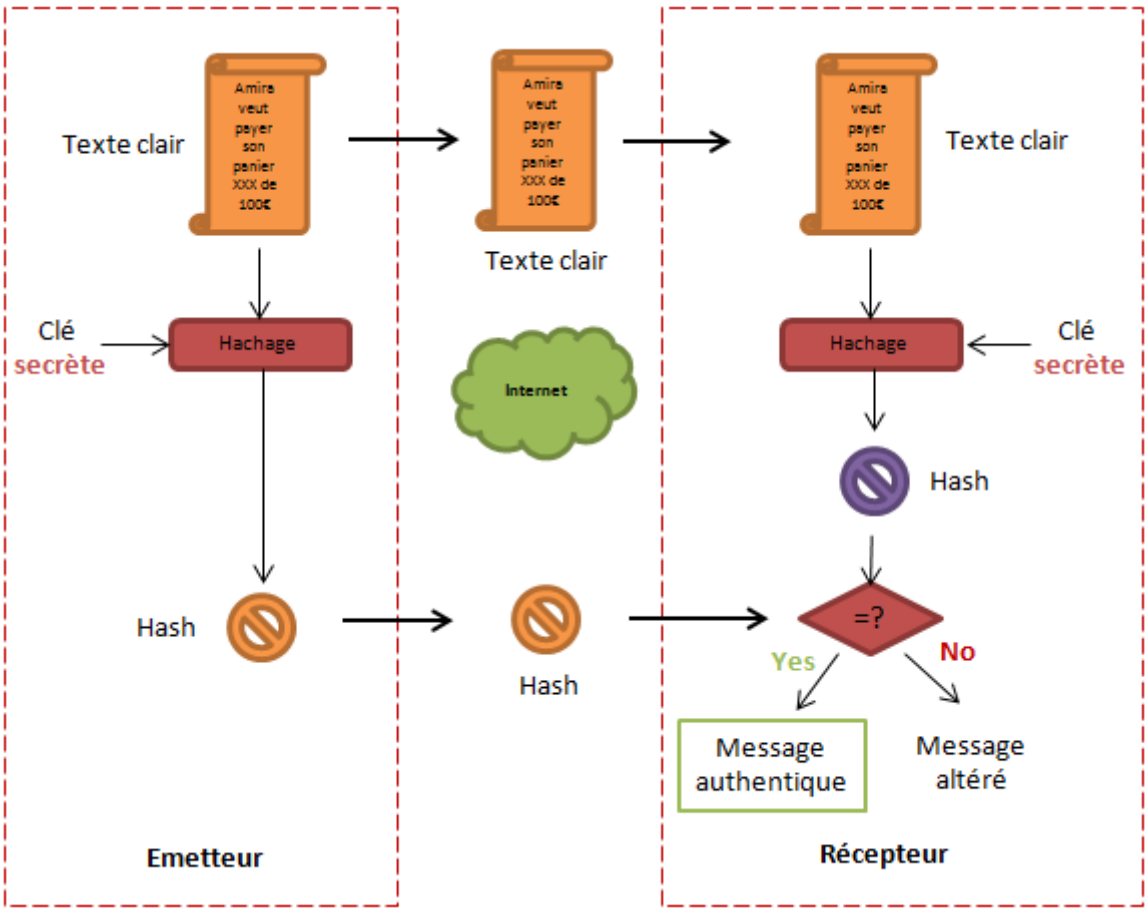


FIGURE 2.11 – Principe de génération du Message Authentication Code (MAC)

2.6.2 Exemple

Afin d'intégrer Ogone l'E-commerçant doit demander un accès à un back-office où il renseigne dans un onglet technique plusieurs informations concernant la gestion de la page de paiement, y compris les données de sécurité telles que le mot de passe qui servira de clé secrète entre le marchand et Ogone. Le lien entre le site marchand et la page de paiement du prestataire de paiement est établi sur la dernière page du panier d'achat, c'est-à-dire la dernière page du site marchand présentée à l'acheteur. Un formulaire avec des champs HTML cachés contenant les données de la commande est intégré dans la dernière page. Le marchand envoi les données de la commande via ce formulaire HTML, et afin d'empêcher un client malveillant de modifier ces données, Ogone exige l'envoie d'une signature numérique « SHASign » qui permet de garantir l'authenticité et l'intégrité des données envoyées.

Règle : La chaîne est créée en concaténant les valeurs des champs orderID, amount, currency, PSPID du formulaire et le mot de passe du marchand défini dans le back-office d'Ogone. Exemple : orderID : 1234 amount : 15.00 -> 1500 currency : EUR PSPID : MyPSPID mot de passe : Mysecretsig1875!? Chaîne avant le hash : 12341500EURMyPSPIDMysecretsig1875!? Chaîne après le hash : DC60B48E780C38137EB5B86CEC037427062B30CC SHASign dans les champs cachés du formulaire : DC60B48E780C38137EB5B86CEC037427062B30CC

TABLE 2.7: Exemple de calcul du MAC

Généralement, le prestataire de paiement exige un algorithme de calcul de la signature numérique que le marchand doit appliquer afin de générer sa signature avant de l'envoyer via le formulaire HTML. Un exemple de calcul de signature est présenté dans la table 2.7.

La transaction Ogone est décrite dans la figure 2.12 qui correspond aux étapes suivantes :

1. Le client navigue sur le site E-commerce, remplit son panier et valide sa commande.
2. Le marchand génère un formulaire HTML contenant les différentes données de paiement sécurisées par la signature numérique tel qu'il est défini dans la table

2.7 et l'insère dans la page de choix de moyen de paiement, lorsque le client choisit le moyen de paiement, il est redirigé vers la page de paiement d'Ogone suite à l'envoi du formulaire HTML.

3. A la réception de la requête du client, Ogone vérifie l'intégrité et l'authenticité des données envoyées en vérifiant la valeur du SHASign reçu et affiche la page de paiement au client.

4. Le client communique alors ses coordonnées de paiement au partenaire de paiement qui achemine la demande d'autorisation à l'émetteur du moyen de paiement en passant par le front-office de la banque du marchand. Si l'autorisation de paiement est accordée, le prestataire de paiement redirige le client vers le site marchand en envoyant le résultat de paiement avec une signature SHASign.

5. Le marchand vérifie alors l'intégrité et l'authenticité des données reçues et affiche une page de résultat de paiement.

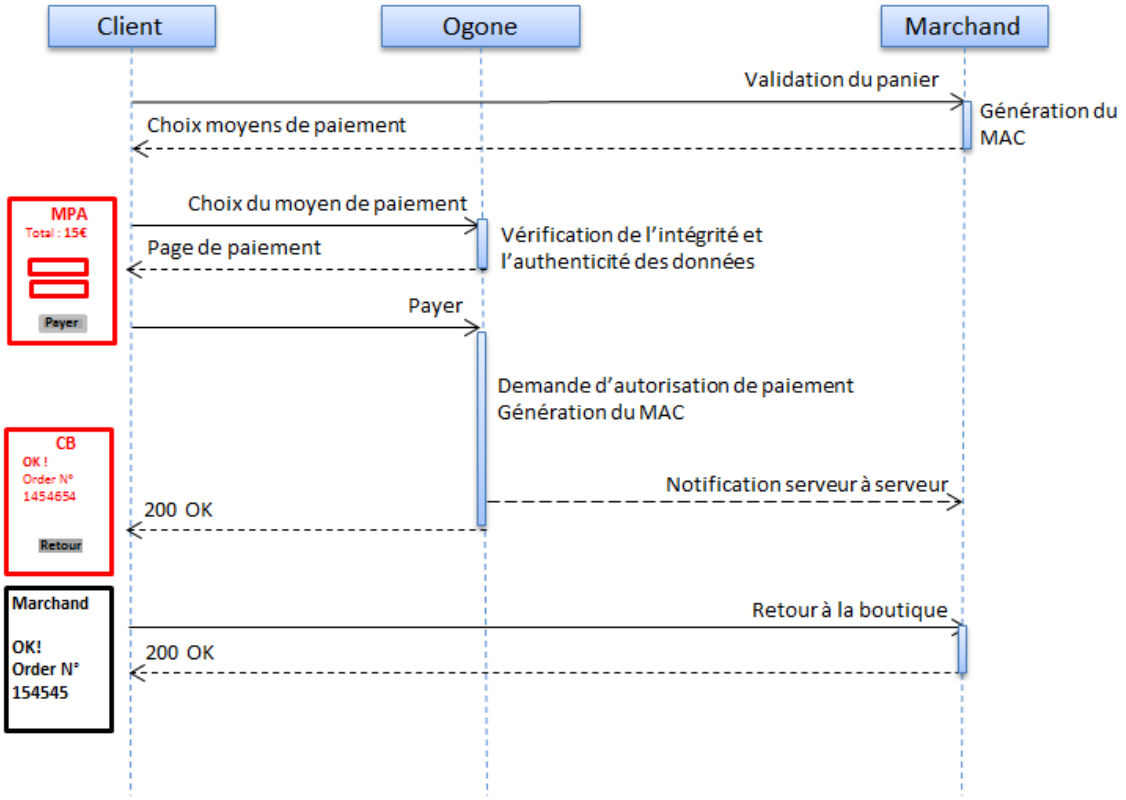


FIGURE 2.12 – Transaction Ogone

2.7 Etude comparative

Maintenant que nous avons décrit les différents modes d'intégration des systèmes de paiement existants, nous allons procéder à leur comparaison selon les critères définis dans le chapitre précédent (sécurité, ergonomie, complexité) afin de décrire les limites de l'existant. Pour ce faire, nous allons reprendre les deux typologies des systèmes présentés au début de ce chapitre (figure 2.1). En effet, selon le mode d'intégration du système de paiement (intégré ou déporté), les problématiques de sécurité, ergonomie et complexité d'intégration ne se posent pas de la même manière.

2.7.1 Sécurité

Si le système de paiement est hébergé par le site marchand, ce dernier doit bien verrouiller son serveur de paiement afin d'éviter l'utilisation frauduleuse des cartes de paiement des clients. Dans le cas de paiement bancaire, le marchand doit être conforme à la norme Payment Card Industry Data Security Standard (PCI DSS) qui a été développée pour favoriser l'adoption à vaste échelle des mesures consistantes de sécurité des données. En plus, aucun transfert de donnée à une entité extérieure n'est nécessaire pour afficher la page de paiement. La même entité qui détient les données de la commande affiche la page de paiement, ce qui constitue un grand avantage de sécurité.

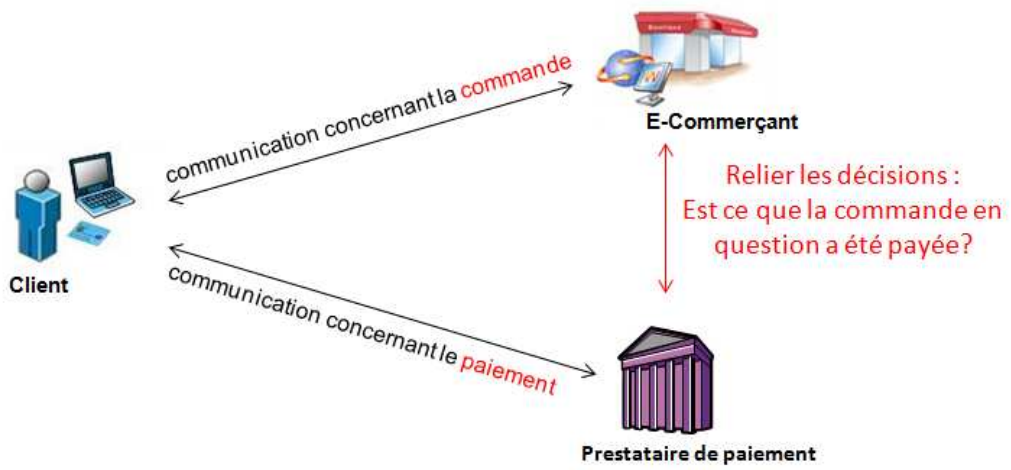


FIGURE 2.13 – Communication tripartite dans un système de paiement

Cependant, vu la difficulté et les coûts d'obtention de la certification PCI DSS, la majorité des sites marchands ont choisi de déléguer leur page de paiement à un prestataire de paiement et d'introduire ainsi un nouvel acteur dans le processus de la transaction électronique sur Internet. En effet, si un marchand délègue sa page de

paiement à un partenaire technique, c'est parce qu'il ne dispose pas généralement des outils de sécurité nécessaires pour sécuriser les paiements sur son site E-commerce. Donc, il se base sur ceux proposés par son prestataire afin de sécuriser la redirection du client vers la page de paiement externe. L'introduction de ce nouvel acteur impose une vérification explicite des données transmises pour assurer la liaison entre le message échangé et la commande en question (figure 2.13).

Nous avons effectué une étude de la relation tripartite dans un système de paiement [Abdellaoui R. et Pasquet M., 2010] qui nous a permis d'identifier deux canaux de communication : celui entre le client et le partenaire de paiement (qui concerne le paiement) et celui entre le marchand et le prestataire de paiement (qui concerne la communication des données de la commande avant le paiement et la validation du résultat du paiement par la suite). Nous allons nous intéresser au deuxième canal de communication, car nous estimons qu'il mérite encore plus de travaux de R&D et que le premier canal peut être sécurisé seulement grâce à SSL. Nous proposons alors d'analyser la communication entre le marchand et le prestataire de paiement en deux phases : « avant le paiement » et « après le paiement ».

La première phase « avant paiement », consiste à communiquer au prestataire de paiement les données de la commande (essentiellement le numéro de commande et le montant) afin d'afficher la page de paiement correspondante au client. Cependant, afin de prouver l'importance de sécuriser cette phase de la communication entre le marchand et le prestataire de paiement, nous proposons une analyse des éventuelles attaques de sécurité qui peuvent causer des dégâts financiers considérables au marchand. Dans la littérature, plusieurs scénarios de fraudes ont été découverts qui permettent de diminuer le prix de la commande voire d'acheter sur Internet sans rien payer [Wang R., Chen S., Wang X. et Qadeer S., 2011].

La deuxième phase « après le paiement » est également très importante car il s'agit de la phase pendant laquelle le prestataire de paiement communique le résultat de paiement au marchand. Une mauvaise interprétation des messages envoyés par le partenaire de paiement ou une communication implicite concernant la commande peut également causer des dégâts financiers considérables à l'E-commerçant. Nous présentons dans la figure 2.14 un exemple d'une mauvaise communication exploitée par un client malveillant pour payer une commande fictive (C') au lieu de la vraie commande (C). En effet, du moment où la redirection vers le prestataire de paiement se fait via le navigateur du client, ce dernier peut modifier les données envoyées et essayer de payer une commande moins cher. La confirmation de paiement du partenaire de paiement doit alors être sécurisée et doit contenir des éléments distinctifs de la commande payée (numéro de commande, montant payé, date).

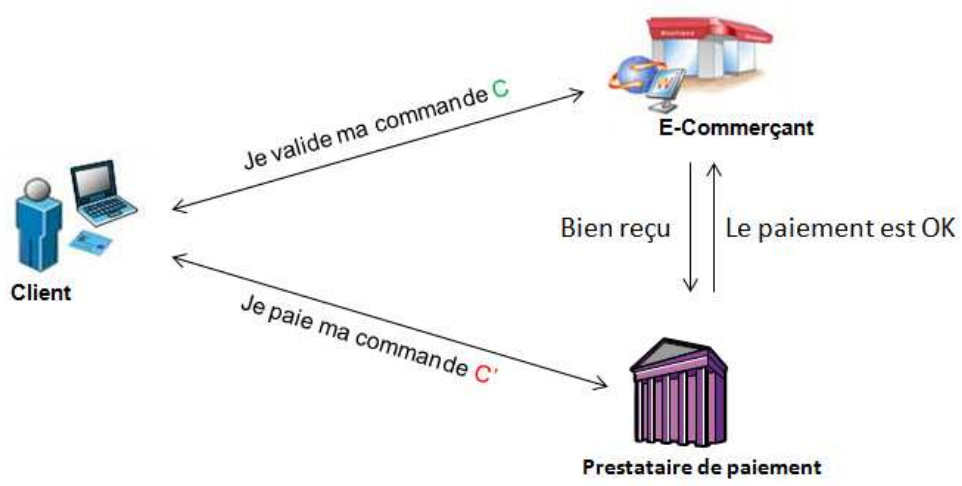


FIGURE 2.14 – Conséquence d'une mauvaise communication tripartite dans un système de paiement

Nous constatons alors que, malgré la facilité d'intégration d'un terminal de paiement déporté comparé à un terminal de paiement intégré, le système de paiement devient plus vulnérable car il fait intervenir une autre entité au moment de paiement. En fait, il s'agit de sécuriser une communication tripartite et non bipartite. En plus, le niveau de sécurité du système de paiement déporté dépend des outils de sécurisation qui sont mis en place par chaque prestataire de paiement (chiffrement, signature ou hachage). Une étude comparative de niveau de sécurité de ces différents modes de redirection est présentée dans le tableau 2.8.

Mode d'intégration	Outils de sécurisation	Critères de sécurité			
		Intégrité	Authentification	Confidentialité	Non-répudiation
Direct Site marchand	SSL sans intermédiaire	x	x	x	-
	SSL avec signature	x	x	x	x
Service Web	Jeton Cryptographique	x	x	-	-
	Signature Numérique	x	x	x	x
Redirection HTTP chiffrée	Chiffrement Symétrique	x	x	x	-
Redirection HTTP signée	MAC	x	x	-	-

TABLE 2.8: Etude comparative de la sécurité des modes d'intégration existants

Comme nous pouvons le constater, le niveau de sécurité d'un système de paiement déporté dépend du mode d'intégration (en direct, via service Web, via une redirection

HTTP chiffrée ou via une redirection HTTP signée). Les modes qui ont le score le plus élevé sont ceux qui sont basés sur la signature numérique, puis on trouve ceux qui sont basées sur le chiffrement des données envoyées lors de la redirection en passant par le navigateur du client. Enfin, on trouve, au troisième rang, les systèmes qui sont basés sur le hachage (avec une clé) des informations échangées.

2.7.2 Ergonomie

Afin de comparer les modes d'intégration existants selon le critère de l'ergonomie, nous allons nous baser sur l'étude de l'expérience utilisateur depuis la page de choix des moyens de paiement. En effet, dans le cas d'un paiement intégré, la redirection vers la page de paiement est complètement transparente pour le client car il s'agit d'une page hébergée par le site marchand. Cependant, dans le cas d'un paiement déporté, la redirection vers la page de paiement peut altérer l'expérience utilisateur. Pour remédier à ce problème, les prestataires de paiement ont trouvé deux solutions qui consistent essentiellement : à proposer une intégration en mode Iframe ou à proposer un mode d'intégration complètement déporté avec la possibilité de personnaliser les pages de paiement par le marchand.

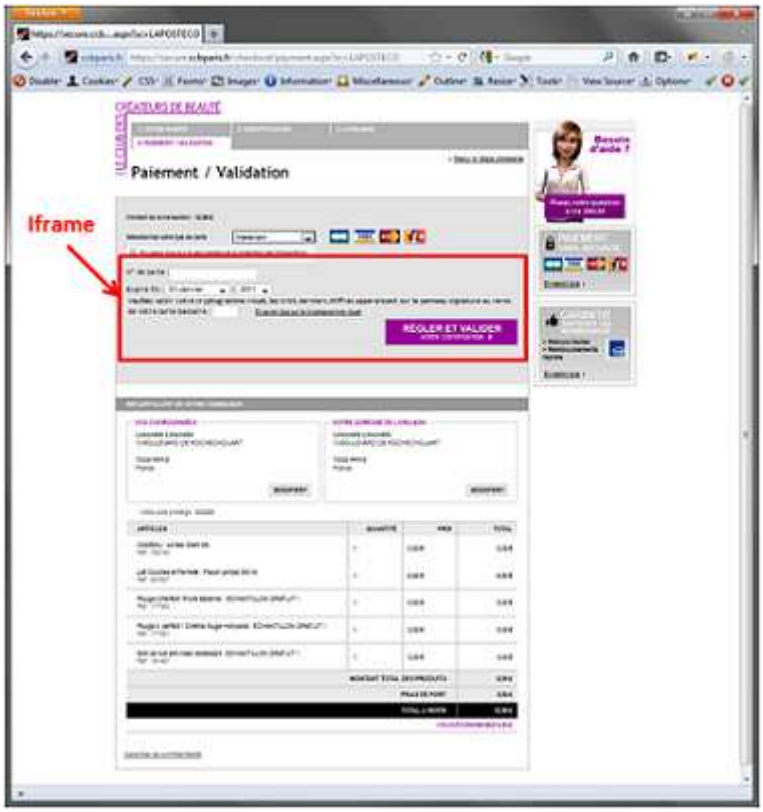


FIGURE 2.15 – Exemple de page de paiement déportée en Iframe

Le mode Iframe, consiste à afficher la page de paiement hébergée par le partenaire de paiement dans une page du site marchand. En effet, il est possible de définir à l'intérieur d'une page HTML, un cadre local à l'intérieur duquel s'affichera le contenu d'une autre page HTML grâce à la balise HTML <IFRAME>. Il s'agit d'une solution très efficace pour ne pas altérer l'expérience client, car ce dernier croit qu'il navigue encore sur le site marchand. Un exemple de cette intégration est présenté dans la figure 2.15.

Le deuxième mode consiste à personnaliser la page de paiement même si elle est déportée chez le prestataire de paiement. Le marchand a la possibilité soit d'envoyer les valeurs de personnalisation avec les données de paiement lors de la redirection du client vers la page de paiement, soit de personnaliser la page de paiement depuis son compte back-office sur le serveur du prestataire de paiement. Cette personnalisation permet de mettre la page de paiement aux couleurs du marchand afin de faire croire au client qu'il paie sur le site marchand. Un exemple de personnalisation de page de paiement déportée est présenté dans la figure 2.16.

FIGURE 2.16 – Exemple de page de paiement déportée personnalisée

L'arrivée de 3D-Secure (présenté dans l'annexe A) a également altéré l'expérience client sur Internet. Rappelons qu'il s'agit d'un protocole ayant vocation à authentifier le client en lui affichant une page hébergée par la banque émetteur après la validation des données de paiement. Dans ce cas, le client passe de l'environnement du site marchand, après avoir validé sa commande, à l'environnement du prestataire de paiement afin de payer, puis à celui de sa banque pour s'authentifier. Un scénario 3D-Secure est présenté dans la figure 2.17 : la première page est la page de choix

de moyen de paiement sur le site E-commerce, la deuxième est la page de paiement, hébergée par le prestataire de paiement bancaire et la troisième page est celle de l'authentification 3D-Secure, hébergée par la banque du client. Nous constatons que les trois pages sont très différentes l'une de l'autre. Evidemment, une telle expérience client n'est pas rassurante pour les internautes, ce qui explique l'abandon par certains marchands de ce protocole [Fauconnier F., 2010].

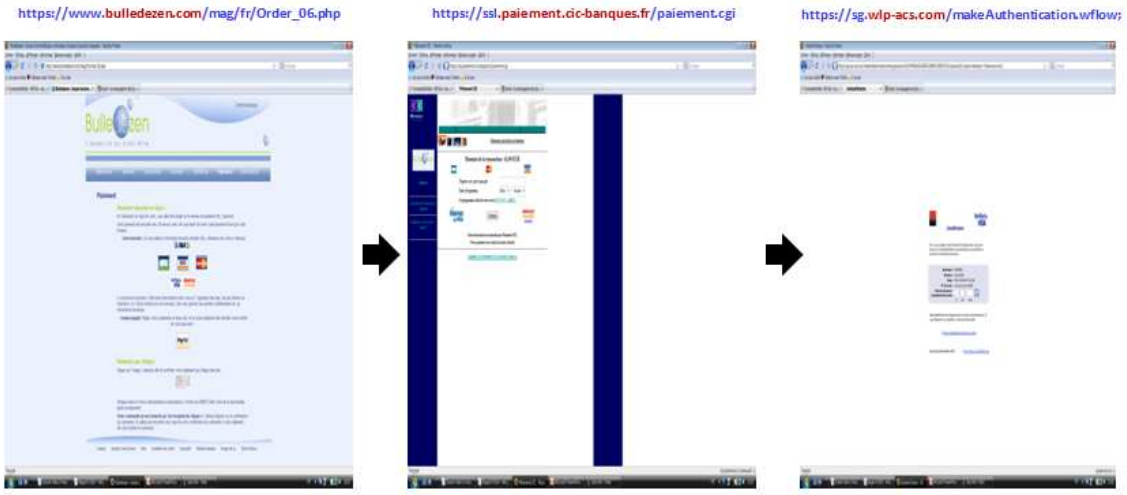


FIGURE 2.17 – Exemple de page de paiement déportée avec 3D-Secure

On constate alors que certaines pages de paiement déportées chez des prestataires de paiement peuvent atteindre le même niveau d'ergonomie que les pages de paiement intégrées directement dans le site marchand. Pour éviter l'altération de l'expérience utilisateur sur les sites E-commerce lors de la redirection des clients vers les pages de paiement déportées, les prestataires de paiement ont donc réussi à trouver les solutions à ce problème qui ne dépend pas du mode d'intégration choisi (via service Web, via redirection HTTP signée ou redirection HTTP chiffrée).

2.7.3 Complexité

Après avoir décrit les différentes méthodes d'intégration d'un système de paiement sur Internet, nous allons maintenant les comparer selon le critère de la complexité. Pour ce faire, nous avons effectué une enquête auprès de quelques E-commerçants, ayant opté pour les différents modes d'intégration présentés dans notre étude. Le but de l'enquête étant de mesurer le coût de l'intégration du système de paiement afin d'évaluer sa complexité. Comme nous l'avons cité au début de ce chapitre, les valeurs fournies par cette enquête sont à titre indicatif, elles servent seulement pour comparer les différents modes d'intégration entre eux.

Mode d'intégration	Temps	Coût
Intégration directe	80-100 jours/homme	Environ 44 000€
Intégration via Services Web	60-80 jours/homme	Environ 33 000€
Intégration via redirection HTTP chiffrée	40-60 jours/homme	Environ 22 000€
Intégration via redirection HTTP signée	20-40 jours/homme	Environ 11 000€

TABLE 2.9: Etude comparative des coûts d'intégration d'un système de paiement sur Internet

Le mode d'intégration direct dans le site E-commerce semble être le mode le plus difficile, car il ne s'agit pas seulement d'ajouter la page de paiement sur le site mais aussi de sécuriser les données de paiement des clients ainsi que tous les échanges avec les entités financières impliquées dans la transaction. Si nous prenons l'exemple de l'intégration d'un système bancaire, nous constatons qu'au-delà des contraintes techniques de l'implémentation des politiques de sécurité ou de renforcement des authentifications, le standard PCI DSS demande également la mise en place des processus organisationnels, la rédaction de documentation précise et l'audit régulier des systèmes [Security Standards Council, 2010]. Vu la difficulté et les coûts d'obtention de la certification PCI DSS, la majorité des sites marchands ont choisi alors de déléguer leur page de paiement à des prestataires de paiement. Aujourd'hui, seulement les grands sites marchands intègrent leur page de paiement directement dans leur boutique car ils souhaitent gérer leurs flux financiers. Dans le cas des systèmes de paiement non bancaires, cette contrainte de conformité au standard PCI DSS n'est pas présente. Cependant, le marchand doit veiller à bien sécuriser les pages de paiement hébergées par son serveur Web et à protéger les données privées des clients.

Concernant l'intégration des systèmes de paiement déportés sur Internet, le mode d'intégration via service Web semble être le plus coûteux pour l'E-commerçant. En effet, implémenter des services Web est généralement plus complexe que réaliser une redirection HTTP signée ou chiffrée, surtout que, généralement, dans ces deux modes d'intégration, le partenaire de paiement fournit des éléments et des outils (module CGI, exemple de code, etc.) afin de faciliter l'intégration pour l'E-commerçant. Le coût de l'intégration dépend également de la taille du site marchand : plus le site marchand est grand, plus l'intégration d'un système de paiement est chère.

L'intégration via redirection HTTP chiffrée semble être plus compliquée que l'intégration via redirection HTTP signée, même si, dans le premier cas, le prestataire de paiement fournit généralement un module CGI facilitant le chiffrement les données de la commande. L'E-commerçant doit, tout de même, générer un certificat, le stocker d'une manière sécurisée et paramétrer le module CGI.

L'intégration d'un système de paiement comporte trois étapes (figure 2.3), les modes d'intégration présentés concernent seulement la partie « front-office » de l'intégration qui représente essentiellement la première phase de l'intégration (page choix de moyen de paiement). La deuxième phase, étant généralement déléguée à un prestataire de paiement, n'est pas intégrée dans notre étude comparative. Et la troisième phase, qui concerne les fonctionnalités « back-office » de rapprochement des paiements et de la gestion des opérations financières, semble être plus compliquée dans le cas des systèmes de paiement « alternatifs ». En effet, vu la particularité des instruments de paiements alternatifs, l'E-commerçant doit prendre en compte de nouvelles contraintes lors de la gestion de la commande. Citons comme exemple, les bons de réduction qui expirent après un certain délai ou les cartes cadeaux qui risquent d'être jetées après le paiement. De plus, comme nous l'avons évoqué dans le premier chapitre (figure 1.9), la complexité du rapprochement augmente dès lors qu'il s'agit d'accepter plusieurs moyens de paiement via plusieurs prestataires de paiement différents. Notre objectif est alors de proposer une nouvelle architecture qui soit plus facile à intégrer que les solutions existantes.

2.8 Conclusion

Ce chapitre présente un panorama des modes d'intégration d'un système de paiement sur Internet. L'intégration d'un moyen de paiement dans une boutique E-commerce consiste à gérer trois phases différentes : la première concerne l'affichage du moyen de paiement dans le site Web du marchand, la deuxième consiste à gérer le paiement du client et la troisième consiste à attacher le paiement à une commande donnée et à gérer tous les flux financiers durant le cycle de vie d'une transaction (validation, livraison, annulation, etc.). La complexité de l'intégration d'un système de paiement dans une boutique sur Internet concerne alors la gestion de ces trois phases. Généralement, cette complexité a tendance à augmenter dès qu'on commence à s'intéresser à des fonctionnalités monétaires compliquées comme : autoriser plusieurs types de paiement dans une même commande ou gérer des opérations financières compliquées de types débit partiel ou annulation partielle. La situation se complique encore plus si on souhaite intégrer des moyens de paiement « alternatifs » qui ne sont pas des instruments de paiement standards que l'E-commerçant a l'habitude de manipuler. Il s'agit des moyens de paiement très divers et peu ordinaires dans l'histoire de l'E-commerce. Citons à titre d'exemple les cartes cadeaux qui risquent d'être jetées après usage, les programmes de fidélité qui permettent d'attribuer des points de dépense aux clients ou encore les coupons de réduction valables sur

certains articles dans une boutique E-commerce et pour un certain temps. Toute cette complexité est complètement transparente pour le client qui dispose d'un moyen de paiement et qui souhaite l'utiliser pour payer son panier sur Internet. Cependant, le marchand doit étudier tous ces éléments avant de décider l'intégration ou non d'un nouveau moyen de paiement.

Sachant que, dans notre travail, nous optons pour une approche orientée marchand « Merchant-Centric », notre objectif consiste alors à proposer un mode d'intégration permettant au marchand de parer à toute la complexité de l'intégration d'un nouveau moyen de paiement. Pour ce faire, nous avons étudié dans ce chapitre les modes d'intégration des systèmes de paiement existants dans le but de les comparer selon les trois critères retenus dans le chapitre précédent. Le tableau 2.10 présente les avantages et les inconvénients de chaque mode d'intégration.

Nous constatons alors que bien que les prestataires de paiement aient cherché à faciliter l'intégration de leurs terminaux de paiement virtuels, certains modes d'intégration existants présentent un certain niveau de complexité pour les marchands. Sachant que les moyens de paiement non bancaires ne sont pas des instruments communément utilisés par les internautes, certains marchands ne voient pas forcément l'intérêt de les intégrer dans leur boutique surtout si cette intégration peut s'avérer complexe et coûteuse. Le chapitre suivant présente une nouvelle architecture de système de paiement permettant d'intégrer facilement, les nouveaux moyens de paiement alternatifs.

Mode d'intégration		Sécurité		Ergonomie		Complexité	
		Avantages	Inconvénients	Avantages	Inconvénients	Avantages	Inconvénients
Intégré		- Le paiement sécurisé car le client n'est pas redirigé vers une page déportée	- Certification PCI DSS obligatoire et coûteuse	- La page de paiement a la même charte graphique que le site E-commerce	-	- La page de paiement est facilement paramétrable pour le site marchand	- Intégration lourde et compliquée parfois
Déporté	Services Web	- La communication entre le marchand et le prestataire de paiement ne passe pas par le navigateur de client	- Le site marchand est le seul responsable de la sécurité de ses requêtes	Généralement pas de page intermédiaire de redirection	-	- Le marchand est très impliqué dans l'intégration	- Le marchand doit bien tester son implémentation des services Web
	Redirection HTTP chiffrée	- Même si la redirection s'effectue via le navigateur du client, les données de la commande sont chiffrées	Selon le choix de sécurité du prestataire de paiement, le marchand peut être amené à générer son certificat, il est, dans ce cas, le seul responsable de la sécurité de la génération et du stockage du certificat	-	- Le redirection du client vers la page de paiement n'est pas généralement maîtrisée par le marchand, ce qui peut altérer l'expérience client en ajoutant une redirection supplémentaire au module afin de rediriger le client vers le prestataire de paiement	- Le marchand récupère un Module CGI du prestataire de paiement, il ne doit pas implémenter les opération cryptographiques nécessaires pour sécuriser la redirection du client vers la page de paiement déportée	- La configuration du Module CGI peut être un peu compliquée selon la politique de sécurité imposée par le prestataire de paiement
	Redirection HTTP signée	-	- Le marchand est responsable de son choix de clé secrète (mot de passe), de son stockage et de sa sécurisation - Les données de la commande transitent en clair via le navigateur du client	- Le marchand effectue la redirection sans passer par un Module CGI, ce qui améliore l'expérience client	-	- L'intégration est plus rapide par rapport aux autres types d'intégration car le marchand est plus autonome et l'intégration n'est pas compliquée	- Le marchand doit effectuer les opérations cryptographiques afin de sécuriser les données de commande envoyées au prestataire de paiement lors de la redirection du client

TABLE 2.10: Etude comparative des différents modes d'intégration

Chapitre 3

Nouvelle architecture de paiement sur Internet

Nous nous intéressons à l'intégration des systèmes de paiement non bancaires (« alternatifs ») dans l'E-commerce. A notre connaissance, aucun travail ne propose une solution qui peut répondre aux contraintes décrites au début de cette étude tout en étant facile à intégrer chez l'E-commerçant. Ce chapitre présente notre première contribution : la définition d'une nouvelle architecture de paiement pour l'E-commerce. Elle permet d'intégrer plusieurs moyens de paiement alternatifs sur Internet. Ce chapitre est organisé de la manière suivante : la section 3.2 présente la nouvelle architecture en définissant les nouveaux acteurs, le principe de fonctionnement ainsi que le processus de conversion de paiement. La section 3.3 présente les différents flux financiers au sein de l'architecture proposée. Enfin, la section 3.4 s'intéresse au nouveau système de paiement et décrit ses différentes composantes.

Sommaire

3.1 Introduction

Comme nous avons pu le constater suite à l'étude de l'existant, les moyens de paiement non bancaires sont peu présents sur Internet, malgré le potentiel grandissant de ce nouveau marché. Le commerce électronique actuel en Europe est essentiellement bancaire et s'articule autour des moyens de paiement traditionnels : carte bancaire, chèque, prélèvement, virement, etc. Certains moyens de paiement alternatifs ne sont pas encore proposés sur Internet, d'autres, sont proposés par un nombre limité de sites E-commerce ce qui ne les rend pas accessibles pour tous les internautes. A notre connaissance, il n'existe pas un travail qui propose une solution qui permet d'intégrer plusieurs moyens de paiement alternatifs et qui peut répondre aux contraintes décrites au début de cette étude, tout en étant facile à intégrer chez l'E-commerçant. De plus, le commerce électronique sur Internet est encore très restreint en fonctionnalités comparé à celui de proximité. Plusieurs facilités de paiement ne sont pas encore disponibles dans les boutiques en ligne. La nécessité de proposer une nouvelle architecture de paiement émerge donc clairement de la situation actuelle.

3.2 Description de la nouvelle architecture

Dans cette section, nous allons décrire la nouvelle architecture proposée, son principe de fonctionnement, ses nouveaux acteurs ainsi que ses principales fonctionnalités. Rappelons que le but de cette étude est de proposer un système de paiement alternatif facile à intégrer dans le site E-commerce tout en garantissant les exigences et les critères définis dans le chapitre 1.

3.2.1 Principe de fonctionnement

L'étude des étapes de l'intégration d'un moyen de paiement de paiement sur Internet, effectuée dans le chapitre précédent, montre que cette intégration doit être réalisée dans deux sous-systèmes du système de paiement (généralement « quatre coins »). Le premier sous-système est le système accepteur, qui concerne la partie « front-office » d'un système de paiement et qui permet d'ajouter le moyen de paiement sur le site E-commerce et de rediriger le client vers la page de paiement. Le deuxième sous-système est le système acquéreur, qui concerne la partie « back-office » d'un système de paiement et qui permet de demander l'autorisation de paiement à l'émetteur, de garantir le paiement de l'E-commerçant, de gérer les différentes opérations financières et de mettre à jour des statuts des transactions.

En étudiant les différentes solutions qui peuvent être apportées à cette problématique, nous avons constaté qu'il existe deux possibilités. La première consiste à intégrer le moyen de paiement alternatif en utilisant un des modes décrits dans l'état de l'art (chapitre 2). Cela veut dire que l'E-commerçant effectue l'intégration dans les deux systèmes accepteur et acquéreur, afin de proposer le nouveau moyen de paiement sur son site E-commerce et encaisser les paiements par la suite. Cependant, puisqu'il ne s'agit pas de moyens de paiement communément utilisés par les internautes, les E-commerçants sont généralement réticents. De plus, comme nous l'avons présenté dans l'étude des différents modes d'intégration d'un système de paiement, il s'agit d'approches d'intégration qui demandent un investissement, du côté du marchand, qui peut être important. La deuxième possibilité consiste à réutiliser le système de paiement bancaire déjà intégré par la plupart des E-commerçants en convertissant les paiements alternatifs en paiements bancaires. Dans ce cas, l'E-commerçant n'a qu'à intégrer le moyen de paiement dans le système accepteur, puisque le système acquéreur sera celui de son système de paiement bancaire.

S'agissant de proposer un système de paiement facile à intégrer pour l'E-commerçant, la deuxième solution semble être plus appropriée que la première. En effet, il paraît judicieux de se baser sur le système de paiement communément utilisé par les E-commerçants sur Internet afin de profiter de la robustesse et l'interopérabilité de ce système bancaire et de proposer des moyens de paiement alternatifs. Ainsi, nous intéresserons-nous, aux E-commerçants qui ont déjà intégré le moyen de paiement par carte bancaire et qui souhaitent ajouter un moyen de paiement alternatif, ce qui est le cas de la majorité des E-commerçants, puisque le moyen de paiement bancaire est le premier instrument de paiement accepté sur Internet.

3.2.2 Nouveaux acteurs

Avant d'aller plus loin, présentons les différents acteurs de cette nouvelle architecture en reprenant la description du système bancaire « quatre coins » présenté dans la figure 1.6 du premier chapitre, afin de positionner le nouveau système par rapport au système bancaire et présenter les nouveaux acteurs.

La figure 3.1 présente la structure générale de la nouvelle architecture de paiement qui fait intervenir quatre nouveaux acteurs en plus de ceux du système bancaire.

- Le prestataire de paiement alternatif : le prestataire de paiement qui gère les paiements alternatifs pour l'E-commerçant. Nous verrons dans la suite de ce chapitre qu'il ne s'agit pas d'un simple prestataire de paiement. Il s'agit d'une plateforme de paiement qui permet plusieurs fonctionnalités en plus de la gestion technique des paiements.

- Les émetteurs : les entités qui émettent les moyens de paiement du client. Ces dernières peuvent être bancaires ou non bancaires.
- L'émetteur de monnaie électronique : un organisme financier qui est autorisé à émettre de la monnaie électronique. Il joue un rôle important dans le processus de conversion de la monnaie électronique non bancaire en monnaie bancaire (scripturale).
- La banque « intermédiaire » : la banque partenaire du prestataire de paiement alternatif. Nous l'avons nommé « intermédiaire » afin de la distinguer des autres banques présentes dans l'architecture (acquéreur, émetteur). Grâce à la banque intermédiaire, le prestataire de paiement alternatif peut convertir le paiement non bancaire en paiement bancaire à l'aide de cartes virtuelles dynamiques émises par cette banque.

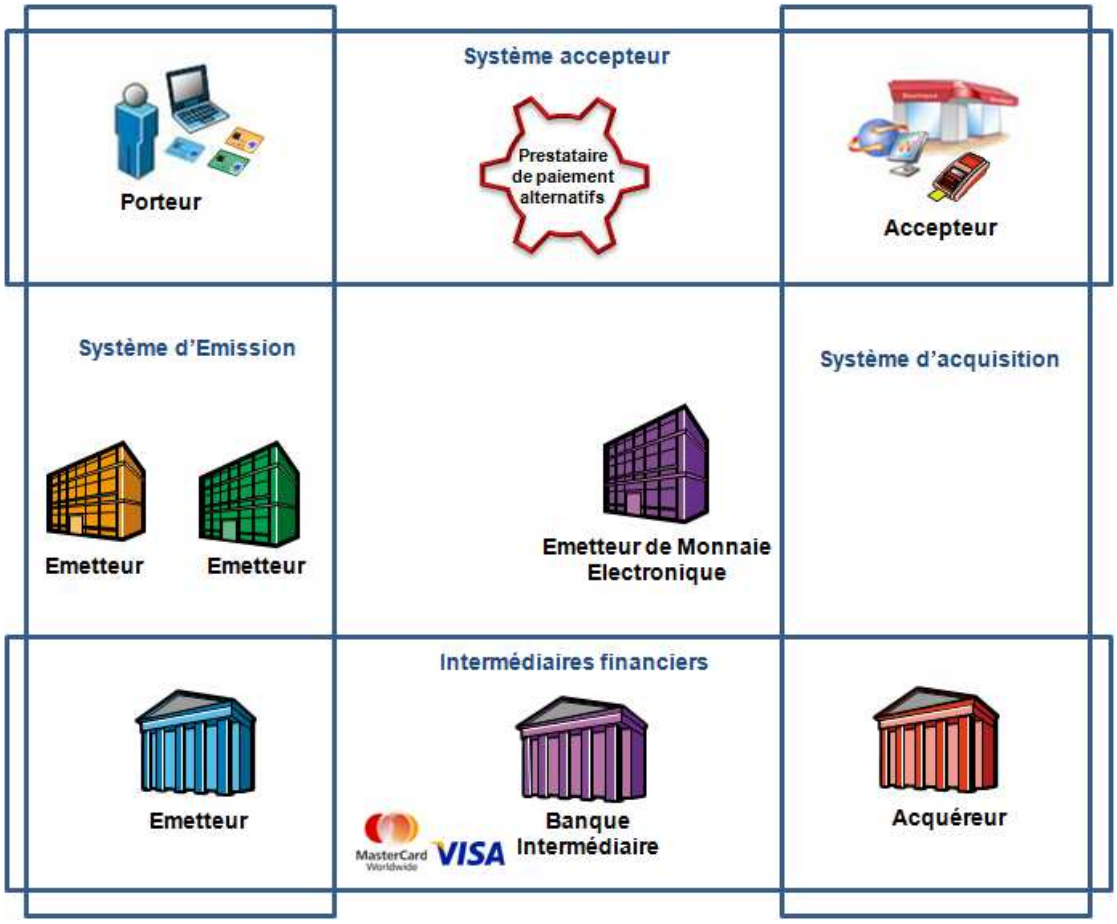


FIGURE 3.1 – Nouvelle architecture de paiement

3.2.3 Carte Virtuelle Dynamique (CVD)

La carte virtuelle dynamique, comment son nom l'indique, est une carte générée dynamiquement pour une transaction donnée. Ce moyen de paiement présente plusieurs avantages ; il s'agit d'un numéro de carte à usage unique ce qui diminue les risques de fraude. Le client est authentifié avant la génération de la carte, ce qui élimine les usurpations d'identité. Le principe de fonctionnement de la CVD est décrit dans la figure 3.2.

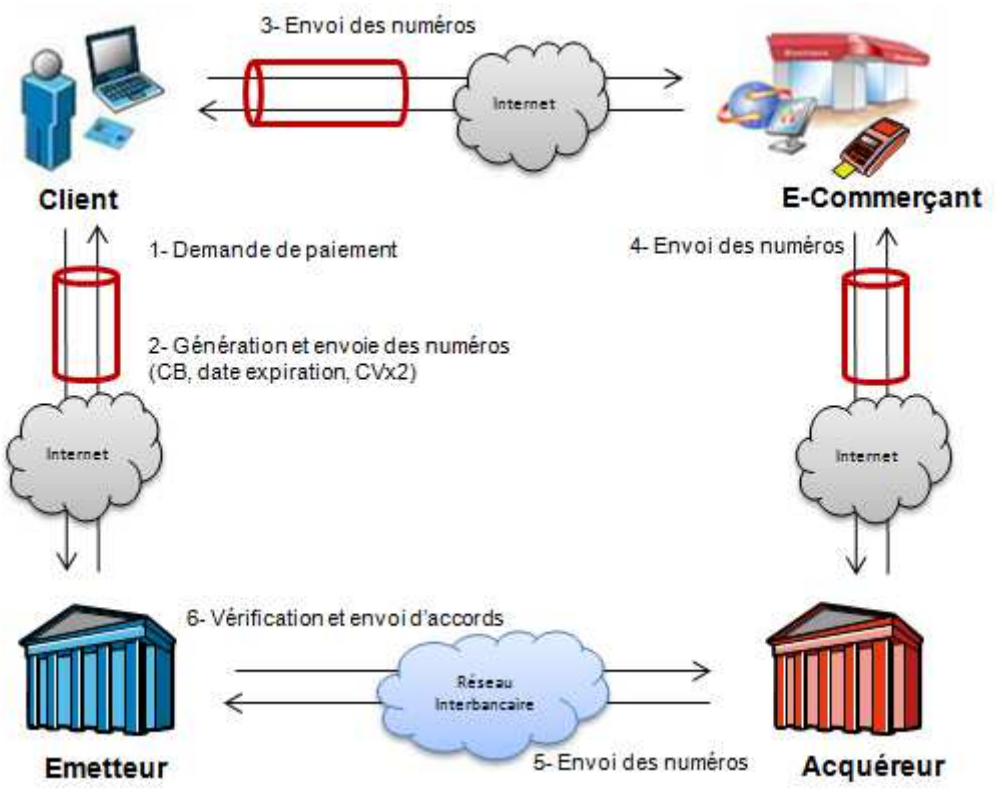


FIGURE 3.2 – Principe de la carte virtuelle dynamique

Au moment du paiement, le client contacte sa banque (via un logiciel installé sur son poste ou un plug-in installé dans son navigateur) afin de récupérer un numéro de carte bancaire qui servira de carte de paiement de son panier sur le site marchand. La banque émettrice authentifie le client, vérifie la solvabilité de son compte bancaire, puis génère une carte virtuelle dynamique de la valeur du panier et la renvoie au client. Ce dernier peut alors payer le site marchand. Après vérification des données de la carte par le terminal de paiement virtuel du marchand, sa commande sera validée.

3.2.4 Principe de fonctionnement

Afin de présenter le principe de fonctionnement du nouveau système de paiement, nous présentons dans la figure 3.3 le déroulement de la nouvelle transaction sur un site d'E-commerce.

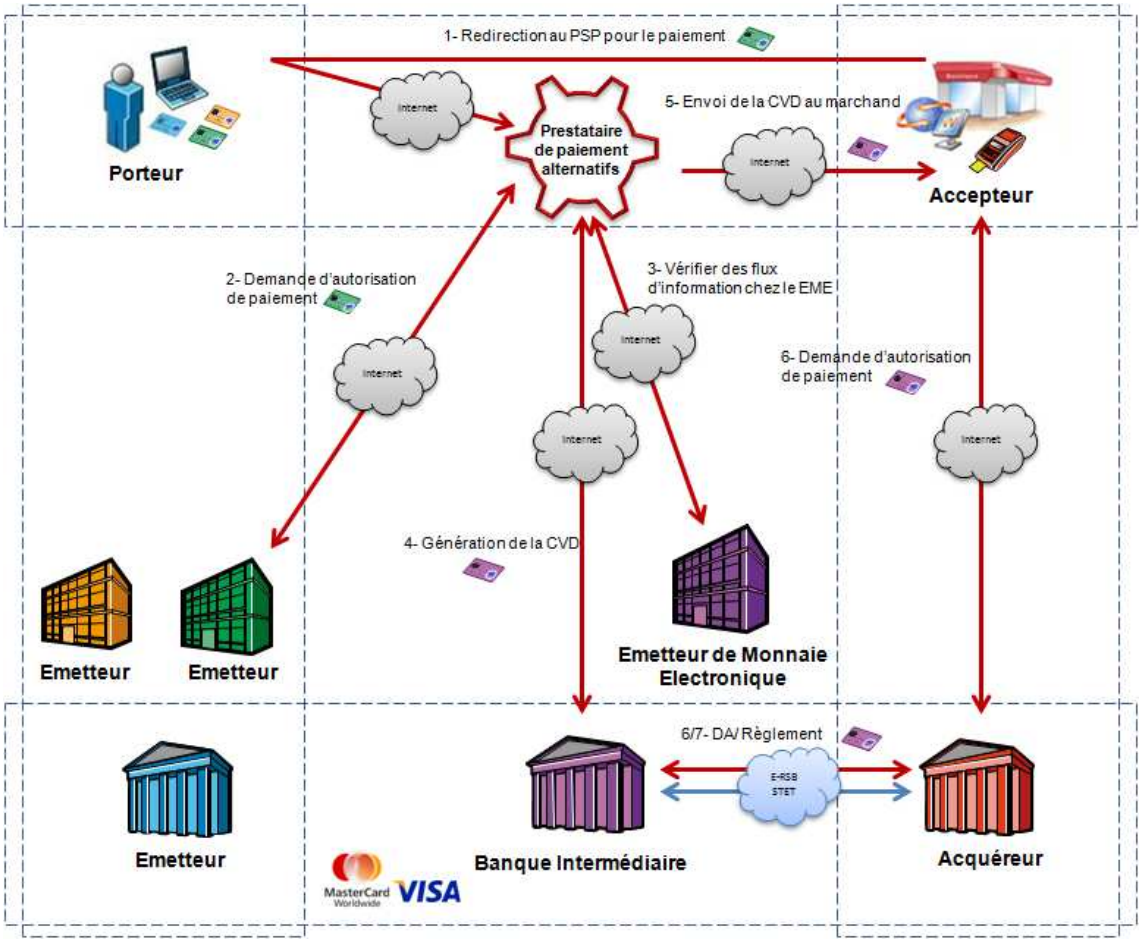


FIGURE 3.3 – Paiement alternatif au sein de la nouvelle architecture

L'intégration de cette nouvelle architecture fait l'objet d'une analyse plus approfondie dans la suite du document. Nous nous limitons, dans le présent chapitre, à mettre en évidence les caractéristiques de l'architecture proposée. Après avoir choisi le moyen de paiement alternatif, le client est redirigé vers le prestataire de paiement alternatif (flux 1) qui se charge de demander l'autorisation de paiement à l'émetteur de l'instrument de paiement correspondant (flux 2). Une fois l'autorisation de paiement accordée, le prestataire de paiement vérifie certaines informations chez l'émetteur de monnaie électronique (qui seront explicitées plus tard dans le document) et demande à la banque « intermédiaire » de générer une CVD du montant global du panier du client (flux 4). Après la réception des données de la CVD (numéro de

carte, date d'expiration et cryptogramme), le prestataire de paiement la transfère au marchand via son terminal de paiement bancaire. Le prestataire de paiement alternatif paie ainsi la commande au nom du client.

3.2.5 Processus de conversion

Nous avons décrit, dans le premier chapitre (figure 1.4), la monnaie électronique que nous avons classifiée en deux catégories : bancaire et non bancaire. Nous avons choisi de réserver le terme « monnaie électronique » à la monnaie électronique non bancaire et le terme « monnaie scripturale » pour désigner la monnaie électronique bancaire. Le processus de conversion des paiements alternatifs en paiements bancaires acceptés par les E-commerçants revient alors à convertir la monnaie électronique en une monnaie scripturale. Cette conversion est réalisable grâce à la nouvelle architecture présentée dans la figure 3.1 qui permet de gérer l'émission de la monnaie électronique et sa dépense par la suite.

FIGURE 3.4 – Processus de conversion de la monnaie

Afin d'assurer cette fonctionnalité de conversion de paiement, nous proposons d'utiliser des comptes de monnaie électronique détenus par un émetteur de monnaie électronique et un compte de monnaie scripturale détenu par une banque intermédiaire. Le processus de conversion comporte deux transformations de la monnaie : de la monnaie scripturale à la monnaie électronique et puis de la monnaie électronique à la monnaie scripturale.

De la monnaie scripturale à la monnaie électronique

Dans le cadre de la nouvelle architecture de paiement, la première phase de conversion consiste à convertir la monnaie électronique scripturale en monnaie électronique, ce qui revient à émettre de la monnaie électronique. En effet, afin de pouvoir l'intégrer dans la nouvelle architecture de paiement, l'émetteur du moyen de paiement doit acheter de monnaie électronique auprès de l'émetteur de la monnaie électronique. Cette monnaie électronique achetée servira de monnaie intermédiaire pour assurer la conversion des paiements alternatifs en paiements bancaires. Si l'émetteur du moyen de paiement alternatif n'a pas encore émis ses moyens de

paiement, nous pouvons imaginer que cette première phase sert alors à émettre le moyen de paiement. Sinon, il s'agit d'une phase d'intégration de l'émetteur dans la nouvelle architecture de paiement.

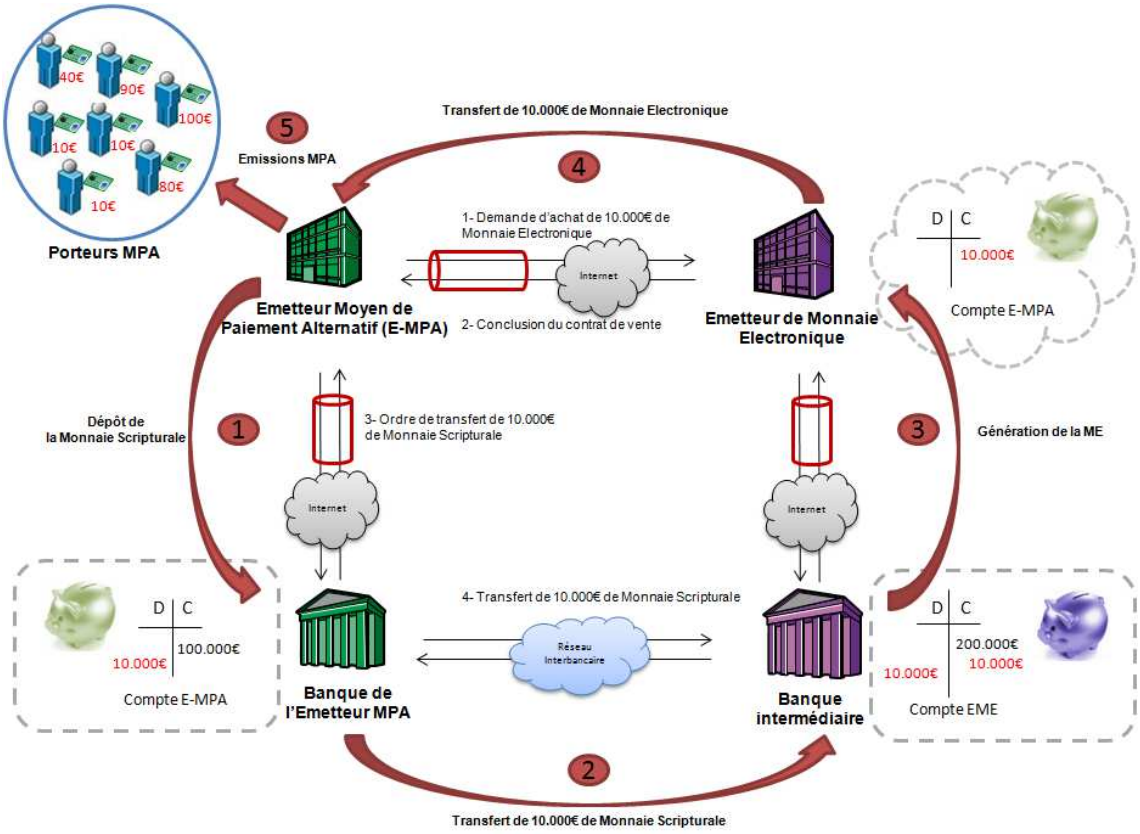


FIGURE 3.5 – Emission de la monnaie électronique

La figure 3.5 présente le système d'émission de la monnaie électronique dans le cadre de la nouvelle architecture. Il s'agit d'un système quatre coins dans lequel le client « achète de la monnaie électronique » et paie en monnaie scripturale. Nous précisons tout de suite que le terme « achat de monnaie électronique » est trompeur car le client ne possède pas les fonds sous-jacents à la monnaie électronique. Les fonds ne sont que prêtés au client. Nous retrouvons les quatre acteurs du système bancaire : le porteur (l'émetteur du moyen de paiement alternatif), l'émetteur (la banque de l'émetteur du moyen de paiement alternatif), l'accepteur (l'émetteur de la monnaie électronique) et l'acquéreur (la banque de l'émetteur de la monnaie électronique nommée banque « intermédiaire »).

Afin d'expliciter ce processus d'achat de la monnaie électronique, nous présentons le scénario décrit dans la figure 3.5. Nous considérons un émetteur d'un moyen de paiement alternatif (E-MPA) qui souhaite intégrer la nouvelle architecture afin

d'être accepté dans des sites E-commerces. Il crée alors un compte bancaire chez sa banque qu'il alimente avec une certaine somme d'argent (flux 1). Ensuite, il effectue un transfert monétaire à la banque de l'émetteur de la monnaie électronique (flux 2). Ce transfert correspond à la valeur de la monnaie électronique achetée. Une fois le paiement accepté par la banque « intermédiaire », la monnaie électronique correspondant à la somme d'argent perçue peut alors être générée (flux 3). Cette génération correspond à la création d'un compte chez l'émetteur de la monnaie électronique au nom de l'émetteur de paiement alternatif. A la fin de la commande, la monnaie électronique est « livrée » à l'émetteur du moyen de paiement alternatif (flux 4) qui peut éventuellement l'utiliser pour émettre ses moyens de paiement (flux 5).

Les inscriptions dans le compte de monnaie électronique représentent des informations numériques concernant la création et la destruction de la monnaie électronique. En effet, le but principal de ce compte est d'éviter que la même monnaie électronique puisse être dépensée deux fois. L'émetteur du moyen de paiement alternatif peut alors créer plusieurs moyens de paiement électroniques sur la base des fonds disponibles sur son compte de monnaie électronique. Toute émission d'un moyen de paiement débouche sur la substitution de la valeur émise des fonds disponibles sur le compte de monnaie électronique de l'émetteur du moyen de paiement chez le émetteur de la monnaie électronique (EME). Cependant, la dépense de ces monnaies électroniques émises engendre un débit sur le compte bancaire de l'émetteur de la monnaie électronique chez la banque intermédiaire. La dépense correspond ainsi à la conversion de la monnaie électronique en monnaie scripturale décrite dans la section suivante.

De la monnaie électronique à la monnaie scripturale

La monnaie électronique se voulant une version électronique des billets de banque, les concepteurs des différents systèmes de paiement en monnaie électronique ont veillé à que l'utilisateur perçoive ce lien direct entre la monnaie divisionnaire et la monnaie électronique, afin de souligner que la monnaie électronique possède des caractéristiques similaires à celles de l'argent comptant utilisé dans les paiements « Face to Face ». Nous décrivons, plus en détail, dans cette section, le circuit de dépense de la monnaie électronique dans le cas général (figure 3.6). La monnaie électronique est émise au profit du payeur A (flux 1) seulement dans le but d'effectuer un paiement. A la réception du flux (flux 2), le payé B doit remettre à l'émetteur la monnaie électronique reçue (flux 3). Après que B aura rendu la monnaie électronique et aura été crédité d'un dépôt (flux 4), l'opération de paiement sera terminée. A

chaque opération de paiement, une nouvelle monnaie électronique est créée et détruite.

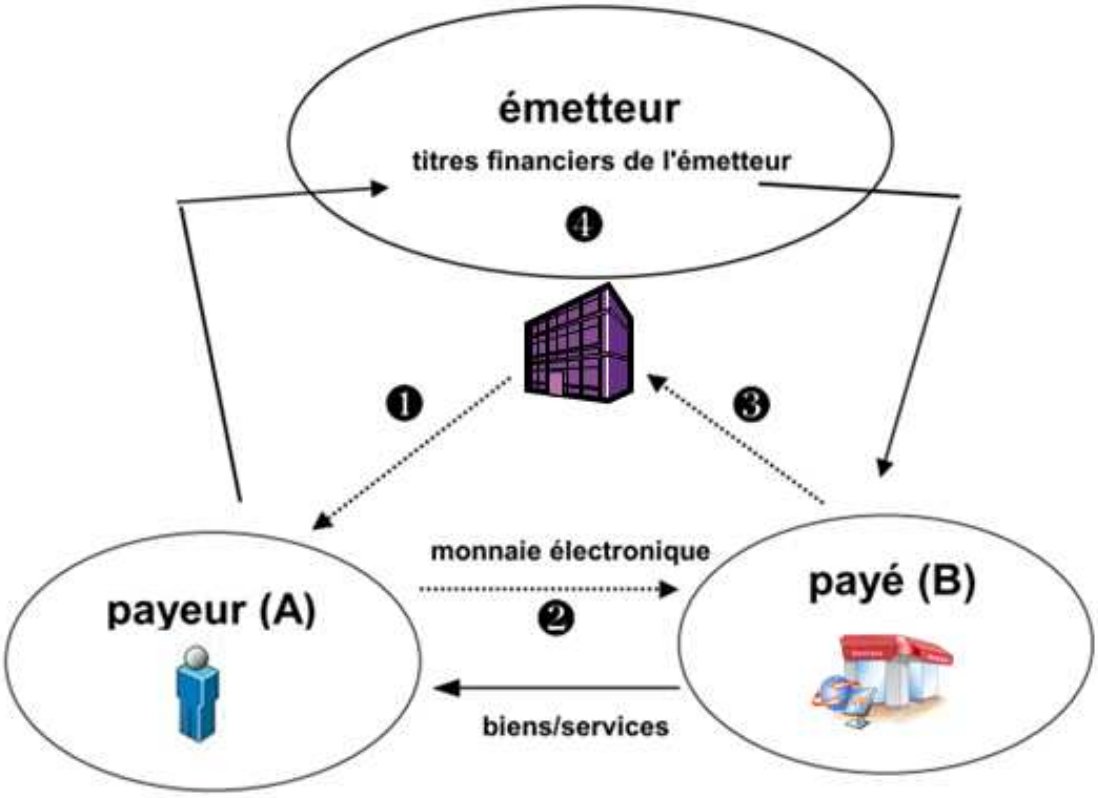


FIGURE 3.6 – Principe de paiement en monnaie électronique [Piffaretti N., 2000]

Avant de décrire la solution que nous proposons afin d'assurer la destruction de la monnaie électronique émise dans le cadre de cette nouvelle architecture de paiement, rappelons quelques caractéristiques de la monnaie électronique qui découlent de ses propriétés techniques [Piffaretti N., 2000] :

1. La monnaie électronique est émise dans le seul but d'effectuer un paiement.
2. Chaque paiement en monnaie électronique sous-entend une relation triangulaire entre le payeur (A), le payé (B) et l'émetteur.
3. Afin que le paiement soit effectif, le payé doit rendre la monnaie électronique à l'émetteur. La monnaie électronique est alors détruite (ce qui implique que la monnaie électronique a une existence limitée au paiement).

La troisième caractéristique suppose que le payé (B) peut communiquer d'une manière sécurisée avec l'émetteur de la monnaie électronique afin de lui rendre cette monnaie. Cette connexion se traduit dans le cas d'un paiement bancaire par l'installation d'un terminal de paiement électronique connecté à la banque du payé qui se charge de rendre la monnaie électronique à la banque émettrice et de récupérer

de la monnaie scripturale en contrepartie (qui sera versée sur le compte du payé). Il se trouve que, dans le cas d'un paiement avec une monnaie électronique non bancaire, et comme nous l'avons évoqué dans le premier chapitre de cette thèse, la connexion à l'émetteur de la monnaie est complexe, ce qui limite l'acceptation des nouveaux moyens de paiement alternatifs. C'est pourquoi nous proposons qu'au lieu que le payé B rende la monnaie électronique (non bancaire) à son émetteur, un prestataire de paiement se charge de convertir cette monnaie avant sa transmission au payé B en monnaie scripturale gérée par ce dernier. Pour ce faire, nous proposons d'utiliser le moyen de paiement carte virtuelle dynamique (CVD) qui permet de réaliser des paiements bancaires à l'aide des cartes générées dynamiquement pour un usage unique et un montant précis. Ces CVDs sont générées sur le compte bancaire de l'émetteur de la monnaie électronique chez la banque « intermédiaire » (figure 3.5). Les flux financiers générés suite à la dépense de la monnaie électronique sont décrits dans la section suivante.

3.3 Flux financiers

Après avoir décrit le principe de la conversion des paiements non bancaires en paiement bancaire à l'aide de la carte virtuelle dynamique. Nous allons décrire les différents flux financiers générés par le nouveau système de paiement et présenter plus en détail la transposition des opérations de la monnaie électronique dans les transactions bancaires selon les différentes cinématiques. Pour ce faire, nous allons commencer par rappeler les flux financiers dans un système bancaire classique avant de décrire ceux du nouveau système.

3.3.1 Système bancaire

Dans un système de paiement bancaire, l'argent est transmis depuis le compte client (détenu par l'émetteur) au compte du marchand détenu par l'acquéreur. A chaque fois qu'une transaction est réglée par carte bancaire, l'acquéreur verse à l'émetteur une commission proportionnelle au montant de la transaction (figure 3.7). Cette commission, appelée commission interbancaire de paiement ou commission d'interchange, permet de transférer les coûts correspondant aux risques de fraude et d'insolvabilité de la banque émettrice vers la banque acquéreuse. Il s'agit d'une des conditions financières entre acteurs financiers dans les systèmes de paiement quatre parties. Cette commission d'interchange rémunère les services que les banques se rendent entre elles dans un système multilatéral, notamment la garantie que les transactions cartes soient honorées aux points de vente. Ainsi, généralement,

la banque du commerçant verse une commission de service à la banque du client, qui doit refléter un juste équilibre entre les coûts et les avantages, tant pour les émetteurs de cartes que pour les banques des commerçants. Cette commission de service est objet de débats dans la mesure où elle est considérée comme renchérissant les commissions de services appliquées aux commerçants.

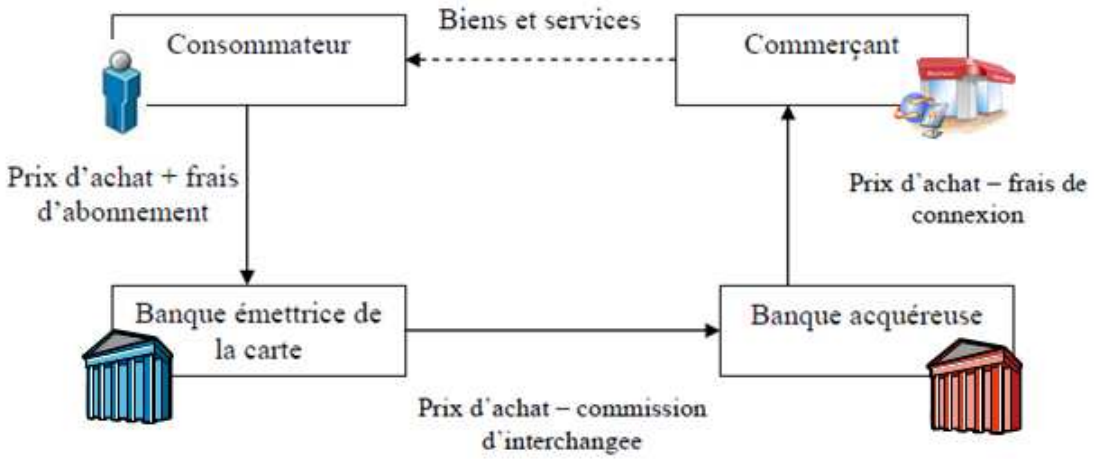


FIGURE 3.7 – Les flux financiers dans un système bancaire classique

Depuis quelques années, cette commission fait l'objet d'une attention toute particulière aussi bien de la part des économistes que des autorités réglementaires. En effet lorsqu'une telle commission devient un élément déterminant du coût de la transaction, puisque les émetteurs et les acquéreurs la répercutent sur les prix facturés respectivement aux consommateurs et aux commerçants, se pose la question de sa neutralité vis-à-vis du choix du système bancaire. Depuis l'avènement de SEPA (Single European Payment Area) et l'unification des réseaux bancaires en Europe, toutes les banques européennes ont été obligées de revoir leurs commissions face à la concurrence des autres banques.

Il existe généralement deux types de commissions : nationale (dans la zone euro) et internationale (en dehors de la zone euro). La commission nationale comprend 2 types de commissions, les CIP (Commissions Interbancaires de Paiement) et les CIR (Commissions Interbancaires de Retrait). Les commissions interbancaires de paiement représentent une part significative des frais acquittés par les commerçants, variant, selon les banques, entre 62% et 100% du total des frais [Autorité de la concurrence, 2011].

La deuxième catégorie des frais d'interchange sont les commissions internationales ou Commissions Multilatérales d'Interchange (CMI). Son montant est une partie des frais de service que la banque acquéreuse déduit également du paiement fait au

commerçant par le client dans le cas d'une transaction internationale. Le montant de la commission d'interchange varie selon la marque et le type de carte (crédit ou débit), le mode de transaction (de proximité, vente par correspondance ou à distance). Actuellement, en Europe, les commissions de Visa sont plafonnées à 0,7% des paiements effectués avec une carte de crédit ou de débit et celles de MasterCard vont de 0,4% à 1,2% de la valeur de la transaction.

3.3.2 Nouveau système

Le nouveau système proposé permet de garder le même schéma de flux financiers bancaires car il convertit les paiements non bancaires en paiements bancaires. Le prestataire des paiements alternatifs facture des frais de service à l'émetteur du moyen de paiement. L'E-commerçant paie seulement les commissions bancaires classiques suite à la conversion des paiements alternatifs en paiements bancaires à l'aide de la CVD. Afin de mieux comprendre les différents flux financiers au sein de la nouvelle architecture, nous proposons de détailler davantage les mouvements financiers lors d'un paiement alternatif. Pour ce faire, nous présenterons deux scénarios différents : un paiement simple (avec un seul moyen de paiement) et un paiement agrégeant plusieurs moyens de paiement.

Paiement simple

Cette section décrit les flux financiers dans le cas d'un paiement simple à l'aide d'un seul moyen de paiement alternatif. Pour ce faire, nous présentons un exemple permettant d'illustrer cette transaction (figure 3.8).

Considérons le porteur d'une carte cadeau de 100€ qui souhaite payer son panier de 100€ chez un E-commerçant. Nous supposons que l'émetteur de la carte cadeau a déjà créé un compte de monnaie électronique chez l'émetteur de monnaie électronique (tel qu'il est décrit dans la figure 3.5). Une fois que le client a choisi la carte cadeau comme moyen de paiement sur le site E-commerce, il est redirigé vers la page de paiement correspondante (flux 1), où il peut communiquer ses coordonnées de paiement (login, mot de passe, code, numéro de carte, etc.).

Si la page de paiement est hébergée par le prestataire de paiement alternatif, ce dernier adresse une demande d'autorisation de paiement à l'émetteur de la carte cadeau (flux 2) afin de vérifier que le client peut être débité du montant de la transaction. Si l'autorisation de paiement est accordée, le prestataire de paiement alternatif contacte l'émetteur de la monnaie électronique afin de vérifier que l'émetteur de la carte cadeau dispose de la monnaie électronique dans son compte (flux 3). Si

c'est le cas, un virement interne de 100€ est effectué depuis le compte de l'émetteur de la carte cadeau à un compte temporaire de transaction créé au nom du client. L'émetteur de monnaie électronique renvoie alors une confirmation au prestataire de paiement. Ce dernier contacte la banque « intermédiaire » au nom de l'émetteur de monnaie électronique afin de générer une CVD sur son compte (flux 4). La banque intermédiaire vérifie alors le compte de l'émetteur de monnaie électronique et génère une carte virtuelle dynamique de 100€. Le prestataire de paiement alternatif utilise la CVD générée pour payer l'E-commerçant en passant par son terminal de paiement bancaire (flux 5). La CVD est alors vérifiée par le serveur de paiement bancaire de l'E-commerçant (ou son partenaire de paiement bancaire) et une demande d'autorisation est envoyée à la banque émettrice qui est la banque intermédiaire (flux 6). Une fois la demande d'autorisation acceptée, l'E-commerçant valide la commande et confirme le paiement au client.

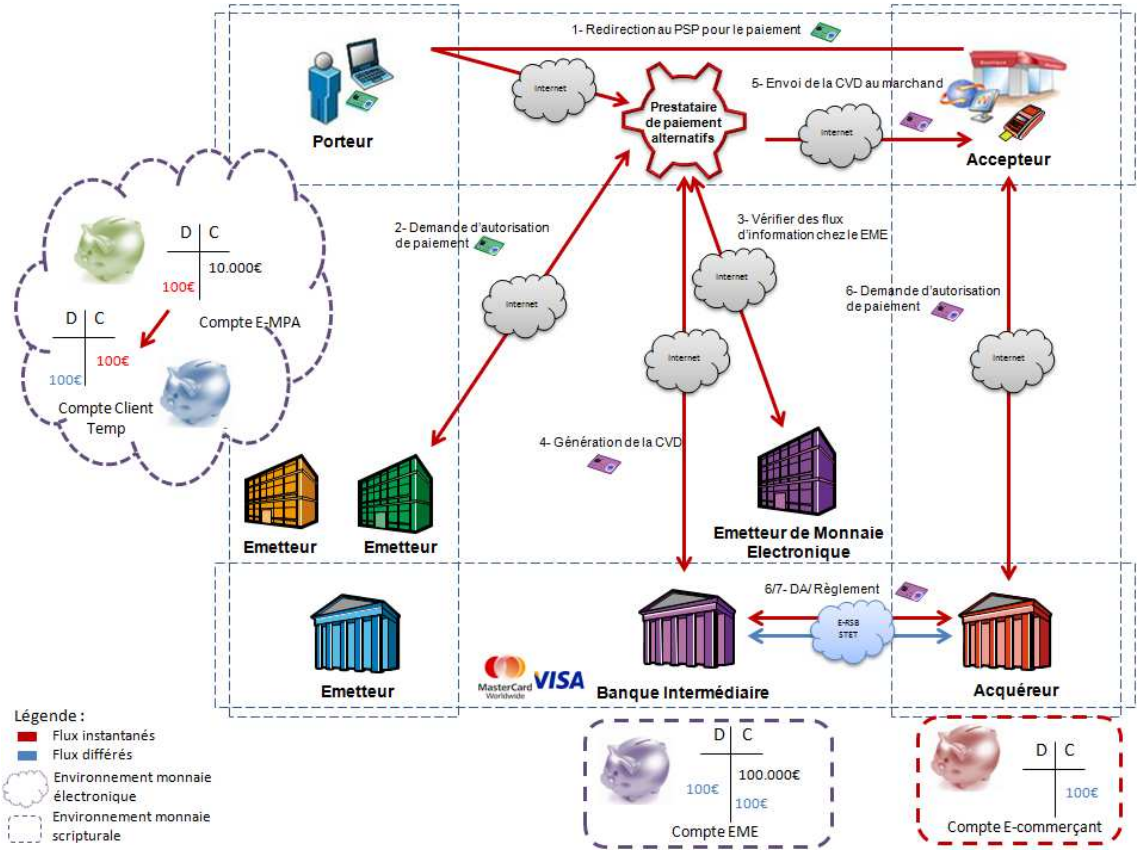


FIGURE 3.8 – Flux financiers - paiement simple

Le débit du montant de la transaction (100€) du compte bancaire de l'émetteur de monnaie électronique (flux 7) engendre le débit de 100€ du compte temporaire de transaction chez l'émetteur de monnaie électronique et la clôture de ce compte,

ce qui garantit la destruction de la monnaie électronique créée.

Paiement avec plusieurs moyens de paiement alternatifs

Maintenant que nous avons décrit les flux financiers dans le cas d'un paiement simple, nous pouvons décrire ceux d'un paiement plus complexe qui agrège plusieurs paiements. Pour ce faire, nous prenons l'exemple décrit dans la figure 3.9.

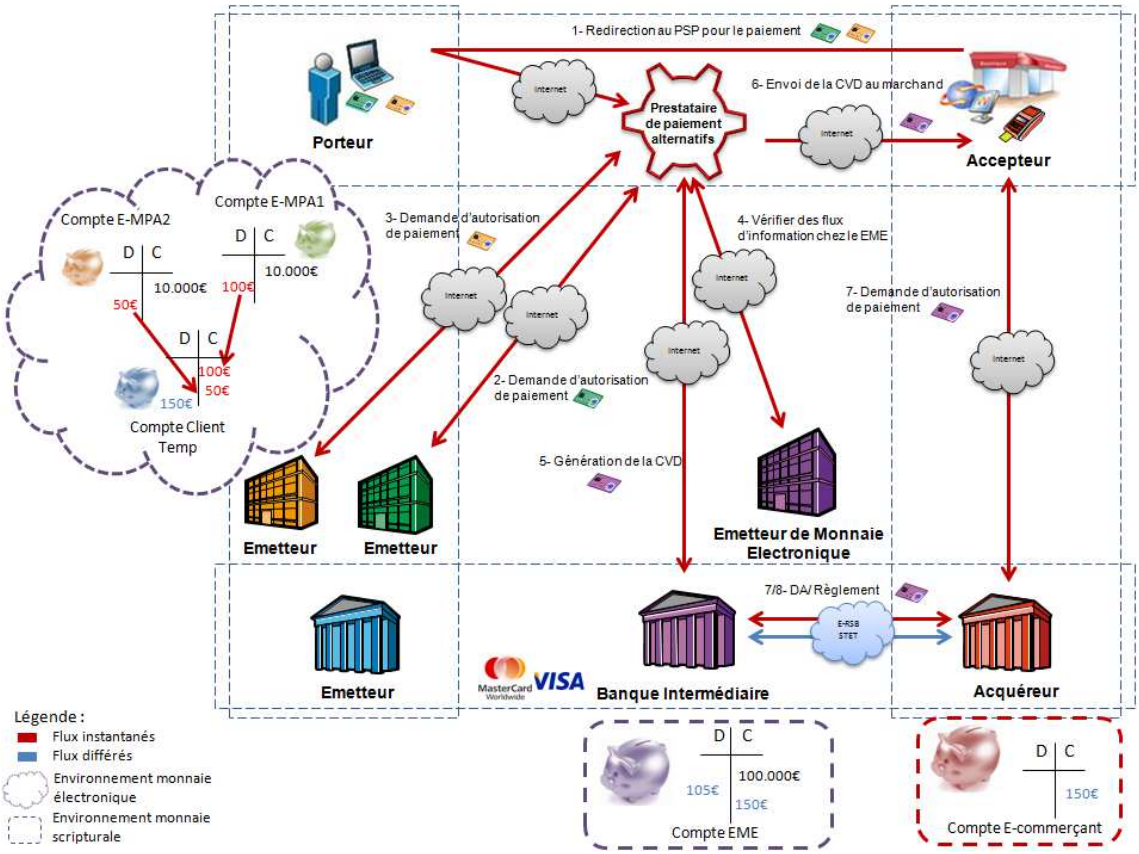


FIGURE 3.9 – Flux financiers - paiement agrégé

Considérons un client qui dispose de deux moyens de paiement alternatifs : une carte cadeau de 100 € et un porte-monnaie électronique de 50€. Il navigue sur le site E-commerce, remplit son panier et valide sa commande de 150€. L'E-commerçant le redirige vers le prestataire de paiement alternatif (flux 1). Le prestataire de paiement affiche au client une page de paiement d'un montant de 150€, le client saisit les données de sa carte cadeau et valide. Le prestataire de paiement contacte par la suite l'émetteur de la carte afin de demander l'autorisation de paiement (flux 2). Si l'émetteur de la carte cadeau autorise le paiement de 100€, le prestataire de paiements alternatifs propose au client de compléter son paiement avec d'autres moyens de paiement. Le client choisit alors de compléter son paiement avec son

porte-monnaie électronique et saisit ses données de paiement. Le prestataire demande une autorisation de paiement à l'émetteur du porte-monnaie (flux 3). Si l'autorisation de paiement est accordée, le prestataire de paiement contacte l'émetteur de monnaie électronique afin de vérifier la validité des comptes des deux émetteurs de moyens de paiement alternatifs (flux 4). De son côté, l'émetteur de monnaie électronique vérifie que l'émetteur de la carte cadeau dispose de 100€ sur son compte et vire ce montant à un compte temporaire de transaction. Ensuite, il vérifie que le compte de l'émetteur du porte-monnaie électronique contient 50€ et transfère ce montant au compte temporaire déjà créé. Une fois que la somme de la commande (150€) est réunie dans le compte de transaction, l'émetteur de monnaie électronique valide la transaction et autorise le prestataire de paiement alternatif à demander la génération d'une CVD d'un montant total de la transaction sur son compte bancaire chez la banque intermédiaire (flux 5). Si un des émetteurs des moyens de paiement alternatifs du client ne dispose pas de fonds suffisants sur son compte de monnaie électronique, la transaction est annulée ainsi que toutes les autorisations de paiement qui ont été accordées. Après la réception de la CVD correspondant au montant total de la commande (150€), le prestataire de paiement alternatif l'envoie à l'E-commerçant (flux 6). Ce dernier demande une autorisation de paiement à la banque intermédiaire (flux 7). Si cette demande d'autorisation est approuvée, il valide la commande et confirme le paiement au client. Selon le choix effectué par l'E-commerçant, un débit peut être constaté dans un délai de 2 à 3 jours sur le compte de l'émetteur de monnaie électronique chez la banque intermédiaire (voire plusieurs jours si le marchand a choisi un débit différé). A ce moment, l'émetteur de la monnaie électronique peut procéder à la destruction de la monnaie électronique présente dans le compte temporaire du client créé lors de la transaction.

Paiement complémentaire bancaire

Nous avons choisi d'isoler le cas d'un paiement complémentaire bancaire car il est plus compliqué que le précédent. En effet, il ne s'agit pas ici de manipuler seulement la monnaie électronique, mais également la monnaie scripturale lors du paiement bancaire du client. La question que nous posons est la suivante : à quel acquéreur le terminal de paiement bancaire qui servira pour encaisser le paiement complémentaire bancaire du client, sera-t-il connecté ? Autrement dit, qui encaissera le paiement complémentaire bancaire du client ? On pourrait être tenté de désigner l'E-commerçant, puisqu'il s'agit du vrai accepteur du moyen de paiement du client, mais, dans ce cas, l'orchestration de paiement est complètement déléguée à l'E-commerçant, ce qui réduit à néant l'intérêt premier de la nouvelle architecture

proposée qui était, rappelons-le, de faciliter l'intégration des nouveaux moyens de paiement pour l'E-commerçant. D'autant que le moyen de paiement bancaire sera probablement le moyen le plus utilisé pour les paiements complémentaires. C'est pourquoi nous proposons plutôt le scénario de transaction décrit dans la figure 3.10.

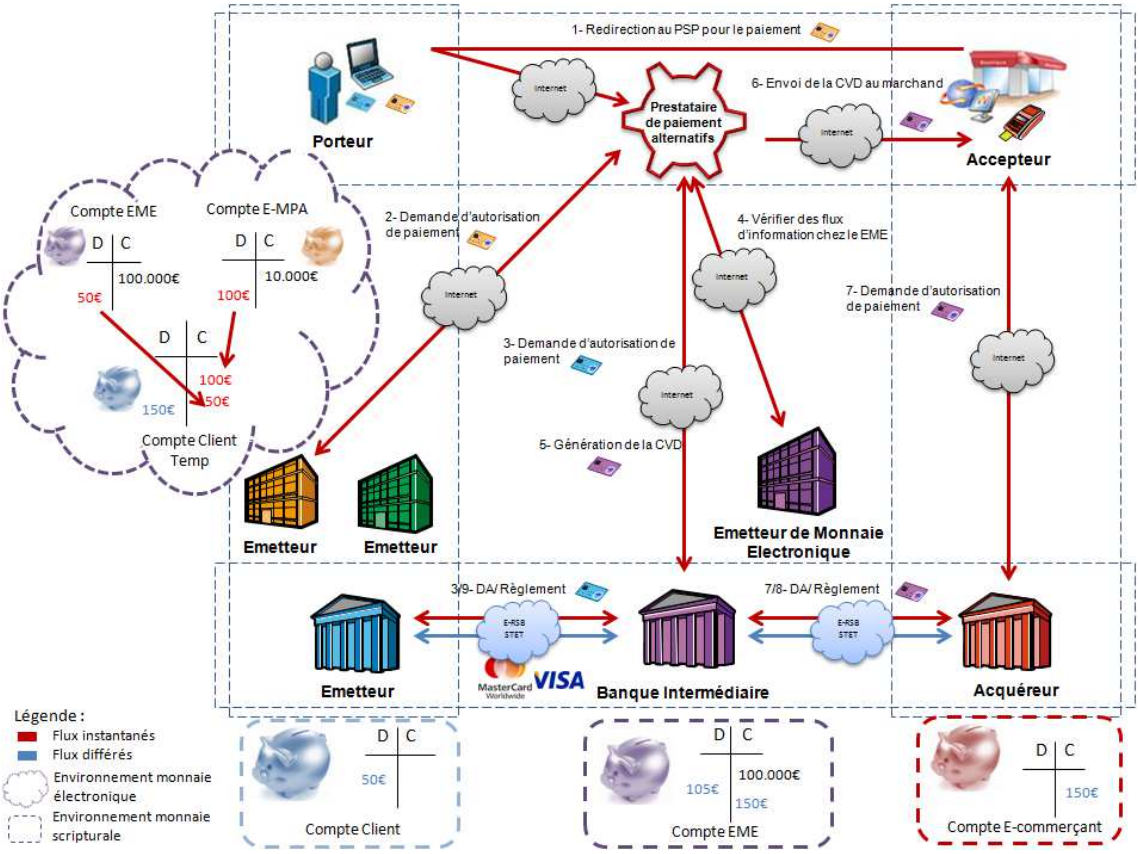


FIGURE 3.10 – Flux financiers d'un paiement alternatif avec un paiement complémentaire bancaire

Sachant que les CVDs qui servent à payer l'E-commerçant sont générées sur le compte bancaire de l'émetteur de monnaie électronique, il semble naturel que les paiements complémentaires soient encaissés par ce dernier. Nous présentons dans la figure 3.10 les flux financiers échangés dans le cas d'un paiement de 150€ avec une carte cadeau de 100€ et un paiement complémentaire bancaire de 50€. Après avoir demandé l'autorisation de paiement auprès de l'émetteur de la carte cadeau (flux 2), une demande d'autorisation est acheminée à la banque du client via la banque intermédiaire (flux 3). Une fois les demandes d'autorisation acceptées, l'émetteur de monnaie électronique effectue un transfert de la somme de 100€ depuis le compte de l'émetteur de la carte cadeau à un compte temporaire de transaction et un transfert de la somme du paiement complémentaire (50€) depuis son compte de

monnaie électronique au compte temporaire de transaction. Il confirme par la suite au prestataire de paiement alternatif la possibilité de générer une CVD du montant total de la transaction (flux 4). Le prestataire de paiement demande alors à la banque intermédiaire de générer une CVD sur le compte bancaire de l'émetteur de monnaie électronique (flux 5). Puis il envoie cette CVD à l'E-commerçant afin de payer la commande du client.

Enfin, la constatation du débit sur le compte de l'émetteur de monnaie électronique chez la banque intermédiaire (flux 8) entraîne la destruction de la monnaie électronique présente dans le compte temporaire de transaction créé lors du paiement.

3.4 Prestataire de paiement alternatif

Dans cette étude, nous nous intéressons aux services offerts par le prestataire de paiement alternatif. Afin de faciliter l'intégration des nouveaux moyens de paiement dans un site E-commerce et l'adoption de la nouvelle architecture de paiement, le prestataire de paiement alternatif propose trois systèmes : un système d'accès émetteur d'un moyen de paiement, un terminal de paiement et un système d'accès commerçant (figure 3.11).

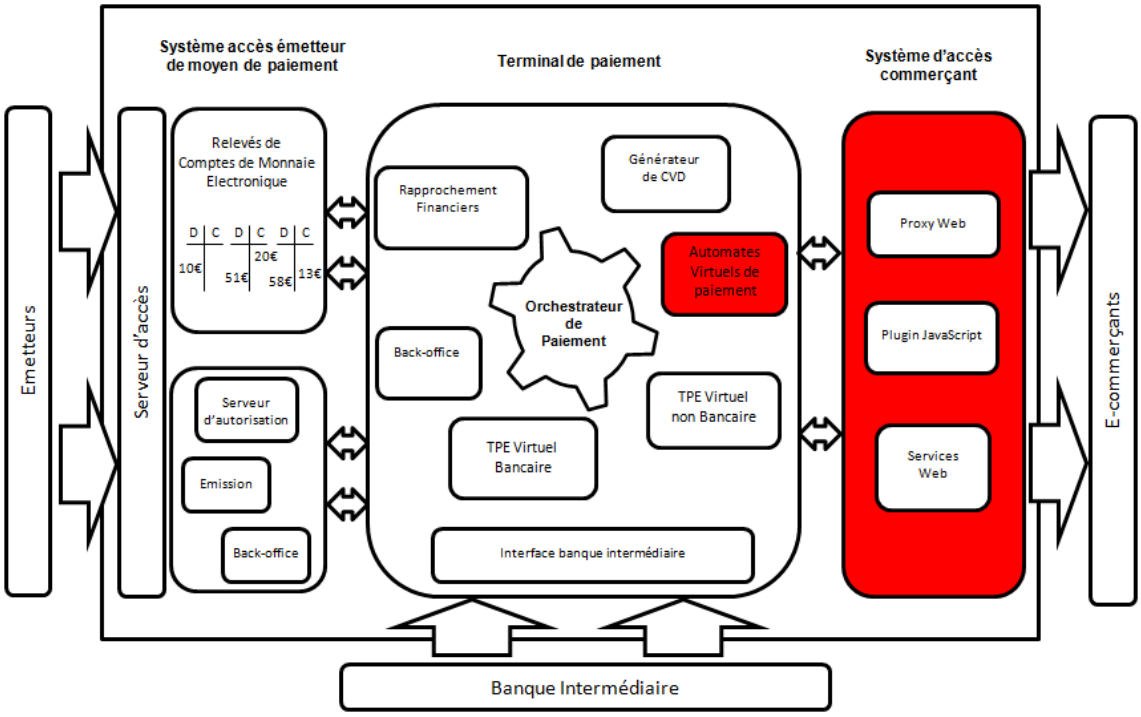


FIGURE 3.11 – Principe de fonctionnement du prestataire de paiement alternatif

Il ne s'agit pas d'une simple passerelle technique permettant de gérer les paiements

sur un site E-commerce. Il propose également de nouvelles fonctionnalités à l'E-commerçant afin d'intégrer plusieurs moyens de paiement alternatifs et de gérer le rapprochement de ces transactions. De plus, aucun changement n'est apporté au système de paiement bancaire de l'E-commerçant. Comme nous pouvons le constater dans la description de la nouvelle architecture, l'E-commerçant n'a pas à créer de compte bancaire (ni compte de monnaie électronique), ce qui constitue un avantage pour encourager les E-commerçants à intégrer le nouveau système de paiement dans leur boutique en ligne.

Nous présentons dans cette section les différentes composantes du nouveau système de paiement afin de positionner notre contribution dans le cadre de la nouvelle architecture.

3.4.1 Système d'accès émetteur de moyens de paiement

La première composante du système de paiement est le système d'accès des émetteurs de moyens de paiement qui permet à ces derniers d'être acceptés chez les E-commerçants. Comme son nom l'indique, ce système permet de connecter les autres composantes du système de paiement aux émetteurs des moyens de paiement. Cette connexion est nécessaire dans le cas d'une demande d'autorisation de paiement ou pour rediriger le client vers la page de paiement si elle n'est pas hébergée par le prestataire de paiement. Ce système permet également de gérer les comptes de monnaie électronique des émetteurs détenus par l'émetteur de monnaie électronique tout au long de la durée de vie de la transaction.

3.4.2 Terminal de paiement

La deuxième composante du nouveau système de paiement est le terminal de paiement qui permet de gérer les paiements non bancaires et d'orchestrer plusieurs moyens de paiement. La page de paiement peut être hébergée par le serveur du prestataire de paiement ou par l'émetteur du moyen de paiement. Dans le premier cas de figure, le prestataire de paiement alternatif s'occupe de vérifier les coordonnées de paiement du client, de demander l'autorisation de paiement à l'émetteur et de payer l'E-commerçant. Il maîtrise tout le déroulement du processus de paiement et peut ainsi orchestrer plusieurs moyens de paiement. Dans le deuxième cas, comme tout paiement déporté, le prestataire de paiement alternatif joue alors le rôle de la passerelle technique entre le site marchand et l'émetteur. Il redirige le client vers la page de paiement hébergée par l'émetteur. Pour ce faire, le partenaire de paiement alternatif doit intégrer le moyen de paiement alternatif à la place de l'E-commerçant.

Du coup, la complexité de l'intégration est complètement déportée chez le prestataire de paiement alternatif. Cependant, il peut être compliqué, pour le prestataire de paiement alternatif, d'orchestrer plusieurs moyens de paiement lorsque la page de paiement alternatif est déportée chez l'émetteur. Une fois que le paiement alternatif est effectué, le prestataire de paiement se connecte au terminal de paiement bancaire de l'E-commerçant afin de payer le panier du client. Le déroulement du paiement est décrit dans le diagramme 3.12.

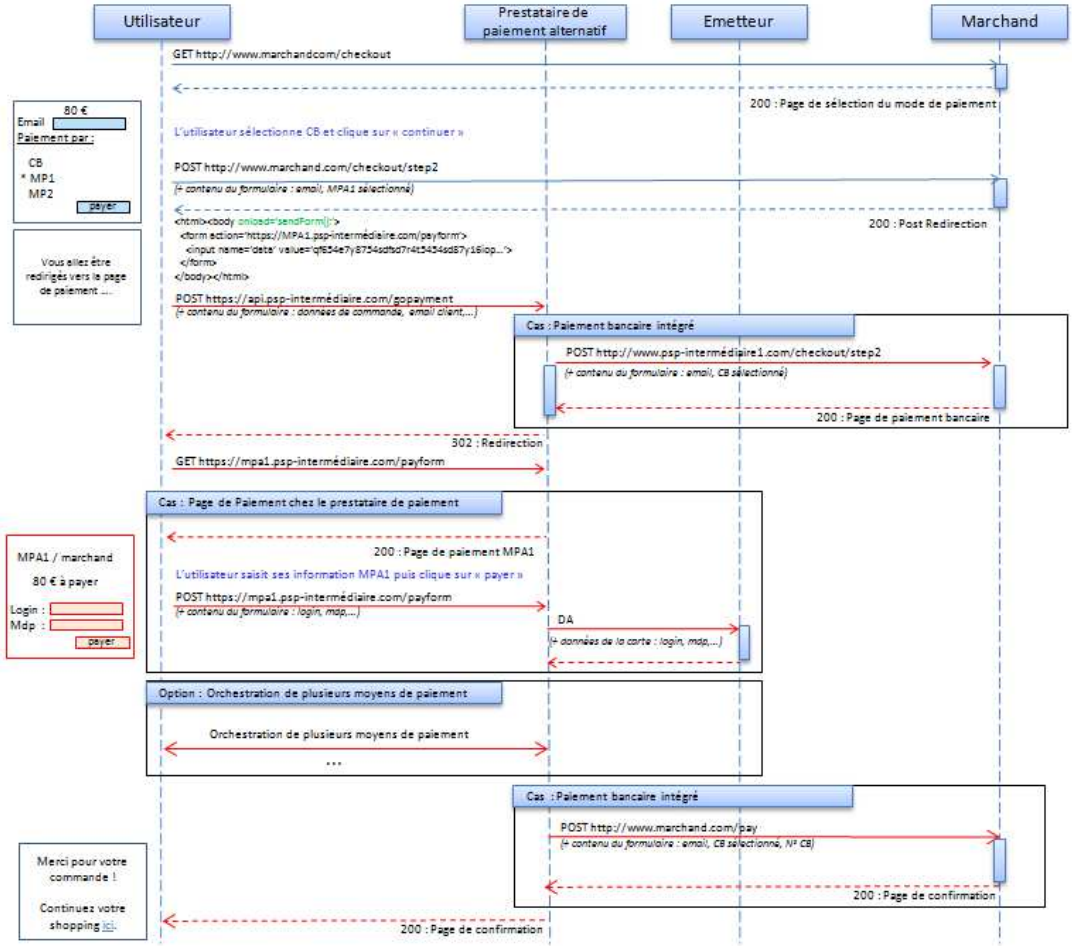


FIGURE 3.12 – Nouveau système de paiement

Le terminal de paiement permet également de combiner plusieurs moyens de paiement (bancaires et non bancaires) avant de convertir le paiement alternatif en paiement bancaire. Cette conversion exige que le terminal de paiement communique avec le système d'accès émetteur d'un moyen de paiement décrit auparavant. Le prestataire de paiement alternatif fournit à l'E-commerçant une liste de toutes les transactions remontées par le terminal de paiement avec toutes les informations nécessaires (montant, numéro de commande, date, statut de la commande, etc.). Le

marchand a également la possibilité d'effectuer certaines opérations financières depuis le back-office (annuler une commande, re-créditer une commande, etc.). Sachant que tous les paiements non bancaires sont convertis en paiements bancaires, le marchand retrouve toutes les transactions dans ses outils traditionnels de gestion des paiements bancaires. L'intérêt du back-office du prestataire de paiement alternatif est de donner à l'E-commerçant la possibilité d'identifier les commandes payées avec les moyens de paiements alternatifs.

3.4.3 Système d'accès commerçant

Le système d'accès commerçant permet aux E-commerçants d'intégrer les moyens de paiement alternatifs proposés par le système de paiement. Ce système apporte au marchand les solutions techniques au problème de la redirection du client vers le prestataire de paiement alternatif. Lors de l'étude de l'existant (chapitre 2), nous avons recensé plusieurs modes d'intégration des systèmes de paiement existants. Nous retrouvons dans ce système quelques solutions de l'état de l'art (Services Web) mais nous proposons également d'autres approches d'intégration (Proxy Web, Plugin JS) qui seront décrits en détail par la suite. Le mode d'intégration via Service Web de cette nouvelle architecture sera volontairement exclu de la suite de notre étude car il a déjà été décrit dans l'état de l'art.

3.5 Conclusion

Dans ce chapitre nous avons proposé une nouvelle architecture de paiement sur Internet qui permet de contourner les problèmes d'intégration des nouveaux moyens de paiement sur Internet. Le principe fondamental de la nouvelle architecture est de convertir les paiements non bancaires en paiements bancaires à l'aide des cartes virtuelles dynamiques.

Nous avons présenté les nouveaux acteurs introduits par la nouvelle architecture en plus de ceux du système quatre coins déjà examinés. En effet, afin de permettre la conversion du paiement alternatif en paiement bancaire, nous avons proposé d'utiliser des comptes de monnaie électronique, ce qui rend nécessaire la présence d'un émetteur de monnaie électronique dans l'architecture. Afin de générer des cartes virtuelles dynamiques, nous avons souligné le besoin d'avoir une banque émettrice. Le prestataire de paiement alternatif permet d'orchestrer les différents échanges entre les acteurs dans la nouvelle architecture afin de gérer le paiement.

Nous avons également décrit, dans ce chapitre, le processus de la conversion de la monnaie électronique en monnaie scripturale en détaillant la description des

flux financiers au sein de la nouvelle architecture dans le cas de trois scénarios de paiement différents. Enfin, nous avons modélisé le nouveau système de paiement proposé par le prestataire de paiement alternatif, en le divisant en trois composantes et décrivant le rôle de chacune.

Dans la suite de notre argumentation, nous nous intéresserons au terminal de paiement et au système d'accès commerçant. Le chapitre suivant présente une première approche d'intégration de ce nouveau moyen de paiement sans demander beaucoup de développement technique à l'E-commerçant.

Chapitre 4

Proposition d'intégration via Proxy Web

Nous proposons, dans le cadre de ce chapitre, une première approche d'intégration de l'architecture de paiement proposée dans le chapitre précédent [Abdellaoui R., Pasquet M., Berthelier O., 2011]. Il s'agit d'une approche qui exploite le contexte particulier d'Internet et se base sur des outils purement Web. Ce chapitre décrit les différentes caractéristiques du mode d'intégration via Proxy Web (section 4.2) ainsi que le processus de proxification (section 4.3). Nous présentons par la suite la procédure d'intégration de la nouvelle architecture via Proxy Web (section 4.4). Enfin, nous validons l'approche proposée selon l'état de l'art et les besoins fixés au début de notre étude (section 4.5) afin de déduire les avantages et les inconvénients de cette proposition.

Sommaire

4.1 Introduction

A partir de l'étude bibliographique (chapitre 2) nous déduisons qu'il existe plusieurs modes d'intégration d'un système de paiement sur Internet. La complexité de ces modes d'intégration varie selon le mode de redirection choisi (redirection HTTP simple basée sur des Services Web, redirection HTTP chiffrée ou redirection signée) ainsi que le modèle de sécurité choisi (cryptographie symétrique ou asymétrique). Après avoir décrit l'architecture de paiement proposée dans le cadre notre travail, nous allons présenter, dans ce chapitre, une première approche d'intégration de la nouvelle architecture, tout en prenant en compte les contraintes d'intégration présentées au début de cette étude : la sécurité, l'ergonomie et la complexité. Sachant que nous nous intéressons au commerce électronique sur Internet, nous proposons d'exploiter les outils caractéristiques de cet environnement. Notre approche se base sur des outils purement Web et exploite ainsi le contexte de l'E-commerce [Abdellaoui R., Pasquet M., Berthelier O., 2011]. Cependant, rappelons que nous ne nous intéressons qu'aux E-commerçants qui disposent, au préalable, d'un système de paiement bancaire qui est indispensable pour convertir les paiements alternatifs en paiements bancaires tels que décrits dans le chapitre précédent.

La conception de cette approche a été effectuée avec l'assistance de l'équipe R&D de Limonetik, le partenaire industriel de notre travail de recherche, notre contribution consiste en la formalisation et la validation de cette approche. Cette approche consiste à utiliser un Proxy Web afin d'intégrer les moyens de paiement dans les sites E-commerce. Dans la suite de ce chapitre, nous verrons que cette approche évite à l'E-commerçant d'avoir à investir dans un développement technique pour intégrer les moyens de paiement non bancaires. Cependant, malgré la simplicité de l'intégration du nouveau système de paiement via Proxy Web du côté des E-commerçants et des émetteurs des moyens de paiement alternatifs, ce mode d'intégration semble exiger un grand travail de maintenance du côté du prestataire de paiement alternatif.

4.2 Proxy Web : principe

Proxy est un terme informatique général qui désigne un composant logiciel qui se place entre deux autres pour faciliter ou surveiller leurs échanges [Wikipedia, 2000b]. Le prestataire de paiement alternatif, dans le cadre de cette approche, agit alors comme un Proxy Web entre le navigateur du client et le serveur de l'E-commerçant, c'est-à-dire qu'il transmet les données depuis le navigateur du client vers le serveur de l'E-commerçant et inversement (figure 4.1).

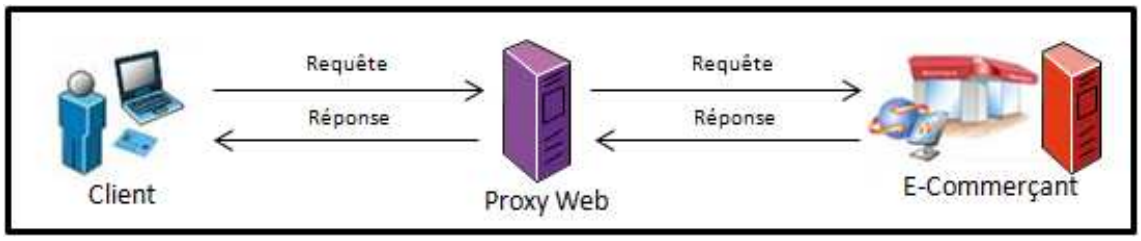


FIGURE 4.1 – Principe du Proxy Web

Un Proxy Web est *un simple site Web dont la page offre un champ permettant de taper l'adresse du site que l'on souhaite visiter. Une fois saisie, la page demandée est affichée à l'intérieur de la première page. Mais l'adresse qui apparaît dans la barre d'adresse est toujours celle du proxy* [Wikipedia, 2000b]. A partir de cette définition, nous allons décrire le principe de l'intégration des moyens de paiement en passant par un Proxy Web. Pour ce faire, nous présentons dans la figure 4.2 l'enchaînement des pages lors d'un paiement via le Proxy Web qui décrit l'expérience utilisateur dans ce cas.

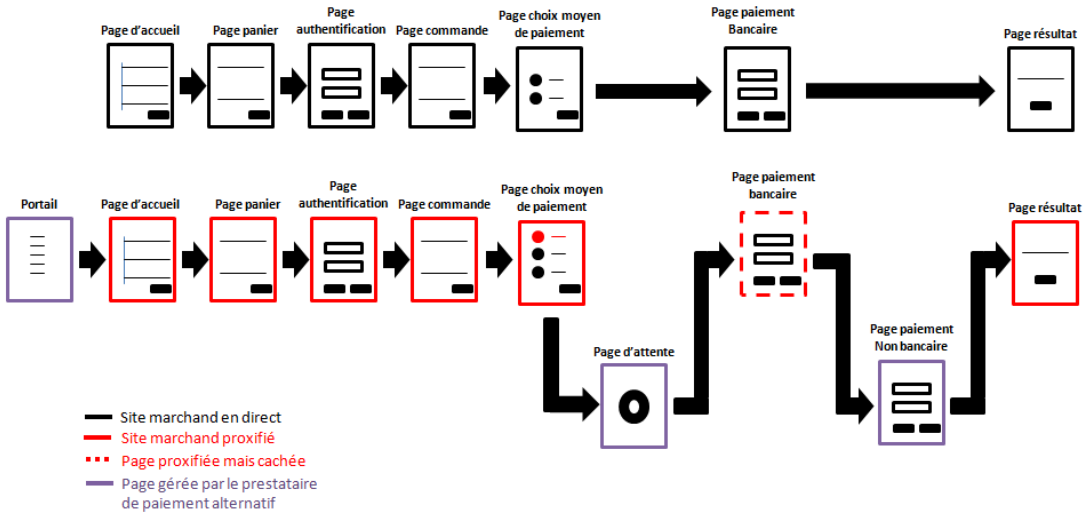


FIGURE 4.2 – Expérience utilisateur en passant par le Proxy Web

Lors d'un paiement via le Proxy Web, le client doit passer par une page hébergée par le prestataire de paiement alternatif qui lui permet de sélectionner le site E-commerce sur lequel il souhaite payer avec son moyen de paiement non bancaire. Ensuite, il est redirigé vers le site Web de l'E-commerçant « proxifié ». En d'autres termes, le client navigue sur des pages Web ayant le même contenu que celles du site Web de l'E-commerçant mais avec une adresse qui appartient au serveur du prestataire de paiement alternatif. Le client remplit alors son panier, s'authentifie

auprès de l'E-commerçant et valide sa commande. L'E-commerçant lui renvoie ensuite la page de choix de moyen de paiement qui ne contient pas le moyen de paiement alternatif du client (car l'E-commerçant n'a pas intégré ce moyen de paiement dans son site E-commerce). Le prestataire de service de paiement, qui joue le rôle d'une passerelle entre le client et l'E-commerçant, ajoute alors le moyen de paiement du client, déjà programmé dans la configuration proxy pour ce site E-commerce. Si le client choisit le nouveau moyen de paiement (ce qui est probablement le cas, car il est passé par le portail au début de sa navigation), le prestataire de paiement alternatif lui affiche une page d'attente afin d'effectuer certaines opérations nécessaires pour afficher la page de paiement (transparentes pour le client) et puis le redirige vers la page de paiement correspondante. Une fois la page de paiement affichée, le client peut alors utiliser son moyen de paiement non bancaire pour payer sa commande. Le prestataire de paiement valide le paiement du client et le convertit en paiement bancaire (chapitre 3). Après la validation du paiement par l'E-commerçant, le client est redirigé vers la page de résultat de paiement du marchand « proxifiée ».

La figure 4.2 montre également que toutes les pages Web qui précèdent la page de choix de paiement (page de choix des articles, remplissage du panier, authentification au compte marchand, choix du mode de livraison, validation de l'adresse du client, etc.) sont proxifiées sans modification. En effet, il est très important de rassurer le client et de rester fidèle à la charte graphique du site E-commerce afin que le client ait l'impression de naviguer sur le site marchand en direct. Il s'agit d'un défi technique pour le prestataire de paiement alternatif car il faut garantir que le client arrive à la page de choix de moyen pour sélectionner le nouveau moyen de paiement. Or, parfois, à cause de problème de proxification de flash ou de JavaScript, le client risque de rester bloqué dans une page postérieure à la page de paiement ou perdre la connexion avec le Proxy Web. Dans le cadre de cette approche le prestataire de paiement alternatif joue un rôle particulier car, contrairement à la définition classique d'un prestataire de paiement qui gère seulement la redirection du client depuis le site E-commerce et l'affichage de page de paiement, le prestataire de paiement alternatif s'occupe également de la gestion de la navigation du client sur tout le site E-commerce.

Avant de détailler les différentes caractéristiques techniques de ce mode d'intégration, nous proposons de décrire un scénario de transaction simple qui consiste à utiliser un seul moyen de paiement alternatif. La figure 4.3 présente une vue générale du mode d'intégration via Proxy Web. Ayant le rôle d'un Proxy Web, le prestataire de paiement alternatif peut alors intercepter les échanges HTTP entre le client et l'E-commerçant, ce qui lui permet d'analyser le contenu des pages Web renvoyées

par le serveur de l'E-commerçant et insérer le moyen de paiement alternatif parmi les choix de moyens de paiement.

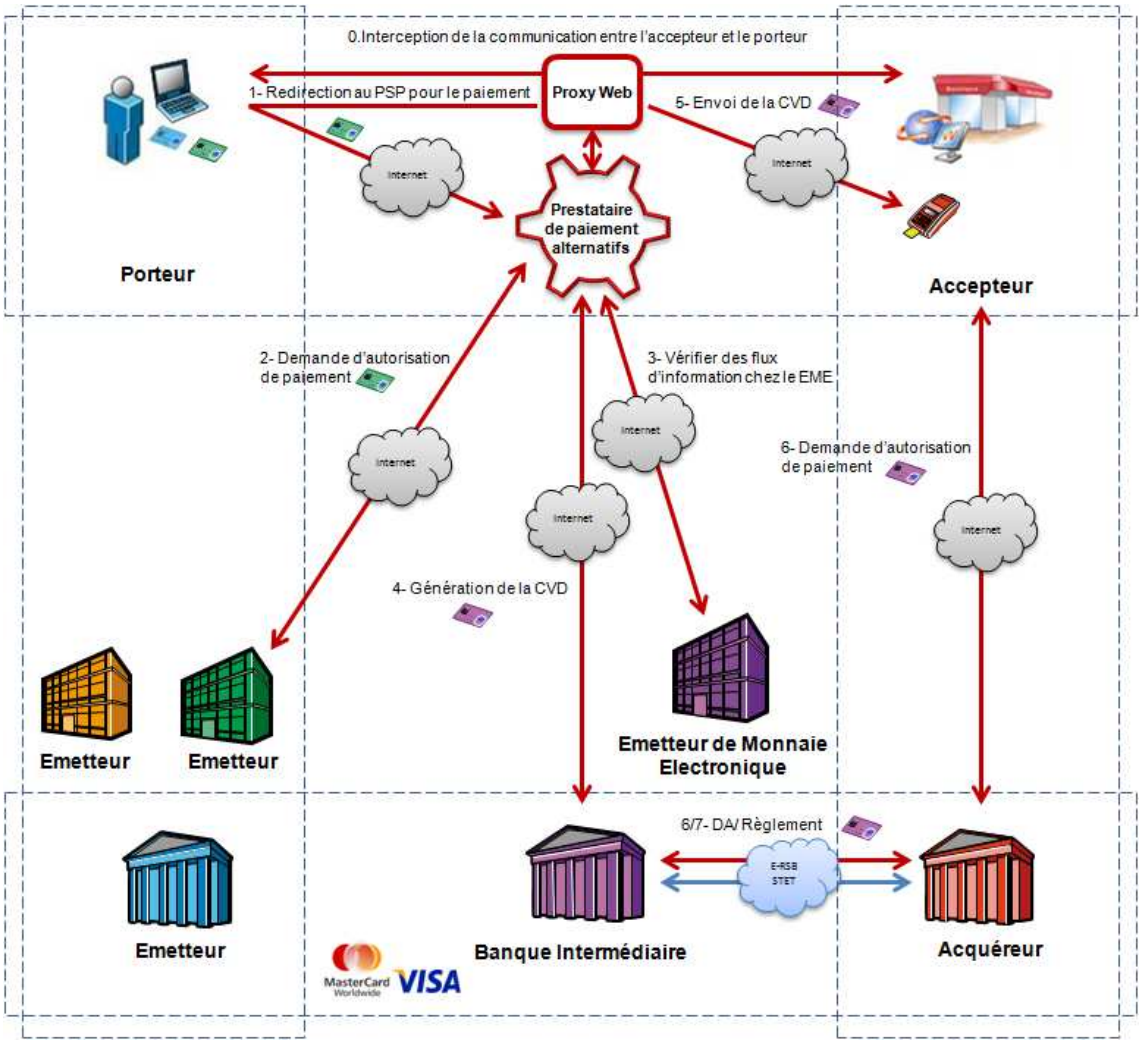


FIGURE 4.3 – Transaction via le Proxy Web

Nous constatons également qu'afin d'intégrer les moyens de paiement non bancaires dans un site E-commerce et de rediriger ce dernier vers la page de paiement correspondant à son moyen de paiement, le Proxy Web doit intercepter les différents échanges entre le client et l'E-commerçant (flux 0). C'est la seule façon pour le prestataire de paiement d'injecter du code dans les pages Web du site E-commerce et d'ajouter le nouveau moyen de paiement. Le paiement de l'E-commerçant se fait ensuite via le Proxy Web (flux 5). Nous présentons dans la suite de ce chapitre plus en détail les différentes étapes d'intégration du Proxy Web : le choix de moyen de paiement, le paiement et le rapprochement.

4.3 Processus de proxification

Sachant que chaque site marchand est spécifique, il a fallu créer un fichier de configuration par site marchand afin de définir les règles de réécriture relatives à ce site. Par exemple, l'intégration du nouveau moyen de paiement se fait dans une page propre au marchand (page de choix de moyen de paiement) et nécessite donc des règles d'insertion spécifiques. Il a fallu également définir des règles d'accès spécifiques à chaque contexte de site marchand, car, généralement, le site Web définit beaucoup de liens sortants vers des partenaires commerciaux qui ne font pas partie du contexte du paiement et qui doivent être bloqués car cela peut nuire à l'expérience utilisateur. Le Proxy Web se base sur le nom domaine du site marchand, qui est un identifiant unique du site sur le réseau d'Internet, afin de savoir quelle configuration utiliser. Il se base également sur ces noms de domaines pour accepter ou bloquer l'accès aux autres sites Web lors d'une navigation sur un site E-commerce. Nous présentons dans cette section le processus de proxification ainsi que les différents outils mis en place par le prestataire de paiement alternatif afin de réussir l'intégration des nouveaux moyens de paiement sans altérer l'expérience utilisateur sur le site E-commerce.

4.3.1 Principe général d'injection de code

Afin de pouvoir ajouter de nouveaux moyens de paiement dans les pages de choix de moyen de paiement du site marchand, le prestataire de paiement alternatif a besoin de pouvoir injecter un nouveau code HTML. En informatique, l'ajout de contrôles sur les pages Web peut être réalisé de plusieurs manières, en particulier :

- Navigation via des frames
- Navigation via Proxy Web

Les frames en HTML permettent de diviser une page en plusieurs parties, pour ensuite insérer dans chaque partie une page à part entière. Cette outil permet de mettre à jour le contenu d'une page HTML sans demander pour autant au site marchand de modifier tout son code source. Un exemple de code HTML de page qui contient des frames est présenté dans le tableau 4.1. Il suffit de prévoir des frames à la création de la page HTML et de les faire pointer vers des pages extérieures. Le contenu de ces frames sera affiché dans la page mère mais géré par une entité extérieure. Nous avons évoqué ce mode d'injection de contenu dans une page HTML dans le chapitre 2 en décrivant le mode d'intégration déporté en Iframe où la page de paiement est déportée chez un prestataire de paiement externe mais affichée dans une page du site marchand.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Frameset//EN"
"http ://www.w3.org/TR/html4/frameset.dtd">
<HTML>
<HEAD>
<TITLE>A simple frameset document</TITLE>
</HEAD>
<BODY>
<FRAMESET cols="20%, 80%">
      <FRAMESET rows="100, 200">
            <FRAME src="frame1.html">
            <FRAME src="frame2.gif">
      </FRAMESET>
      <FRAME src="frame3.html">
</FRAMESET>
</BODY>
</HTML>
```

TABLE 4.1: Processus d'injection de code avec Frame

La deuxième méthode d'injection de code dans une page HTML, est la navigation via un Proxy Web qui réécrit le code source des pages du site marchand. La solution d'ajout de code à la volée dans les pages des sites marchands représente un défi technique. Des éléments HTML, Javascript et CSS doivent être insérés à des emplacements bien précis dans le code source des pages des sites marchands sans modifier l'expérience utilisateur du site. Les contrôles ne doivent en aucune manière se télescoper avec les éléments du site marchand. Le Proxy Web doit se baser sur des éléments discriminants afin d'ajouter le code HTML au bon endroit dans la page. Nous avons effectué une étude des différentes typologies des sites marchands afin d'analyser leur structure avant la conception du Proxy Web. Nous avons constaté que sur l'échantillon des sites d'E-commerce étudiés, les Urls permettent de discriminer les pages pendant la navigation et donc les insertions à effectuer. Selon la phase de paiement, les règles d'injection sont différentes : ajouter un nouveau moyen de paiement, remplir un formulaire de paiement, rediriger le client, etc. Parmi les éléments discriminants permettant la bonne injection du code, citons : l'url de la page, le code HTML de la page, les entêtes de la réponse HTTP (Content, Content-Type, UserAgent, etc.), les entêtes de la requêtes HTTP (Referer, Cookies, etc.), la méthode HTTP de la requête (POST, GET, PUT, etc.), le StatusCode de la réponse HTTP (200, 302, 404, etc.).

Comme tout serveur Proxy Web, le serveur du Proxy Web du prestataire de paiement alternatif est basé sur des règles de filtrage et il évalue les requêtes du client selon ces règles de filtrage. Si la demande est validée par le filtre, Le Proxy se

connecte au serveur du site marchand en envoyant la requête du client et achemine par la suite la ressource demandée au client. Une petite description du processus d'injection dans le Proxy Web est présentée dans la figure 4.4.

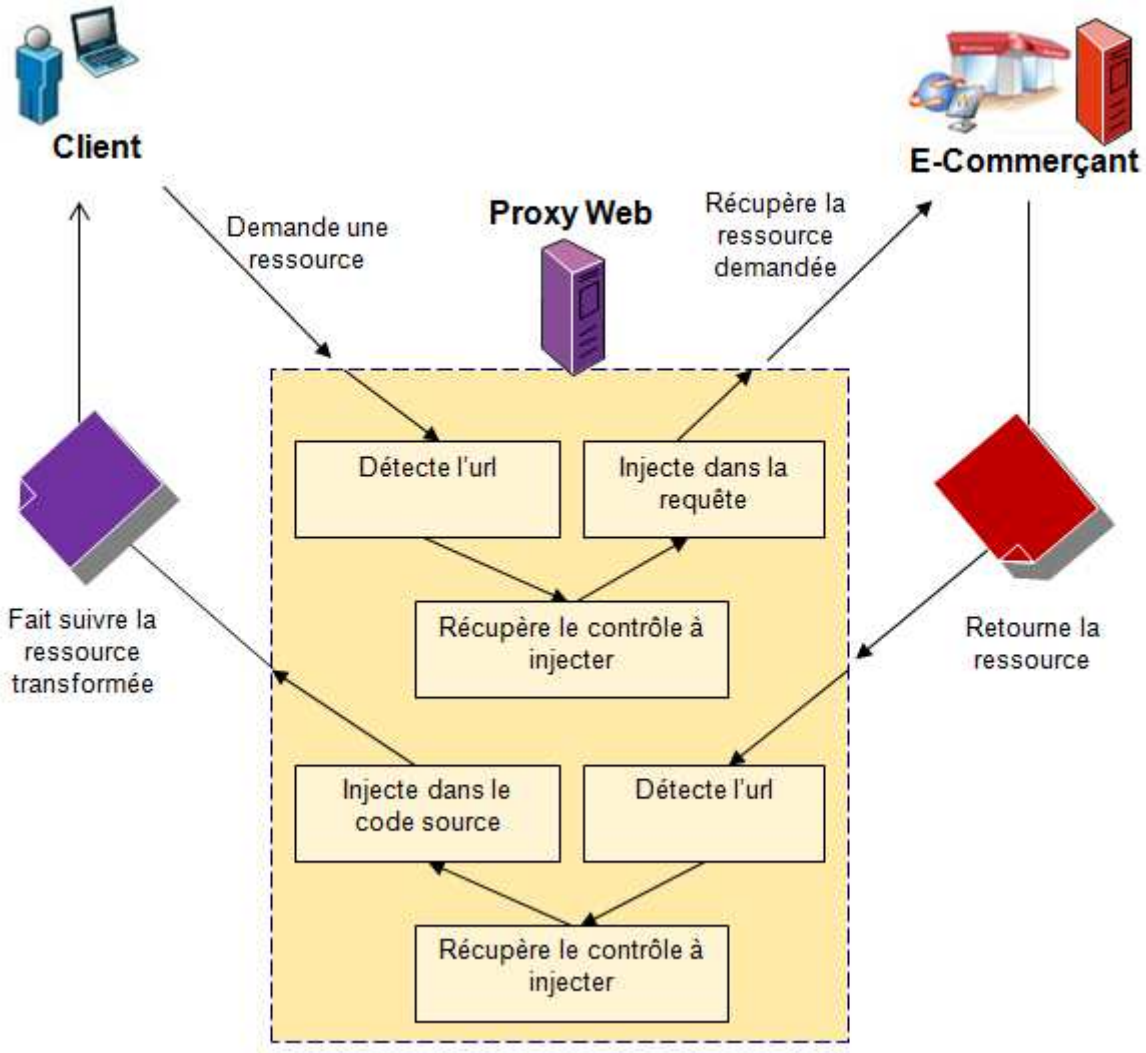


FIGURE 4.4 – Processus d'injection avec Proxy Web

4.3.2 Fichiers de configuration

Afin de réussir le processus de proxification décrit dans la section précédente, le Proxy Web se base sur des fichiers de configuration qui permettent de configurer les règles de gestion de chaque site Web lors de la navigation via le Proxy. Les fichier de configuration dans le Proxy sont des fichiers XML avec l'extension « .config ».

Un fichier config est donc un fichier XML qui permet de gérer les règles de filtrage concernant un site Web donné. Nous présentons un exemple de fichier de configuration dans la figure 4.5.

```
<?xml version="1.0" encoding="utf-8"?>

<lmkWebSiteConfig  xmlns="http://www.limonetik.com/LmkProxyConfig">

  <managedDomains>
    <clear />
    <add targetDomain="ogone.citronrose.com" domainGroup="NonSecuredWebSites"/>
    <add targetDomain="ogone.citronroseci.com" domainGroup="NonSecuredWebSites"/>
    <add targetDomain="ogone.citronrosedev.com" domainGroup="NonSecuredWebSites"/>
  </managedDomains>

  <domainAccessRights>
    <add domain="*" path="*" access="Deny"/>
    <add domain="*.citronrose.com" path="*" access="Proxy"/>
    <add domain="*.citronroseci.com" path="*" access="Proxy"/>
    <add domain="*.citronrosedev.com" path="*" access="Proxy"/>
    <add domain="*.ogone.com" path="*" access="Proxy"/>
  </domainAccessRights>

  <targetResponseProcessPlan>
    <preMainProcessors>
      <add name="PaymentStepLastProcessor"/>
    </preMainProcessors>
    <mainProcessors>
      <add name="PaymentConfirmationProcessor"/>
    </mainProcessors>
  </targetResponseProcessPlan>

  <processors>

    <processor name="PaymentStepLastProcessor">
      <if>
        <testValue navStateKey="PaymentEnable">true</testValue>
        <testValue navStateKey="IsHtml">true</testValue>
        <regExpFind scope="2"><![CDATA[<input[^>]*?value="CB"[^>]*?>]]></regExpFind>
        <regExpFind scope="1"><![CDATA[/PaymentSelection\.aspx]]></regExpFind>
      </if>
      <then>
        <regExpAction>
          <regExpFind scope="2"><![CDATA[(value="CB")[^>]"checked="checked"]]></regExpFind>
          <regExpReplace><![CDATA[$1]]></regExpReplace>
        </regExpAction>
      </then>
    </processor>

    <processor name="PaymentConfirmationProcessor">
      <if>
        <testValue contextKey="OrderExternalID" navStateKey="DvcSentToShop">true</testValue>
        <regExpFind scope="1"><![CDATA[Return_OK\.aspx]]></regExpFind>
        <regExpFind scope="2" contextKey="OrderExternalID" storeGroupsInNavState="true">
          <![CDATA[>CitronRose_(?<ShopOperationID>\d*)<]]>
        </regExpFind>
      </if>
      <then>
        <setValueAction navStateKey="PaymentConfirmation">true</setValueAction>
      </then>
    </processor>

  </processors>
</lmkWebSiteConfig>
```

FIGURE 4.5 – Exemple de fichier configuration marchand dans le Proxy Web

Le moteur de proxification du Proxy Web permet d'analyser les différents noeuds contenus dans ce fichier de configuration afin de proxifier un site donné. Nous présentons dans le tableau 4.2, la liste des noeuds présents dans un fichier de configuration tout en expliquant leurs fonctionnalités.

Noeud	Description
ManagedDomains	Ce noeud représente les domaines que cette configuration doit prendre en charge. Plusieurs configurations ne peuvent pas avoir les mêmes domaines dans ce noeud. Lors de la navigation, le serveur Proxy charge la configuration qui prend en compte le domaine demandé par le client. Exemple : <managedDomains> <add targetDomain="citronrose.com"/> <add targetDomain="*.citronrosedev.com"/> </managedDomains>
DomainAccessRights	Ce noeud contient les règles de proxification des domaines. En effet, selon les règles définies dans ce noeud, le Proxy peut modifier les ressources hébergées par certains domaines, les transmettre tel qu'elles sont au client ou les bloquer. Exemple : <domainAccessRights> <add domain="*" path="*" access="Redirect"/> <add domain="*.citronrose.com" path="*" access="Proxy"/> </domainAccessRights>
ProcessPlans	Une configuration du site Web contient deux types de ProcessPlan : un UserRequestProcessPlan qui concerne les requêtes HTTP envoyées du client vers le site marchand et un TargetResponseProcessPlan qui concerne les réponses HTTP renvoyées du site marchand au client. Exemple : <targetResponseProcessPlan> <mainProcessors> <add name="PaymentConfirmationProcessor"/> </mainProcessors> <preRenderProcessors> <add name="AddBottomSpaceByDivProcessor"/> </preRenderProcessors> </targetResponseProcessPlan>
Processor	Ce noeud contient la définition des processeurs d'une configuration. Un processeur permet de manipuler les ressources d'un site (modification, suppression, ajout...). Afin qu'un processeur soit pris en compte, il doit être appeler dans le noeud « UserRequestProcessPlan » ou « TargetResponseProcessPlan » selon son usage. Exemple : <processor name="HelloWorldProcessor"> <if> <testValue navStateKey="IsHtmlPage">true</testValue> </if> <then> <regExpAction> <regExpFind scope="1"><![CDATA[$]]></regExpFind> <regExpReplace><![CDATA[?Proxy]]></regExpReplace> </regExpAction> </then> </processor>

TABLE 4.2: Description des noeuds du fichier de configuration Proxy

4.3.3 Gestion des domaines

Le Proxy attribue à chaque site marchand un nouveau domaine, ce qui permet au client de naviguer sur un domaine différent de celui du site marchand tout en ayant accès au même contenu que sur le site marchand. Le Proxy définit deux types de domaines ; des domaines non sécurisés (qui correspondent à la navigation classique sur le site marchand) et des domaines sécurisés (qui correspondent au paiement et à toute navigation sécurisée) tel que présenté sur la figure 4.6. Un groupe de domaines est attribué pour chaque ensemble de noms de domaines de sites marchands. Cette définition est effectuée dans un fichier central qui permet de gérer les différents domaines des sites marchands proxifiés.

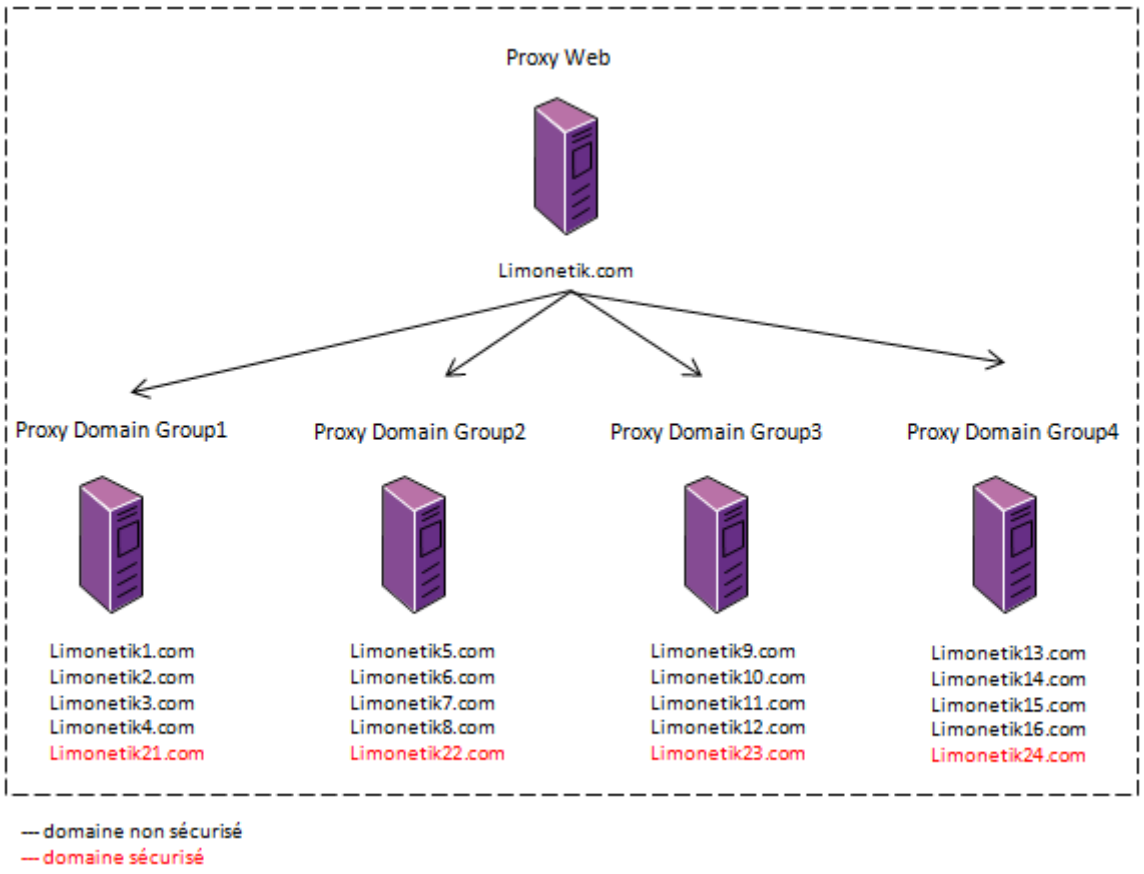


FIGURE 4.6 – Gestion des domaines par le Proxy Web

Afin de pouvoir attribuer un nom de domaine pour le site marchand choisi, le client doit démarrer sa navigation depuis un portail. Ainsi, le Proxy Web sélectionne un des domaines disponibles du groupe du site marchand.

4.3.4 Expressions régulières

Le Proxy utilise les expressions régulières (Regular Expression - RegExp) pour identifier les tags HTML à réécrire. Il s'agit d'une suite de caractères typographiques « pattern » chargée de décrire une chaîne de caractères pour la trouver dans un bloc de texte et lui appliquer un traitement automatisé, comme un ajout, un remplacement ou une suppression [Wikipedia, 2012].

Cet outil permet au Proxy d'insérer n'importe quel élément graphique dans un site marchand, ce qui permet d'insérer de nouveaux moyens de paiement sans exiger aucun développement technique de la part de l'E-commerçant en question. Dans le cas d'échec de l'injection du code, la ressource demandée par le client n'est pas proxifiée et est renvoyée au client sans modification. Plusieurs précautions ont été prises afin de ne pas altérer le fonctionnement du site Web en cas d'erreur. Nous montrerons, dans la section 4.5, que le Proxy Web permet de préserver l'intégrité des paiements déjà proposés par le site avant l'intégration du Proxy Web, notamment le paiement bancaire sur le site.

4.3.5 Gestion des formulaires HTML

Les formulaires HTML permettent d'envoyer des données depuis une page HTML à une autre page (ou à un autre serveur). Le formulaire est délimité dans le code HTML par le conteneur : <FORM> </FORM>, c'est-à-dire que toutes les balises de base propres aux formulaires devront être contenues entre ce couple de balises. A l'intérieur de ce conteneur, pourront aussi figurer les autres balises HTML. La balise <FORM> possède des attributs permettant de choisir le nom du formulaire ou l'identifiant du formulaire nécessaire en cas d'utilisation de JavaScript pour identifier le formulaire de manière unique, de spécifier l'adresse (URL ou e-mail) vers laquelle les données seront envoyées grâce à ACTION et de sélectionner une méthode d'envoi des données avec METHOD.

Toutes les pages de paiement sur Internet contiennent un formulaire qui permet d'envoyer les données de la carte bancaire au serveur de paiement. Un exemple de ces formulaires est présenté dans la table 4.3. Afin de pouvoir payer à la place du client, le Proxy Web doit pouvoir analyser ces formulaires de paiement et les remplir avec les valeurs correspondantes de la CVD. Pour ce faire, une librairie Javascript a été développée. Elle permet de sélectionner un formulaire HTML identifié d'une manière unique (avec son attribut name ou id) et de remplir les champs cachés du formulaire depuis une description XML de ce dernier. Nous présentons dans la table 4.4 un exemple d'une description XML du formulaire CB présenté dans la table 4.3.

```
<form autocomplete="off" action="paiement.cgi" method="post" name="Cyb">
    <input type="text" name="Payment_Card_Name" id="Payment_Card_Name">
     <label for="Payment_Card_Number">Numéro de carte bancaire</label>
    <input type="text" name="Payment_Card_Number" id="Payment_Card_Number">
    <label for="Payment_Card_ExpDate_Month">Date d'expiration</label>
    <select name="Payment_Card_ExpDate_Month" id="Payment_Card_ExpDate_Month">
        <option selected="selected" value="">Mois</option>
        <option value="01">01</option>
        <option value="02">02</option>
        <option value="03">03</option>
        <option value="04">04</option>
        <option value="05">05</option>
        <option value="06">06</option>
        <option value="07">07</option>
        <option value="08">08</option>
        <option value="09">09</option>
        <option value="10">10</option>
        <option value="11">11</option>
        <option value="12">12</option>
     </select>
    <select name="Payment_Card_ExpDate_Year" id="Payment_Card_ExpDate_Year">
        <option selected="selected" value="">Année</option>
        <option value="2011">2011</option>
        <option value="2012">2012</option>
     </select>
     <label for="Paymen_Card_Verification">Code de vérification</label>
     <input type="text" name="Payment_Card_Verification" id="Payment_Card_Verification">
     <input type="hidden" value="SSL" name="protocole">
     <input type="hidden" value="3.0" name="version">
     <input type="hidden" value="limonetik" name="societe">
     <input type="hidden" value="FR" name="lgue">
     <input type="hidden" value="0002043" name="TPE">
     <input type="hidden" value="24/11/2011 :16 :37 :16" name="date">
     <input type="hidden" value="20EUR" name="montant">
     <input type="hidden" value="885781" name="reference">
     <input type="hidden" value="899f4c2470f473c822f02eaf69ce20bb1fee694f" name="MAC">
     <input type="hidden" value="refka.abdellaoui@limonetik.com" name="mail">
     <input type="hidden" value="" name="texte-libre">
     <input type="hidden" value="http ://www.citronrose.com" name="url_retour">
     <input type="hidden" value="http ://www.citronrose.com/OK.aspx" name="url_retour_ok">
     <input type="hidden" value="http ://www.citronrose.com/Err.aspx" name="url_retour_err">
     <input type="hidden" value="" name="mobile">
     <input type="hidden" value="" name="options" >
     <input type="hidden" value="480" name="screenwidth">
     <input type="hidden" size="1" value="0" name="is_javascript_enabled">
     <input type="hidden" value="" name="Payment_Card_Type">
     <input type="hidden" value="http ://www.ecml.org/version/1.0" name="Ecom_SchemaVersion">
     <input type="hidden" size="1" name="TransactionComplete">
     <input type="image" alt="Valider" src="/cm/fr/images/std/valider.gif" class="image">
     <a href="http ://www.citronrose.com/Err.aspx" name="">
</form>
```

TABLE 4.3: Exemple de formulaire de paiement CB

```
<?xml version="1.0" encoding="utf-8" ?>
<XmlFormDescription xmlns="http ://www.limonetik.com/LmkXmlFormDescription">
    <ClientName>Cyb</ClientName>
    <Fields>
        <Field>
            <Name>LmkContainsDvc</Name>
            <Type>hidden</Type>
            <ClientValue>true</ClientValue>
            <AddIfMissing>true</AddIfMissing>
            <RemoveServerSide>true</RemoveServerSide>
        </Field>
        <Field>
            <Name>LmkRedirectToPaymOrc</Name>
            <Type>hidden</Type>
            <ClientValue>true</ClientValue>
            <AddIfMissing>true</AddIfMissing>
            <RemoveServerSide>true</RemoveServerSide>
        </Field>
        <Field>
            <Name>Payment_Card_Name</Name>
            <Type>text</Type>
            <ClientValue>#DvcPool_CardHolder</ClientValue>
            <ServerValue>#CardHolder</ServerValue>
        </Field>
        <Field>
            <Name>Payment_Card_Number</Name>
            <Type>text</Type>
            <ClientValue>#DvcPool_FullCardNumber</ClientValue>
            <ServerValue>#FullCardNumber</ServerValue>
        </Field>
        <Field>
            <Name>Payment_Card_ExpDate_Month</Name>
            <Type>select</Type>
            <ClientValue>#DvcPool_MonthNumber2</ClientValue>
            <ServerValue>#MonthNumber2</ServerValue>
        </Field>
        <Field>
            <Name>Payment_Card_ExpDate_Year</Name>
            <Type>select</Type>
            <ClientValue>#DvcPool_YearNumber4</ClientValue>
            <ServerValue>#YearNumber4</ServerValue>
        </Field>
        <Field>
            <Name>Payment_Card_Verification</Name>
            <Type>text</Type>
            <ClientValue>#DvcPool_SecurityTag</ClientValue>
            <ServerValue>#SecurityTag</ServerValue>
        </Field>
        </Fields>
</XmlFormDescription>
```

TABLE 4.4: Exemple de description XML du formulaire de la table 4.3

4.4 Procédure d'intégration

Cette section décrit la procédure d'intégration via Proxy Web en se basant sur les trois étapes d'intégration décrits dans la figure 2.3 qui sont : l'affichage du moyen de paiement, le paiement et le rapprochement. Le but est de montrer, à chaque fois, quelles sont les tâches à effectuer par l'E-commerçant afin d'accomplir chaque étape d'intégration.

4.4.1 Ajout du moyen de paiement

La première phase d'ajout d'un nouveau moyen de paiement est d'ajouter un lien dans la page de choix de moyen de paiement du site marchand qui redirige le client vers la page de paiement. Nous avons vu que le Proxy est capable d'éditer n'importe quelle page du site marchand et de lui ajouter des éléments graphiques divers. Cependant, cet ajout ne doit pas altérer l'expérience utilisateur sur le site E-commerce. C'est pour cela qu'il faut faire attention aux critères ergonomiques de la page et respecter la charte graphique du site marchand. Il s'agit d'un véritable défi technique à relever par le prestataire de paiement alternatif. L'E-commerçant n'intervient pas dans cette phase d'intégration.

Les pages de choix de moyen de paiement sont très différentes d'un site marchand à un autre. Il a fallu également s'adapter à chaque type de page de choix de moyen de paiement. En effet, il a fallu programmer dans chaque configuration Proxy de site, l'insertion du moyen de paiement alternatif différemment suivant que le choix se présente sous forme de liste de liens, de liste déroulante, de radios boutons, etc. Afin d'ajouter un nouveau moyen de paiement, le Proxy tâche d'ajouter un lien au nom du nouveau moyen de paiement dans la liste déjà existante, sans altérer le fonctionnement de l'ancienne liste. Ce nouveau lien redirige le client vers la page de paiement, généralement gérée par le prestataire de paiement alternatif. Le nouveau moyen de paiement doit être bien placé dans la page d'une manière visible afin d'inciter le client à payer avec ce moyen de paiement. Nous présentons quelques exemples d'ajout de nouveau moyen de paiement (par exemple « SaCarte ») via le Proxy Web dans les figures 4.7 et 4.8.

Ces exemples montrent qu'il s'agit d'une insertion élégante et claire pour le client, car ce dernier peut avoir l'impression que c'est le site marchand qui a inséré le nouveau moyen de paiement parmi les autres moyens de paiement acceptés. Cependant, nous notons que cette façon d'ajouter les nouveaux moyens de paiement est très coûteuse en intégration et en maintenance pour le prestataire de paiement alternatif, car elle dépend fortement du site marchand ; si ce dernier change la structure de sa page de

choix de paiement, les expressions régulières utilisées dans la configuration du site ne correspondent plus aux tags HTML en question et, de ce fait, le nouveau moyen de paiement n'est plus inséré.

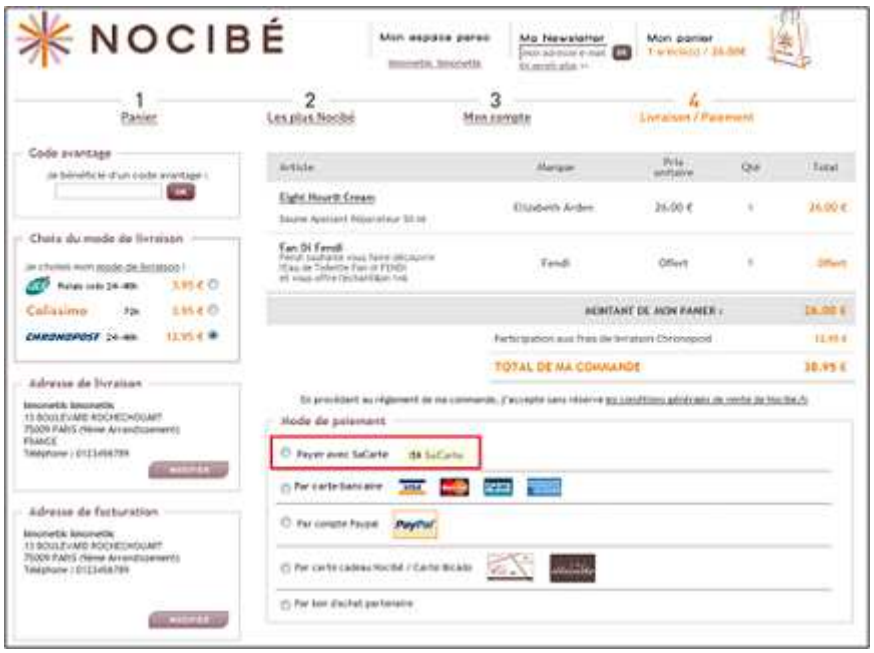


FIGURE 4.7 – Exemple d'ajout d'un nouveau moyen de paiement via le Proxy Web

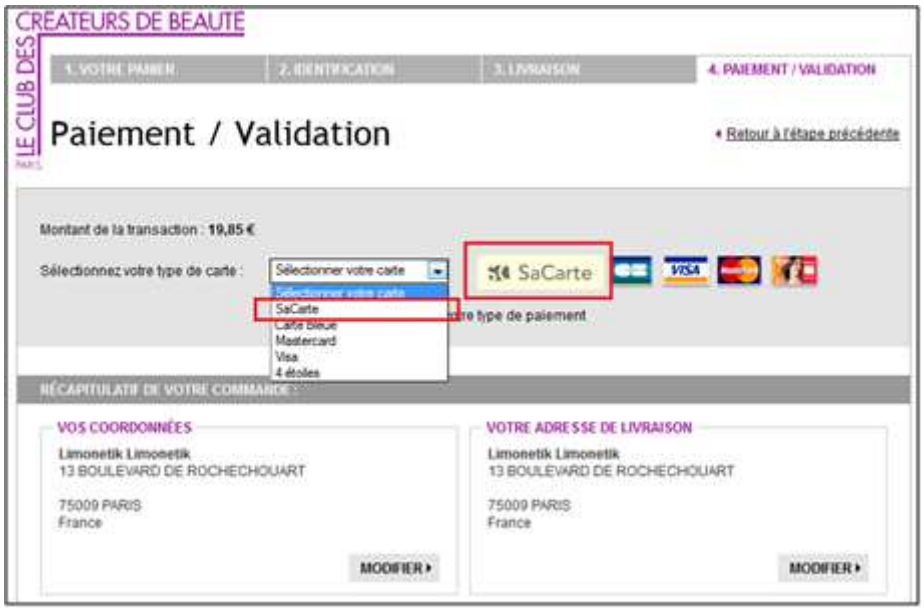


FIGURE 4.8 – Exemple d'ajout d'un nouveau moyen de paiement via le Proxy Web

Sachant que le but de cette intégration est de permettre au marchand d'accepter de nouveaux moyens de paiement, le Proxy Web est configuré de telle sorte que si le

client choisit un autre moyen de paiement déjà accepté par le site, il sera redirigé vers la page de paiement correspondante sans passer par le Proxy Web, ce qui permet de conserver le même niveau de sécurité des paiements proposés par le marchand puisqu'ils ne sont pas interceptés par le serveur du Proxy Web.

4.4.2 Paiement

Une fois que le nouveau moyen de paiement est inséré dans la page de choix du site marchand, la prochaine phase d'intégration d'un système de paiement est le paiement proprement dit (figure 2.3). Dans le cas des systèmes de paiement déportés classiques, le marchand (ou un module CGI installé chez le marchand) se charge d'envoyer les données de la commande nécessaires pour le paiement au prestataire de paiement. Mais, dans notre cas, puisque ce n'est pas le marchand qui effectue l'intégration dans son site Web, il faut récupérer ces données autrement.

Afin de pouvoir afficher la page de paiement, le prestataire de paiement alternatif a besoin essentiellement du montant de la commande et du numéro de la commande chez l'E-commerçant. Comme chaque site E-commerce est différent des autres, la récupération du montant de la transaction doit être réalisée différemment selon les sites marchands. Elle est indispensable pour afficher la page de paiement correspondante avec le bon montant. Cette information est également indispensable pour l'orchestration des paiements par la suite, car, parmi les avantages du nouveau système de paiement, nous trouvons l'agrégation de plusieurs moyens de paiement. Sachant qu'il s'agit d'une information très sensible, il faut s'assurer que le montant récupéré est le vrai montant de la commande (qui ne sera pas mis à jour après suite à une réduction ou l'ajout de frais de livraison, etc.) et que le client ne peut pas corrompre sa valeur. Comme le prestataire de paiement alternatif doit appeler la page de paiement bancaire de l'E-commerçant afin de convertir le paiement alternatif du client (une fois validé) en paiement bancaire et afin de garantir l'intégrité du montant de la commande, nous préconisons deux méthodes de récupération du montant :

1. La première méthode consiste à récupérer le montant depuis la dernière page précédant la page de paiement bancaire du site marchand (intégrée ou déportée) : le Proxy récupère le montant en parcourant la page retournée par le site marchand. L'information est sûre, puisque le client n'a pas pu la corrompre. Il est important que cette page soit la toute dernière page qui précède celle du paiement bancaire afin de s'assurer qu'il s'agit de la valeur communiquée par le marchand à son prestataire de paiement bancaire pour accomplir le paiement bancaire. Mais, cette valeur n'étant pas toujours disponible sur le site marchand, il faut parfois opter pour la deuxième solution.

2. La deuxième méthode consiste à récupérer le montant depuis la page de paiement bancaire du marchand (ou de son prestataire de paiement dans le cas d'un paiement bancaire déporté). Il s'agit d'une méthode très sûre car la valeur récupérée correspond au montant final de la commande à payer. Nous optons donc pour cette méthode pour récupérer la valeur du montant de la commande.

La récupération du montant ne doit pas être effectuée à l'aide d'un Javascript inséré par le Proxy dans la page en question, car cette valeur peut être modifiée facilement par le client. La valeur est récupérée via la configuration du site en essayant de trouver le montant dans la page en utilisant des expressions régulières. Une fois récupérée, cette information est conservée dans la session du client, ce qui permet sa conservation côté serveur d'une manière sécurisée. Sachant que le Proxy Web sera amené à gérer plusieurs sessions en parallèle dans le cas de plusieurs navigations simultanées, les valeurs des montants sont associées à une session d'une manière unique, ce qui permet à un client de naviguer sur plusieurs sites marchands et d'avancer dans les processus d'achat sur ceux-ci en même temps (dans plusieurs fenêtres ou onglets de navigateur). Cependant, un client ne peut naviguer sur un même site marchand dans deux onglets différents, car il s'agira de la même session dans ce cas.

Après avoir récupéré le montant de la transaction, le Proxy Web redirige le client vers le prestataire de paiement alternatif avec les données de la commande. Le prestataire de paiement alternatif peut ainsi afficher la page de paiement correspondante. Nous remarquons ici que le Proxy Web permet de remplacer l'E-commerçant vis-à-vis du prestataire de paiement alternatif. En effet, le Proxy Web effectue l'insertion du moyen de paiement dans la boutique E-commerce à la place du marchand et contacte le prestataire de paiement alternatif au nom de l'E-commerçant également.

Afin de pouvoir payer à la place du client sur le site marchand, le Proxy Web doit pouvoir remplir un formulaire de paiement CB. En effet, comme nous l'avons mentionné lors de la description de la transaction via le Proxy Web, le prestataire de paiement alternatif valide le paiement du client (figure 4.3, flux 2), récupère la carte virtuelle dynamique de la banque intermédiaire (figure 4.3, flux 4) et la transmet au Proxy Web qui paie l'E-commerçant (figure 4.3, flux 5). Pour ce faire, le Proxy Web utilise des fichiers XML qui représentent la structure du formulaire de paiement bancaire de l'E-commerçant. Ces fichiers contiennent les identifiants uniques du formulaire (name ou Id) et les champs invisibles du formulaire qui sont destinés à recevoir les données de la carte bancaire de paiement.

La description du formulaire (fichier XML) associée à une page de paiement est

injectée sous forme de variable Javascript dans la page du site marchand (ou de son prestataire de paiement bancaire). Cette description permet de venir injecter un contenu dans les champs du formulaire de paiement (figure 4.9). Le remplissage du formulaire est effectué deux fois pendant la procédure de paiement de deux manières différentes. La première fois a lieu avant la redirection du client vers la page de paiement alternatif. Les valeurs injectées dans les champs du formulaire bancaire sont des valeurs de test qui permettent seulement de « tromper » les vérifications Javascript de la page Web en question (numéro de carte valide, algorithme de Luhn validé, date d'expiration valide). Cette étape permet d'avoir un formulaire bancaire valide à remplir par la suite avec la vraie CVD.

FIGURE 4.9 – Remplissage du formulaire de paiement bancaire

Le Javascript injecté ajoute également d'autres valeurs dans le formulaire afin d'indiquer au Proxy Web, s'il s'agit du formulaire de paiement et non pas d'un autre formulaire HTML dans la page. Lorsque les champs du formulaire sont remplis et validés par les contrôles de la page HTML, le formulaire est envoyé au serveur du Proxy qui le stocke en session afin de le récupérer plus tard, après le paiement non bancaire. La deuxième étape de remplissage du formulaire bancaire de l'E-commerçant a lieu après le paiement alternatif. Elle permet de remplir les champs de la carte bancaire avec la vraie CVD générée afin de payer le marchand. Contrairement à la première phase de remplissage du formulaire bancaire qui est effectuée à l'aide d'une librairie Javascript, le deuxième remplissage (avec la vraie donnée de la CVD) est effectué de serveur à serveur afin d'éviter qu'un client malveillant puisse récupérer les données de la carte virtuelle dynamique et en détourner l'usage.

4.4.3 Rapprochement

La dernière phase d'intégration est la gestion du rapprochement entre le paiement et la commande chez le site marchand. Dans le cadre de l'intégration via un Proxy Web, cette phase comporte trois sous-étapes qui sont : la récupération du résultat de paiement bancaire, la récupération du numéro de commande et la redirection du client vers le site E-commerce. Toutes les informations liées aux transactions effectuées via Proxy Web sont, par la suite, centralisées dans un back-office accessible à l'E-commerçant, ce qui lui permet de rapprocher les paiements effectués par les clients et les commandes à livrer.

La récupération du résultat de paiement nécessite l'analyse de la réponse envoyée par le serveur de paiement bancaire de l'E-commerçant. Nous nous intéressons, tout d'abord, au cas des paiements bancaires déportés chez un prestataire de paiement. Nous avons étudié les différents scénarios de redirection de client après le paiement bancaire et nous avons relevé deux cinématiques possibles.

FIGURE 4.10 – Cinématique n°1 : l'E-commerçant délègue l'affichage du ticket de paiement à son prestataire de paiement bancaire

Dans la première cinématique, le marchand délègue l'affichage de la page de résultat de paiement à son prestataire de paiement qui affiche le ticket de paiement avec un lien de redirection vers le site marchand (figure 4.10). Sachant que, dans le cas d'un paiement via le Proxy Web, les pages affichées par le prestataire de paiement bancaire ne sont jamais aperçues par le client (car le paiement bancaire est complètement transparent pour lui), le prestataire de paiement alternatif doit alors afficher une page qui permet d'annoncer le résultat de paiement au client, d'afficher le numéro de commande renvoyé par le prestataire de paiement bancaire et de rediriger le client vers le site E-commerce.

Dans la deuxième cinématique, le prestataire de paiement bancaire redirige directement le client vers la page de résultat de paiement de l'E-commerçant, sans afficher aucun ticket de paiement (figure 4.11). Dans ce cas, le Proxy Web redirige le client vers la page de confirmation de l'E-commerçant « proxifiée ». Ainsi, l'expérience utilisateur n'est pas altérée en passant par le Proxy Web et le client prend connaissance

du résultat de son paiement. De plus, le Proxy Web peut récupérer le résultat du paiement bancaire en analysant le contenu HTML de la page de confirmation de l'E-commerçant car elle est proxifiée.

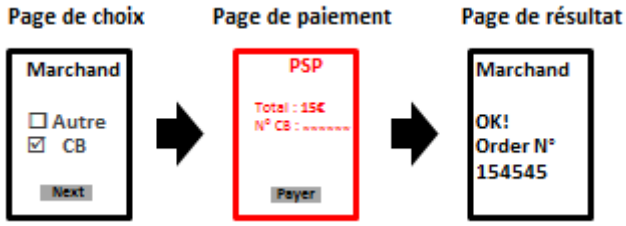


FIGURE 4.11 – Cinématique n°2 : le prestataire de paiement redirige directement le client après le paiement vers le site E-commerce

Nous présentons, dans les figures 4.12 et 4.13, les scénarios de récupération du résultat de paiement et de redirection du client par le Proxy Web, dans le cas des deux cinématiques. Une fois le résultat de paiement récupéré, le Proxy Web peut le communiquer au prestataire de paiement alternatif afin de mettre à jour le statut de la transaction dans le back-office commerçant.

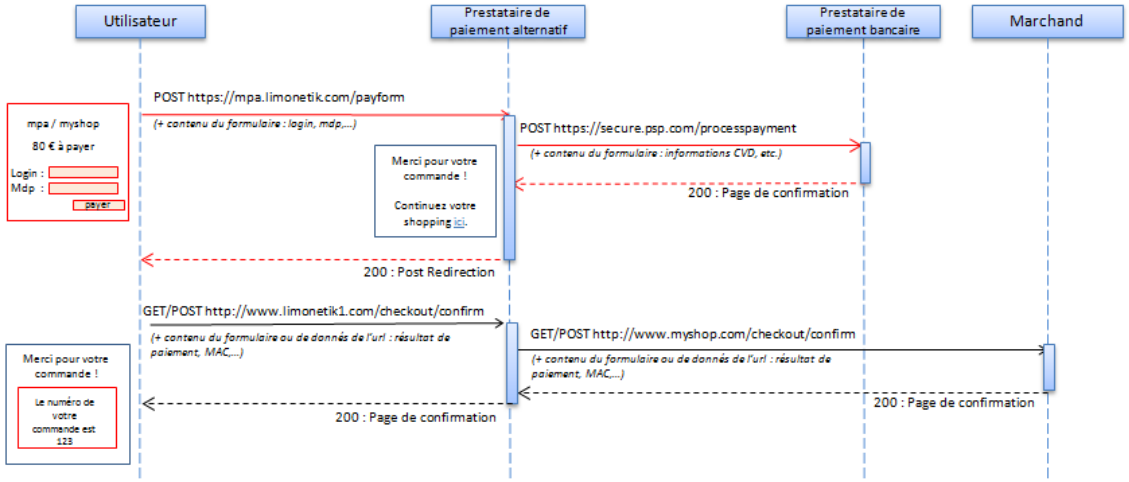


FIGURE 4.12 – Récupération du résultat de paiement par le prestataire de paiement alternatif dans le cas de la cinématique n°1

Dans le cas d'un site E-commerce hébergeant sa page de paiement bancaire, le résultat de paiement est directement envoyé au Proxy Web après l'envoi des données de la CVD. Lors de l'étude de cette cinématique de paiement, nous avons noté quelques problèmes techniques liés généralement au fait que la plupart des pages de confirmation des sites marchands ne peuvent pas être appelées deux fois. En effet, dans le cas de l'intégration via Proxy Web, le contenu de la page de confirmation de

l'E-commerçant est récupéré deux fois : la première fois en réponse à la requête de paiement et la deuxième fois lors de la redirection du client vers le site E-commerce (figure 4.14).

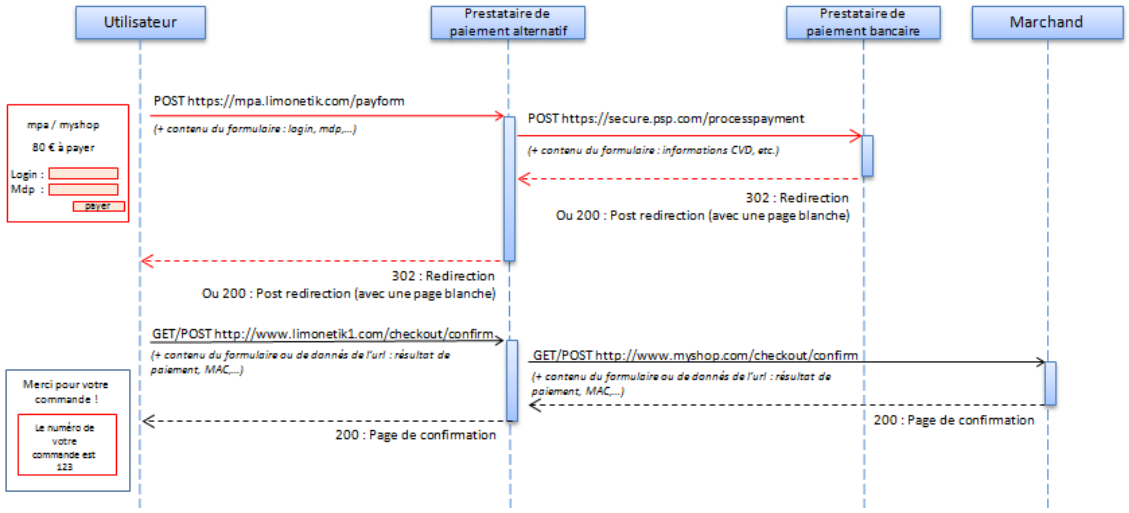


FIGURE 4.13 – Récupération du résultat de paiement par le prestataire de paiement alternatif dans le cas de la cinématique n°2

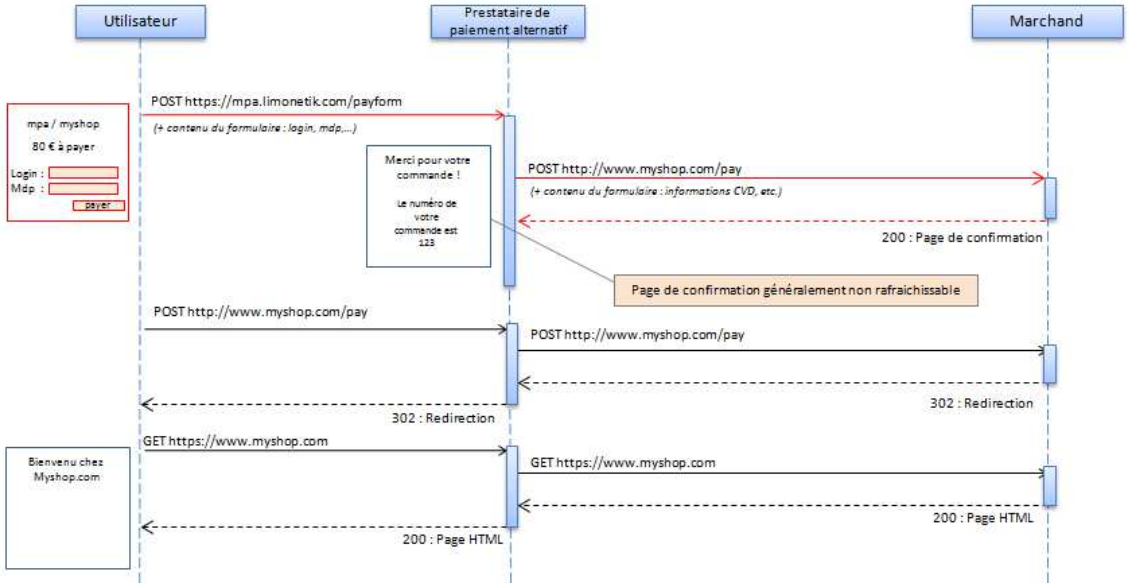


FIGURE 4.14 – Page de confirmation du prestataire de paiement dans le cas d'un paiement intégré

Si la page de confirmation du site marchand n'est pas « rafraîchissable », le client ne sera pas redirigé vers la page de confirmation du marchand, puisqu'elle a été affichée avant (suite à la requête du Proxy) et, dans ce cas, le client sera redirigé

vers une autre page du site marchand, probablement celle d'accueil. Ceci présente un inconvénient majeur, car, généralement, la page de confirmation du site marchand n'affiche pas seulement le résultat de paiement, mais permet également de valider des liens commerciaux avec des partenaires (ce qu'on appelle l'affiliation) et de proposer de nouvelles offres aux clients.

FIGURE 4.15 – Exemple de page de confirmation de paiement d'un site marchand

Nous présentons un exemple de page de confirmation dans la figure 4.15 qui montre que la page de confirmation d'un site marchand peut comporter cinq fonctionnalités en plus de la confirmation de la commande. Ces fonctionnalités sont : la proposition du suivi de commande (figure 4.15, zone 1), le contact client (figure 4.15, zone 2),

la proposition d'impression des détails de la commande (figure 4.15, zone 3), la proposition d'inscription à la newsletter de la boutique (figure 4.15, zone 4) et la proposition d'un chèque de réduction pour les prochaines commandes (figure 4.15, zone 5).

Afin de résoudre ce problème et d'afficher une partie du contenu de la page de confirmation du site marchand, nous proposons d'afficher la confirmation de paiement et le numéro de la commande dans une pop-up insérée dans la page Web du marchand, affichée en réponse à la dernière requête du client (figure 4.15). Etant un Proxy Web, ce dernier peut injecter le code de la pop-up dans le contenu HTML de la page renvoyée par l'E-commerçant en réponse de la requête du client. Un exemple d'affichage de cette pop-up est présenté dans la figure 4.16.

FIGURE 4.16 – Page de confirmation du prestataire de paiement alternatif en mode pop-up

La deuxième étape dans la phase de rapprochement après la récupération du résultat de paiement est la récupération du numéro de la commande chez l'E-commerçant qui permet d'identifier la commande d'une manière unique. Cette donnée doit, également, être récupérée automatiquement en analysant le code HTML des pages interceptées par le Proxy Web. En effet, afin d'identifier la commande, le Proxy Web récupère deux valeurs : le numéro de la commande envoyée par l'E-commerçant et celui affiché par son prestataire de paiement bancaire. Les deux valeurs récupérées sont affichées dans le back-office commerçant qui constitue un tableau de bord permettant au marchand de suivre l'état de ses transactions et d'effectuer les différentes opérations financières en cas de besoin (recrédit, débit, etc.).

Les transactions des paiements alternatifs étant transformées en paiements bancaires, l'E-commerçant peut également les retrouver dans son back-office bancaire et continuer à les traiter comme toutes les autres transactions.

4.5 Validation et limites

Comme nous l'avons présenté dans le premier chapitre de cette étude, plusieurs facteurs doivent être pris en considération lors la conception d'un nouveau système de paiement sur Internet. Dans cette section, nous allons analyser comment la première approche proposée apporte des réponses aux problèmes d'intégration d'un nouveau moyen de paiement et surtout aux principaux freins d'intégration annoncés dans l'état de l'art. Nous étudierons par la suite les limites de ce mode d'intégration.

4.5.1 Validation

La première partie de cette section sera une validation de l'approche d'intégration via Proxy Web selon les critères suivants : la sécurité, l'ergonomie et la complexité.

Sécurité

Nous allons commencer par étudier la sécurité de l'approche proposée en utilisant deux méthodes comme nous l'avons annoncé au chapitre 2.

La première méthode consiste à effectuer une analyse sécuritaire de l'approche proposée. Dans cette analyse, nous partons de l'hypothèse que le site E-commerce est connecté à un prestataire de paiement bancaire d'une manière sécurisée. Nous allons montrer que le paiement alternatif du client est sécurisé, c'est-à-dire que, les flux d'information B, C, D, E, F et G dans la figure 4.17 sont sécurisés et que le système dans son ensemble reste sécurisé. Ayant supposé, dans cette étude, que le système bancaire de l'E-commerçant est sécurisé, le but est donc de prouver la sécurité du paiement alternatif et de sa conversion en paiement bancaire via le Proxy Web. Rappelons que cette conversion est effectuée à l'aide d'une carte virtuelle dynamique, ce qui permet de garantir à l'E-commerçant un paiement sécurisé, conforme à 3D-Secure et non répudiable. La deuxième méthode consiste à prouver que l'approche proposée résiste aux attaques classiques qui peuvent menacer un système de paiement sur Internet. Il ne s'agit pas d'une liste exhaustive d'attaques, mais d'un exemple illustrant le niveau de sécurité du nouveau système. Nous proposons de détailler ces attaques après avoir présenté la première analyse sécuritaire.

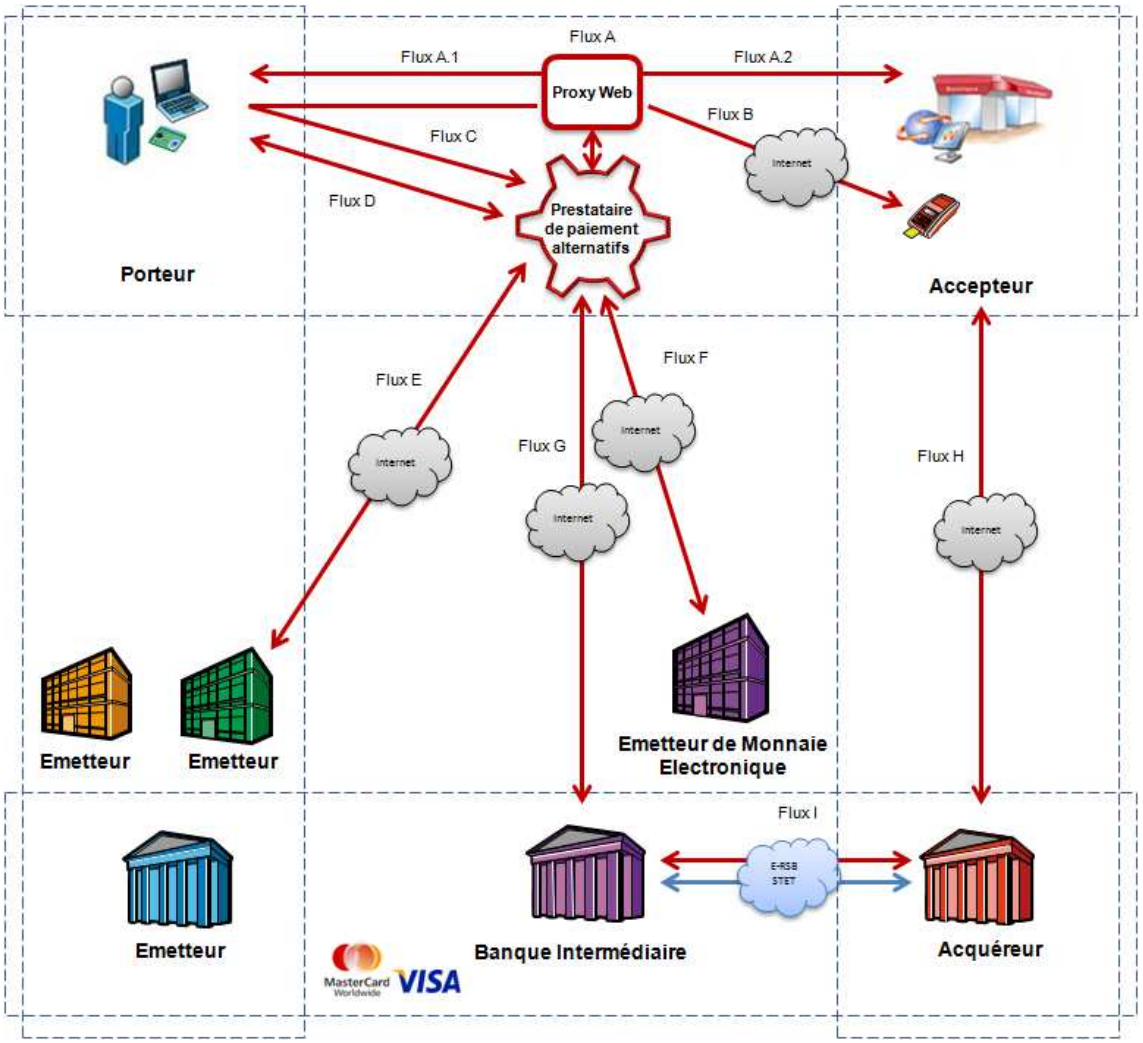


FIGURE 4.17 – Etude de la sécurité de l'intégration via Proxy Web

La communication au sein du flux A est établie entre le client et l'E-commerçant en passant par le Proxy Web. En effet, comme décrit ci-dessus, le client ne navigue pas directement sur le site marchand, d'où les deux flux, A.1 et A.2. De ce fait, le niveau de sécurité de ce flux est inférieur à celui produit par une navigation en direct sur le site. Le Proxy Web a la position, dans cette approche, d'un « Man in The Middle » qui intercepte tous les échanges entre le client et le marchand. Ce qui nous fait perdre le critère de la confidentialité et l'authentification de ce flux. Cependant, comme les données échangées dans le cadre du flux A concernent généralement les données de la commande (adresse de livraison, détail du panier, etc.) et ne sont pas des données de paiement (numéro de carte bancaire, etc.), il n'existe pas de vraie menace de sécurité concernant l'interception de ce flux par le Proxy Web. Certains sites E-commerce, le plus souvent à paiement déporté, ne cherchent même pas à

sécuriser ce flux de communication. L'échange est alors effectué sans passer par le protocole SSL. En revanche, le Proxy Web ne doit stocker aucune information interceptée lors de l'échange d'information au sein de ce flux.

Le Flux B concerne la communication entre le Proxy Web et le terminal de paiement bancaire de l'E-commerçant afin de récupérer la page de paiement bancaire. Ce flux est très important, car il permet au Proxy Web de récupérer les informations de la commande (montant du panier et numéro de la commande). Sachant que le Proxy Web simule le choix de moyen de paiement bancaire sur le site E-commerce afin de récupérer les données à envoyer au terminal de paiement bancaire de l'E-commerçant, le niveau de sécurité de ce flux dépend de celui garanti par le mode d'intégration du terminal de paiement de l'E-commerçant. La communication au sein du flux B est effectuée de deux façons différentes selon la phase de la transaction. Avant la redirection du client vers la page de paiement alternatif, la communication est effectuée en passant par le navigateur du client, car la récupération de la structure du formulaire HTML de paiement bancaire est faite à l'aide d'une librairie JavaScript (figure 4.9). Le niveau de sécurité de cette partie est très dépendant de celui de l'intégration du terminal bancaire dans la boutique E-commerce. En effet, un client malveillant ne peut pas changer les données envoyées à ce stade, car, s'il arrive à le faire, cela veut dire qu'il peut appliquer la même attaque sur le système bancaire du marchand, ce qui contredit notre hypothèse de départ dans le cadre de cette analyse. Après le paiement alternatif du client, la communication au sein de ce flux est effectuée de serveur à serveur sans passer par le navigateur du client. Il s'agit de l'envoi des données d'une carte virtuelle dynamique afin de payer le panier du client. Cet échange est similaire à l'envoi des données bancaires par le client sur la page de paiement du prestataire de paiement bancaire, il s'agit alors d'une communication sécurisée par le protocole SSL.

Le flux C, concerne la redirection du client vers la page de paiement alternatif. Dans le cadre de cette approche d'intégration, le Proxy Web joue le rôle du marchand auprès du serveur du prestataire de paiement alternatif. Il contacte le prestataire afin de lui communiquer les données de la commande et de récupérer l'url de la page de paiement. La communication entre le Proxy Web et le prestataire de paiement alternatif est effectuée via des Services Web (serveur à serveur). Lors de la redirection de client vers la page de paiement alternatif, le Proxy Web envoie un jeton cryptographique au prestataire de paiement alternatif qui lui permet d'identifier d'une manière unique la commande. Un client malveillant ne peut pas ainsi modifier les données de la commande à payer.

Les flux D et E concernent la gestion du paiement non bancaire. Le flux D consiste

à afficher une page de paiement sécurisée afin que le client puisse saisir ses coordonnées de paiement (numéro de carte, login, mot de passe, etc.). Il s'agit d'un flux sécurisé par le partenaire de paiement alternatif (ou éventuellement l'émetteur du moyen de paiement si la page de paiement est hébergée par ce dernier). Il s'agit d'authentifier le client à l'aide de ses données de paiement. Le niveau de sécurité de ce flux dépend alors du type de l'authentification (simple ou forte) en question. Cependant, dans le cadre des paiements alternatifs, le client est généralement authentifié à l'aide d'un seul facteur (mot de passe, date de naissance, code secret, etc.). Ceci était le cas également des paiements bancaires pendant longtemps avant l'invention du protocole 3D-Secure. Le client peut alors répudier son paiement facilement puisqu'il n'est pas fortement authentifié et il ne signe aucune donnée échangée dans ce flux. En revanche, dans la perspective de la conversion du paiement alternatif en paiement bancaire, il a fallu conserver le niveau de sécurité de ce dernier. Nous avons choisi, dans notre approche d'étude de la sécurité, de nous référer au système bancaire 3D-Secure (chapitre 2) qui garantit la non-répudiation des paiements effectués par le client. Pour garantir ce critère, nous avons eu recours à une solution contractuelle (puisque que cette technique s'avère difficile à mettre en place) en imposant aux clients la non-répudiation de leurs paiements alternatifs et en les sensibilisant à l'importance de sécuriser leurs moyens de paiement.

Le flux E contient des informations concernant la demande d'autorisation de paiement, envoyées par le prestataire de paiement alternatif à l'émetteur du moyen de paiement du client. Contrairement au cas des paiements bancaires où la demande d'autorisation est redirigée vers le front-office de la banque « acquéreur » qui se charge de l'aiguiller vers la banque « émetteur », généralement, dans le cas d'un paiement non bancaire, le prestataire de paiement alternatif contacte directement l'émetteur. Dans ce cas, charge au prestataire de paiement et à l'émetteur de convenir d'un protocole de communication sécurisé (généralement basée sur des échanges SSL). Une fois que la demande d'autorisation est attribuée, le prestataire contacte l'émetteur de monnaie électronique (flux F) afin de vérifier les comptes de monnaie électronique de l'émetteur de moyen de paiement et de demander l'autorisation de générer une carte virtuelle dynamique pour payer l'E-commerçant. Les deux entités sont mutuellement authentifiées à l'aide des certificats électroniques et l'échange d'information est réalisé au sein du protocole SSL.

Une fois que l'autorisation de l'émetteur de monnaie électronique est accordée, le prestataire de paiement alternatif contacte la banque intermédiaire pour générer la CVD (flux G). Cette communication est alors soumise aux exigences de sécurité définies par la banque intermédiaire (qui sont relatives à l'usage du moyen de paiement

Carte Virtuelle Dynamique). Les flux H et I sont supposés sécurisés, car ils font partie des flux émis dans le cadre du système de paiement bancaire. Le résultat de cette analyse est présenté dans le tableau 4.5 qui permet de recenser les critères de sécurité garantis par cette approche d'intégration via le Proxy Web.

Flux	Authentification	Confidentialité	Intégrité	Non-Répudiation
Flux A	-	-	-	-
Flux B	x	x	x	-
Flux C	x	x	x	-
Flux D	x	x	x	-
Flux E	x	x	x	x
Flux F	x	x	x	x
Flux G	x	x	x	x
Flux H	x	x	x	x
Flux I	x	x	x	x

TABLE 4.5: Evaluation de la sécurité de l'intégration via Proxy Web

Abordons maintenant l'évaluation de la sécurité de l'intégration via Proxy Web. L'objectif de cette partie est de montrer que l'intégration via Proxy Web est sécurisée et résiste aux différentes attaques décrites dans le tableau 2.2 du chapitre 2. Nous commençons par étudier le scénario d'attaque de l'homme au milieu (tableau 4.6).

Nous allons maintenant nous intéresser à l'attaque de modification et étudier l'impact de ce type d'attaque sur le système proposé. Nous avons choisi d'étudier deux exemples d'attaques : la modification du montant et la modification du résultat de paiement (tableau 2.2) par un client malveillant. La modification du montant ne peut être effectuée qu'au moment de l'appel de la page de paiement bancaire de l'E-commerçant (flux B), car, une fois cette page affichée, le Proxy récupère le montant et le client ne pourra plus le changer. Sachant que le flux B passe par le navigateur du client lors de l'appel de la page de paiement bancaire, nous pouvons imaginer qu'un client malveillant puisse essayer de changer la valeur du montant de son panier. Dans ce cas, le Proxy Web ne peut pas s'en rendre compte, car seul le prestataire de paiement bancaire de l'E-commerçant peut vérifier l'intégrité de ces données. Ayant supposé, au début de cette étude de sécurité, que le système de paiement bancaire du marchand est sécurisé, nous concluons alors que cette attaque ne pourra pas réussir et que le nouveau système résiste à ce type d'attaque. De même, pour la modification du résultat de paiement envoyé par le prestataire de paiement bancaire au marchand, la résistance à cette attaque s'appuie sur le fait que le système bancaire de l'E-commerçant n'y est pas vulnérable.

Dans le cas d'une attaque par Flooding (déni de service) qui consiste à envoyer plusieurs requêtes à une cible, le Proxy Web, bloque toutes les requêtes venant de l'adresse IP de l'attaquant protégeant ainsi l'E-commerçant contre ce type d'attaque.

Flux	Conséquences
Flux A	Un attaquant qui arrive à intercepter ce canal de communication pourra avoir accès à des données personnelles du client : son adresse, sa date de naissance, l'historique de ses commandes, son numéro de téléphone...
Flux B	Avant la page de paiement, ce flux contient les informations de la commande (montant, numéro de la commande) qui ne sont pas des données confidentielles, donc il n'existe pas un risque majeur lié à leur interception par un attaquant. Le risque réside plutôt dans la possibilité de les modifier par « l'homme au milieu ». Cependant, et comme nous l'avons montré dans l'état de l'art, ce flux garantit l'intégrité et l'authenticité des données envoyées grâce à la politique de sécurité choisie par le prestataire de paiement bancaire de l'E-commerçant. En revanche, après le paiement alternatif du client, si un attaquant arrive à intercepter les données de la CVD envoyées, il ne pourra pas en tirer profit systématiquement, car il s'agit de carte de paiement à usage unique. Cela veut dire qu'il doit l'utiliser dans les secondes qui suivent son interception, avant que le paiement soit validé par le terminal de paiement bancaire de l'E-commerçant.
Flux C	Si un attaquant réussit à intercepter ce flux de communication, il peut rediriger le client vers une « fausse » page de paiement afin d'intercepter les données de paiement du client.
Flux D	Si un attaquant intercepte ce flux, il sera en possession des données de paiement du client qu'il peut utiliser plus tard.
Flux E	Il s'agit du flux de demande d'autorisation de paiement, qui ne contient donc pas de données confidentielles, cependant, un attaquant interceptant ce flux peut essayer de causer des dégâts à l'émetteur en autorisant systématiquement toutes les demandes de paiement. Une attaque qui nécessite de forger la signature de l'émetteur.
Flux F	Ce flux ne contient pas de données confidentielles. Cependant, si l'attaquant arrive à modifier les données échangées dans ce flux, il peut causer des dégâts financiers pour l'émetteur de monnaie électronique en acceptant de générer des CVDs sur son compte sans vérifier les comptes de monnaie électronique des émetteurs.
Flux G	Un attaquant qui arrive à intercepter ce flux, peut avoir accès à la CVD de paiement. Par contre, il faut qu'il l'utilise très rapidement avant que le prestataire de paiement alternatif l'utilise pour payer le marchand (un délai estimé à 1 minute maximum), car il s'agit d'un numéro de carte à usage unique.

TABLE 4.6: Etude des impacts de l'attaque de l'homme au milieu dans le cas de l'intégration via Proxy Web

Ergonomie

Du point de vue de l'ergonomie du site marchand, nous notons que l'intégration via Proxy altère légèrement l'expérience utilisateur, celui-ci ayant généralement tendance à aller directement sur le site E-commerce afin d'utiliser son moyen de paiement et non pas à passer par un portail. Cette modification de l'expérience utilisateur peut être considérée comme un inconvénient de cette approche d'intégration. Il est important, également, de rassurer le client tout au long de sa navigation. Il ne faut pas qu'un site E-commerce « proxifié » ressemble à du phishing. Dans ce but, nous avons décidé d'insérer une barre en bas des pages Web en permanence. Cette barre affiche le logo du prestataire de paiement alternatif et de l'émetteur du moyen de paiement alternatif afin de rassurer l'utilisateur. En plus de cette barre, la configuration proxy des sites E-commerce permet de rester le plus fidèle possible à l'ergonomie du site en question comme nous pouvons le constater dans les deux exemples de page proxifiée présentés dans les figures 4.8 et 4.7.

Complexité

Dans la nouvelle approche d'intégration via Proxy Web, et afin d'accepter des nouveaux moyens de paiement, il suffit que l'E-commerçant intègre un système de paiement bancaire. Le marchand n'intervient dans aucune étape de l'intégration du système de paiement alternatif. Le Proxy Web ajoute dynamiquement le nouveau moyen de paiement parmi les autres choix de moyen de paiement sans modification du site E-commerce, ce qui réduit l'intégration technique chez le marchand, qui constitue un des freins majeurs à l'acceptation d'un nouveau moyen de paiement, à zéro jours/homme. Ainsi, plusieurs moyens de paiement peuvent être ajoutés dynamiquement dans une boutique E-commerce sans aucune intégration technique du côté de l'E-commerçant. Par ailleurs, l'E-commerçant n'a pas à traiter de nouveaux flux financiers, car tous les nouveaux paiements sont convertis en paiements bancaires. Le prestataire de paiement alternatif gère les paiements non bancaires (page de paiement, demande d'autorisation, etc.) et les transforme en paiement par carte bancaire accepté par l'E-commerçant. De plus, le marchand n'a pas à gérer l'orchestration de plusieurs moyens de paiement, le prestataire de paiement alternatif s'en occupe et génère un seul paiement par carte bancaire à la fin. Il gère également les différents flux financiers liés aux transactions (demande d'autorisation, débit, remboursement, etc.). Les nouveaux paiements sont transformés en paiements par carte virtuelle dynamique afin qu'ils soient traités de la même manière que les autres paiements bancaires sur le site E-commerce. De plus, en transformant les paiements alternatifs en paiements bancaires, le prestataire de paiement alternatif permet de garantir à

l'E-commerçant un paiement sécurisé, non répudiable et conforme à 3D-Secure.

4.5.2 Limites

Malgré tous les avantages que présente ce mode d'intégration pour les sites E-commerce et les émetteurs des moyens de paiement alternatifs, le prestataire de paiement alternatif doit fournir un grand travail afin de maintenir les configurations des sites marchands à jour et de garantir une bonne qualité de service. Lors de l'implémentation et la validation de cette approche d'intégration, nous avons effectué une étude sur un panel représentatif des sites E-commerce francophones (La Redoute, La Fnac, Priceminister, 3Suisses, La Camif, Lastminute, Yves Rocher, King-Jouet, MyPix, Boulanger, Quelle, CDiscount, etc.) qui montre que les sites sont rarement valides : le HTML / XHTML des sites Web ne respecte pas les recommandations et les bonnes pratiques du W3C. Nous avons également noté des erreurs Javascript qui sont déclenchées automatiquement sur certaines pages des sites. Donc il a fallu corriger ces erreurs dans les configurations de sites marchands afin de pouvoir injecter correctement du code HTML dans les pages. Sans oublier que les sites changent régulièrement. Sur une période de deux mois, presque tous les sites ont subi des modifications mineures ou majeures. Certains sites ont été largement modifiés. Comme nous l'avons signalé dans l'étude de l'ergonomie de ce mode d'intégration, l'expérience utilisateur est légèrement modifiée, car le client doit démarrer sa navigation depuis un portail et non pas depuis le site E-commerce en direct.

4.6 Conclusion

Nous avons présenté dans ce chapitre une approche d'intégration de la nouvelle architecture de paiement décrite dans le chapitre 3. Il s'agit d'une approche qui permet de contourner les problèmes d'intégration des nouveaux moyens de paiement sur Internet en passant par un Proxy Web qui permet d'effectuer l'intégration du nouveau système de paiement à la place de l'E-commerçant. Nous avons présenté le principe de fonctionnement du Proxy Web ainsi que les différentes étapes d'intégration du moyen de paiement alternatif. Ensuite, nous avons évalué ce nouveau mode d'intégration selon les critères annoncés dans l'état de l'art (la sécurité, l'ergonomie et la complexité). Nous résumons cette évaluation dans le tableau 4.7 qui présente les avantages et les inconvénients de ce mode d'intégration.

Cette approche a été implémentée et testée au sein de « Limonetik », le partenaire industriel de nos travaux de recherche. Plusieurs moyens de paiement ont pu ainsi être acceptés par un grand nombre de sites marchands, sans que ces derniers

aient à effectuer du développement technique de leur côté. L'intégration via Proxy Web s'avère donc sans aucun coût ni complexité pour le site marchand. De plus, cette intégration permet à l'E-commerçant de proposer un système de paiement non bancaire (alternatif) sécurisé. Cependant, elle modifie le parcours client qui est obligé de démarrer sa navigation depuis un portail et non pas directement depuis le site marchand. Nous démontrons, dans le tableau récapitulatif 4.7, que ce mode d'intégration présente plusieurs avantages pour les sites E-commerce, car, contrairement aux autres modes d'intégration, l'E-commerçant n'a aucune intégration technique à effectuer. Toute la complexité de l'intégration est reportée chez le prestataire de paiement alternatif qui doit s'assurer continuellement que le Proxy Web est opérationnel. Cependant, la nouvelle approche d'intégration, telle qu'elle est conçue, ne gère pas uniquement le paiement, mais également la navigation du client sur le site E-commerce afin de lui permettre de choisir son moyen de paiement parmi ceux acceptés par l'E-commerçant, ce qui exige une maintenance très coûteuse du côté du Proxy Web. C'est pour cette raison que nous avons cherché une deuxième approche d'intégration qui permet d'avoir une solution moins dépendante des évolutions des pages Web du site marchand et qui demande un minimum d'intégration à l'E-commerçant. Cette nouvelle approche sera présentée dans le chapitre suivant.

	Sécurité	Ergonomie	Complexité
Avantages	- Les données de la commande (montant, référence...), envoyées au prestataire de paiement alternatif, sont sécurisées, car il s'agit des même données envoyées au prestataire de paiement bancaire de l'E-commerçant (supposé sécurisé). - Un client malveillant ne peut pas modifier le montant de la commande, ni le résultat du paiement - L'envoi des données de la CVD à l'E-commerçant, qui permet de convertir le paiement alternatif en paiement bancaire, se fait de serveur à serveur, donc le client ne peut pas intercepter cette donnée. - La CVD correspond à un montant fixe et est à usage unique, ce qui limite les risques de fraude.	- Le nouveau moyen de paiement est inséré parmi ceux acceptés par l'E-commerçant, tout en respectant la charte graphique du site E-commerce. - La proxification du site E-commerce est effectuée sans modification de ses pages Web.	- Les moyens de paiement alternatifs sont acceptés sur le site E-commerce sans que l'E-commerçant ait à s'investir dans un développement technique. Le coût d'intégration est donc réduit à zéro euro. - Le paiement alternatif est converti en paiement bancaire, l'E-commerçant n'a pas donc à traiter de nouveaux flux financiers. - Plusieurs moyens de paiement peuvent être ajoutés par le Proxy Web sans développement technique du côté de l'E-commerçant. - L'orchestration de plusieurs moyens de paiement du client est également géré par le prestataire de paiement alternatif.
Inconvénients.	- Le Proxy intercepte la communication entre le client et l'E-commerçant tout au long de la navigation sur le site (adresse du client, données d'authentification au compte du client sur le site...).	- La navigation sur le site « proxifié », qui n'a pas la même Url que le site en direct, peut ressembler à du « phishing » et par conséquent, ne pas rassurer le client. - Le client doit démarrer sa navigation depuis un portail et non pas depuis le site en direct. - Les configurations Proxy de sites E-commerce sont fortement dépendantes des ces derniers, si un site change la structure de sa page de choix de paiement, les expressions régulières utilisées dans la configuration de ce site ne correspondent plus aux tags HTML en question et, de ce fait, le nouveau moyen de paiement n'est plus inséré.	

TABLE 4.7: Avantages et inconvénients de l'intégration via Proxy Web

Chapitre 5

Proposition d'intégration via Plugin JavaScript

Le chapitre précédent présente une première approche d'intégration de l'architecture de paiement proposée dans le chapitre 3. Il s'agit d'une intégration via Proxy Web sans aucune intégration technique chez l'E-commerçant. Cependant, cette approche présente quelques limites. Ce chapitre propose une deuxième approche d'intégration via Plugin Javascript. Tout d'abord, nous décrivons le principe de fonctionnement de ce mode d'intégration (section 5.2), ainsi que le processus de redirection du client (section 5.4). Nous présentons par la suite la procédure d'intégration (section 5.5). Puis, nous validons l'approche proposée selon l'état de l'art (section 5.6) afin d'en déduire les avantages et les inconvénients. Enfin, nous soumettons une amélioration de cette approche en utilisant des automates de paiement (section 5.7).

Sommaire

5.1 Introduction

Nous avons présenté dans le chapitre précédent une première proposition de mode d'intégration de la nouvelle architecture décrite dans le chapitre 3, via Proxy Web. En effet, afin de faciliter l'intégration des nouveaux moyens de paiement non bancaire (alternatifs) via la nouvelle architecture de paiement, l'idée était de créer une entité qui effectue l'intégration technique du système de paiement alternatif à la place de l'E-commerçant, de façon que ce dernier n'ait aucun développement technique à réaliser. Cette entité est un Proxy Web qui intercepte la communication entre le client et l'E-commerçant ce qui lui permet d'injecter du code HTML dans les pages Web du site E-commerce et ajouter ainsi dynamiquement le nouveau moyen de paiement alternatif. De ce fait, le moyen de paiement alternatif est accepté par l'E-commerçant et le client peut l'utiliser pour payer sa commande. Or, nous avons constaté que, malgré les avantages majeurs de ce mode d'intégration pour l'E-commerçant, il présente quelques inconvénients, notamment la forte dépendance de toutes les pages Web du site marchand (non seulement celles concernant le paiement) et la nécessité d'une maintenance continuelle des configurations Proxy des sites E-commerce afin de prendre en compte les modifications des pages Web des sites. Ces inconvénients nous ont amené à proposer une deuxième approche d'intégration moins dépendante du parcours client sur le site E-commerce tout en facilitant l'intégration technique pour l'E-commerçant.

5.2 Plugin JavaScript : principe

Nous proposons, dans ce chapitre, un nouveau mode d'intégration du nouveau système de paiement en utilisant des Plugin JavaScript. En informatique, le terme Plugin désigne *un paquet qui complète un logiciel hôte pour lui apporter de nouvelles fonctionnalités* [Wikipedia, 2000a]. En effet, il s'agit d'une librairie JavaScript qui est destinée à compléter une page « hôte » (la page Web du site E-commerce qui l'appelle) afin de permettre la redirection du client vers le moyen de paiement alternatif. Contrairement au premier mode d'intégration (Proxy Web), cette méthode impose à l'E-commerçant d'effectuer quelques développements techniques dans son site E-commerce afin d'ajouter le nouveau moyen de paiement parmi la liste des moyens de paiement acceptés sur son site et un lien vers le Plugin JavaScript. Une fois que le nouveau moyen est ajouté par l'E-commerçant, le Plugin se charge de rediriger le client vers la page de paiement correspondante. Dans ce cas, le client navigue sur le site E-commerce en direct (sans passer par un portail), remplit son panier et valide sa

commande. La liste de choix de moyens de paiement affichée au client contient alors le nouveau moyen de paiement (ajouté au préalable par l'E-commerçant). Le choix de ce moyen de paiement redirige le client vers la page de paiement correspondante (grâce au Plugin JavaScript intégré dans le site E-commerce).

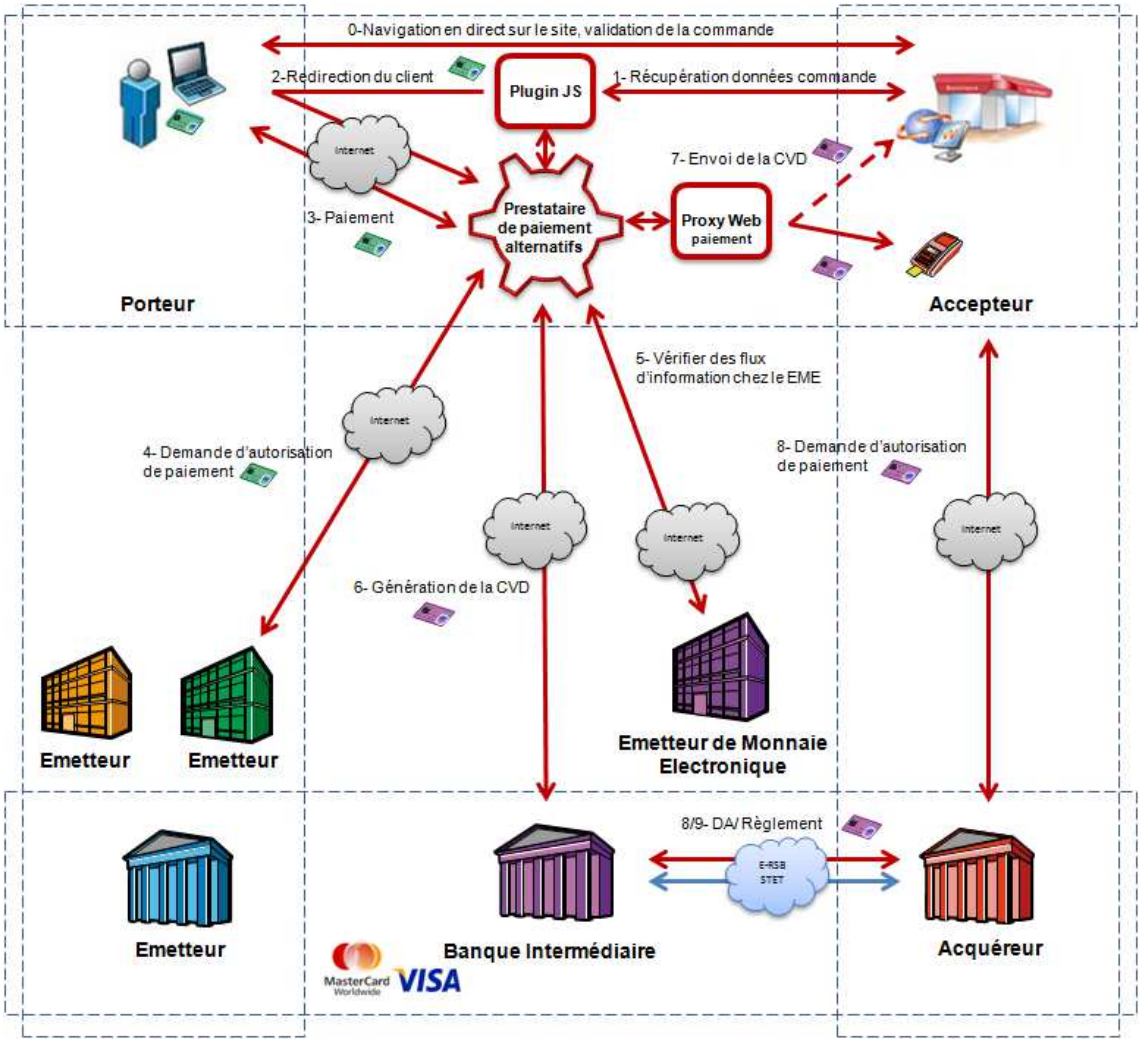


FIGURE 5.1 – Transaction via Plugin JavaScript

La figure 5.1 montre que le client navigue directement sur le site Web de l'E-commerçant sans passer par le Proxy, ce qui permet d'éliminer un des inconvénients de la première intégration proposée qui consiste à maintenir toute la navigation du client depuis la page d'accueil du site jusqu'à la page de choix de moyen de paiement. Cependant, le prestataire de paiement alternatif a besoin de récupérer les données de la commande (montant de la commande, référence du marchand, etc.). Pour ce faire, il existe deux possibilités :

1. La première possibilité consiste à demander ces informations à l'E-commerçant.

Dans ce cas, il faut sécuriser l'envoi de ces données. Cette solution revient à proposer à l'E-commerçant un des modes d'intégration décrits dans l'état de l'art (chapitre 2).

2. La deuxième possibilité consiste à utiliser le Proxy Web pour récupérer ces informations de la façon décrite dans le chapitre précédent. Pour cela, il faut « proxifier » la page de paiement bancaire du site E-commerce. Ensuite, le Proxy Web envoie les données de la commande à la place de l'E-commerçant.

La première proposition a été rapidement éliminée, car le but de nos travaux de recherche est de proposer un système de paiement facile à intégrer. Nous avons alors retenu la deuxième solution. Avant d'aller plus loin, une définition de quelques éléments techniques s'avère nécessaire pour la compréhension de la suite du chapitre.

5.3 Quelques éléments techniques

Avant de décrire le processus d'intégration via Plugin JavaScript, nous avons besoin d'expliquer quelques notions techniques.

5.3.1 Langage JavaScript

Le JavaScript est un langage de script incorporé dans un document HTML mis au point par Netscape en 1995. Historiquement, il s'agit même du premier langage de script pour le Web. Ce langage est un langage de programmation qui permet d'apporter des améliorations au langage HTML en permettant d'exécuter des commandes du côté client, c'est-à-dire au niveau du client (navigateur) et non du serveur Web. Ainsi, le langage Javascript est fortement dépendant du navigateur appelant la page Web dans laquelle le script est incorporé. Mais, en contrepartie, il ne nécessite pas de compilateur, contrairement au langage Java, avec lequel il a longtemps été confondu. Un script est une portion de code qui vient s'insérer dans une page HTML. Le code du script n'est toutefois pas visible dans la fenêtre du navigateur, car il est compris entre des balises (ou tags) spécifiques qui signalent au navigateur qu'il s'agit d'un script écrit en langage JavaScript. Il s'agit de la balise <SCRIPT>. Un script JavaScript permet de récupérer plusieurs informations contenues dans la page qui l'héberge et d'exécuter certaines commandes du côté du client. D'où l'intérêt de proposer une intégration via un Plugin écrit en JavaScript. Cependant, malgré les avantages de ce langage, il faut faire attention aux informations manipulées par le code JavaScript, car il s'agit d'un code interprété par le client et donc vulnérable. Un des problèmes techniques qui peut se présenter est le risque

d'avoir des réactions différentes selon le navigateur du client et notamment avec Internet Explorer de Microsoft qui propose une version de JavaScript différente de ce que préconise la norme. Donc, il faut s'assurer le Plugin JavaScript est compatible avec tous les navigateurs.

5.3.2 DOM : Document Object Model

Le DOM (Document Object Model) est très utilisé en JavaScript, il s'agit d'une description structurée d'un document HTML ou XML qui permet d'accéder individuellement à chaque élément du document HTML. Il permet également de construire une arborescence de la structure d'un document et de ses éléments comme l'indique la figure 5.2.

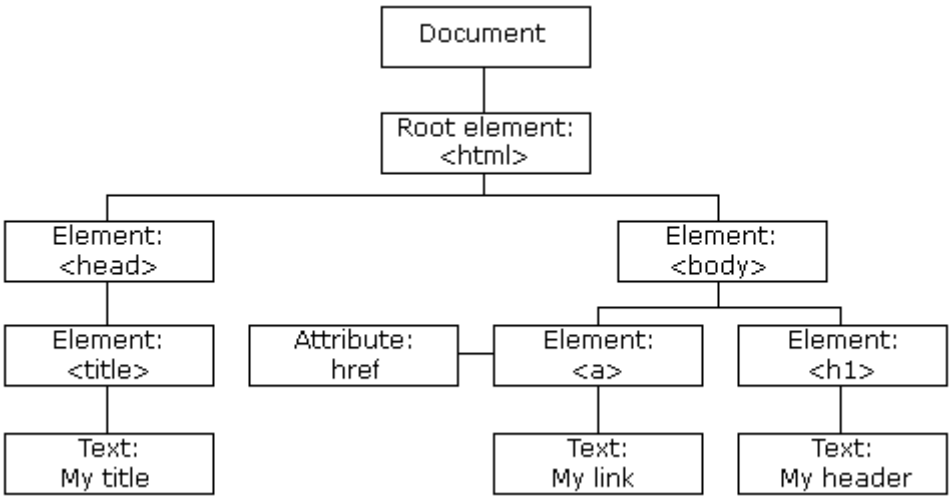


FIGURE 5.2 – Exemple d'arbre DOM d'un document HTML

Il s'agit d'un arbre avec des noeuds où chaque noeud est un objet pour lequel on peut définir une série de méthodes et de propriétés avec lesquelles on peut interroger et modifier n'importe quel élément d'un document HTML. Le DOM est généralement utilisé pour pouvoir modifier facilement des documents HTML ou XML ou accéder au contenu des pages Web. Dans notre contexte, il est utilisé afin de parcourir les pages Web du site marchand (page de choix de moyen de paiement, page de paiement bancaire, etc.) afin d'identifier et mettre à jour des éléments des pages et manipuler des formulaires HTML. Le DOM gère spécialement trois variables importantes : « document » qui permet d'accéder et de manipuler les contenus et les styles d'une page, « window » qui permet de récupérer des informations sur les fenêtres et la création de nouvelles fenêtres et « navigator » qui permet de

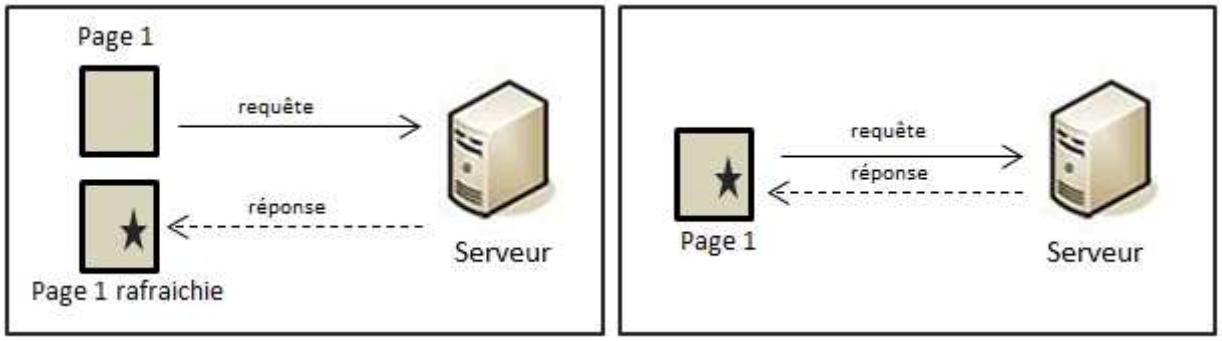
récupérer des informations sur le navigateur. Un exemple d'utilisation du DOM dans le JavaScript est présenté dans la table 5.1. Le code en souligné représente les éléments liés au DOM. Nous pouvons constater alors la forte utilisation du DOM par le langage JavaScript.

```
var listeBalisesA = document.getElementsByTagName("a");
if(listeBalisesA.length == 0)
    alert("Aucune balise <a>");
var listeForms = document.forms;
for (i = 0; i < listeForms.length; i++) {
    var form = listeForms[i];
    alert("action form : " + form.action);
}
```

TABLE 5.1: Utilisation du DOM dans un code JavaScript

5.3.3 AJAX : Asynchronous JavaScript And XML

Le terme AJAX a été introduit par Jesse James Garrett en 2005, dans un article sur le site Web Adaptive Path [Garrett J., 2005]. Depuis, il a rapidement gagné en popularité. Il s'agit d'une technique qui fait usage des éléments suivants : HTML, CSS, Javascript et DOM. Le terme « Asynchronous » dans « Asynchronous JavaScript And XML », signifie que l'exécution de JavaScript continue sans attendre la réponse du serveur qui sera traitée quand elle arrivera tandis qu'en mode synchrone, le navigateur serait « gelé » en attendant la réponse du serveur.



Sans Ajax Avec Ajax

FIGURE 5.3 – Comparaison de la mise à jour d'une page Web sans et avec Ajax

Avant l'arrivée d'AJAX, il fallait rafraîchir toute la page Web afin de la mettre à jour. Ajax permet de modifier partiellement la page affichée par le navigateur pour la mettre à jour sans avoir à recharger la page entière (figure 5.3). Par exemple, le

contenu d'un champ d'un formulaire HTML peut être changé, sans avoir à recharger la page avec le titre, les images, le menu, etc. Ajax permet ainsi d'effectuer des traitements sur le poste client (avec JavaScript) à partir d'informations prises sur le serveur. Auparavant, toutes les modifications de pages étaient faites sur le serveur, ce qui nécessitait des échanges maintenant inutiles. Ajax a simplifié l'interaction entre le client et le serveur Web en envoyant notamment de l'information au serveur de manière transparente ou encore en s'affranchissant du rafraîchissement de la page Web. Le plugin JavaScript utilise Ajax afin d'effectuer des appels au serveur du site marchand d'une manière totalement transparente pour le client. Nous allons voir, dans les prochaines sections, le type de ces appels et leur intérêt.

Ajax permet la communication avec le serveur distant grâce à l'objet XMLHttpRequest. Pour recueillir des informations sur le serveur, cet objet dispose de deux méthodes : open (établit une connexion) et send (envoie une requête au serveur). Les données fournies par le serveur seront récupérées dans les champs de l'objet XMLHttpRequest : responseXml pour un fichier XML ou responseText pour un fichier de texte brut. Le Cross-domain (croisement de domaine) est un principe qui vise à faire communiquer deux domaines ensemble. Par exemple, site1.com peut envoyer des données à site2.com, tout comme ce dernier peut renvoyer des données à site1.com. La plupart des techniques AJAX ne sont pas cross-domain pour des raisons évidentes de sécurité ; pour qu'une application cross-domain fonctionne, il faut que le domaine qui reçoit la requête soit autorisé à la traiter, il s'agit d'une mesure de sécurité obligatoire. Cette contrainte de sécurité risque de rendre l'intégration via Plugin JavaScript contraignante.

5.3.4 Cookies

Le protocole HTTP est dit « stateless » ou sans état. Pour un serveur, chaque requête qu'il reçoit est indépendante de la précédente, ainsi que de la suivante. Cela peut être gênant à plusieurs titres : le serveur ne peut pas se rappeler si le client a été authentifié à une page donnée, il n'est pas en mesure de conserver les paramètres ou les préférences utilisateur ni l'historique de la navigation du client, etc. D'où l'intérêt des cookies, inventés par Netscape, afin de donner une « mémoire » aux serveurs et aux navigateurs Web et remédier ainsi à ces problèmes. Il existe d'autres solutions pour les contourner, mais les cookies sont très simples à maintenir et très souples d'emploi. Un cookie n'est rien d'autre qu'un petit fichier texte stocké par le navigateur qui peut être lu par un code JavaScript. Il contient certaines données :

- Une paire nom/valeur contenant les informations.
- Une date d'expiration au-delà de laquelle il n'est plus valide.

- Un domaine indiquant quel répertoire de quel serveur y aura accès.

En rajoutant l'en-tête Set-Cookie, dans sa réponse, le serveur indique au client (navigateur) qu'il souhaite y stocker un cookie. Le client crée le cookie demandé et le joint ensuite à l'en-tête de toutes les requêtes vers le même serveur. Le serveur peut alors le lire et décider, par exemple, si le client a le droit de voir la page ou si le client a déjà rempli son panier. Cependant, les cookies peuvent nuire à la vie privée des clients, car ils permettent de mémoriser les préférences des utilisateurs sur les sites Web. De plus, les cookies figurent dans les en-têtes HTTP. Si l'échange entre le serveur et le client n'est pas sécurisé (sous SSL), ces en-têtes peuvent être consultées et modifiés par n'importe quelle entité qui intercepte la communication. Afin de sécuriser certains cookies, plusieurs solutions ont été apportées : le chiffrement qui permet de les rendre confidentiels, le hachage qui permet d'empêcher leur modification ou l'activation de l'attribut HTTPOnly du cookie qui permet d'empêcher sa manipulation par JavaScript ou tout autre interpréteur pouvant y accéder. Le cookie ne sera envoyé que par HTTP, et stocké dans une zone mémoire sûre sur le navigateur. Cet attribut est d'une importance capitale pour contrer les attaques de vol de session. Par contre, il n'est pas utilisé par défaut, car, si le navigateur ne connaît pas ce type de cookie, ce qui est surtout le cas des anciens navigateurs, il risque tout simplement de l'ignorer. Nous verrons dans la suite du chapitre, que, dans certains cas, le Plugin Javascript a besoin de récupérer la session du client afin de démarrer une navigation via le Proxy Web. L'activation de l'attribut HTTPOnly peut alors mettre en péril le fonctionnement du Plugin Javascript intégré dans le site E-commerce.

5.3.5 Session

Maintenant qu'on a vu qu'on peut garder une trace d'un utilisateur grâce aux cookies, la session vient pallier un défaut des cookies, qui est leur faible capacité de stockage. En effet, les données de session sont un fichier stocké non pas sur le disque du visiteur, mais sur le serveur (à l'inverse du cookie). Ainsi, il est impossible d'avoir accès aux variables de session via JavaScript par exemple. De plus, elles ne transitent pas sans arrêt entre le navigateur et le serveur (à la différence des cookies). Une session permet, comme le cookie, de stocker temporairement des valeurs relatives à un même internaute dans un même contexte de navigation. Les sessions ont plusieurs utilités, elles sont utilisées généralement en complément des cookies dans les scripts d'identification, car, parfois, le navigateur du client n'accepte pas les cookies, et donc dans ce cas, la session remplace parfaitement le cookie, stocke l'identifiant du client et son mot de passe chiffré afin de l'authentifier dans ses prochaines requêtes pendant la durée de la session (qui est définie par le serveur).

5.4 Processus de redirection

L'intégration via Plugin JavaScript consiste à demander à l'E-commerçant d'ajouter le nouveau moyen de paiement parmi la liste des autres moyens de paiement acceptés sur son site et d'appeler une librairie JavaScript lorsque le client choisit ce moyen de paiement. Le Plugin se charge, ensuite, de rediriger le client vers le prestataire de paiement alternatif. Lors de cette redirection, le Plugin doit transmettre au prestataire de paiement alternatif les éléments nécessaires à l'affichage de la page de paiement bancaire de l'E-commerçant (où le montant de la commande sera affiché). Il s'agit des données envoyées par l'E-commerçant à son prestataire de paiement bancaire lorsque le client choisit de payer avec sa carte bancaire. Dans le cas d'un site E-commerce qui héberge sa page de paiement bancaire (paiement intégré), le Plugin JavaScript doit alors envoyer les données de la session du client au prestataire de paiement alternatif lors de la redirection du client. Nous présentons dans la figure 5.4 plus en détail les échanges entre le client et le serveur de l'E-commerçant dans le cas d'un paiement bancaire intégré.

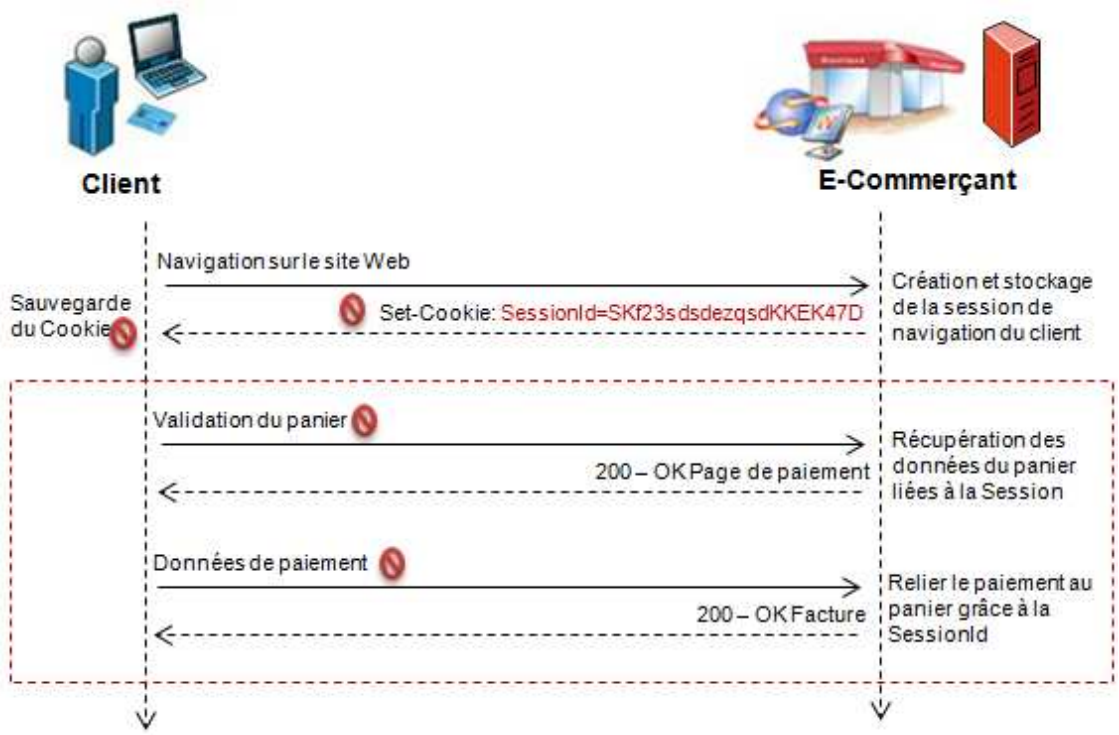


FIGURE 5.4 – Gestion de la session dans le cas d'un paiement intégré

En effet, le marchand se base sur les données liées à la session afin de présenter la page de paiement au client. Donc, si le prestataire de paiement alternatif souhaite se substituer au client pour demander la page de paiement bancaire et payer la

commande à sa place, il doit disposer des cookies de ce dernier qui lui permettent de s'authentifier auprès du serveur de l'E-commerçant. Cependant, dans le cas d'un paiement bancaire déporté, la session du client (liée à sa navigation sur le site marchand) n'est pas indispensable pour récupérer la page de paiement. Comme nous pouvons le constater dans la figure 2.4, lors de la demande de la page de paiement, le client n'est pas encore authentifié chez le prestataire de paiement (pas de session ni de cookie défini sur le serveur de ce dernier). Le prestataire de paiement bancaire se base uniquement sur les données envoyées dans la requête afin de retrouver les données de la commande et afficher la page de paiement.

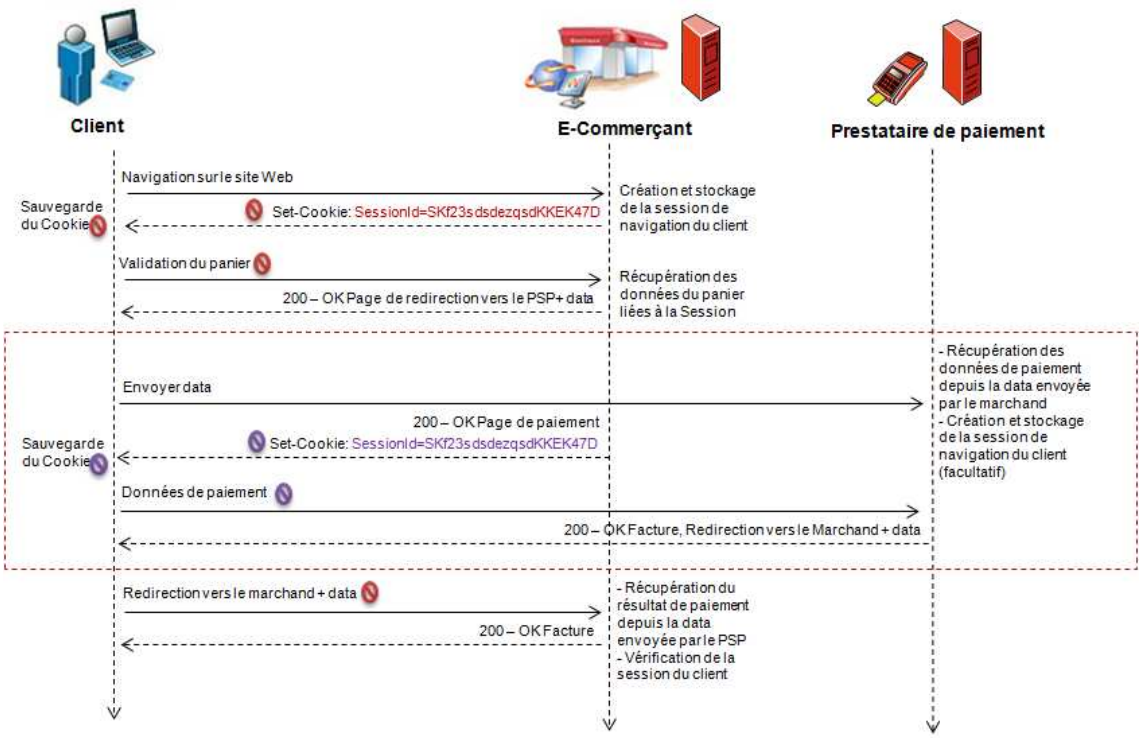


FIGURE 5.5 – Gestion de la session dans le cas d'un paiement déporté

Nous constatons alors que dans le cas d'un site E-commerce à paiement bancaire déporté, le prestataire de paiement alternatif n'a pas besoin de récupérer la session du client pour payer le marchand plus tard avec la CVD. L'absence de cette forte contrainte va nous permettre d'améliorer la qualité de l'intégration via Plugin JavaScript (section 5.7).

5.4.1 Récupération de la session du client

Lors de la conception du Plugin JavaScript, nous avons étudié l'impact de la session sur l'intégration du système de paiement alternatif et la gestion du paiement.

Cette étude n'était pas nécessaire dans le cas de la première approche d'intégration via Proxy Web, car ce dernier intercepte tous les échanges entre le client et le serveur de l'E-commerçant. Il est même le véritable client vis-à-vis de l'E-commerçant car c'est lui qui envoie les requêtes et reçoit les réponses HTTP. Cependant, dans le cas du Plugin Javascript, le prestataire de paiement alternatif est absent au moment de l'établissement de la session entre le client et le marchand et n'intervient qu'au moment du paiement pour honorer la commande du client. Or, comme nous venons de le montrer dans la section précédente, dans le cas d'un paiement bancaire intégré, il ne peut pas payer la commande du client sans avoir récupéré la session du client. Pour ce faire, il existe deux possibilités :

1. La première possibilité consiste à demander au site marchand d'envoyer les données de la session du client au prestataire de paiement alternatif lors de la redirection du client.

2. La deuxième possibilité consiste à récupérer la session du client en JavaScript (c'est ce qu'on appelle le « Vol de Session »). Dans ce cas, l'E-commerçant n'a rien à faire à part intégrer le Plugin JavaScript afin de rediriger le client vers la page de paiement non bancaire.

Nous avons rapidement décliné la première possibilité car nous cherchons à proposer un système de paiement facile à intégrer pour l'E-commerçant. Le fait de demander au marchand d'envoyer les données de la session peut complexifier l'intégration via Plugin JavaScript. Nous avons alors retenu la deuxième possibilité afin de faciliter l'intégration pour l'E-commerçant. Cependant, cette solution ne s'applique que sur les sites marchands qui n'utilisent pas des politiques de sécurité très dures concernant les cookies (HttpOnly, contrôle de l'adresse IP), car la récupération des cookies est effectuée en JavaScript.

Afin de vérifier la faisabilité de l'intégration via Plugin JavaScript dans les sites E-commerces à paiement bancaire intégré, nous avons mis en place une procédure de test de « vol de session » du client. Cette procédure de test consiste à tester la récupération des cookies du client avec un changement de l'adresse IP. En effet, il faut s'assurer également que le serveur de l'E-commerçant n'effectue pas un contrôle sur les adresses IP des clients, car le serveur du prestataire de paiement possède une adresse différente de celle du client. Dans ce cas, il risque d'être rejeté lors du paiement bancaire sur le serveur de l'E-commerçant. Le testeur doit alors pouvoir changer d'adresse IP au moins deux fois durant le test. Un moyen de le faire consiste à passer par des proxies publiques. Nous présentons ci-après (tableau 5.2) un exemple de code JavaScript de test de vol de session :

```
var dc = document.cookie;
var cookies = dc.split(";");
alert(" Supprimer les cookies ET changez IP, Puis appuyez sur OK");
for (var i = 0; i < cookies.length; i++)
{
        var splits = cookies[i].split("=");
        var name = splits[0];
        var value = "";
        for(var j = 1; j < splits.length; j++)
        {
             value += escape(splits[j]);
             if(j < splits.length-1)
             value += "=";
        }
        document.cookie = name + "=" + value;
}
```

TABLE 5.2: Exemple de code JavaScript de test de récupération de la session

5.4.2 Récupération de la requête de paiement CB

Rappelons que le principe de la nouvelle architecture de paiement proposée dans le chapitre 3 est de convertir les paiements alternatifs en paiements bancaires. Il est donc indispensable de récupérer la page de paiement CB du site marchand. Sachant que, dans notre travail, nous avons une approche orientée marchand et que nous cherchons à proposer un mode d'intégration facile pour l'E-commerçant, le Plugin doit pouvoir récupérer les éléments de la commande d'une manière indépendante. Cependant, selon la structure du site E-commerce, certaines cinématiques s'avèrent un peu compliquées à réaliser en Javascript.

Nous notons que, dans le cas des sites E-commerce à paiement bancaire intégré, la récupération de la session du client suffit pour avoir toutes les informations concernant la commande. Cependant, dans le cas d'un paiement bancaire déporté, il faut réussir à récupérer la requête HTTP qui part vers le serveur du prestataire de paiement. Généralement, il s'agit de la requête déclenchée par la sélection du moyen de paiement bancaire sur la page de choix de moyen de paiement. Mais, parfois, l'E-commerçant affiche des pages intermédiaires afin d'afficher un récapitulatif de commande au client avant de le rediriger vers la page de paiement. Nous présentons dans la table 5.3 une étude des différentes cinématiques possibles dans le cas des sites E-commerce à paiement bancaire déporté. Nous constatons qu'il existe des cinématiques de redirection très compliquées à effectuer en JavaScript et que dans certains cas, il faut demander au marchand d'envoyer les données directement au prestataire de paiement alternatif sans passer par un Plugin JavaScript.

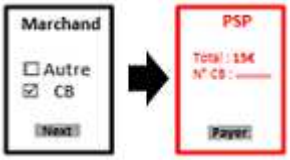
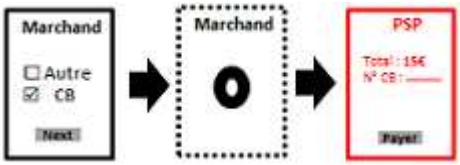
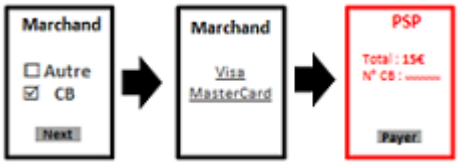
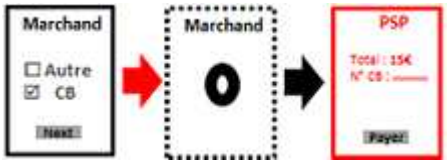
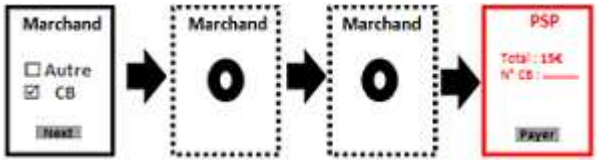
Cinématique	Solution d'intégration
Cinématique 1 : Une requête facile à reproduire en JavaScript amenant directement chez le prestataire 	Le Plugin récupère la requête du marchand vers le prestataire de paiement bancaire en cas de choix du paiement CB et l'envoie au serveur du prestataire de paiement alternatif.
Cinématique 2 : Une requête facile à reproduire en JavaScript suivie d'une redirection vers le prestataire  **Cinématique 3** : Une requête facile à reproduire en JavaScript suivie d'une page intermédiaire qu'on peut cacher sans nuire à l'expérience utilisateur 	Le Plugin appelé dans la première page récupère le contenu de la 2ème page en AJAX. Il y récupère ensuite la requête qui part vers le prestataire de paiement bancaire et l'envoie au serveur du prestataire de paiement alternatif.
Cinématique 4 : Une requête difficile à reproduire en JavaScript suivie d'une redirection vers le prestataire  **Cinématique 5** : Une page intermédiaire que l'on ne peut pas cacher sans nuire à l'expérience utilisateur  **Cinématique 6** : Au moins 3 requêtes sont nécessaires pour arriver chez le prestataire 	On demande à l'E-commerçant d'envoyer au prestataire de paiement alternatif la requête nécessaire à la récupération de la page de paiement bancaire.

TABLE 5.3: Les cinématiques de récupération de la requête de paiement CB

5.5 Procédure d'intégration

Après avoir décrit le mode d'intégration via Plugin JavaScript, nous allons présenter la procédure d'intégration afin de l'analyser selon les critères retenus au début de notre travail. Nous reprenons alors les étapes décrites dans la figure 2.3 du chapitre 2 : ajout du moyen de paiement, paiement et rapprochement.

5.5.1 Ajout du moyen de paiement

La première étape d'intégration d'un moyen de paiement dans un site E-commerce consiste à ajouter le nouvel instrument de paiement sur le site. Contrairement au mode d'intégration via Proxy Web, où le marchand n'a rien à faire pour afficher le moyen de paiement sur son site Web et rediriger le client vers la page de paiement, dans le cas de la deuxième approche d'intégration, le marchand doit ajouter le nouveau moyen de paiement sur son site Web. Il doit également inclure un appel au Plugin JavaScript lorsque le client choisit ce nouveau moyen de paiement. Le Plugin permet dans ce cas de récupérer les données de la commande et de rediriger le client vers la page de paiement. Cependant, dans le cas de l'impossibilité de récupérer ces données en JavaScript, l'E-commerçant peut être amené à les envoyer (tableau 5.3, cinématiques 4, 5, 6). Sachant que ce mode d'intégration s'adresse aux E-commerçants ayant déjà intégré un terminal de paiement bancaire, cette tâche revient à copier la requête vers le prestataire de paiement bancaire et l'envoyer à celui alternatif.

5.5.2 Paiement

Une fois le client redirigé vers la page de paiement alternatif, la prochaine étape est la gestion du paiement. Comme tout système de paiement déporté, cette phase ne concerne pas spécifiquement l'E-commerçant. C'est le prestataire de paiement qui se charge d'authentifier le client et de demander l'autorisation de paiement à l'émetteur. Dans le cadre de la nouvelle approche, le prestataire de paiement alternatif peut utiliser le Proxy Web décrit dans le chapitre précédent afin de payer l'E-commerçant. En effet, le Proxy Web a deux fonctions : la première consiste à gérer la navigation du client et à ajouter le nouveau moyen de paiement sur le site E-commerce et la deuxième fonction permet de payer le marchand avec la CVD. Dans le cas d'intégration via un Plugin JavasScript, on peut alors utiliser la deuxième fontion du Proxy Web afin de gérer le paiement. Nous retrouvons dans ce cas la description de l'étape paiement par le Proxy Web présentée dans la section 4.4 du chapitre précédent.

5.5.3 Rapprochement

Une fois que le paiement est validé par l'E-commerçant, la dernière phase d'intégration d'un système de paiement sur Internet est le rapprochement entre le paiement et la commande. Cette phase peut être divisée en trois sous-étapes : la récupération de la requête HTTP vers la page de résultat de paiement chez l'E-commerçant, la récupération du numéro de la commande et la centralisation de toutes les transactions dans un back-office. Sachant que nous venons de supposer qu'on peut réutiliser le Proxy Web afin de payer l'E-commerçant, nous retrouvons alors la même description de cette phase dans la section 4.4 du chapitre précédent.

Cependant, l'usage du Proxy Web doit se limiter au paiement, c'est-à-dire que lors de la redirection du client vers le site E-commerce après le paiement, le prestataire de paiement alternatif doit s'assurer que le client ne va pas continuer à naviguer via le Proxy Web par la suite. Dans le cas d'un E-commerçant ayant déporté sa page de paiement bancaire chez un prestataire de paiement, le client est redirigé vers l'Url de retour affichée par le prestataire de paiement bancaire après le paiement. Dans le cas d'un paiement sur un site qui héberge sa page de paiement bancaire, la page de résultat de paiement du site marchand est affichée « proxifiée » au client. En revanche, tous les liens dans cette page redirigent directement vers le site marchand sans passer par le Proxy Web.

5.6 Validation et limites

La proposition de l'intégration via Plugin JavaScript, dans ce chapitre, a été effectuée afin de pallier les inconvénients de l'approche d'intégration via Proxy Web, présentée dans le chapitre précédent, qui demande une maintenance continuelle des configurations Proxy des sites E-commerce et est très dépendante de tout le parcours client sur le site E-commerce. Après avoir décrit le principe de fonctionnement du Plugin JavaScript et les différentes étapes de son intégration dans un site E-commerce, nous cherchons, dans cette section, à valider cette approche d'intégration selon les contraintes présentées dans l'état de l'art et à présenter les éventuelles limites de cette approche afin d'essayer de l'améliorer.

5.6.1 Validation

Nous allons analyser l'approche d'intégration via Plugin JavaScript selon les critères annoncés dans l'état de l'art, à savoir : la sécurité, l'ergonomie et la complexité.

Sécurité

Afin d'étudier la sécurité de l'intégration via un Plugin JavaScript, nous allons suivre la méthodologie définie au chapitre 2. Nous allons commencer tout d'abord par effectuer une analyse sécuritaire du nouveau système de paiement présenté dans la figure 5.6. Pendant cette analyse, nous supposons que le marchand a installé un système de paiement bancaire sécurisé. Nous proposons dans cette section d'étudier le niveau de sécurité des flux B, C, D, E, F, G, H et I qui constituent les flux d'informations gérés par le prestataire de paiement alternatif.

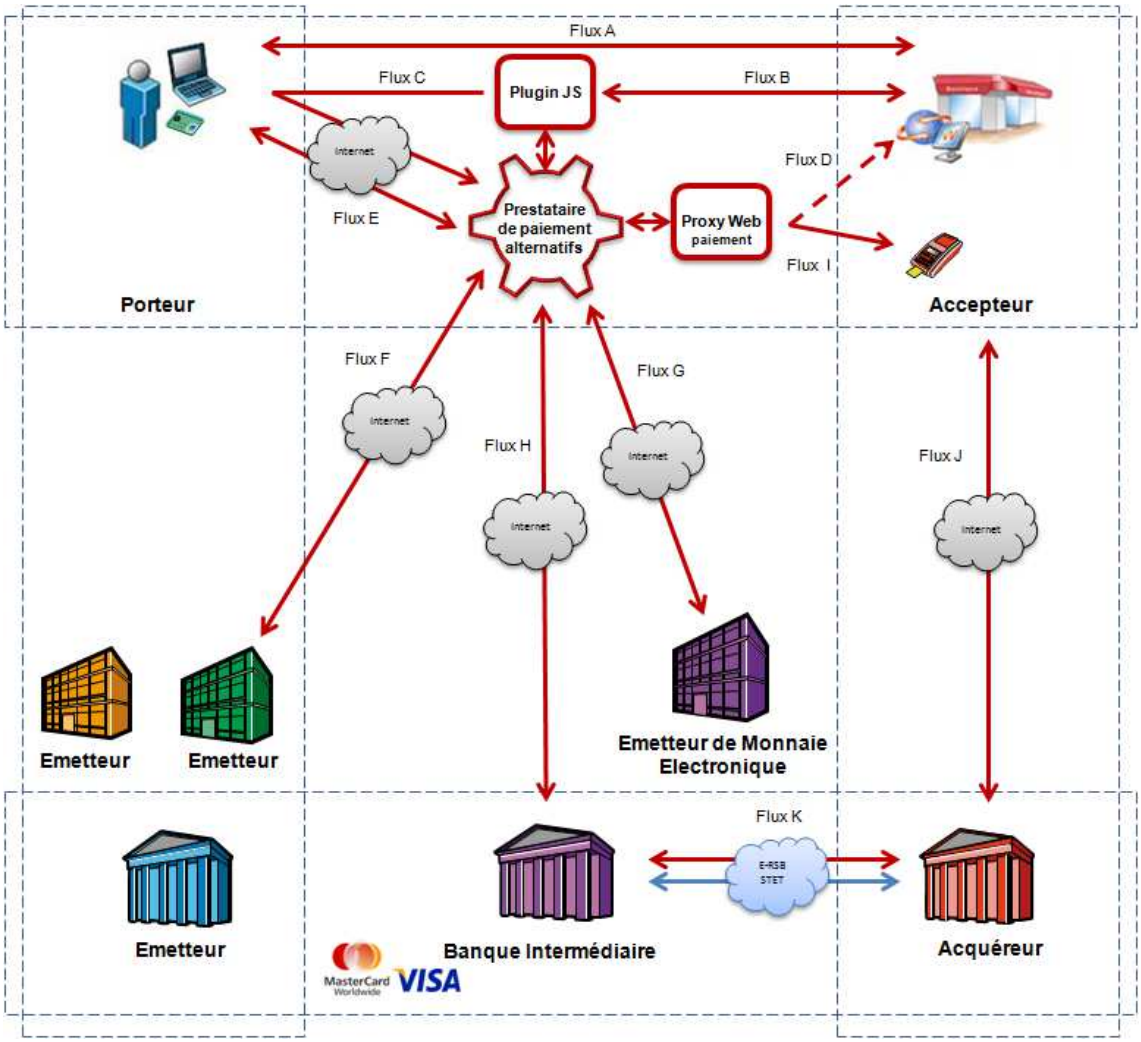


FIGURE 5.6 – Étude de sécurité du Plugin JavaScript

Le flux A concerne la navigation du client sur le site marchand. Il s'agit d'une navigation directe, donc aucune information n'est interceptée par le prestataire de paiement alternatif. Une fois que le client a rempli son panier et choisit de payer avec un moyen de paiement « alternatif », l'E-commerçant appelle le Plugin

Javascript afin de rediriger le client vers la page de paiement correspondante. D'où le flux d'information B. L'appel au Plugin Javascript se fait via le protocole SSL, l'E-commerçant est ainsi sûr d'appeler le bon Plugin (grâce à l'authentification du serveur garantie par SSL). Une fois appelé, le JavaScript est incorporé dans la page HTML affichée dans le navigateur du client. Il simule la sélection du moyen de paiement bancaire et enchaîne les requêtes HTTP nécessaires afin de récupérer les données nécessaires pour la récupération de la page de paiement. Ce flux d'information est identique à celui généré lorsque le client choisit le mode de paiement bancaire. Les informations transitant au sein de ce flux ne sont pas très sensibles, car il ne s'agit pas encore de données confidentielles. Sachant qu'on a supposé au début de cette analyse que le système de paiement bancaire du marchand est sécurisé, nous retrouvons alors le même niveau de sécurité.

Le flux C contient les informations nécessaires à l'affichage de la page de paiement bancaire. Ce flux contient deux lots de données :

1. Le premier lot d'information concerne les données de redirection vers la page de paiement bancaire (hébergée par le marchand ou par son prestataire de paiement bancaire), il s'agit généralement des données de la commande (montant, numéro de la commande, identifiant du marchand, etc.) sécurisée à l'aide d'un chiffrement symétrique, une signature numérique, ou un jeton cryptographique (chapitre 2) selon le mode d'intégration du terminal de paiement bancaire du marchand.
2. Le deuxième lot d'information contient quelques informations à destination du prestataire de paiement alternatif. Il s'agit de l'identifiant de l'émetteur du moyen de paiement et l'identifiant de l'E-commerçant. Ce lot contient aussi l'Url de la page de paiement bancaire de l'E-commerçant afin de récupérer la page de paiement bancaire correspondant à la commande.

Le niveau du flux C repose sur celui du premier lot de données (déjà sécurisé lors de l'installation du système de paiement bancaire dans le site E-commerce). Le deuxième lot ne contient pas des données confidentielles. Les Flux D et I consistent à passer par le Proxy Web pour récupérer la page de paiement bancaire dans un premier temps, puis payer l'E-commerçant. Le flux D a lieu dans le cas d'un site E-commerce à paiement bancaire intégré et le flux I dans le cas d'un site E-commerce à paiement bancaire déporté. Comme nous l'avons décrit dans le chapitre précédent, afin de récupérer la page de paiement, le Proxy Web a besoin de le faire via le navigateur du client en simulant le choix de paiement carte bancaire. Cependant, la deuxième partie du flux, qui concerne l'envoi des données de la carte virtuelle dynamique, est effectuée de serveur à serveur.

Le flux E concerne le paiement alternatif. Il contient les données du moyen de paiement du client. Il s'agit d'un flux sécurisé par le prestataire de paiement alternatif (ou éventuellement l'émetteur du moyen de paiement). Il s'agit d'authentifier le client à l'aide de ses données de paiement, le niveau de sécurité de ce flux dépend alors du type de l'authentification (simple ou forte). Cependant, dans le cadre des paiements alternatifs, le client est généralement authentifié à l'aide d'un seul facteur (mot de passe, date de naissance, code secret, etc.). Ceci était le cas également des paiements bancaires pendant plusieurs années avant l'adoption du protocole 3D-Secure. Le client peut alors répudier son paiement facilement puisqu'il n'est pas fortement authentifié et il ne signe aucune donnée échangée dans ce flux. Pour garantir la non-répudiation des clients, vu la difficulté à mettre en place la solution technique, nous avons eu recours à une solution contractuelle, en imposant aux clients ce critère et en les sensibilisant à l'importance de sécuriser leur moyen de paiement..

Les flux F, G, H concernent la demande d'autorisation de paiement à l'émetteur, la validation des comptes de monnaie électronique et la génération de la carte virtuelle dynamique. La sécurité de ces flux a été prouvée dans la section 4.5 du chapitre 4. Les flux J et K font partie des flux du système bancaire supposé sécurisé.

Le résultat de cette analyse de sécurité est présenté dans le tableau 5.4 qui permet de recenser les critères de sécurité garantis par cette approche d'intégration via le Plugin Javascript.

Relation	Authentification	Confidentialité	Intégrité	Non-Répudiation
Flux B	x	-	x	-
Flux C	x	-	x	-
Flux D	x	-	x	-
Flux E	x	x	x	x
Flux F	x	x	x	x
Flux G	x	x	x	x
Flux H	x	x	x	x
Flux I	x	x	x	x

TABLE 5.4: Evaluation de la sécurité de l'intégration via Plugin JavaScript

Après avoir étudié la sécurité de chaque flux d'information, nous allons étudier la sécurité du nouveau système de paiement dans son ensemble. Pour ce faire, nous présentons une étude de quelques exemples d'attaques (tableau 2.2). Les résultats de l'étude des scénarios de l'attaque de l'homme au milieu sont présentés dans le tableau 5.5. Ensuite, nous nous intéressons aux conséquences de l'attaque de modification. Nous avons choisi d'étudier deux exemples d'attaque : la modification du montant et la modification du résultat de paiement (tableau 2.2) par un client malveillant. Sachant que ces deux données ne sont pas manipulées en JavaScript (du côté du

client) et qu'elles sont récupérées par le Proxy Web, nous retrouvons alors le même niveau de résistance à cette attaque que dans le cas de l'intégration via Proxy Web.

Flux	Conséquences
Flux B	Un attaquant qui arrive à intercepter ce canal de communication pourra modifier le contenu du Plugin Javascript et injecter du code malveillant. Si le site Web du marchand ne résiste pas à l'attaque du Cross-Site Scripting [Zuchlinski G., 2003]. Cette attaque peut être dangereuse. Cependant, dans ce cas, la faille de sécurité n'est pas liée à l'intégration du Plugin JavaScript. Il s'agit d'une faille dans le site Web du marchand.
Flux C	Le flux C est généré par le Plugin JavaScript et exécuté par le navigateur du client. Il contient les échanges permettant de sélectionner le choix du moyen de paiement bancaire. Un attaquant qui arrive à intercepter ce canal ne pourra pas nuire à la sécurité du système de paiement, car nous supposons que ces données sont sécurisées par la politique de sécurité déjà mise en place lors de l'intégration du système de paiement bancaire. Un attaquant qui intercepte ce flux peut essayer de rediriger le client vers une « fausse » page de paiement afin d'intercepter les données de paiement du client.
Flux D	Ces flux contiennent les informations de la commande (montant, numéro de la commande) qui ne sont pas des données confidentielles, donc il n'existe pas un risque majeur lié à leur interception par un attaquant. Le risque réside dans la possibilité de les modifier par l'homme du milieu. Cependant, et comme nous l'avons montré auparavant, ces flux garantissent l'intégrité et l'authenticité des données envoyées.
Flux E	Un attaquant qui intercepte le flux E peut avoir accès aux données de paiement du client et les utiliser plus tard.
Flux F	Il s'agit du flux de demande d'autorisation de paiement, qui ne contient pas de données confidentielles, cependant, un attaquant interceptant ce flux peut essayer de causer des dégâts à l'émetteur en autorisant systématiquement toutes les demandes de paiement. Chose qui nécessite un forge de la signature de l'émetteur.
Flux G	Ce flux ne contient pas de données confidentielles. Cependant, si l'attaquant arrive à modifier les données échangées dans ce flux, il peut causer des dégâts financiers pour l'émetteur de monnaie électronique en acceptant de générer des CVDs sur son compte sans vérifier les comptes de monnaie électronique des émetteurs.
Flux H	Un attaquant qui arrive à intercepter ce flux peut avoir accès à la CVD de paiement. Par contre, il faut qu'il l'utilise très rapidement avant que le prestataire de paiement alternatif l'utilise pour payer l'E-commerçant (un délai estimé à 1 minute maximum), car il s'agit d'un numéro de carte à usage unique.
Flux I	Ce flux contient les données de la carte virtuelle dynamique. Même si un attaquant arrive à intercepter ce flux, il ne pourra pas en tirer profit systématiquement, car il s'agit de carte de paiement à usage unique.

TABLE 5.5: Impact de l'attaque de l'homme du milieu sur le système Plugin JavaScript

En effet, la modification du montant ne peut être effectuée qu'au moment de l'appel de la page de paiement bancaire de l'E-commerçant (flux D ou I), car une fois que cette page est affichée, le Proxy récupère le montant et le client ne pourra plus le changer. Ayant supposé au début de cette étude de sécurité que le système de paiement bancaire du marchand est sécurisé, nous concluons alors que cette attaque

ne pourra pas réussir et que le nouveau système résiste à ce type d'attaque. Il va de même pour la modification du résultat de paiement envoyé par le prestataire de paiement bancaire au marchand. La résistance à cette attaque s'appuie sur le fait que le système bancaire de l'E-commerçant n'est pas vulnérable à ce type d'attaque.

Dans le cas d'une attaque par Flooding (déni de service), qui consiste à envoyer plusieurs requêtes à une cible, le prestataire de paiement alternatif bloque toutes les requêtes venant de l'adresse IP de l'attaquant se protégeant ainsi de ce type d'attaque.

Ergonomie

Nous constatons, depuis la figure 5.1, que l'expérience utilisateur sur le site E-commerce ne change pas suite à l'intégration du nouveau moyen de paiement via Plugin JavaScript. En effet, le client navigue directement sur le site de l'E-commerçant puis il est redirigé vers le serveur du prestataire de paiement suite au choix du moyen de paiement alternatif. Sachant que le mode d'intégration via Plugin Javascript s'appuie sur le Proxy Web afin de payer le marchand, nous retrouvons ainsi quelques inconvénients du Proxy Web qui consistent à passer obligatoirement par le navigateur du client afin de récupérer le contenu des pages HTML, ce qui peut parfois allonger la redirection du client vers la page de paiement alternatif, le temps que le Proxy Web récupère la page de paiement bancaire et analyse son contenu.

Complexité

Dans le cas de cette approche d'intégration, et afin d'accepter des nouveaux moyens de paiement, l'E-commerçant doit disposer d'un système de paiement bancaire. Contrairement à l'intégration via Proxy Web, l'intégration via Plugin JavaScript exige que l'E-commerçant ajoute le nouveau moyen de paiement sur son site et appelle une librairie JavaScript pour rediriger le client vers la page de paiement. Généralement, il s'agit du seul développement technique à effectuer par l'E-commerçant qui a été estimé à un jour/homme de développement. Cependant, dans certains cas (tableau 5.3), le marchand peut être amené à envoyer les données nécessaires à la récupération de sa page de paiement bancaire et l'envoyer au prestataire de paiement alternatif. Il s'agit des cas où cette récupération est impossible via JavaScript (généralement un problème de sécurité Cross-Domain). Ce développement reste tout de même moins complexe que celui imposé par les autres modes d'intégration présentés dans l'état de l'art (chapitre 2).

5.6.2 Limites

Nous avons présenté dans ce chapitre l'approche d'intégration des moyens de paiement alternatifs via Plugin JavaScript ainsi que le principe de fonctionnement de cette approche. Nous avons également décrit le nouveau scénario de paiement, les nouveaux flux d'information et le processus d'intégration de cette solution. Enfin, nous avons évalué ce nouveau modèle d'intégration par rapport aux critères définis au début de notre travail (la sécurité, l'ergonomie et la complexité). Nous avons montré que ce mode d'intégration ne permet pas d'altérer le niveau de sécurité du système de paiement bancaire de l'E-commerçant. Bien qu'il s'agisse d'un mode d'intégration moins facile que celui via Proxy Web pour l'E-commerçant, il s'agit d'un mode moins complexe que ceux décrits dans l'état de l'art.

Malgré les avantages de l'intégration via Plugin JavaScript, notamment au niveau de l'ergonomie et de la sécurité, la réutilisation du Proxy Web pour payer l'E-commerçant avec la carte virtuelle dynamique présente quelques inconvénients :

1. La nécessité d'avoir la session du client pour démarrer une navigation Proxy Web et afficher la page de paiement dans le cas d'un E-commerçant ayant intégré directement sa page de paiement bancaire dans son site.

2. L'ajout des pages intermédiaires d'attente afin de faire patienter le client, en attendant que le Proxy Web analyse le contenu de la page de paiement et récupère les données de la commande (le montant, la référence de la commande, etc.), ce qui peut altérer l'expérience utilisateur.

3. La vérification de la validité des données à envoyer pour payer l'E-commerçant dépend du navigateur du client, car le Proxy Web utilise des librairies JavaScript pour remplir le formulaire de paiement bancaire et vérifier sa cohérence avant de rediriger le client vers la page de paiement (figure 4.9).

4. Le retour vers une page de confirmation « proxifiée » dans le cas d'un paiement alternatif sur un site E-commerce ayant une page de paiement bancaire intégrée.

Afin de pallier tous ces inconvénients, nous proposons dans la prochaine section d'implémenter un automate de paiement, ce qui nous permet de nous dispenser de l'usage du Proxy Web pendant la phase de paiement. L'idée est de permettre au prestataire de paiement alternatif de payer l'E-commerçant d'une manière complètement transparente pour le client. La section suivante décrit plus en détail le principe de l'automate de paiement ainsi que la nouvelle cinématique de paiement.

5.7 Automate de paiement

Un automate est *un dispositif se comportant de manière automatique, c'est-à-dire sans intervention d'un humain. Ce comportement peut être figé, le système fera toujours la même chose, ou bien peut s'adapter à son environnement* [Wikipedia, 2003]. Un automate de paiement est donc une entité qui permet d'exécuter d'une manière automatique certaines tâches. Dans le cadre de notre travail, nous cherchons à définir un automate de paiement qui permet de réaliser principalement deux missions : d'une part, appeler la page de paiement bancaire de l'E-commerçant et récupérer les données de la commande affichées sur cette dernière et, d'autre part, payer l'E-commerçant avec la carte virtuelle dynamique générée dans ce but. Cet automate intervient donc à deux moments différents de la transaction (figure 5.8).

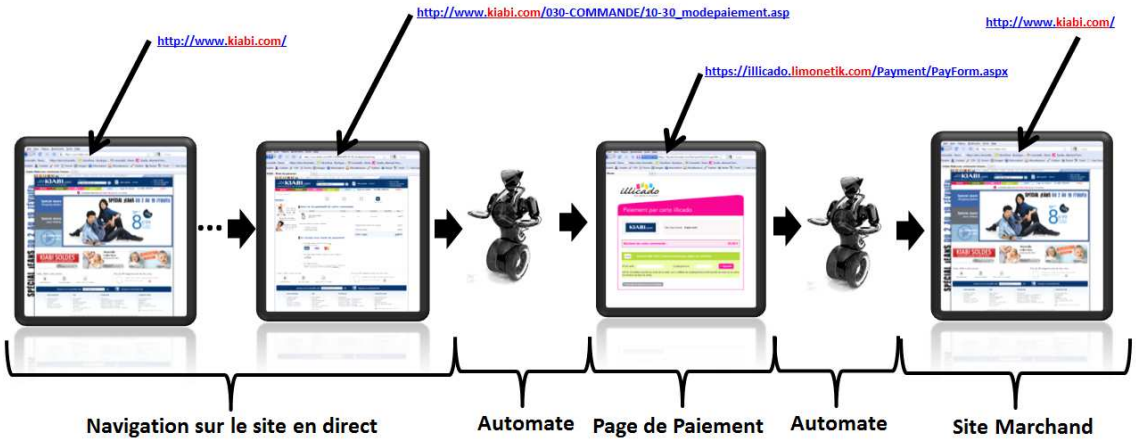


FIGURE 5.7 – Automate de paiement

5.7.1 Automate de paiement : principe

Contrairement au Proxy Web, l'automate de paiement doit pouvoir récupérer la page de paiement bancaire de l'E-commerçant sans passer par le navigateur. Il s'agit d'une entité qui envoie des requêtes HTTP directement au serveur de paiement bancaire et analyse les réponses HTTP de ce dernier. Cette analyse consiste à parcourir le corps (body) de la réponse HTTP et utiliser des expressions régulières afin de retrouver les données cherchées. Dans ce cas, l'automate ne dépend pas du type du navigateur du client. Sachant que l'automate de paiement est appelé à deux moments distincts de la transaction, il doit sauvegarder les différents échanges avec le serveur de paiement bancaire de l'E-commerçant afin de pouvoir retrouver facilement l'historique de la communication une fois qu'il est appelé pour payer l'E-commerçant.

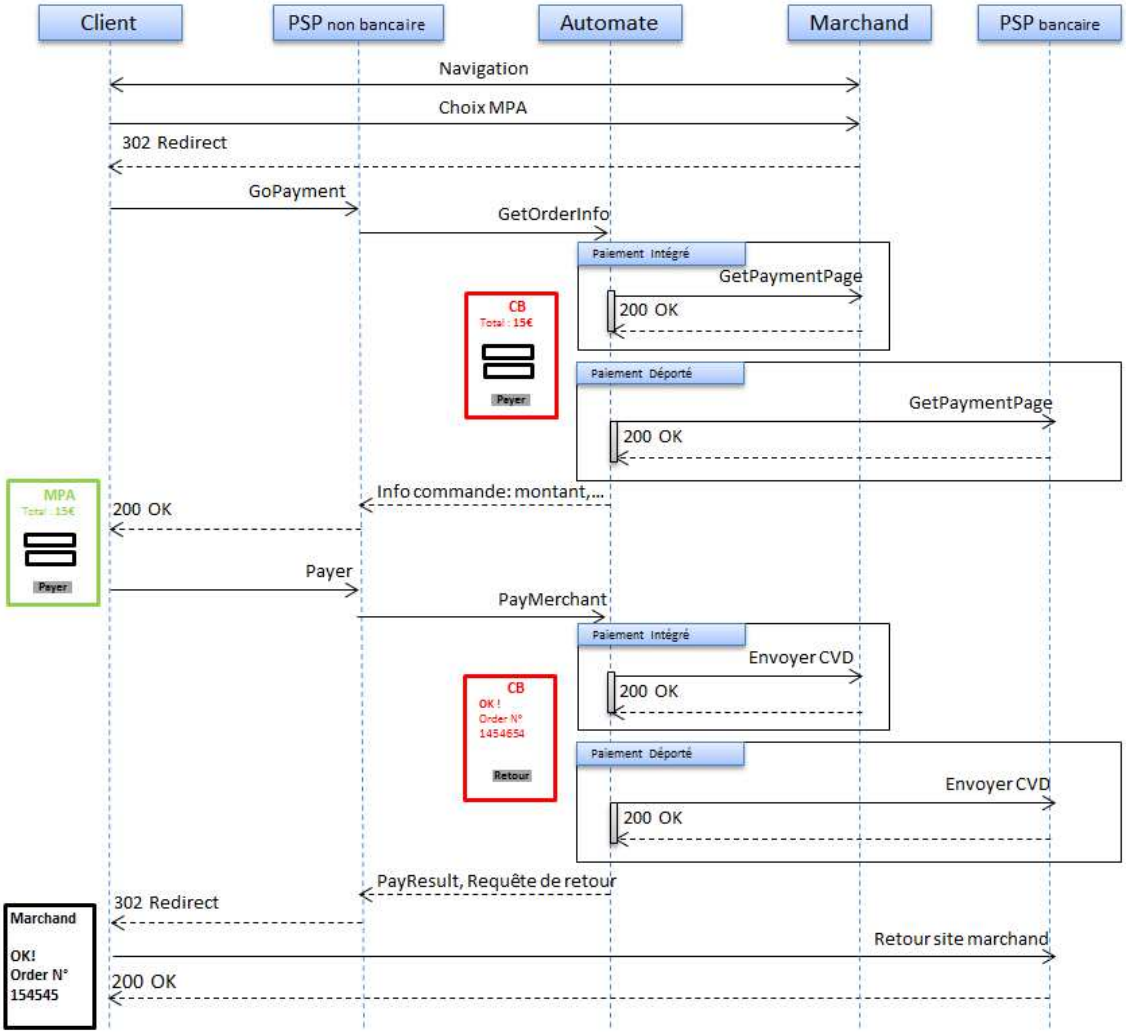


FIGURE 5.8 – Scénario de transaction Plugin JavaScript avec paiement automate

Un scénario de transaction Plugin JavaScript avec un paiement automate est décrit dans la figure 5.8. Nous constatons que l'automate, comme le Proxy Web, se charge d'envoyer les données de la commande au prestataire de paiement alternatif, ce qui diminue la complexité de l'intégration pour l'E-commerçant. L'automate permet également de communiquer le résultat de paiement bancaire effectué avec la carte virtuelle dynamique afin de valider le paiement du client.

L'automate de paiement doit également pouvoir gérer les deux types de pages de paiement bancaire : déportée et intégrée. Dans le cadre de ce chapitre, nous nous intéressons essentiellement au cas des paiements déportés puisqu'il s'agit du cas de la majorité des sites E-commerce. Dans le cas des paiements intégrés, le Plugin JavaScript doit envoyer les données de la session du client à l'automate pour qu'il puisse payer l'E-commerçant.

5.7.2 Fonctionnalités de l'automate

Afin de comprendre les fonctionnalités de l'automate de paiement, nous présentons dans la figure 5.9, une vue d'ensemble du diagramme d'activité de ce dernier. Nous détaillons par la suite chaque fonctionnalité en analysant les choix stratégiques que nous avons été amenés à effectuer. L'automate a trois fonctionnalités, qui sont : la récupération des données de la commande avant le paiement, l'annulation de la commande (en cas de besoin) et le paiement.

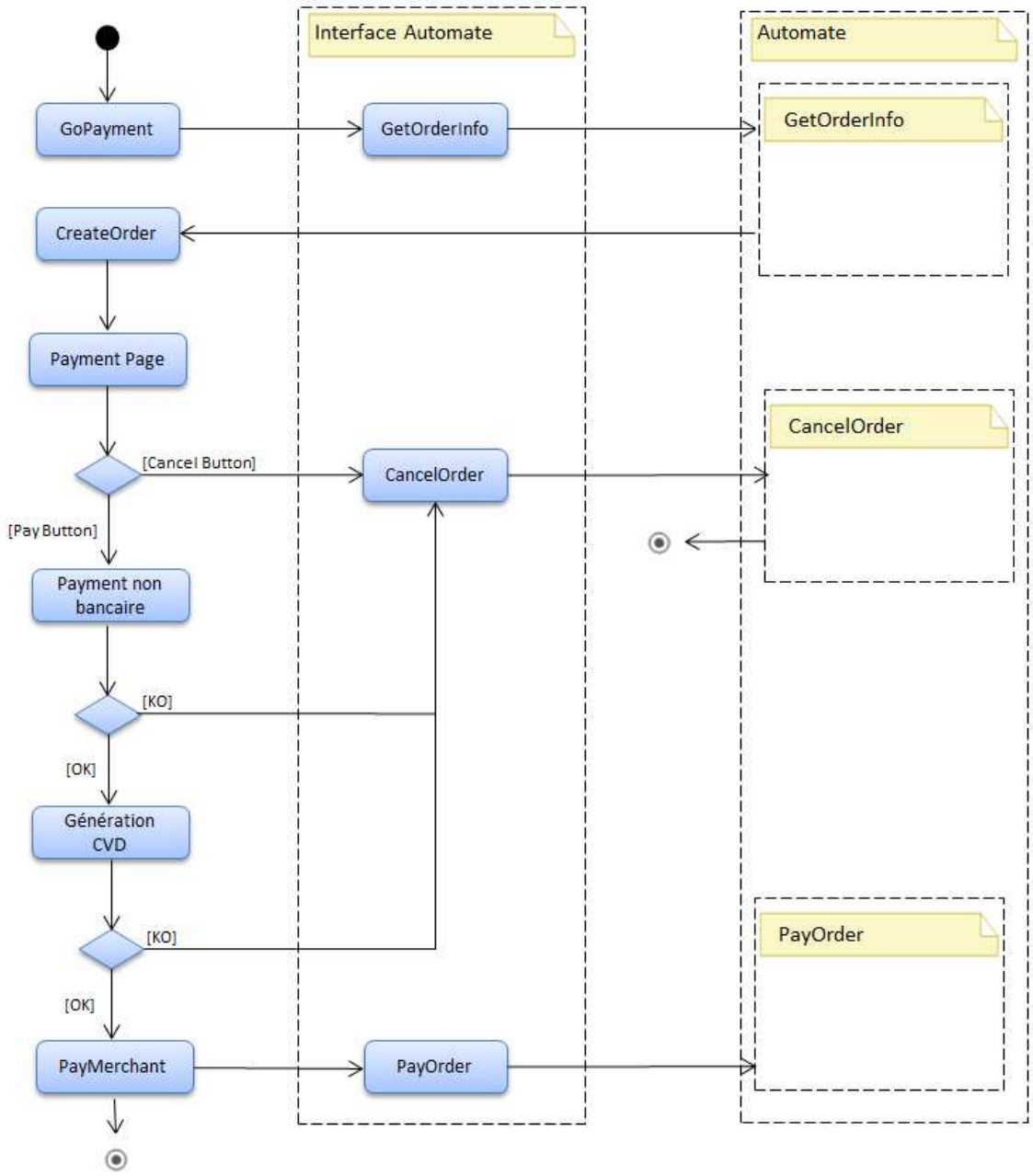


FIGURE 5.9 – Le diagramme d'activité de l'automate de paiement

Récupération des informations de la commande

La récupération des informations de la commande est réalisée avant l'affichage de la page de paiement alternatif. Nous présentons dans la figure 5.10 l'expérience utilisateur sur le site E-commerce à partir de la page de choix de moyen de paiement.

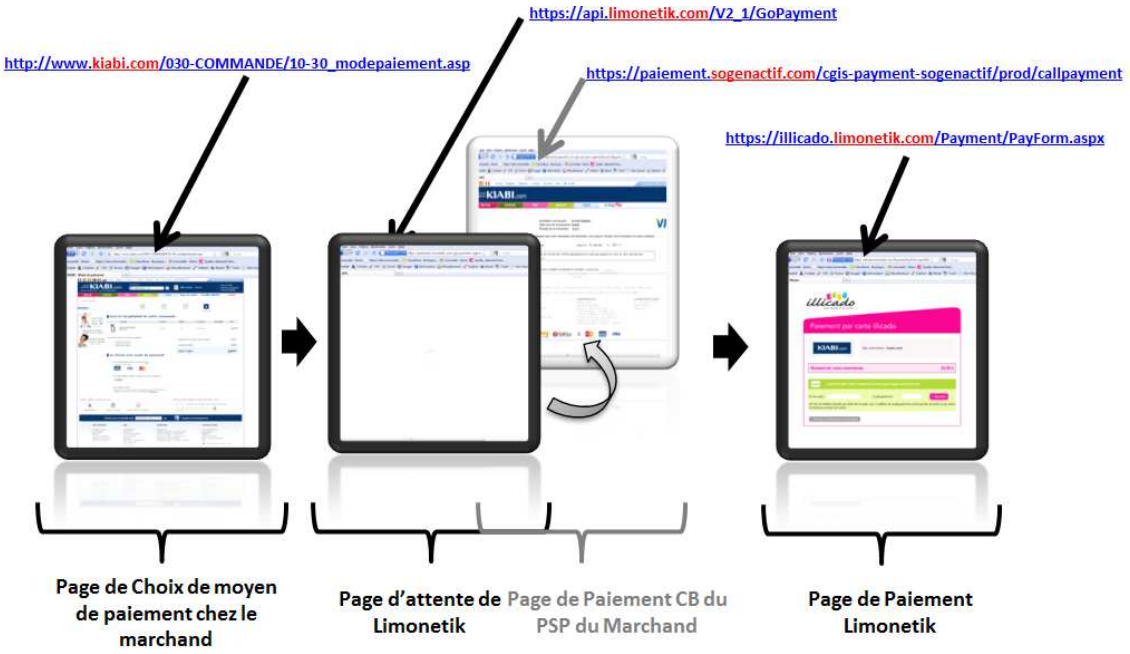


FIGURE 5.10 – Expérience utilisateur dans le cas d'un paiement avec un automate

La récupération des données de la commande contient deux étapes : la récupération de la page de paiement et la récupération des données (figure 5.11). Dans certains cas, la requête HTTP envoyée par le Plugin Javascript au prestataire de paiement alternatif ne permet pas de récupérer directement la page de paiement bancaire. Il faut effectuer d'autres requêtes pour avoir cette page. En effet, selon les paramètres envoyés au prestataire de paiement bancaire, ce dernier peut proposer une page de choix de moyen de paiement au client ou effectuer certaines redirections HTTP avant d'afficher la page de paiement. L'automate de paiement doit alors enchaîner les requêtes nécessaires pour l'affichage de la page de paiement bancaire. Nous avons réalisé une étude des différents cas de redirection possibles avant l'affichage de la page de paiement. Nous avons identifié quatre cinématiques possibles présentées dans le tableau 5.6. La deuxième étape consiste à retrouver le montant et le numéro de la commande. Pour ce faire, l'automate de paiement se base sur des expressions régulières afin d'analyser le contenu de la page HTML renvoyée par le prestataire de paiement bancaire. L'automate stocke par la suite les traces des échanges avec le prestataire de paiement bancaire dans une base de données. Ces traces contiennent

les requêtes et les réponses HTTP et sont identifiées d'une manière unique par l'identifiant de la transaction en question.

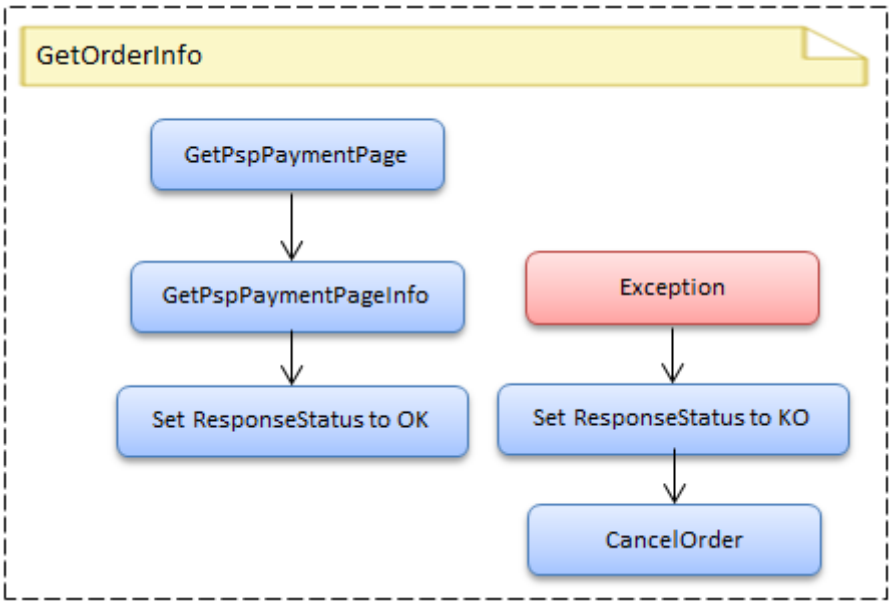


FIGURE 5.11 – Récupération des données de la commande par l'automate

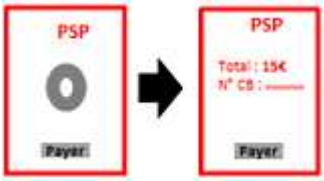
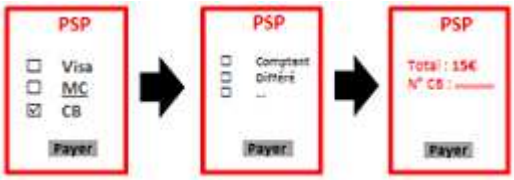
Cinématique 1 : Le prestataire de paiement bancaire affiche directement la page de paiement 	**Cinématique 2** : Le prestataire de paiement bancaire affiche une page de choix de moyen de paiement avant la page de paiement 
Cinématique 3 : Le prestataire de paiement bancaire affiche une page blanche de redirection vers la page de paiement 	**Cinématique 4** : Le prestataire de paiement bancaire affiche deux pages intermédiaires avant la page de paiement 

TABLE 5.6: Cinématiques de redirection HTTP avant l'affichage de la page de paiement bancaire

L'automate doit également pouvoir annuler les requêtes envoyées au serveur de paiement bancaire de l'E-commerçant si au cours de processus de récupération des

données de la commande, une erreur technique est survenue (par exemple la page de paiement bancaire n'est pas accessible, une erreur dans la requête HTTP, etc.). Il s'agit d'une mesure de sécurité qui permet de ne pas altérer le fonctionnement du paiement bancaire sur le site E-commerce.

Paiement

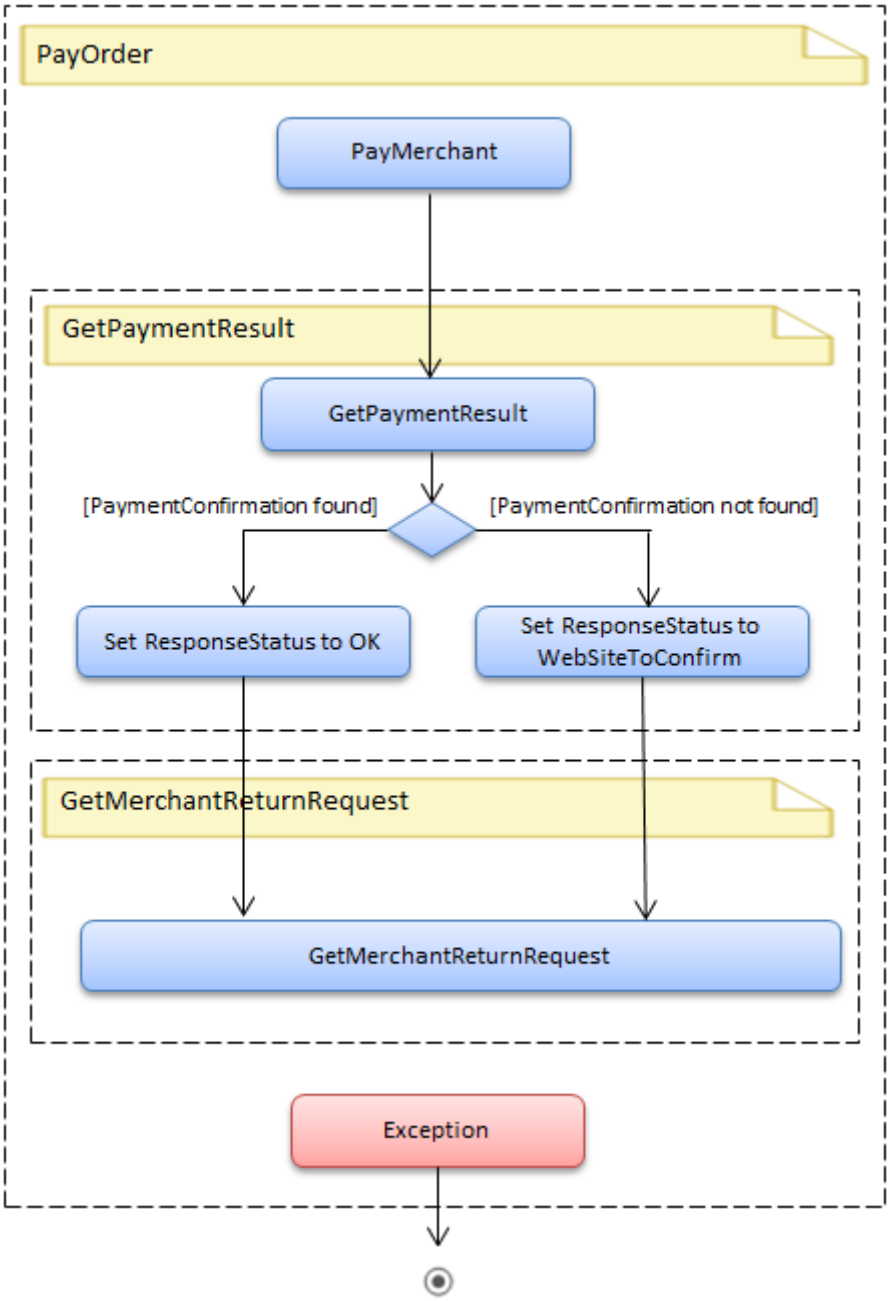


FIGURE 5.12 – Récupération des données de la commande par l'automate

Après la récupération des données de la commande, le prestataire de paiement alternatif affiche une page de paiement au client. Ce dernier peut alors payer sa commande en utilisant son moyen de paiement alternatif. Une fois que le paiement est validé et que la carte virtuelle est générée, le prestataire de paiement alternatif fait à nouveau appel à l'automate de paiement afin de payer l'E-commerçant. La figure 5.12 présente les différentes étapes de cette tâche qui sont : l'envoi des données de paiement, la récupération du résultat de paiement et la récupération de la requête HTTP de retour vers le site E-commerce. La première étape consiste à payer le marchand, c'est-à-dire envoyer les données de la carte virtuelle dynamique au prestataire de paiement bancaire de l'E-commerçant. Pour cela, l'automate construit la requête de paiement en analysant le code HTML de la page de paiement bancaire et envoie le formulaire HTML de paiement avec les données de la carte virtuelle dynamique. A la réception de cette requête, le prestataire de paiement bancaire procède à la demande d'autorisation et à la validation du paiement. Selon le paramétrage choisi par l'E-commerçant lors de l'installation du terminal de paiement bancaire, une page de confirmation de paiement peut être affichée au client ou il peut être directement redirigé vers le site E-commerce. L'automate de paiement doit alors prendre en compte ces deux cinématiques afin de récupérer le résultat du paiement ainsi que la requête de retour vers le site E-commerce.

Afin d'accomplir les deux dernières étapes de paiement, l'automate doit se baser sur le code HTTP de la réponse du prestataire de paiement (200, 302, 404, etc.). En effet, le code HTTP 200, par exemple, signifie que le prestataire de paiement affiche probablement un ticket de paiement. Le code HTTP 302 signifie qu'il n'affiche pas de résultat de paiement et redirige directement le client vers le site E-commerce. Dans le premier cas, l'automate se base sur le code HTML de la page retournée afin de trouver le résultat de paiement. Dans le deuxième cas, il se base sur les données QueryString envoyées en paramètre dans l'Url de retour vers le site E-commerce. Cependant, dans le cas d'envoi de données chiffrées, l'automate ne peut pas retrouver le résultat de paiement, l'E-commerçant est le seul à pouvoir le faire. Dans ce cas, nous proposons de nous baser, dans la mesure du possible, sur une autre information afin de détecter le succès de paiement. Il s'agit de l'autorisation de paiement envoyée par la banque « intermédiaire ». En effet, le prestataire de paiement alternatif reçoit des fichiers d'une manière régulière de la part de la banque « intermédiaire » l'informant des différentes opérations financières effectuées sur le CVD qui a servi pour payer l'E-commerçant. C'est ainsi qu'il peut constater les opérations financières (débit, crédit, annulation) à effectuer sur les moyens de paiement alternatifs du client.

Cependant, selon les E-commerçants, la gestion des cartes bancaires peut se

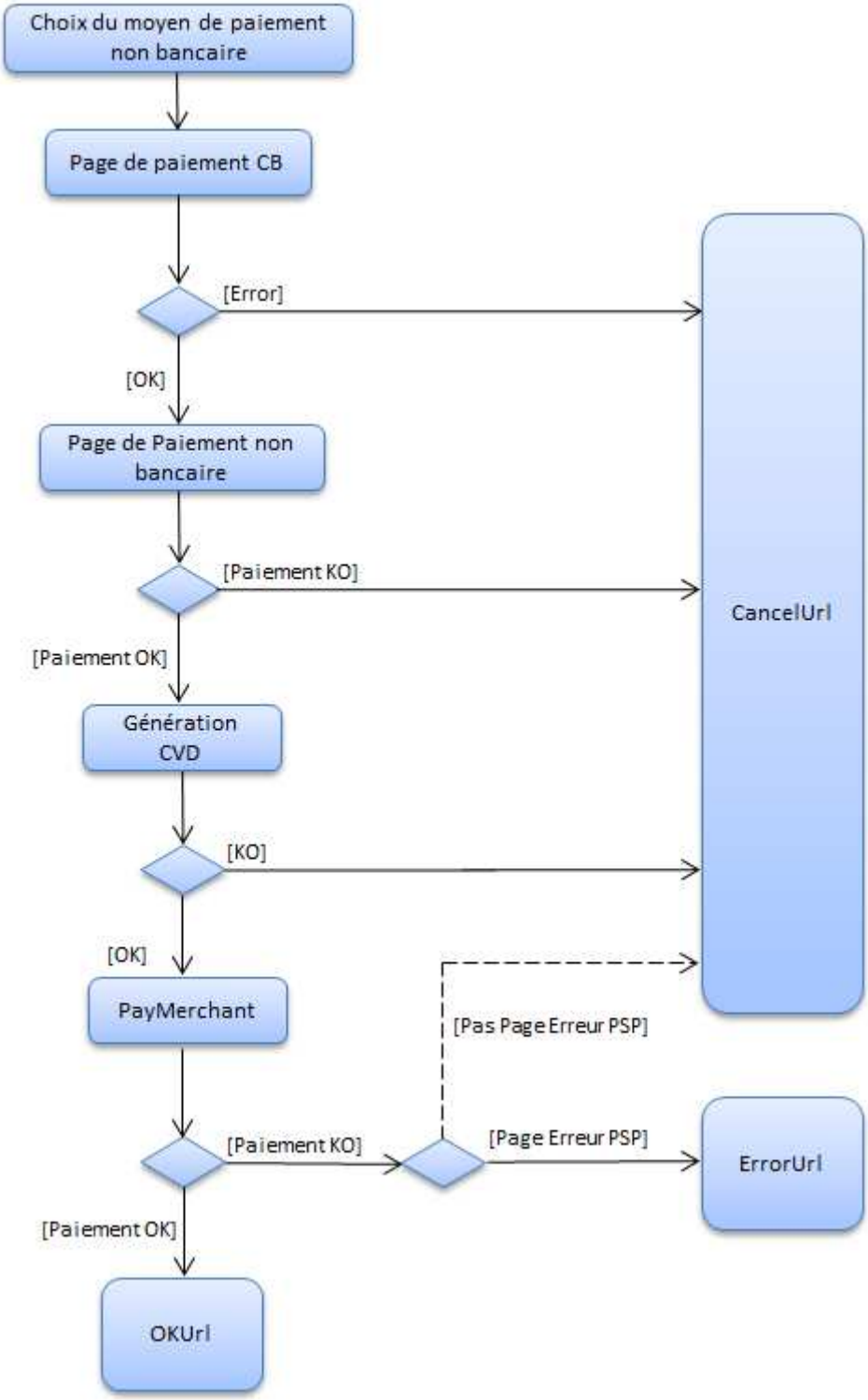


FIGURE 5.13 – Gestion des Urls de retour de l'E-commerçant par l'automate de paiement

faire selon deux scénarios différents : le premier scénario consiste à demander une autorisation de paiement immédiate suite à la réception des données de la carte bancaire, le deuxième scénario consiste à effectuer uniquement une empreinte qui est une demande d'autorisation de 1 ou 2 euros, permettant à l'E-commerçant de s'assurer de la validité de la carte. La demande d'empreinte de paiement n'étant pas reportée dans les journaux de la banque intermédiaire, le prestataire de paiement alternatif doit alors se baser sur les demandes d'autorisation.

Quant à la récupération de la requête de retour vers le site E-commerce, l'automate de paiement analyse également la réponse HTTP du prestataire de paiement en cherchant l'Url de retour vers le site E-commerce. Généralement, l'E-commerçant communique trois types d'Url de retour à son prestataire de paiement : une Url de succès de paiement, une Url d'erreur de paiement, une Url d'annulation de paiement. Nous présentons, dans la figure 5.13, la gestion de l'automate de paiement de ces différentes Urls récupérées depuis les réponses du prestataire de paiement bancaire de l'E-commerçant.

Annulation de la commande

L'intérêt d'annuler le paiement bancaire, dans le cas d'échec de paiement ou lorsque le client annule son paiement alternatif, est d'avertir le prestataire de paiement bancaire de l'E-commerçant. Ce qui permet à l'automate, lors du prochain essai de paiement (dans les minutes qui suivent l'annulation), de récupérer une nouvelle page de paiement bancaire, sans quoi le prestataire de paiement bancaire lui renvoie une erreur signalant que le paiement est en cours de traitement. Selon les prestataires de paiement bancaires, l'automate peut être amené à enchaîner quelques requêtes HTTP afin d'annuler « proprement » le paiement.

5.7.3 Implémentation

Sachant que les plateformes de paiement des prestataires de paiement bancaire sont différentes les unes des autres, nous avons décidé d'implémenter un automate de paiement par prestataire de paiement bancaire. Les automates de paiement seront identifiés par les Urls des pages de paiement appartenant à la plateforme de paiement correspondante. Ainsi, à la réception de données lors de la redirection du client par le Plugin JavaScript, le prestataire de paiement alternatif peut facilement savoir quel automate de paiement il faut utiliser selon l'Url de la page de paiement bancaire du site E-commerce. Afin de savoir quels sont les automates de paiement à implémenter, nous avons tiré profit de la base de données des sites E-commerce clients

de notre partenaire industriel Limonetik. En effet, étant présent dans le marché du commerce électronique français depuis plusieurs années, Limonetik dispose de plusieurs partenariats avec les sites E-commerce les plus présents dans le marché français, qui ont pu accepter plusieurs moyens de paiement grâce au Proxy Web décrit dans le chapitre 4. Nous avons alors mené une étude sur une centaine de sites afin de recenser les prestataires de paiement bancaire les plus utilisés par ces derniers. Les résultats de cette étude sont présentés dans le tableau 5.7.

Prestataire de paiement	Nombre de site marchand	Pourcentage
Sips	49	47,57%
Ogone	18	17,47%
Cybermut	10	9,70%
Paybox	9	8,73%
CyberPlus/Payzen	6	5,82%
Spplus	3	2,91%
Payline	2	1,94%
WorldPay	2	1,94%
GcSip	1	0,97%
NetKauf	1	0,97%
SecureShoppingBasket	1	0,97%
ClickPay	1	0,97%

TABLE 5.7: Pourcentage d'intégration des prestataires de paiement

Nous constatons que les prestataires de paiement bancaire les plus utilisés sont Sips, Cybermut, Ogone, Paybox, CyberPlus/Payzen et Spplus. Nous présentons dans l'annexe B l'implémentation technique de quelques automates de paiement.

5.7.4 Validation et limites

Maintenant que nous avons décrit le principe de fonctionnement des automates de paiement, nous allons tenter de valider cette proposition et étudier ses éventuelles limites.

Validation

L'usage des automates de paiement permet de garantir une meilleure expérience client. En effet, tous les échanges avec le prestataire de paiement bancaire sont effectués de serveur à serveur sans passer par le navigateur du client. Afin de mettre en évidence cet avantage, nous avons comparé la liste des Urls affichées dans le navigateur du client dans le cas d'un paiement Proxy Web et celle dans le cas d'un paiement par automate lors d'un paiement alternatif sur un site E-commerce (tableau 5.8). Nous pouvons constater que le nombre d'Urls affichées par le navigateur du client

lors de la redirection vers la page de paiement alternatif diminue considérablement dans le cas de l'automate de paiement.

La liste des Urls appelées par le navigateur du client :
Cas du Proxy Web : 1-http://www.kiabi.com/030-COMMANDE/10-30_modepaiement.asp 2-https://api.limonetik.com/V2_1/GoPayment 3-https://Proxycore.limonetik.com/LmkIssuer/illicado/RefDomain/limonetik.com/AddAnyCards/LmkUserId/testachat@limonetik.com/LmkDomain/GoShop/kiabi-fr/StartUrl/paiement.sogenactif.com/cgis-payment-sogenactif/prod/callpayment 4-https://paiement.limonetik1.com/LmkSession/lb4sm0qkvksino55gzlkhone/https/paiement.sogenactif.com/cgis-payment-sogenactif/prod/callpayment 5-https://paiement.limonetik1.com/cgis-payment-sogenactif/prod/callpayment 6-https://illicado.limonetik.com/Pages/Wait.aspx 7-https://illicado.limonetik.com/Payment/PayForm.aspx?634336456245028447
Cas de l'automate de paiement : 1-http://www.kiabi.com/030-COMMANDE/10-30_modepaiement.asp 2-https://merchant.limonetik.com/api/v2/paymentorder/create 3-https://illicado.limonetik.com/Payment/PayGoto.aspx?LmkOrderExternalID=999995723001&AddAnyCards=true 4-https://illicado.limonetik.com/Payment/PayForm.aspx?634251810523605836

TABLE 5.8: illustration de la diminution du nombre des pages intermédiaires dans le cas de l'automate de paiement

En plus de l'avantage ergonomique et l'amélioration de la qualité de l'expérience utilisateur sur le site E-commerce, nous notons également que l'automate de paiement permet de garantir le même niveau de sécurité que celui apporté par le Proxy Web, voire qu'il améliore la sécurité du système de paiement alternatif, car la récupération de la page de paiement bancaire ne se fait pas via le navigateur du client. Cependant, l'usage de l'automate de paiement au lieu du Proxy Web ne change rien au niveau de la complexité de l'intégration via Plugin JavaScript. En effet, cette partie de l'intégration qui concerne la deuxième phase (paiement) présentée dans la figure 2.3 est complètement transparente pour l'E-commerçant.

Limites

Malgré les différents avantages de l'automate de paiement, il reste, tout de même, très dépendant du contenu HTML des pages de paiement bancaires du site E-commerce ou du prestataire de paiement bancaire. En effet, tout comme le Proxy Web, l'automate de paiement se base sur le contenu des pages HTML afin d'effectuer le paiement et de récupérer les données recherchées. Tout changement des pages de paiement bancaire de l'E-commerçant engendre une mise à jour des expressions

régulières de l'automate. De plus, dans certains cas, contrairement au paiement via le Proxy Web, l'utilisation de l'automate de paiement semble impossible. En effet, comme nous l'avons montré dans l'état de l'art, certaines pages de paiement bancaire sont intégrées en Iframe chez l'E-commerçant. Dans ce cas, elles n'affichent pas le montant de la transaction, puisqu'elles sont destinées à être affichées dans une page « mère » sur le site E-commerce, qui affiche toutes les données de la commande (y compris le récapitulatif du panier du client). Le paiement via Proxy Web semble alors être mieux adapté.

5.8 Conclusion

Nous avons proposé, dans ce chapitre, une deuxième approche d'intégration de la nouvelle architecture de paiement, présentée dans le chapitre 3. Il s'agit d'une approche d'intégration via Plugin Javascript. Contrairement à l'intégration via Proxy Web, présentée dans le chapitre précédent, l'E-commerçant doit intégrer une librairie JavaScript dans la page de choix de moyens de paiement sur son site, qui se charge de rediriger le client vers la page de paiement alternatif, une fois que ce moyen de paiement est sélectionné. En proposant cette nouvelle approche d'intégration, nous cherchons à pallier les inconvénients de la première approche qui exige un maintenance très coûteuse du côté du prestataire de paiement alternatif, afin de mettre à jour les configurations Proxy des sites E-commerce.

Nous avons présenté, dans ce chapitre, le principe de fonctionnement du Plugin JavaScript, ainsi que les différentes étapes d'intégration du moyen de paiement alternatif dans un site E-commerce. Ensuite, nous avons évalué ce nouveau mode d'intégration selon les critères annoncés dans l'état de l'art (la sécurité, l'ergonomie et la complexité). Nous résumons cette évaluation dans le tableau 5.9 qui présente les avantages et les inconvénients de ce mode d'intégration.

L'intégration via Plugin JavaScript ne nécessite pas beaucoup de développement technique du côté de l'E-commerçant, qui n'a qu'à intégrer un appel à une librairie JavaScript dans sa page de choix de moyen de paiement. Cette nouvelle approche, permet également de ne pas altérer l'expérience utilisateur sur le site E-commerce. En effet, le client démarre sa navigation depuis le site en direct et est redirigé vers la page de paiement alternatif au moment de choix du nouveau moyen de paiement. De plus, cette intégration permet à l'E-commerçant de proposer un système de paiement non bancaire (alternatif) sécurisé qui garantit les différents critères cryptographique, qui sont : la confidentialité, l'authentification, l'intégrité et la non-répudiation.

Dans le cadre de cette approche, et afin d'effectuer la conversion du paiement

alternatif en paiement bancaire, le prestataire de paiement alternatif a deux possibilités : la première consiste à payer à l'aide du Proxy Web, en redirigeant le client vers le serveur du Proxy Web, une fois le moyen de paiement alternatif est choisi. Cependant cette solution présente quelques inconvénients, notamment concernant l'expérience utilisateur lors de la redirection du client vers la page de paiement. D'où la deuxième possibilité qui consiste à payer à l'aide d'un automate de paiement qui permet de garantir une meilleure expérience client et améliorer le niveau de sécurité du paiement, puisque tous les échanges avec le prestataire de paiement bancaire sont effectués de serveur à serveur sans passer par le navigateur du client.

	Sécurité	Ergonomie	Complexité
Avantages	- Les données de la commande (montant, référence...), envoyées au prestataire de paiement alternatif, sont sécurisées, car il s'agit des même données envoyées au prestataire de paiement bancaire de l'E-commerçant (supposé sécurisé). - Un client malveillant ne peut pas modifier le montant de la commande, ni le résultat du paiement - L'envoi des données de la CVD à l'E-commerçant, qui permet de convertir le paiement alternatif en paiement bancaire, se fait de serveur à serveur, donc le client ne peut pas intercepter cette donnée. - La CVD correspond à un montant fixe et est à usage unique, ce qui limite les risques de fraude. - Dans le cas d'un paiement par un automate de paiement, la récupération des données de la commande est effectuée de serveur à serveur, sans passer par le navigateur du client.	- Le nouveau moyen de paiement est inséré par l'E-commerçant, l'ajout est alors conforme à la charte graphique du site. - Le client démarre sa navigation depuis le site en directe, sans passer par un portail, l'expérience utilisateur n'est donc pas altérée.	- L'E-commerçant doit ajouter seulement une librairie JavaScript dans la page de choix de moyens de paiement. Le coût d'intégration est donc inférieur à celui des modes d'intégration existants, qui étaient décrits dans l'état de l'art. - Le paiement alternatif est converti en paiement bancaire, l'E-commerçant n'a pas donc à traiter de nouveaux flux financiers. - L'orchestration de plusieurs moyens de paiement du client est également gérée par le prestataire de paiement alternatif.
Inconvénients		- Le Plugin Javascript est fortement dépendant du navigateur du client.	- Contrairement à l'intégration via Proxy Web, l'E-commerçant doit effectuer un développement technique pour ajouter le moyen de paiement sur son site.

TABLE 5.9: Avantages et inconvénients de l'intégration via Plugin JavaScript

Conclusion générale et perspectives

Dans le cadre de la collaboration avec le partenaire industriel « Limonetik », éditeur et intégrateur d'une nouvelle architecture de paiement sur Internet, la problématique traitée dans cette thèse se trouve à l'intersection des disciplines de la monétique et de l'informatique. A partir de ces deux disciplines, notre travail de recherche a consisté en la proposition d'une solution de paiement sur le Web, sécurisée et facile à intégrer par les boutiques E-commerce actuelles. Cette solution a été construite à partir de travaux académiques tout en prenant en compte l'expérience acquise par notre partenaire industriel.

Nous revenons, dans un premier temps, sur les résultats liés à notre thèse, tant sur le plan académique qu'industriel. Dans un deuxième temps, nous proposons quelques pistes de réflexion sur les perspectives de poursuivre des recherches que nous inspirent les résultats obtenus.

Bilan académique et industriel

Au cours de cette thèse, nous nous sommes intéressés à l'émergence de nouveaux moyens de paiement dans l'E-commerce et à leur intégration dans les boutiques en ligne. En effet, malgré les évolutions technologiques, le commerce électronique sur Internet est encore très restreint en fonctionnalités comparé à celui de proximité. Dans la première partie de notre étude, nous nous sommes attachés à définir le contexte de nos travaux de recherche, à présenter l'évolution de l'E-commerce, à présenter les nouveaux moyens alternatifs émergents, et à mettre en évidence les nouveaux besoins d'acceptation de ces nouveaux instruments de paiement sur la toile.

Dans un premier temps, nous avons situé, à partir d'une analyse bibliographique effectuée dans le chapitre 1, la place du système de paiement dans le commerce

électronique. Nous avons souligné, qu'il s'agit d'un système central permettant l'achat de services et de biens sur Internet, en définissant la terminologie qui sera utilisée dans le cadre de cette étude. Dans un deuxième temps, nous nous sommes intéressés à définir les moyens de paiement objet de nos recherches et aux différentes contraintes empêchant leur intégration sur Internet. A partir d'une étude de la littérature et de l'expérience de notre partenaire industriel, nous avons pu relever trois contraintes majeures d'intégration d'un système de paiement sur Internet : la sécurité, l'ergonomie et la complexité, que nous avons considérées comme des critères d'évaluation de l'intégration des systèmes de paiement sur Internet.

Ensuite, nous avons étudié, dans le chapitre 2, le paysage des approches d'intégration existantes afin de comprendre les solutions existantes et les comparer entre elles. A partir de cette base bibliographique, nous avons produit un cadre de référence pour l'intégration des moyens de paiement sur Internet. La définition de l'architecture de paiement intégrant les nouveaux moyens de paiement devient alors de plus en plus complexe. Nous ne pouvons pas demander au marchand d'utiliser les approches d'intégration existantes, qui nécessitent un investissement, afin d'intégrer des moyens de paiement dont certains ne sont pas utilisés par plusieurs clients. Par conséquent, il est nécessaire de faciliter l'intégration de ces nouveaux moyens de paiement « alternatifs ».

Ces deux premiers chapitres définissent le contexte de cette thèse, ainsi que les outils préalables à notre étude. Nous avons ensuite présenté les différentes contributions de cette thèse liées à l'intégration des moyens de paiement non bancaires sur Internet.

Dans le cadre de nos travaux de thèse, nous nous sommes particulièrement intéressés à l'aspect technique de ce problème, afin de proposer des solutions faciles à intégrer dans la boutique E-commerce du marchand tout en respectant les exigences technologiques définies au début de notre étude. La première contribution, présentée dans le chapitre 3, concerne la proposition d'une nouvelle architecture de paiement permettant de convertir les paiements non bancaires en paiements bancaires à l'aide des cartes virtuelles dynamiques. Ainsi, l'intégration chez l'E-commerçant se réduit au système « accepteur », puisque le système « acquéreur » sera le même que celui du système bancaire, déjà intégré par l'E-commerçant. Nous avons décrit le principe de fonctionnement de cette nouvelle architecture ainsi que le processus de conversion des paiements et la gestion des différents flux financiers nécessitant l'intervention d'un émetteur de monnaie électronique et d'une banque. Cette architecture permet d'appréhender facilement des échanges complexes entre les différents acteurs du système de paiement afin de diminuer la complexité de l'intégration des moyens de

paiement alternatifs pour l'E-commerçant.

La deuxième contribution, présentée dans le chapitre 4, est une approche d'intégration, via Proxy Web, de cette nouvelle architecture de paiement. Il s'agit d'un nouveau mode d'intégration de moyens de paiement sur Internet, qui ne nécessite aucune intervention de la part de l'E-commerçant. Cette approche est basée sur un Proxy Web qui permet d'interpréter le contenu HTML des pages Web du site marchand et d'injecter le code nécessaire afin d'ajouter les nouveaux moyens de paiement alternatifs et de rediriger le client vers les pages de paiement correspondantes. Il s'agit donc d'une intégration qui ne demande aucun développement technique du côté de l'E-commerçant et qui respecte les exigences d'un système de paiement. Cette approche a été implémentée au sein de « Limonetik », le partenaire industriel de nos travaux de recherche, et plusieurs moyens de paiement alternatifs (cartes cadeaux, listes de mariage, portes monnaie virtuelles, etc.) ont pu ainsi être acceptés par un grand nombre de sites marchands, sans que ces derniers aient à effectuer du développement technique de leur côté. Cependant, cette approche demande une maintenance continuelle des configurations Proxy des sites E-commerce et est très dépendante de tout le parcours client sur le site E-commerce.

D'où notre troisième contribution, soit la proposition d'une deuxième approche d'intégration via Plugin JavaScript qui consiste à demander à l'E-commerçant d'ajouter le nouveau moyen de paiement et d'intégrer une librairie JavaScript dans la page de choix de moyens de paiement sur son site E-commerce. Cette librairie se charge de récupérer les données de la commande, nécessaires pour gérer les paiements non bancaires sur le site marchand. La conversion du paiement alternatif en paiement bancaire, dans le cadre de l'intégration via Plugin JavaScript, peut être effectuée selon deux méthodes : la première méthode consiste à réutiliser le Proxy Web. Cependant, cette solution présente quelques inconvénients, notamment concernant l'expérience utilisateur. La deuxième solution consiste à payer l'E-commerçant à l'aide d'un automate de paiement, ce qui permet d'améliorer la qualité de l'expérience client et du paiement CVD sur le site E-commerce. Cette approche a été implémentée et testée au sein de « Limonetik ». Elle est actuellement utilisée par certains E-commerçants. Des travaux d'industrialisation de cette approche d'intégration sont actuellement menés par l'équipe R&D de notre partenaire industriel.

Parmi les contributions de nos travaux de recherche, citons également la définition d'une méthodologie d'évaluation de l'intégration d'un système de paiement sur Internet qui consiste en l'analyse des trois critères : la sécurité, l'ergonomie et la complexité. Dans notre travail, nous avons montré comment intégrer des moyens de paiement non bancaires sur Internet d'une manière sécurisée, tout en palliant

la contrainte de la complexité de l'intégration du côté de l'E-commerçant et en garantissant une bonne expérience utilisateur sur le site E-commerce. La solution proposée peut être déployée dans l'espace unique de paiement euro SEPA.

Enfin, les prototypes proposés par cette thèse ont été expérimentés dans le cadre des projets menés par la société « Limonetik » qui ont permis la validation de chacune des solutions présentées dans nos travaux de recherche.

Vers une approche méthodologique plus générale

Dans cette section, nous étudions la possibilité de généraliser les différentes approches d'intégration proposées dans notre travail. Lors de la présentation de la nouvelle architecture de paiement (chapitre 3), nous avons annoncé que nous nous intéressions seulement aux E-commerçants ayant déjà intégré un terminal de paiement virtuel bancaire. Nous étudierons donc, ici, la possibilité de généraliser les approches d'intégration de la nouvelle architecture à la deuxième partie d'E-commerçants qui n'ont pas installé un terminal de paiement bancaire et qui souhaitent intégrer un moyen de paiement alternatif dans leur boutique Web.

Comme nous l'avons expliqué, au début de notre étude, l'intégration d'un système de paiement sur Internet doit être réalisée dans deux sous-systèmes du système de paiement (généralement « quatre coins »). Le premier sous-système est le système accepteur, qui concerne la partie « front-office » d'un système de paiement et qui permet d'ajouter le moyen de paiement sur le site E-commerce et de rediriger le client vers la page de paiement. Le deuxième sous-système est le système acquéreur, qui concerne la partie « back-office » d'un système de paiement et qui permet de demander l'autorisation de paiement à l'émetteur, de garantir le paiement de l'E-commerçant, de gérer les différentes opérations financières et de mettre à jour des statuts des transactions. Notre objectif étant d'exiger le minimum de développement technique du côté de l'E-commerçant, nous avons proposé une nouvelle architecture de paiement qui permet de réduire l'intégration des moyens de paiement alternatifs à l'intégration dans le système accepteur de l'E-commerçant, c'est-à-dire, au « front-office » de son site E-commerce, en convertissant ces paiements alternatifs en paiements bancaires et se basant ainsi sur le système acquéreur bancaire de l'E-commerçant. Nous constatons, alors, que la suppression de l'hypothèse d'installation préalable d'un système de paiement bancaire sur le site E-commerce, entraîne l'intégration du moyen de paiement alternatif dans le système acquéreur de l'E-commerçant, c'est-à-dire la gestion du transfert des fonds depuis le compte du client chez l'émetteur au compte de l'E-commerçant, afin de pouvoir payer l'E-commerçant, après la validation du

paiement alternatif du client. Nous pouvons imaginer que l'E-commerçant ouvre un compte bancaire chez la banque intermédiaire ou un compte de monnaie électronique chez l'émetteur de monnaie électronique afin recevoir les fonds liés aux paiements alternatifs sur son site.

Intéressons-nous, maintenant, à l'intégration dans le système accepteur (« front-office ») de l'E-commerçant. Dans un premier temps, analysons la possibilité de généraliser l'intégration via Proxy Web. Comme nous l'avons décrit dans le chapitre 4, cette approche consiste à intercepter les échanges entre le client et le marchand afin d'injecter du code HTML dans les pages renvoyées par le serveur de l'E-commerçant. Ainsi, le nouveau moyen de paiement peut être ajouté parmi les instruments de paiement proposés par le site E-commerce. Cependant, au moment du choix du nouveau moyen de paiement, le Proxy Web doit pouvoir récupérer le montant du panier ainsi que la référence de la commande depuis le site E-commerce sans se baser forcément sur la page de paiement bancaire (qui est absente du cadre de cette étude). Cela veut dire que l'E-commerçant doit afficher une page de récapitulatif de commande où il rappelle le montant du panier et la référence de la commande. Dans ce cas, le Proxy Web peut récupérer ces valeurs et rediriger le client vers le partenaire de paiement alternatif. Sachant que le Proxy Web ne peut plus se baser sur la sécurité offerte par le système de paiement bancaire de l'E-commerce, il faut donc qu'il sécurise les données de la commande envoyées lors de la redirection du client vers le prestataire de paiement alternatif. Nous pouvons donc imaginer que le Proxy Web intègre le système de paiement alternatif à la place de l'E-commerçant, selon un des modes d'intégration décrits dans l'état de l'art (chapitre 2) : via Services Web, via redirection HTTP chiffrée ou via redirection HTTP signée.

Analysons maintenant la possibilité de généraliser l'intégration via Plugin JavaScript. Rappelons que cette approche consiste à demander à l'E-commerçant d'intégrer une librairie JavaScript dans sa page de choix de moyens de paiement. Ainsi, la récupération des données de la commande et la redirection vers la page de paiement sont effectuées en JavaScript. Dans le cas de la nouvelle architecture, les données récupérées par le Plugin JavaScript sont déjà sécurisées par le système de paiement bancaire de l'E-commerçant, une condition indispensable à la sécurité des données de paiement, car le JavaScript est un langage qui s'exécute du côté client et qui est donc vulnérable. Si on supprime le système de paiement bancaire de l'E-commerçant, cela veut dire que l'E-commerçant doit sécuriser les données de commande avant de les envoyer via le Plugin JavaScript au prestataire de paiement alternatif, ce qui revient à appliquer un des modes d'intégration décrits dans l'état de l'art. De ce fait, l'intégration via Plugin JavaScript ne peut pas être généralisée.

Perspectives et travaux futurs

Le travail présenté dans cette thèse a pour premier objectif de contribuer à la mise en place d'une plateforme de paiement permettant d'intégrer des moyens de paiement non bancaires sur Internet. Les perspectives envisageables de nos travaux de recherche concernent 3 objectifs importants : l'enrichissement du nouveau modèle d'architecture de paiement proposée dans le cadre de cette thèse, l'enrichissement des approches d'intégration des moyens de paiement dans le site E-commerce et l'amélioration du schéma d'agrégation de plusieurs moyens de paiement.

En premier lieu, il semblerait nécessaire d'approfondir l'architecture proposée dans le cadre de cette thèse afin de la rendre générique. Si nous pouvons nous passer de convertir le paiement « alternatif » en paiement bancaire et payer directement le marchand, cela simplifiera les flux financiers du côté du prestataire de paiement alternatif. Nous pouvons proposer d'utiliser un des moyens de paiement SEPA (Single Euro Payment Area) pour payer l'E-commerçant : le virement SCT (SEPA Credit Transfer) ou le prélèvement SDD (SEPA Direct Debit). Nous pouvons également imaginer que l'E-commerçant délègue la gestion de tous les moyens de paiement acceptés sur son site E-commerce au prestataire de paiement alternatif, qui se charge de gérer l'affichage et l'orchestration de ces instruments de paiement.

En deuxième lieu, nous pouvons imaginer que certains moyens de paiement ne seront affichés sur le site E-commerce qu'en cas de besoin, par exemple seulement lorsque le client est passé par un portail de l'émetteur du moyen de paiement, afin de ne pas encombrer la page de choix de moyen du site E-commerce. Cette fonctionnalité peut être réalisée en se basant sur les cookies de l'utilisateur afin de détecter son parcours de navigation.

Dans le cadre de cette thèse, nous nous sommes intéressés au problème de l'intégration du moyen de paiement dans le site E-commerce. Plusieurs autres problèmes restent à résoudre afin de mieux gérer cette intégration et l'orchestration de plusieurs moyens de paiement qui peut s'avérer complexe lorsqu'il s'agit de moyens de paiement très diversifiés.

Il existe également des perspectives plus larges de nos travaux de recherche, qui concernent l'extension de notre étude à l'échelle internationale et l'analyse des différentes caractéristiques de moyens de paiement non bancaires dans d'autres pays ayant des cultures monétiques différentes de celle de l'Europe. D'autres environnements d'étude peuvent être également explorés. Dans le cadre de cette thèse, nous nous sommes intéressés au commerce électronique sur Internet, mais nous pouvons imaginer de réaliser la même étude dans le domaine de M-commerce (mobile) ou S-commerce (Social).

Publications de l'auteur

Chapitre de livre international en cours de publication

1. Pasquet M., **Abdellaoui R.**, Gerbaix S. « E-Payment security : which solutions for which issues ? »

Conférences internationales avec comité de lecture et avec actes

1. **Abdellaoui R.**, Pasquet M., « Secure Communication For Internet Payment In Heterogeneous Networks », IEEE International Conference on Advanced Information Networking and Applications (AINA) 2010, ISBN : 978-0-7695-4018-4
2. **Abdellaoui R.**, Pasquet M., Berthelier O. « Integration of New Payment System into B2C Internet Commerce », International Symposium on Collaborative Technologies and Systems (CTS), 2011. ISBN : 978-1-61284-638-5.

Rapports de recherche

1. **Abdellaoui R.** « Rapport de la 2ème année de thèse », ANRT (Association Nationale de la Recherche et de la Technologie), février 2010,
2. **Abdellaoui R.** « Rapport de la 1ère année de thèse », ANRT (Association Nationale de la Recherche et de la Technologie), février 2009.

Bibliographie

[Abdellaoui R. et Pasquet M., 2010] Abdellaoui R. et Pasquet M. (2010). Secure communication for internet payment in heterogeneous networks. *The 24th IEEE International Conference on Advanced Information Networkingand Applications (AINA), 2010.* [cité p. 58]

[Abdellaoui R., Pasquet M., Berthelier O., 2011] Abdellaoui R., Pasquet M., Berthelier O. (2011). Integration of new electronic payment systems into b2c internet commerce. *Collaboration Technologies and Systems (CTS)*, pages 484 – 491. [cité p. 89, 90]

[Abrazhevich D., 2001] Abrazhevich D. (2001). Electronic payment systems : a user-centered perspective and interaction design. *Computer Science 2115 (2001), p. 81-23.* [cité p. 20]

[ADN'co, 2011] ADN'co (2011). Les moyens de paiements alternatifs : Un secteur en mutation sur le e-commerce. *Une étude réalisée par ADN'co pour Limonetik. Paris, le 22 novembre 2011.* [cité p. 14, 15]

[Albouy M., Schatt A., 2004] Albouy M., Schatt A. (2004). Les prises de contrôle par les actionnaires contestataires : le cas andré. *Finance Contrôle Stratégie - Volume 7, N° 2, juin 2004, p. 33 -65.* [cité p. 40]

[Amami M., Rowe F., 2000] Amami M., Rowe F. (2000). Les opportunités de recherche en commerce electronique sur internet. *5ème colloque de l'AIM, Montpellier IAE Université.* [cité p. 40]

[Asokan N., Janson A., Steiner M, 1997] Asokan N., Janson A., Steiner M (1997). State of the art in electronic payment systems. *IEEE Computer 30 (1997), no. 9, p. 28-35.* [cité p. 20]

[Association Française de la Télématique, 1997] Association Française de la Télématique (1997). *Internet : les enjeux pour la France. Chapitre "Commerce électronique".* Livre Blanc, Edition AFTEL, 1997. [cité p. 9]

[Autorité de la concurrence, 2011] Autorité de la concurrence (2011). Décision n° 11-d-11 du 7 juillet 2011 relative à des pratiques mises en oeuvre par le groupement des cartes bancaires. *http ://www.autoritedelaconcurrence.fr/pdf/avis/11d11.pdf.* [cité p. 78]

[Banque Centrale Européenne, 2003] Banque Centrale Européenne (2003). Normes de surveillance pour les systèmes de paiement de masse en euros. *ISSN 1725-6151, 2003b.* [cité p. 22]

[Banque Centrale Européenne, 2010] Banque Centrale Européenne (2010). The payment system : payments, securities and derivatives, and the role of the eurosystem. *Kokkola Tom (Editeur), ISBN 978-92-899-0632-6.* [cité p. 15]

[Banque des Règlements Internationaux, 2001] Banque des Règlements Internationaux (2001). Principes fondamentaux pour les systèmes de paiement d'importance systémique : rapport du groupe de travail sur les principes et pratiques applicables aux systèmes de paiement. *ISBN 92-9131-220-7.* [cité p. 22]

[Bardet S., 2003] Bardet S. (2003). *Livre blanc : Les Services Web.* [cité p. 42]

[Battini P., 2000] Battini P. (2000). *Capital-risque : Mode d'emploi.* Broché. [cité p. 40]

[Bohle K., 2002] Bohle K. (2002). Integration of electronic payment systems into b2c internet commerce. *Background Paper No. 8 Electronic Payment Systems Observatory (ePSO), 2002.* [cité p. 9, 10]

[Borzmeyer S., 2003] Borzmeyer S. (2003). Les web services : connecter des applications. *AFNIC.* [cité p. 43]

[Bounie D., 2000] Bounie D. (2000.). Ict and electronic fund transfers : Economic stakes and monetary perspectives. *Communications et Stratégies, 38(2), p. 277-309.* [cité p. 13]

[Bounie D. et Bourreau M. , 2004] Bounie D. et Bourreau M. (2004). Sécurité des paiements et développement du commerce électronique. *Presses de Sciences Po - Revue économique, 2004 - Vol. 55*, page pages 689 à 714. [cité p. 24]

[Brousseau E., 1999] Brousseau E. (1999). The governance of transaction by commercial intermediaries : An analysis of the re-engineering of intermediation by electronic commerce. *Third Conference of the International Society for New Institutional Economics September 16-18, 1999 Washington DC, USA- 35 p.* [cité p. 8]

[Brousseau E., 2001] Brousseau E. (2001). Commerce électronique : ce que disent les chiffres et ce qu'il faudrait savoir. *Economie et Statistique, N 339-340.* [cité p. 7]

[Chanel-Reynaud, G. et Chabert, D., 2004] Chanel-Reynaud, G. et Chabert, D. (2004). L'infrastructure financiere europeenne : quels schémas de developpement pour la future europe des titres ? *Paris : Revue Banque edition. Marche finance.*, page 303. [cité p. 15]

[Christos E., Hammond K., 2000] Christos E., Hammond K. (2000). Internet usage : Predictors of active users and frequency of use. *Journal of Interactive Marketing.* [cité p. 24]

[Clusif, 2011] Clusif (2011). Pcidss : un standard contraignant ? ! *CLUSIF (Club de la Sécurité de l'Information Français).* [cité p. 41]

[Commission Commerce Electronique, 2012] Commission Commerce Electronique (2012). Chapitre français de l'isoc ou internet society. *http ://www.isoc.asso.fr.* [cité p. 7]

[CREDOC-FEVAD, 2008] CREDOC-FEVAD (2008). Le profil des acheteurs à distance et en ligne. [cité p. 9]

[CREDOC-FEVAD, 2010] CREDOC-FEVAD (2010). Enquête sur le profil des acheteurs à distance et en ligne. [cité p. 9]

[Credoc-Institut Français de la Mode, 2011] Credoc-Institut Français de la Mode (2011). L'impact du commerce électronique en matiere de soldes et de promotions. [cité p. 9]

[Denis M E., 2010] Denis M E. (2010). *Évaluation d'un outil de mesure de la complexité des procédures.* Thèse de doctorat, Département de mathématiques et de génie industriel école polytechnique de montréal. [cité p. 39, 40]

[Dubois J. et Jreije P., 2006] Dubois J. et Jreije P. (2006). Mechanisms of internet security attacks. *World Academy of Science, Engineering and Technology 20 2006.* [cité p. 37]

[Fauconnier F., 2010] Fauconnier F. (2010). Bilan 3dsecure. *Journal du Net.. http ://www.journaldunet.com/ebusiness/commerce/bilan-3dsecure/multiples-difficultes.shtml.* [cité p. 62]

[Fevad, 2008] Fevad (2008). Etude fevad / médiamétrie sur le paiement en ligne. *Communiqué de presse : http ://www.fevad.com/espace-presse/14-05-08-etude-fevad-mediametrie-sur-le-paiement-en-ligne.* [cité p. 24]

[Fevad, 2010a] Fevad (2010a). Les acheteurs à distance et en ligne en 2010. *http ://www.fevad.com/uploads/files/prez/Fevad_credoc_2010_synthese.pdf.* [cité p. 9]

[Fevad, 2010b] Fevad (2010b). E-commerce au 3ème trimestre 2010. *http ://www.fevad.com/espace-presse/18-11-2010-e-commerce-au-3eme-trimestre-2010-1.* [cité p. 8, 9, 27]

[Fevad, 2010c] Fevad (2010c). Ventes à distance et e-commerce aux particuliers : Chiffres clés 2010. [cité p. 13]

[Fielding R T., 2000] Fielding R T. (2000). *Architectural Styles and the Design of Network-based Software Architectures.* Thèse de doctorat, UNIVERSITY OF CALIFORNIA, IRVINE. [cité p. 45]

[Financial Crimes Enforcement Network, 2000] Financial Crimes Enforcement Network (2000). A survey of electronic cash, electronic banking and internet gaming. *U.S. Department of the Treasury.* [cité p. 12]

[Floridi L., 2005] Floridi L. (2005). Semantic conceptions of information. *Edward N. Zalta (ed.), Stanford Encyclopedia of Philosophy, http ://plato.stanford.edu/entries/information-semantic/.* [cité p. 7]

[Furche, A. et Wrightson, G., 1996] Furche, A. et Wrightson, G. (1996). *Computer Money : A Systematic Overview of Electronic Payment Systems.* Morgan Kaufmann Pub, octobre 1996, 108p. [cité p. 20]

[Gambarotto P., 2009] Gambarotto P. (2009). Technologies pour web services faciles : Rest, json. *Les Journaux Réseaux JRES 2009.* [cité p. 43]

[Garrett J., 2005] Garrett J. (2005). Ajax : A new approach to web applications. *Web Adaptive Path, http ://www.adaptivepath.com/ideas/ajax-new-approach-web-applications.* [cité p. 128]

[Gervais J F., 2007] Gervais J F. (2007). *Web 2.0 - Les internautes au pouvoir.* Dunod. [cité p. 6]

[Gill S., 2003] Gill S. (2003). Type d'attaques. *Document soumis à la licence GNU FDL. http ://sgill.ep.profweb.qc.ca/spip/IMG/pdf/02_TypeAttaque.pdf.* [cité p. 37]

[Hassairi A F., 2001] Hassairi A F. (2001). *L'évaluation des investissements en systèmes et technologies de l'information : cas des échanges de données informatiques chez les équipementiers automobiles.* Thèse de doctorat, Université Toulouse 1. [cité p. 40]

[Havinga M., Smit M., Helme A., 1996] Havinga M., Smit M., Helme A. (1996). Survey of electronic payment methods and systems. *Proceedings Euromedia '96, 1996, p. 180-192.* [cité p. 20]

[Jeffrey K. MacKie M, et Kimberly W, 1997] Jeffrey K. MacKie M, et Kimberly W (1997). Evaluating and selecting digital payment mechanisms. *Interconnection and the Internet, G. Rosston and D. Waterman, eds. Lawrence Erlbaum, 1997 : 113-134.* [cité p. 20]

[Kannen M., Leischner M., Stein T., 2003] Kannen M., Leischner M., Stein T. (2003). A framework for providing electronic payment services. *10th annual workshop of HP-OVUA, July 6-9, 2003 Geneva.* [cité p. 17]

[KONZ S., JOHNSON S., 2000] KONZ S., JOHNSON S. (2000). Work design - industrial ergonomics (5th edition). *Scottsdale, Arizona : Holcomb Hayhaway.* [cité p. 39]

[Ladwein R, 2000] Ladwein R (2000). Le web design et l'ergonomie des sites de e-commerce : vers l'elaboration d'un modèle. *CONVEGNO, Nouvelles Tendances du Marketing en Europe.* [cité p. 25]

[Le Crosnier H., 1997] Le Crosnier H. (1997). Avons-nous besoin des journaux électroniques ?. *[Communication]. SFSIC-ENSSIB, November1997.* [cité p. 8]

[Lehuédé F, 2006] Lehuédé F (2006). Internet donne plus de pouvoir aux consommateurs. *Crédoc -ISSN 0295-9976- N° 197 - octobre 2006.* [cité p. 7]

[Lelieveldt Consultancy, 2001] Lelieveldt Consultancy (2001). Research study on the integration of e-payments into the online transaction process. *Amsterdam, December 12, 2001.* [cité p. 9]

[Lorentz F., 1998] Lorentz F. (1998). Le commerce électronique : une nouvelle donne pour les consommateurs, les entreprises, les citoyens et les pouvoirs publics. *Rapport au ministre de l'économie, des finances et de l'industrie. FRANCE. Ministère de l'économie, des finances et de l'industrie. "http ://www.finances.gouv.fr/commerce_electronique/lorentz/sommaire.html".* [cité p. 7, 8]

[Lyra-Network, 2011] Lyra-Network (2011). *Guide d'implémentation - Interface avec la plateforme de paiement V2.* [cité p. 189]

[Macarez N. et Lesle F., 2001] Macarez N. et Lesle F. (2001). *Le Commerce Electronique, Editions PUF - Collection Que sais-je ?* [cité p. 7, 8]

[Mennis A., 1999] Mennis A. (1999). Les problèmes de mise en oeuvre d'internet et d'intranet et les problèmes de sécurité. *DEA-SI / MATIS.* [cité p. 6]

[Mennis A., 2003] Mennis A. (2003). Le commerce electronique et les changements organisationnels : quelques aspects de la problématique. *8ème colloque de l'AIM 21 - 23 mai, Grenoble, France*, Source : http ://www.aim2003.iut2.upmf-grenoble.fr/Communications/MENNIS.rtf. [cité p. 8]

[Mennis A., 2005] Mennis A. (2005). *Le commerce Electronique : construction d'une approche d'évaluation et de conception pour la prise de décision de sa mise en oeuvre.* Thèse de doctorat, Ecole doctorale sciences de gestion de grenoble - ED275. [cité p. 16]

[Mookhey K., 2011] Mookhey K. (2011). "common security vulnerabilities in e-commerce systems" http ://www.symantec.com/connect/articles/common-security-vulnerabilities-e-commerce-systems. [cité p. 37]

[Neuman, C. and Medvinsky, G., 1995] Neuman, C. and Medvinsky, G. (1995). Requirements for network payment : The netcheque perspective. *Proceedings of IEEE Compcon '95, mars 1995, 5p.* [cité p. 20]

[O'Brien T., 2000] O'Brien T. (2000). *E-commerce Handbook A practical guide to developing a successful e-business strategy.* Tri-Obi Production, Melbourne. [cité p. 7]

[Observatoire de la Sécurité des Cartes de Paiement, 2010] Observatoire de la Sécurité des Cartes de Paiement (2010). Statistiques de fraude pour 2010. [cité p. 23]

[Park J., 2009] Park J. (2009). *The Complexity of Proceduralized Tasks.* [cité p. 39]

[Parlement Européen et du Conseil, 2007] Parlement Européen et du Conseil (2007). Directive 2007/64/ce du parlement europée et du conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/ce, 2002/65/ce, 2005/60/ce ainsi que 2006/48/ce et abrogeant la directive 97/5/ce. *Journal officiel de l'Union européenne.* [cité p. 17]

[Pasquet M., Rosenberger C., Cuozzo F., 2008] Pasquet M., Rosenberger C., Cuozzo F. (2008). Security for electronic commerce. *Book Chapters.* [cité p. 180]

[Paypal, 2009] Paypal (2009). Soap api developer reference. [cité p. 46, 47]

[Peressini C., 2001] Peressini C. (2001). La dématérialisation des marchés publics. *Magazine 01-Informatique, n°1642-1643,13 juillet, pp 48.* [cité p. 8]

[Petit B., 1999] Petit B. (1999). *Guide de l'information européenne : vade-mecum à l'usage de l'enseignement et de la formation professionnelle.* Educagri. [cité p. 12]

[Piffaretti N., 2000] Piffaretti N. (2000). *Monnaie electronique, monnaie et intermediation bancaire.* Thèse de doctorat, Faculté des sciences économiques et sociales de l'Université de Fribourg (Suisse). [cité p. 76]

[Polanyi K., 1968] Polanyi K. (1968). Primitive, archaic and modern economies : Essays of karl polanyi. *Garden City, N.Y., 1968.* [cité p. 11]

[Preneel B., Bosselaers A., Govaerts R. et Vandewalle J., 1990] Preneel B., Bosselaers A., Govaerts R. et Vandewalle J. (1990). A chosen text attack on the modified cryptographic checksum algorithm of cohen and huang. *CRYPTO 1989, Lecture Notes in Computer Science 435, G. Brassard (ed.), Springer-Verlag,*, pages 154–163. [cité p. 36]

[Sahut J M., 2008] Sahut J M. (2008). Internet payment and banks. *INTERNATIONAL JOURNAL OF BUSINESS, 13(4).* [cité p. 20, 36]

[Schmidt, C. et Müller, R., 1999] Schmidt, C. et Müller, R. (1999). A framework for micropayment evaluation. *Netnomics, Volume 1, No. 2, pp. 187-200.* [cité p. 20]

[Security Standards Council, 2010] Security Standards Council (2010). Pci data requirements and security assessment procedures. *https ://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.* [cité p. 63]

[Sitruk H, 2009] Sitruk H (2009). Les cartes de retrait et de paiement dans le cadre du sepa. *Rapport pour le Comité consultatif du secteur financier ; Janvier 2009.* [cité p. 17]

[Solange G H., 2000] Solange G H. (2000). *Securité Internet : Stratégies et technologies.* [cité p. 23]

[Stinson D, 1995] Stinson D (1995). *Cryptographie : Théorie et pratique*. CRC Press, Inc. [cité p. 48]

[Tarazi, M. et Breloff, P., 2010] Tarazi, M. et Breloff, P. (2010). Émetteurs non bancaires de monnaie électronique : approches réglementaires pour protéger les fonds des clients. *CGAP*. [cité p. 12]

[Wagner D. et Schneier B., 1996] Wagner D. et Schneier B. (1996). Analysis of the ssl 3.0 protocol. *In the second USENIX workshop on electronic commerce*. [cité p. 14]

[Wang R., Chen S., Wang X. et Qadeer S., 2011] Wang R., Chen S., Wang X. et Qadeer S. (2011). How to shop for free online : Security analysis of cashier-as-a-service based web stores. [cité p. 58]

[Wikipedia, 2000a] Wikipedia (2000a). Plugin. *http ://fr.wikipedia.org/wiki/Plugin*. [cité p. 124]

[Wikipedia, 2000b] Wikipedia (2000b). Proxy. *http ://fr.wikipedia.org/wiki/Proxy*. [cité p. 90, 91]

[Wikipedia, 2003] Wikipedia (2003). Automate. *http ://fr.wikipedia.org/wiki/Automate*. [cité p. 144]

[Wikipedia, 2012] Wikipedia (2012). Expression rationnelle. *http ://fr.wikipedia.org/wiki/Expression_rationnelle*. [cité p. 100]

[Wilson C., 2005] Wilson C. (2005). Crs report for congress : Computer attack and cyberterrorism : Vulnerabilities and policy issues for congress. [cité p. 37]

[World Wide Web Consortium W3C, 2003] World Wide Web Consortium W3C (2003). Extensible markup language (xml). *http ://www.w3.org/XML/*. [cité p. 43]

[World Wide Web Consortium W3C, 2004] World Wide Web Consortium W3C (2004). Web services architecture. *http ://www.w3.org/TR/ws-arch/*. [cité p. 42]

[Zhao L., Srihari M., Laxmi B., 2005] Zhao L., Srihari M., Laxmi B. (2005). Anatomy and performance of ssl processing. *In Proc. IEEE Int. Symp. Performance Analysis of Systems and Software, pages 197-206, 2005.* [cité p. 14]

[Zuchlinski G., 2003] Zuchlinski G. (2003). The anatomy of cross site scripting : Anatomy, discovery, attack, exploitation. *Hitchhiker's World 8*. [cité p. 141]

Annexes

Annexe A

Outils de sécurisation d'un système de paiement sur Internet

A.1 Le système SSL sans intermédiaire

Le système Secure Socket Layer (SSL) est un protocole de sécurisation des transactions. Ce protocole, conçu à l'origine par Netscape, et normalisé par Internet Engineering Task Force sous le nom de Transport Layer Security (TLS), permet de transmettre de manière sécurisée les numéros des cartes bancaires sur Internet. SSL est aujourd'hui le système le plus utilisé sur Internet (plus de 80% des sites marchands qui permettent d'exécuter une transaction en ligne offrent une sécurisation SSL). Cinq acteurs sont présents dans la transaction : l'internaute, le marchand, l'autorité de certification, la banque du marchand et la banque du client. Le marchand, par l'intermédiaire éventuellement de son hébergeur, exploite le protocole SSL sur son serveur. Mais pour faire usage du protocole, il doit faire appel à une autorité de certification qui lui délivre un certificat électronique (figure A.1). La faiblesse de cet outil de sécurisation du système de paiement est, d'une part, que le marchand n'est jamais sûr de l'identité de l'internaute et n'est pas à l'abri d'une répudiation tardive de la transaction de la part du client. Et d'un autre part, que l'internaute peut s'avérer réticent lors de la communication de ses coordonnées bancaires au marchand car il n'a pas de garantie concernant la fiabilité du serveur du marchand et n'est jamais à l'abri de la réutilisation de ses données de paiement. Aussi, pour faire face au problème de la sécurisation basée seulement sur le protocole SSL, un autre modèle s'est progressivement imposé.

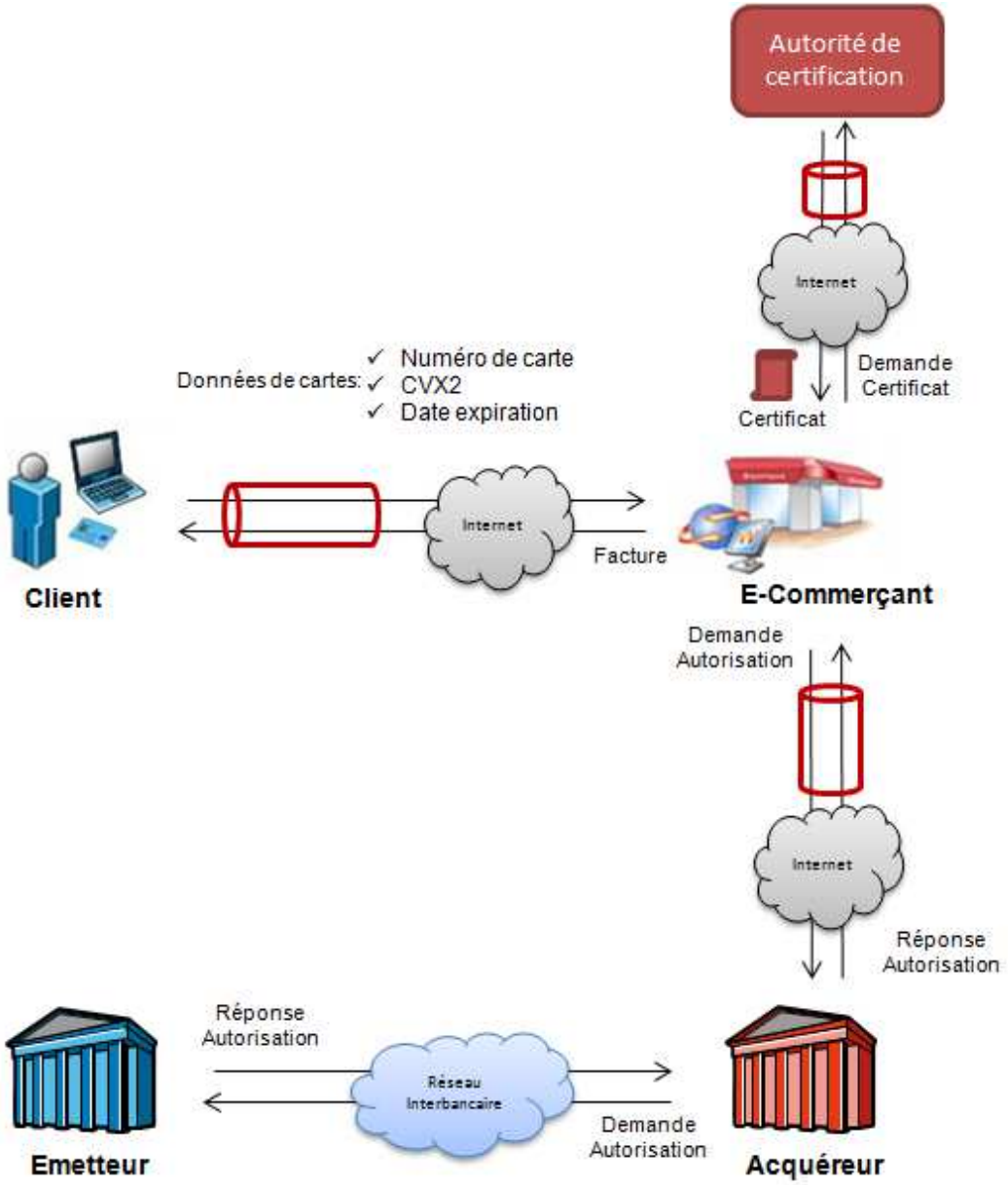


FIGURE A.1 – Système SSL sans intermédiaire

A.2 Le système SSL avec intermédiaire

Dans ce système, le marchand fait appel à un intermédiaire pour exploiter le protocole SSL. L'offreur de sécurité implémente le protocole sur le serveur marchand, distribue le certificat électronique au marchand (acheté au tiers de confiance) et assure la maintenance. L'offreur de sécurité peut être un acteur bancaire (Cybermut du Crédit mutuel, P@iement CIC, etc.), ou alors un acteur non-bancaire (Experian, Atos Origin, etc). L'avantage de ce nouvel outil de sécurisation est l'apport d'une

garantie pour le client concernant l'existant du marchand et la sécurité de l'usage de ses données de paiement (qui ne sont jamais communiquées au marchand). Cependant, ce nouveau modèle de sécurisation ne résout pas le problème de l'authentification de l'internaute et la réduction du risque de non répudiation de la transaction. D'où le troisième modèle de sécurisation, celui avec signature numérique.

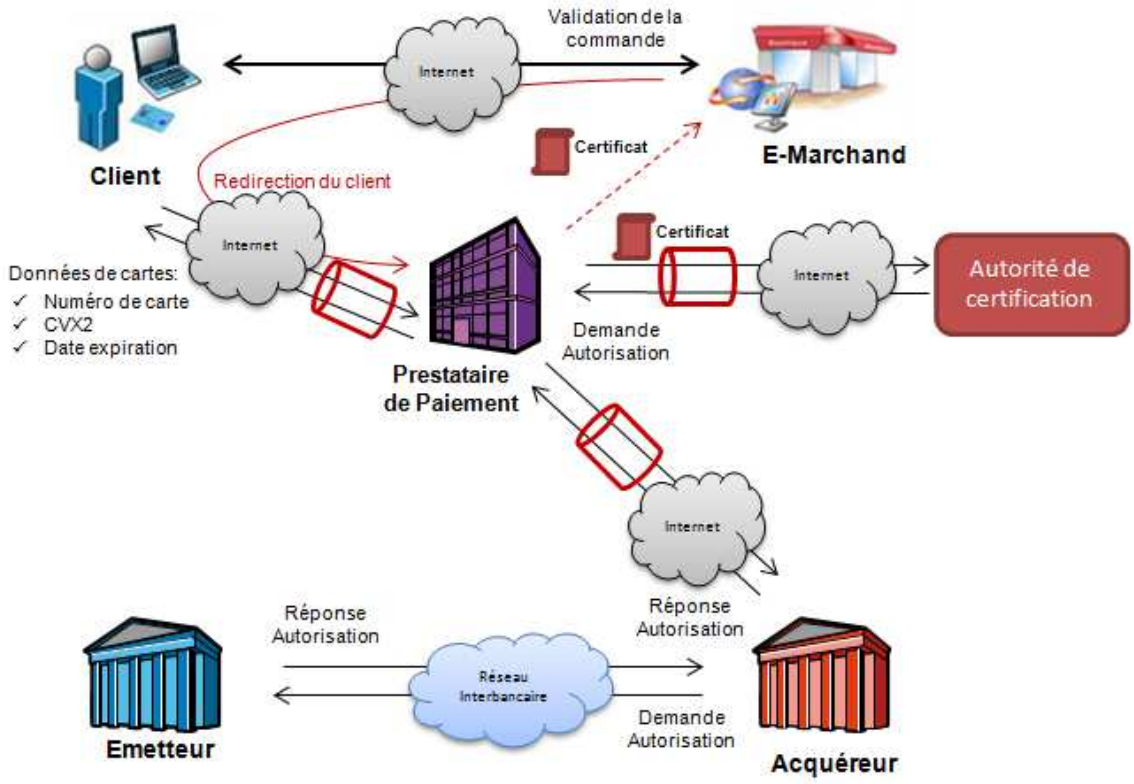


FIGURE A.2 – Système SSL avec intermédiaire

A.3 Le système avec signature numérique

Ce système a pour objet d'assurer la non-répudiation comme dans une transaction de proximité. Sachant que le seul moyen technique pour garantir la non-répudiation est la signature numérique, les banques se sont associées à plusieurs reprises pour mettre au point des protocoles de sécurisation des paiements qui authentifient l'internaute lors d'une transaction sur Internet. D'où l'apparition du système Secure Electronic Transaction (SET) puis de l'architecture 3D-Secure proposés par Visa et MasterCard. Afin d'utiliser le système SET, le porteur doit se porter acquéreur soit d'un lecteur de carte à puce sécurisé s'il possède une carte à puce, soit d'un certificat électronique. De même, le marchand doit obtenir un certificat électronique auprès de sa banque

qui l'autorise à accepter le paiement par carte bancaire. Ces dispositifs matériels ou logiciels ont pour fonction d'authentifier l'internaute et le marchand au cours de la transaction. Les transactions utilisant SET se déroulent comme il est décrit dans la figure A.3

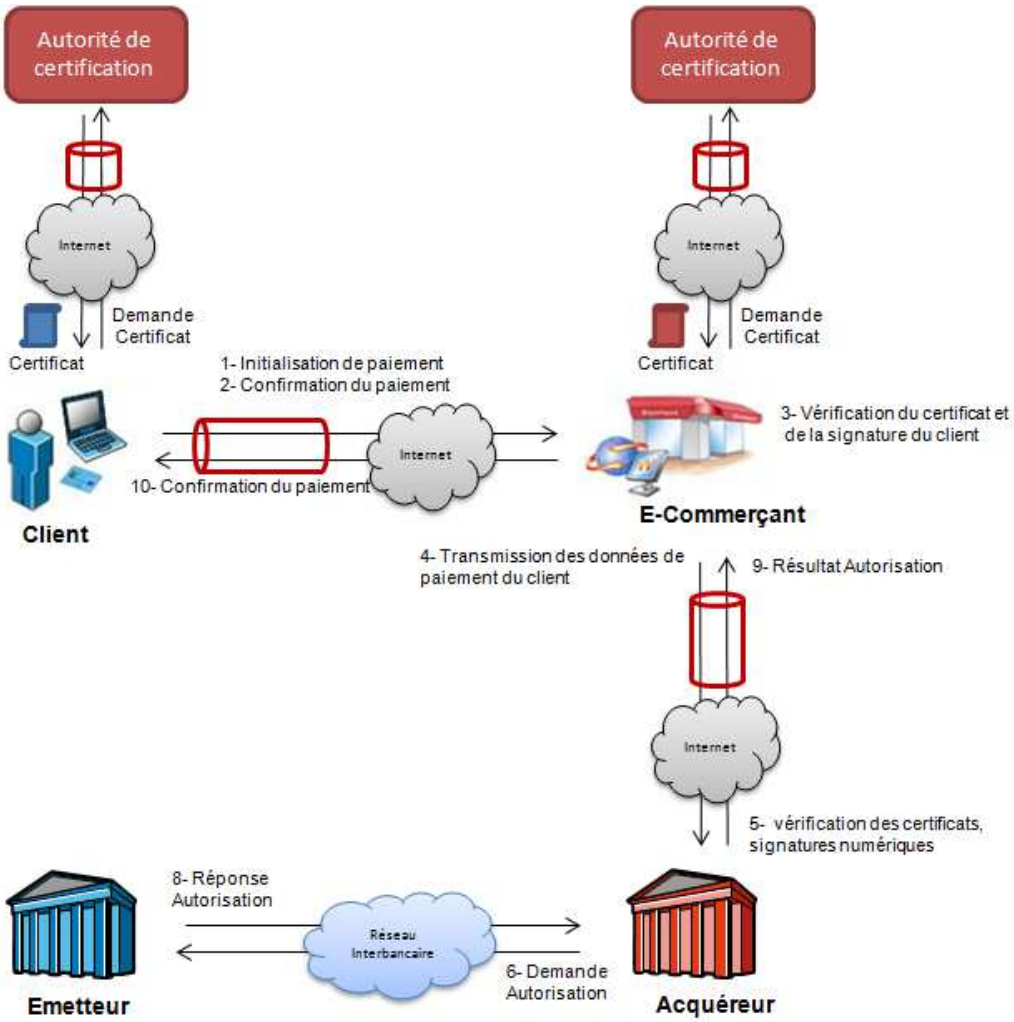


FIGURE A.3 – Système avec signature numérique : SET

Cependant, la sécurisation des paiements est coûteuse dans le cadre de ce système, car elle implique un équipement logiciel ou matériel pour les internautes et les E-commerçants. D'où l'idée de concevoir un nouveau protocole moins coûteux qui est 3D-secure. Il s'agit d'une architecture d'authentification basée sur le modèle « 3 Domaines » qui répartit le traitement de la transaction sur trois domaines distincts : celui de l'émetteur, celui de l'acquéreur et celui d'interopérabilité. Le mécanisme 3D-secure est décrit dans la figure A.4 [Pasquet M., Rosenberger C., Cuozzo F., 2008]. Il permet d'authentifier le client par sa banque à l'aide d'un code secret envoyé au

téléphone du client ou à l'aide d'un générateur OTP (One Time Passeword). Ce type de solution évite au consommateur l'acquisition et l'utilisation de matériels dédiés pour lire la carte de paiement. Au total, un grand nombre de solutions ont été expérimentées, cependant aucune n'a encore réussi à surpasser la popularité du système SSL.

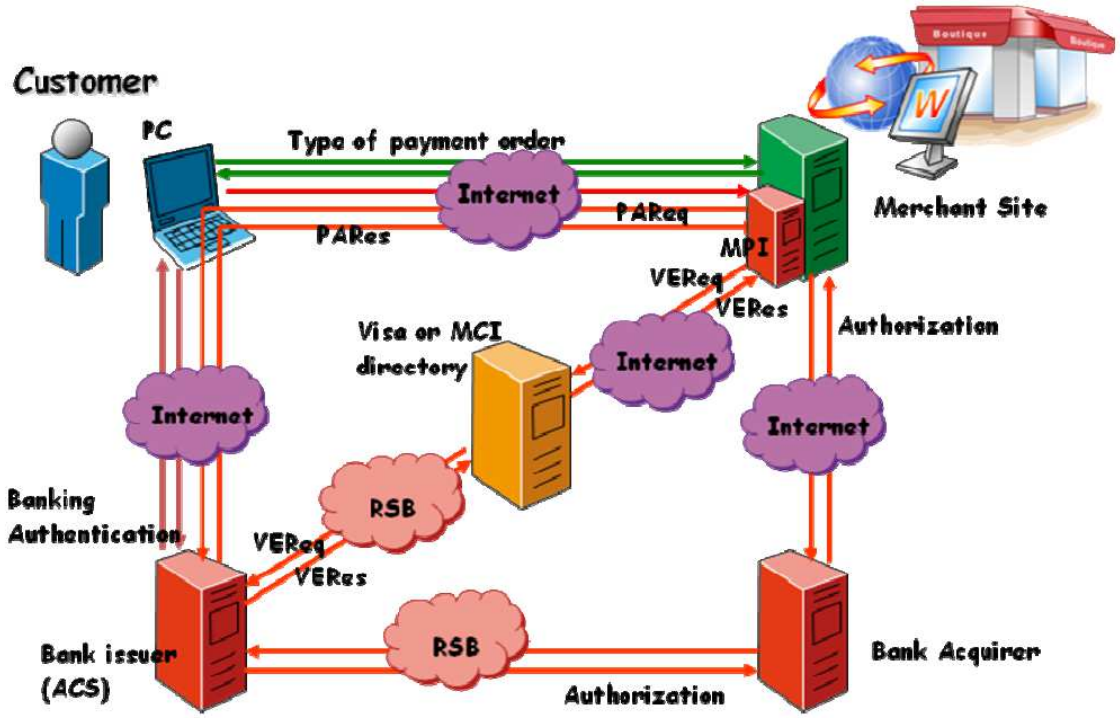


FIGURE A.4 – Système avec signature numérique : 3D-Secure

Annexe B

Exemple d'implémentation d'automate de paiement

Le but de la présente annexe est de présenter un exemple d'implémentation d'un automate de paiement de SystemPay, qui est un prestataire de paiement bancaire sur Internet. L'automate doit être compatible avec toutes les marques blanches de ce prestataire de paiement : PayZen, CyperplusPaiement, etc.

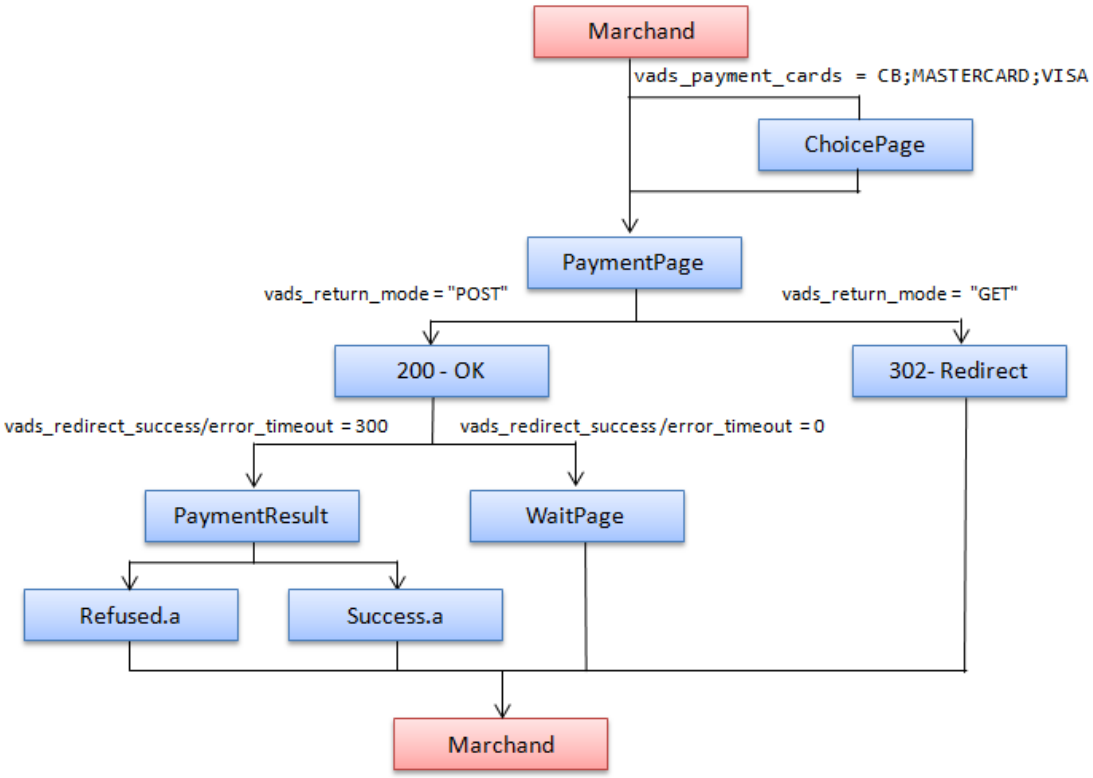


FIGURE B.1 – SystemPay - Paramétrage de la page de paiement

Lors de la spécification de cet automate de paiement, le terminal de paiement de SystemPay a été intégré dans notre boutique de test « Citronrose ». Les différents paramétrages de la page de paiement de SystemPay sont récapitulés dans la figure B.1, ce qui nous permet de tester tous les cas de figure. Avant de détailler l'implémentation de cet automate, rappelons le diagramme d'activité de l'automate de paiement (figure B.2). L'automate a trois fonctionnalités qui sont : la récupération des données de la commande avant le paiement, l'annulation de la commande et le paiement.

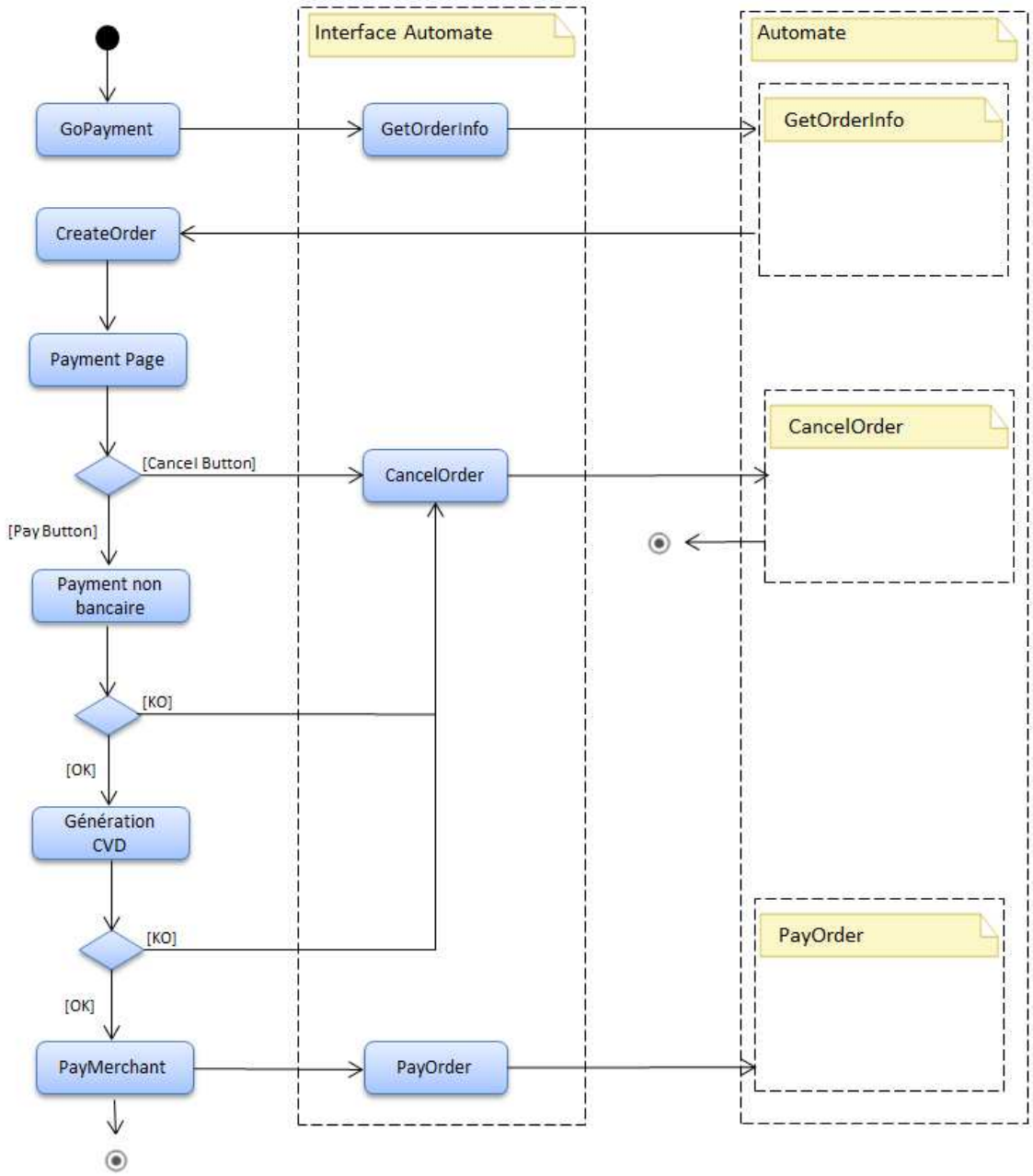


FIGURE B.2 – Le diagramme d'activité de l'automate de paiement

B.1 Récupération des données de la commande

La récupération des données de la commande comportent deux étapes : la récupération de la page de paiement et la récupération des données (figure B.3).

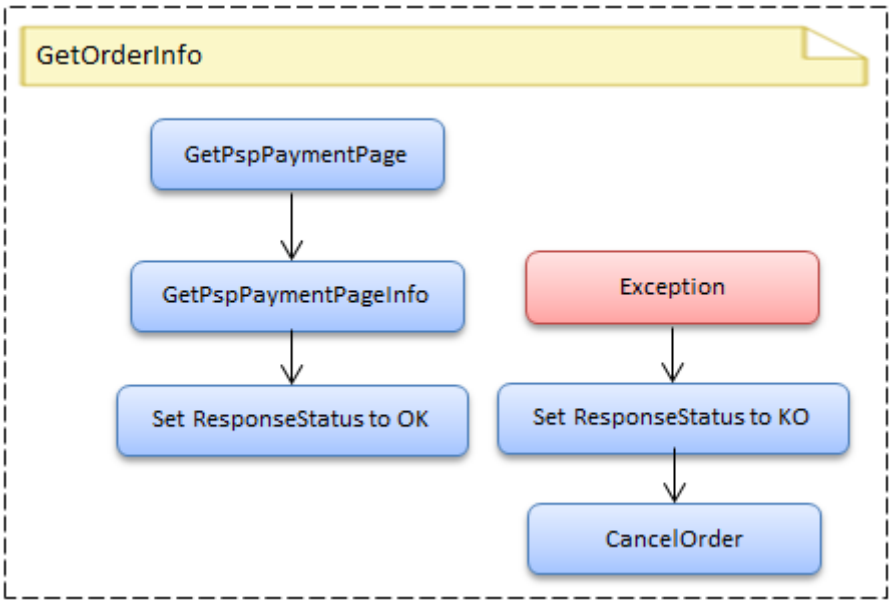


FIGURE B.3 – Récupération des données de la commande par l'automate

B.1.1 Récupération de la page de paiement

Pendant cette phase, l'automate doit récupérer la page de paiement bancaire. Selon les données envoyées par le marchand à SystemPay, ce dernier peut afficher plusieurs pages intermédiaires avant la page de paiement. L'automate doit alors pouvoir gérer ces pages intermédiaires et effectuer les requêtes nécessaires auprès de SystemPay afin de récupérer la page de paiement. Les éventuelles pages intermédiaires proposées par les deux marques blanches de SystemPay (Payzen et CyperplusPaiement) sont présentées dans la figure B.4.

Nous remarquons que le type de bouton, par exemple, est différent selon la marque blanche (Payzen ou CyperplusPaiement). Le but est de trouver une expression régulière unique afin de sélectionner le moyen de paiement CB et récupérer la page de paiement. Sachant que l'automate doit choisir en priorité le moyen de paiement E-CarteBleue si le SystemPay le propose, sinon c'est carte bancaire CB par défaut.

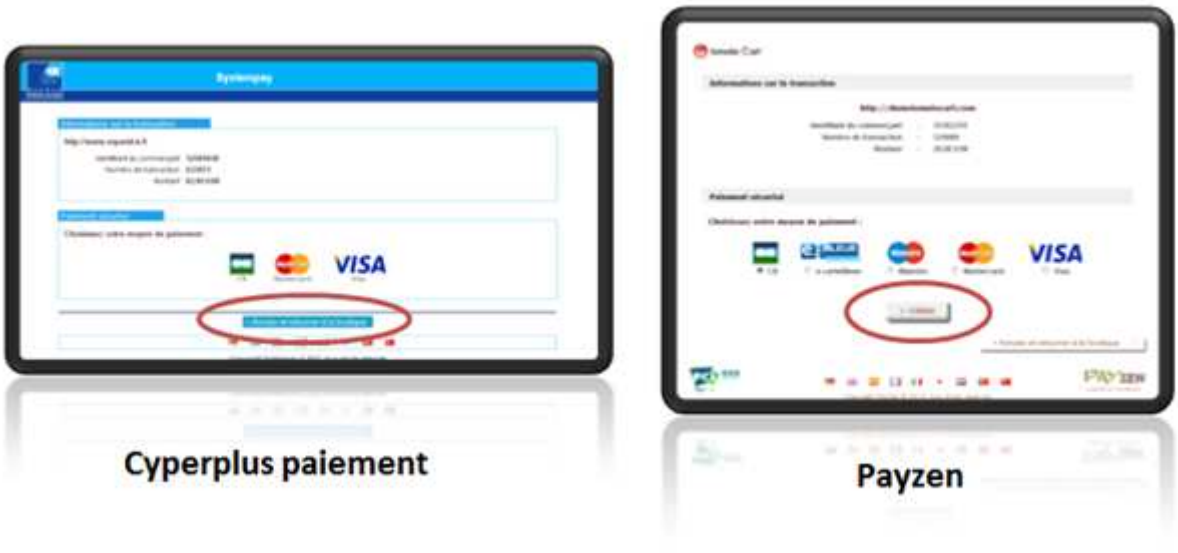


FIGURE B.4 – SystemPay - Page de choix de moyen de paiement

B.1.2 Récupération des données de la page paiement

Pendant cette phase, l'automate de paiement doit récupérer deux informations depuis la page de paiement de SystemPay, qui sont le montant et le numéro de commande (figure B.5).

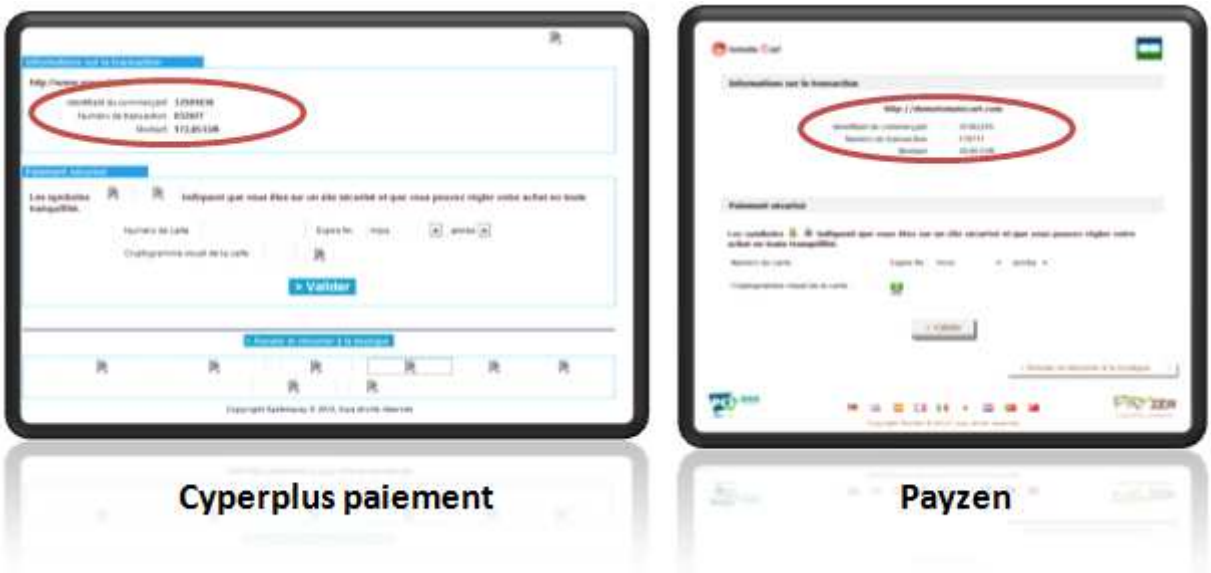


FIGURE B.5 – SystemPay - Page de paiement

B.2 Paiement

Une fois que la page de paiement est récupérée, l'automate peut procéder au paiement. La figure B.6 présente les différentes étapes de cette tâche qui sont : l'envoi des données de paiement, la récupération du résultat de paiement et la récupération de la requête HTTP de retour vers le site E-commerce.

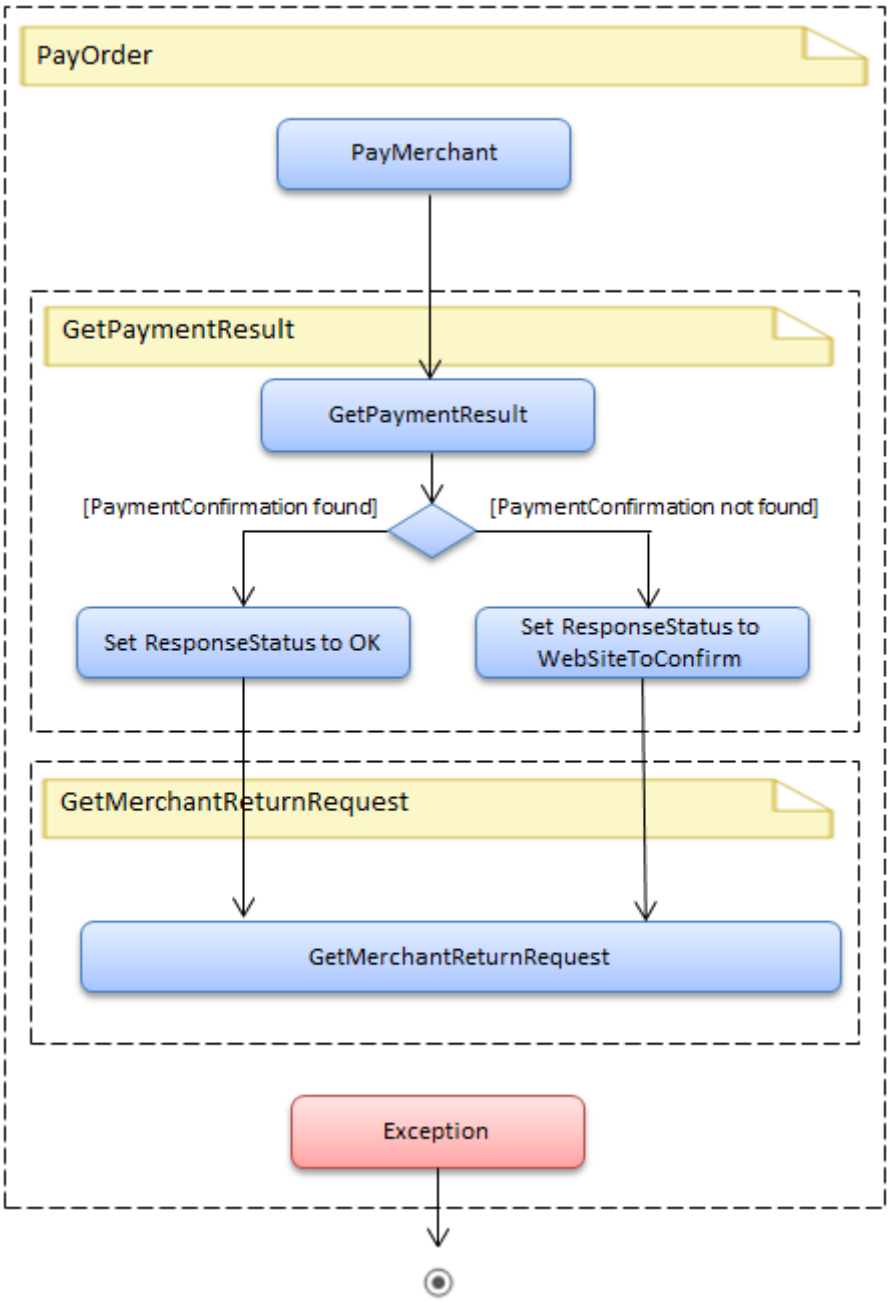


FIGURE B.6 – Récupération des données de la commande par l'automate

B.2.1 Envoi des données de paiement

Afin d'envoyer les données de la carte virtuelle dynamique et payer l'E-commerçant, l'automate doit récupérer le formulaire de paiement contenu dans la page de paiement de SystemPay. L'automate doit également décocher l'option de sauvegarde des données bancaires si elle est proposée par SystemPay, car la CVD de paiement n'appartient pas au client. L'automate récupère alors le formulaire à envoyer à SystemPay afin de payer à l'aide de l'expression régulière suivante :

```
(?<PaymentForm><form(?=[^>]*name=\s*["'])ref_form)[^>]
*action=\s*["'](?<PaymentUrl>[^\s|"|']*)[^>]*>(?:.*?)</form>)
```

Cette expression régulière permet de récupérer le formulaire de paiement dans les deux pages de paiement de Payzen et de CyperplusPaiement à la fois. Une fois la CVD envoyée à SystemPay, l'automate doit vérifier la page retournée par ce dernier afin de vérifier s'il s'agit d'une page de redirection vers le marchand ou pas. Dans le cas où il s'agit d'une page de résultat de paiement et qu'elle ne contient pas la requête vers le site marchand, l'automate doit effecteur les requêtes HTTP nécessaires jusqu'à avoir la page de redirection vers le site marchand. Le prestataire de paiement bancaire peut avoir deux types de réponses après l'envoi de la CVD :

- 302 Redirect : dans ce cas, l'automate n'a rien à faire, car il s'agit d'une redirection vers le site marchand
- 200 OK : L'automate doit traiter le contenu de la réponse de SystemPay et vérifier s'il doit effectuer d'autres requêtes HTTP afin de récupérer la page de redirection vers le marchand. Il doit vérifier qu'il s'agit bien de la dernière page qui redirige vers le marchand. En effet, après le paiement, l'automate peut être amené à enchaîner plusieurs requêtes vers le SystemPay afin de récupérer la requête de retour vers le site marchand. Un exemple de trace de pages de HTML affichées après paiement est présenté dans la figure B.7.

#	Result	Protocol	Host	URL	Body
49	200	HTTPS	systempay.cyberpluspaiement.com	/vads-payment/exec.card_input.a	5 332
54	200	HTTPS	systempay.cyberpluspaiement.com	/vads-payment/acs.silent_authenticate.a	8 184
61	200	HTTPS	systempay.cyberpluspaiement.com	/vads-payment/vads.pares.a	5 660
65	**200**	**HTTPS**	**systempay.cyberpluspaiement.com**	**/vads-payment/exec.success.a**	**954**
66	200	HTTP	systempay.citronrose.com	/PaymentMeans/www/PaymentReturn/Return_OK.aspx	2 004

FIGURE B.7 – SystemPay - Exemple de trace des pages HTML appelées après le paiement

B.2.2 Récupération du résultat de paiement

Après avoir payé, l'automate doit récupérer le résultat de paiement. Il existe deux possibilités dans ce cas :

1. SystemPay affiche le ticket de paiement
2. SystemPay redirige directement le client vers le site marchand

SystemPay redirige le client vers une page « exec.success.a » dans le cas de succès de paiement. Selon les paramètres envoyés par le marchand, il redirige systématiquement le client par la suite vers le site E-commerce, ou affiche une page de confirmation. Afin de détecter le résultat de paiement, l'automate peut se baser sur les paramètres renvoyés dans l'Url de retour vers le site E-commerce (figure B.8) [Lyra-Network, 2011].

Nom	Format	Obligatoire	Remarques
vads_action_mode		oui	idem requête
vads_amount		oui	idem requête
vads_auth_result	n2	oui	vide si erreur avant autorisation
vads_auth_mode		oui	MARK : prise d'empreinte FULL : autorisation du montant total (ou du montant initial dans le cas du paiement en N fois)
vads_auth_number	n6	oui	vide si autorisation échouée.
vads_capture_delay	n..3	oui	valeur par défaut ou valeur spécifiée dans requête
vads_card_brand	an..127	oui	vide si aucune carte n'a été sélectionnée (retour à la boutique).
vads_card_number	an..19	oui	numéro masqué
vads_ctx_mode		oui	idem requête
vads_currency		oui	idem requête
vads_extra_result	n2	oui	numérique, peut être vide.
vads_payment_config	oui	oui	idem requête
Signature		oui	
vads_site_id	oui	oui	idem requête
vads_trans_date	oui	oui	idem requête
vads_trans_id	oui	oui	idem requête
vads_validation_mode	n1	oui	valeur par défaut ou valeur spécifiée dans la requête
vads_warranty_result		oui	vide ou YES, NO, UNKNOWN
vads_payment_certificate	an40	oui	vide si paiement échoué
vads_result	n2	oui	numérique, toujours renseigné
vads_version		oui	Idem requête
vads_order_id			Idem requête
vads_order_info			Idem requête
vads_order_info2			Idem requête
vads_order_info3			Idem requête
vads_cust_address			Idem requête

vads_cust_country			Idem requête
vads_cust_email			Idem requête
vads_cust_id			Idem requête
vads_cust_name			Idem requête
vads_cust_phone			Idem requête
vads_cust_title			Idem requête
vads_cust_city			Idem requête
vads_cust_zip			Idem requête
vads_language			valeur par défaut ou valeur spécifiée dans requête
vads_payment_src			Idem requête
vads_user_info			Idem requête
vads_theme_config			Idem requête
vads_contract_used	ans..250		Contrat commerçant utilisé
vads_expiry_month	n..2		Idem requête
vads_expiry_year	n4		Idem requête
vads_card_info	ans..250		Idem requête
vads_card_options	ans..250		Idem requête
vads_threeds_enrolled	a1		
vads_threeds_cavv	ans28		
vads_threeds_eci	n2		
vads_threeds_xid	ans28		
vads_threeds_cavvAlgorithm	n1		
vads_threeds_status	a1		
vads_threeds_sign_valid	n1		vide ou 0/1

FIGURE B.8 – SystemPay - Paramètre de retour vers le site marchand

Le code retour de la demande d'autorisation retournée par la banque émettrice, s'il est disponible, est renseigné dans le champ de retour « vads_auth_result », donc l'automate peut également se servir de ce champ pour connaître le résultat de paiement. Si le paiement s'est bien déroulé le code retour sera 00. En revanche, ces paramètres de retour ne sont pas envoyés systématiquement au marchand. Cela dépend du paramètre « vads_return_mode » envoyé par le marchand dans la première requête vers SystemPay. Si ce paramètre vaut « POST », SystemPay renvoie tous les paramètres dans les données du post, sinon, seulement quelques paramètres sont envoyés. En cas d'absence de ce paramètre, SystemPay prend la valeur « GET » et donc ne renvoie pas tous les paramètres au marchand après le paiement. Sachant que SystemPay, redirige systématiquement vers une page de résultat de paiement (dont la réponse HTTP est 302 ou 200 selon le cas) et que le nom de cette page peut indiquer le résultat de paiement « exec.success.a » (en cas de succès du paiement) ou « exec.referral.a » (en cas d'erreur de paiement), l'automate peut se baser sur cette première information pour détecter le résultat de paiement. Il peut également essayer de récupérer le paramètre « auth_resultat » et vérifier que sa valeur est égale à 00 (figure B.9).

auth_result	Signification
00	transaction approuvée ou traitée avec succès
02	contacter l'émetteur de carte
03	accepteur invalide
04	conserver la carte
05	ne pas honorer
07	conserver la carte, conditions spéciales
08	approuver après identification
12	transaction invalide
13	montant invalide
14	numéro de porteur invalide
30	erreur de format
31	identifiant de l'organisme acquéreur inconnu
33	date de validité de la carte dépassée
34	suspicion de fraude
41	carte perdue
43	carte volée
51	provision insuffisante ou crédit dépassé
54	date de validité de la carte dépassée
56	carte absente du fichier
57	transaction non permise à ce porteur
58	transaction interdite au terminal
59	suspicion de fraude
60	l'accepteur de carte doit contacter l'acquéreur
61	montant de retrait hors limite
63	règles de sécurité non respectées
68	réponse non parvenue ou reçue trop tard
90	arrêt momentané du système
91	émetteur de cartes inaccessible
96	mauvais fonctionnement du système
94	transaction dupliquée
97	échéance de la temporisation de surveillance globale
98	serveur indisponible routage réseau demandé à nouveau
99	incident domaine initiateur

FIGURE B.9 – SystemPay - Code de retour de la demande d'autorisation

B.2.3 Récupération de la requête de retour vers le marchand

Il s'agit de récupérer la requête vers le site marchand après le résultat de paiement. Pour ce faire, il faut étudier plusieurs pages de résultat de paiement (erreur, échec, succès) afin de pouvoir optimiser l'expression régulière qui récupère les données de la requête HTTP de retour vers le site E-commerce. Il est important, également, de garder la même méthode HTTP (GET, POST) que celle utilisée par SystemPay pour rediriger le client, car cette méthode peut être demandée par l'E-commerçant et si elle n'est pas respectée, le marchand renvoie une page d'erreur au client.

Le premier critère est celui du code HTTP de la réponse de SystemPay :

- Si le code de réponse est 302, dans ce cas c'est simple, il faut rediriger le client en 302 vers l'Url contenue dans l'entête « Location » de la réponse.

- Si le code de la réponse est 200, dans ce cas il faut récupérer :
  - L'Url de retour du site marchand
  - La méthode HTTP (GET, POST) de retour
  - Eventuellement, le formulaire contenant les paramètres de retour envoyés au marchand.

B.3 Annulation de la commande

Il est important de pouvoir annuler proprement une commande dans le cadre d'un automate de paiement. Dans le cas de SystemPay, le clic sur le bouton « annuler et retourner à la boutique » appelle une page du serveur de SystemPay (« exec.cancel.a ») afin d'annuler la commande. La réponse de cette requête peut être une page html (code HTTP 200 OK) ou une redirection (code HTTP 302 Redirect). L'automate doit alors exécuter cette requête et récupérer la requête HTTP de retour vers le site E-commerce (figure B.10).

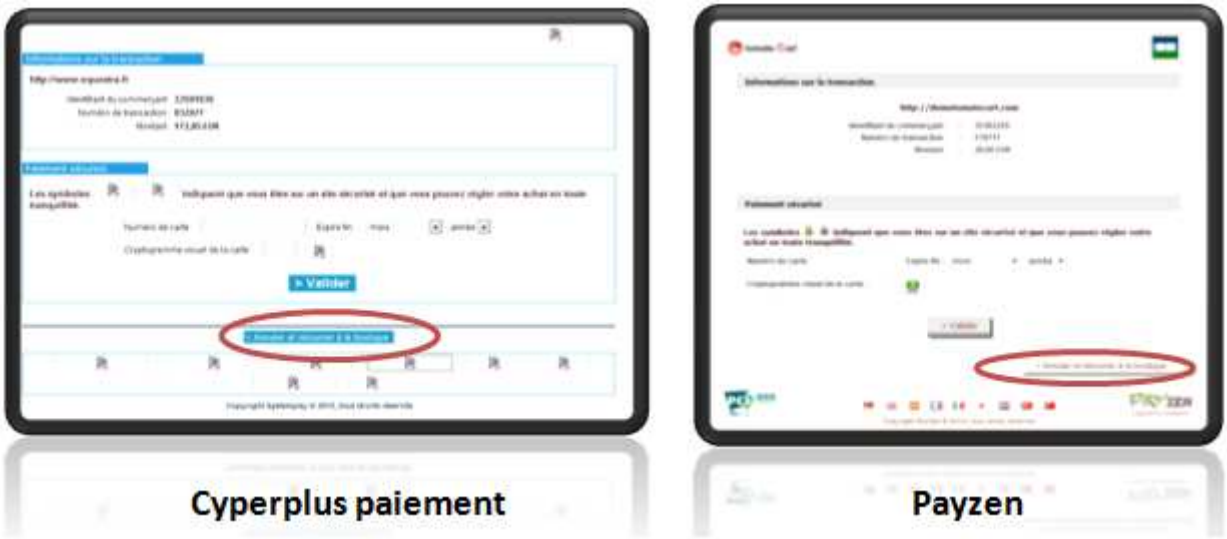


FIGURE B.10 – SystemPay - Annulation du paiement

L'automate doit s'assurer de :

- Récupérer la méthode HTTP de la requête de retour vers le site marchand
- Récupérer l'Url de retour vers le site marchand
- Mettre à jour les traces de paiement avec chaque requête

Liste des abréviations

$SEPA$	Single Euro Payment Area
WWW	World Wide Web
$ACSEL$	Association pour le Commerce et les Service en Ligne
TLS	Transport Layer Security
SSL	Secure Socket Layer
MPA	Moyen de Paiement Alternatif
TPE	Terminal de Paiement Electronique
PSP	Prestataire de Service de Paiement
ROI	Return On Investment
SET	Secure Electronic Transaction
$FEVAD$	Fédération de l'E-commerce et de la Vente A Distance
$PCIDSS$	Payment Card Industry Data Security Standard
$SOAP$	Simple Object Access Protocol
$REST$	REpresentational State Transfer
XML	eXtensible Markup Language
CGI	Common Gateway Interface
MAC	Message Authentication Code
MDC	Modification Detection Code
CVD	Carte Virtuelle Dynamique
$EMPA$	Emetteur du Moyen de Paiement Alternatif
EME	Emetteur de la monnaie électronique
CIP	Commissions Interbancaires de Paiement
CIR	Commissions Interbancaires de Retrait
CMI	Commissions Multilatérales d'Interchange

Table des figures

Liste des tableaux

Le commerce électronique actuel en Europe est essentiellement bancaire et s'articule autour des moyens de paiement traditionnels : carte bancaire, chèque, virement, etc. Cependant, avec l'apparition de nouvelles technologies et l'évolution des règlementations, on a vu émerger progressivement de nouveaux moyens de paiement ainsi que le développement de plusieurs canaux de paiement sur Internet. Au cours de cette thèse, nous nous sommes intéressés donc aux nouveaux moyens de paiement et à leur intégration dans l'E-commerce qui est encore très restreint en fonctionnalités comparé à celui de proximité, malgré les évolutions technologiques.

Nous proposons dans cette thèse une nouvelle architecture de paiement permettant de convertir les paiements non bancaires en paiements bancaires à l'aide des cartes virtuelles dynamiques. Cette architecture permet d'appréhender facilement des échanges complexes entre les différents acteurs du système de paiement afin de diminuer la complexité de l'intégration des moyens de paiement pour l'E-commerçant. Nous avons également mis au point deux approches d'intégration de cette architecture dans les boutiques en ligne. La première est basée sur un Proxy Web qui joue le rôle d'intermédiaire entre le navigateur du client et le serveur du site marchand. La deuxième consiste à intégrer un Plugin JavaScript dans le site E-commerce. Enfin, nous avons montré que les deux approches proposées permettent de pallier les différentes contraintes techniques d'intégration d'un système de paiement sur Internet et d'être conforme aux critères d'évaluation d'un système de paiement sur le Web, à savoir : la sécurité, l'ergonomie et la complexité.

Integration of non-bank payment means on Internet

Nowadays, E-commerce payment system in Europe is mainly based on traditional payment methods such as credit card, check, bank transfer, etc. However, with the advent of new technologies and regulations, new payment methods are emerging gradually and several Internet payment channels are appearing. E-commerce requirements have consequently changed in order to tackle the new challenges. One of those challenges, is to enhance the integration of the new payment methods into the E-commerce. This task is facing many limitations, comparing to proximity payment system. The focus of our research work is on a new approach to enable a smooth migration towards the acceptance and integration of the new payments methods for E-commerce in Europe.

Concretely, We propose a new payment architecture that converts non-bank payments to bank payments using dynamic virtual cards. This architecture can easily handle complex interactions between different actors within the payment system. We have developed two approaches of integration of this architecture in online shops : The first is based on a Web Proxy that acts as a mediator between the client browser and the server of the merchant shop. The second consists in the integration of a Plugin JavaScript in the E-commerce Web site. We prove afterwards that both approaches allow to overcome the various technical integration constraints of an Internet payment system and to comply with the E-commerce payment system requirements, namely : security, ergonomy and complexity.

Indexation Rameau :
Indexation libre :

Informatique et applications

Laboratoire GREYC - UMR CNRS 6072 - Université de Caen Basse-Normandie - Ensicaen
6 Boulevard du Maréchal Juin - 14050 CAEN CEDEX