

PAIEMENT ELECTRONIQUE : MECANISMES ET CARACTERISTIQUES

Khadidja NASSILI¹
Haoues SALAH².

Résumé:

Avec l'essor de l'Internet et l'apparition du e-commerce, de nombreux mécanismes ont été mis en œuvre dans la perspective de développer, faciliter et sécuriser le commerce en ligne. L'un de ces mécanismes, ayant révolutionné le e-commerce, est le paiement électronique (e-payment).

Dans cet article, nous allons analyser les systèmes de paiement électronique les plus répandus au monde (le chèque électronique, la monnaie électronique et la carte de crédit) et détailler les différentes caractéristiques desdits systèmes à savoir l'universalité, la facilité, la rapidité, l'anonymat, l'authenticité de l'argent, l'authentification, l'intégrité du paiement et la confidentialité de la transaction.

Mots clés :

Introduction

Bien avant qu'Internet ne soit né (il y a des centaines et des centaines d'années), les gens cherchaient déjà des moyens plus efficaces pour transférer leur argent. Certes, il n'y avait pas encore de carte de crédit ou de comptes bancaires, encore moins d'action en bourse. Même ce que nous appelons aujourd'hui argent n'existait pas à l'époque.

Maintenant que nous avons bien de la chance, notre argent tient aisément dans une poche, et si nous ne voulons rien mettre dans nos poches, nous disposons de beaucoup d'autres solutions. Effectivement en termes de confort, les choses ont bien évoluées depuis les premiers hommes. Aujourd'hui, qu'Internet existe, nous pouvons faire des achats de chez nous, sans que notre déplacement au marché ne soit nécessaire. Cela est devenu bel et bien possible grâce au commerce électronique.

1. Commerce électronique

Selon l'Organisation pour la Coopération et le Développement Economiques (OCDE), le commerce électronique (ou e-commerce) peut être

¹ Doctorante en sciences commerciales, Université d'Alger 3

² Professeur en sciences économiques, Université d'Alger 3

défini comme toutes formes de transactions liées aux activités commerciales, associant tant les particuliers que les organisations, et reposant sur le traitement et la transmission de données numérisées, notamment texte, son et image [01]. Il désigne aussi les effets que l'échange électronique d'informations commerciales peut avoir sur les institutions et le processus, qui facilitent et encadrent les activités commerciales, et dont l'*OCDE* précise qu'ils sont un vecteur majeur de croissance économique.

Le commerce électronique sur Internet a en effet des particularités qui lui sont propres: c'est une activité dématérialisée s'exerçant à distance, concernant aussi bien les échanges entre professionnels (Business to Business *B2B*) qu'entre commerçants et consommateurs (Business to Consumer *B2C*), voire entre les consommateurs eux-mêmes (Consumer to Consumer *C2C*) lorsqu'il s'agit, par exemple, d'enchères publiques ou de troc sur le Web [02].

Le commerce électronique *B2B* sur Internet augmente plus rapidement que le *B2C* et le *C2C* [03]. Cela n'est pas étonnant puisque le monde des affaires, les secteurs industriels et les organismes privés et publics comprennent maintenant les bénéfices et les avantages d'exploiter le réseau public pour faire des affaires et pour communiquer.

2. Sécurité du commerce électronique :

Accompagnant le développement très rapide de l'Internet, différents systèmes et procédures spécifiques ont été conçus pour prévenir toute atteinte à la sécurité des données transitant sur le réseau électronique. Les sociétés proposant leurs services pour garantir le paiement en ligne se sont ainsi multipliées comme autant de prestataires spécialisés. Par delà cette diversité, l'objectif commun de sécurité a permis de créer des normes de performances uniformes et qui devraient pouvoir contribuer à accroître considérablement le taux de connexion des entreprises et des particuliers. En effet, aujourd'hui, le développement des transactions en ligne (biens et services) dépend pratiquement de la "confiance" accordée à la sécurisation des paiements électronique. Cette confiance est basée sur un ensemble de services que le commerce électronique doit garantir [03]:

Authentification et intégrité des messages : Chaque intervenant peut s'assurer que le message reçu provient bien de la bonne personne. Aussi, chaque autorisation de paiement doit être unique, aucune partie du message envoyé ne pouvant être modifiée lors du transfert de réseau. De ce principe d'intégrité découle celui de fiabilité ; le système devant être assurément pourvu de mesures capables d'éliminer toute possibilité de perte d'argent en cas de panne ou de mauvais fonctionnement.

Confidentialité: Les informations concernant le client, le marchand et la transaction doivent être et rester confidentielles.

Divisibilité: Il s'agit là de la possibilité de faire des micro-paiements via le mode de paiement électronique, ce qui est le principe même des porte-monnaie électroniques.

Disponibilité: Le système de commerce électronique doit être accessible à tout moment.

Non répudiation: La non répudiation de l'achat doit être assurée afin que le marchand et le client se sentent sécurisés et ne peuvent pas nier leurs actions effectuées (achats et livraisons). Aussi, les parties en présence doivent être authentifiées avec certitude. Par ailleurs, la non répudiation est effective par la preuve, ce qui soulève le problème de son archivage.

Il convient cependant de préciser que tous ces critères de performance et de sécurité sont applicables dès la commande.

3. Paiement électronique :

Qui dit commerce dit transaction commerciale et l'on sait que le paiement est un élément important de la transaction d'achat. Ce paiement peut prendre la forme traditionnelle de transfert d'argent entre vendeur et acheteur, ou la forme encore plus ancienne d'échange de produits et services entre les intervenants de cette opération. Dans le cas du commerce électronique, on est tenté d'affirmer : (*S'il n'y a pas de transaction sans paiement, il n'y a pas de paiement sans sécurité de transaction*).

Le paiement électronique sur Internet pose donc certains problèmes de moyens (avec quoi paie-t-on ?) et de protection des intérêts des intervenants dans la transaction (sécurité du transfert d'informations, confidentialité des données personnelles, confirmation de l'identité des intervenants et authentification des transactions).

Tout au long de cette étude, il nous est donc paru fondamental de distinguer entre le commerce électronique dans son ensemble et le paiement électronique. En effet, que ce soit en parlant des systèmes informatiques de paiement et de transaction ou des politiques gouvernementales en matière de commerce électronique, il faut comprendre que le commerce électronique est l'activité générale, le secteur économique et stratégique et l'ensemble des actions transactionnelles réalisées à l'aide de l'informatique, des

télécommunications et autres moyens numériques. Le paiement électronique, lui, est une des actions constituant le commerce électronique. Dans une transaction, le paiement est un moment crucial qui complète l'acte d'acheter et de vendre. Au niveau du système informatique, le paiement est soit un module parmi d'autres modules constituant le système de commerce électronique, soit un système indépendant fourni de façon autonome et qui se complète par des serveurs et des modules Web, des bases de données ou autres [02].

4. Systèmes de paiement

Il y aurait actuellement, plusieurs centaines de systèmes de paiement différents dans le monde [04]. Cette prolifération est évidemment nuisible au développement du commerce électronique, et va à l'encontre de la demande de simplification et de transparence souhaitées par l'utilisateur. On peut quand même dire qu'un nombre très limité de types de systèmes de paiement sur Internet se dégage : il s'agit des systèmes basés sur les cartes bancaires, le porte-monnaie (électronique et virtuel) et les chèques électroniques décrits ci-dessous.

4.1. Systèmes de paiement par cartes:

La carte de paiement constitue le moyen de paiement universel par excellence. Son utilisation est possible dans tous les pays du monde, que ce soit pour du paiement direct (de contact), chez les commerçants, ou pour du retrait d'argent dans les distributeurs. Elle est donc utilisée en commerce électronique, suivant le même modèle de base que pour le commerce de contact [04].

On distingue deux types de cartes de paiement: les cartes magnétiques et les cartes à puce.

4.1.1. Carte magnétique :

Le principe de l'enregistrement magnétique repose sur la magnétisation de très petites zones de la bande magnétique constituée de pigments magnétiques (oxyde de fer, oxyde de chrome ou ferrite de baryum). Cette opération de magnétisation est effectuée par une tête magnétique d'écriture. En fait, il s'agit d'un genre d'électro-aimant. En passant sur la bande magnétique, pour une opération d'écriture, la tête va plonger les pigments dans un champ magnétique proportionnel au courant la traversant. Cette magnétisation va subsister et correspondra alors à un enregistrement [05].

Pour l'opération de lecture, le passage de la tête sur la bande donnera naissance à un flux magnétique dans son noyau, lequel induira une tension

électrique proportionnelle aux variations du flux. Le signal électrique (c'est à dire les informations) préalablement enregistré sur la bande magnétique est alors restitué.

En ce qui concerne la sécurité, il n'y a aucun moyen de sûr pour protéger physiquement les données enregistrées sur un support magnétique [05]. En effet, la lecture et l'écriture sont entièrement libres (contrairement aux cartes à puce qui possèdent des zones où l'écriture voire la lecture est interdite). Il est donc indispensable de sécuriser l'application utilisant ce support. Concrètement, il faut chiffrer les données sensibles enregistrées sur le support et coupler l'utilisation de la carte avec un code secret. En outre, pour une sécurité accrue un contrôle de l'authenticité de la carte en temps réel peut être utilisé (pour les applications fonctionnant on-line, c'est à dire avec une centralisation des traitements).

4.1.2. Carte à puce :

La carte à puce est une carte plastifiée aux dimensions de $85,6 \times 54$ millimètres avec une épaisseur de l'ordre de 70 à 90 centièmes de millimètres. Elle comporte au moins un circuit intégré (la puce) [06].

Avant d'être remises à la personne qui l'utilisera, une carte à puce est normalement 'personnalisée' électriquement (par l'organisme émetteur) via un encodeur de cartes et un programme informatique (outil de personnalisation), afin d'inscrire dans la puce les informations nécessaires à son utilisation. Dans le cas de la carte bancaire, on en inscrira les références bancaires de l'utilisateur [07].

La carte à puce succède : aux cartes à codes barres, aux cartes à pistes magnétiques.

4.1.3. Paiement par carte:

Sans argent liquide, ni chèques, la carte de paiement est l'un des moyens de paiement permettant de régler la plupart des achats chez un nombre important de commerçants affiliés au système CB. Le compte du client sera débité du montant des dépenses réglées par carte à une date qui dépend du contrat que le client s'est engagé envers sa banque. De ce principe, on distingue deux types de cartes de paiement: carte de débit et carte de crédit [06].

a) Carte de débit :

Une carte de débit est une carte de paiement définie par la norme ISO 7810, avec un débit immédiat [05]. Cela signifie que le compte est débité à

chaque utilisation, comme un paiement par chèque, mais avec l'avantage d'une rapidité d'utilisation, d'une meilleure sécurité et d'un nombre illimité d'utilisation.

Bien que beaucoup de cartes de débit soient de la marque de *Visa* ou de *Mastercard*, il y a beaucoup d'autres types de carte de débit, chacun est accepté dans un pays particulier ou région. Exemple *Solo* en Angleterre, *Carte Bleue* en France, *Laser* en Irlande. et *EFTPOS* en Australie.

Il y a actuellement deux manières que des transactions de carte de débit sont traitées: cartes en ligne et cartes en différé. Les cartes de débit en ligne exigent l'autorisation électronique de chaque transaction et les débits sont reflétés dans le compte de l'utilisateur immédiatement. La transaction peut être en plus sécurisée dans le système d'authentification par un numéro d'identification personnel (*PIN*), et quelques cartes en ligne exigent une telle authentification pour chaque transaction. Une difficulté en employant les cartes de débit en ligne est la nécessité d'un dispositif électronique d'autorisation au moment de la vente et parfois également un bloc de touches pour entrer le *PIN*, bien que ceci devienne banal pour toutes les transactions de carte en beaucoup de pays.

b) Carte de crédit :

Une carte de crédit est l'un des moyens de paiement électronique les plus utilisés. Elle est différente de la carte de débit du fait que l'émetteur de carte prête l'argent au client plutôt que d'avoir de l'argent enlevé de son compte (le client) [08]. De même, elle est différente d'une carte de paiement car en possédant une carte de crédit, on peut choisir de régler la totalité du solde mensuel de notre carte à l'échéance et bénéficier ainsi du financement sans intérêt de nos achats. On peut aussi effectuer un versement partiel ou le versement minimum selon notre budget. Mais en possédant une carte de paiement, on doit régler la totalité du solde de notre compte chaque mois [05].

L'émetteur de la carte règle le marchand aussitôt que ce dernier dépose la facture de vente. En retour, les achats effectués au moyen de la carte de crédit sont facturés au compte du client et figurent sur son relevé mensuel.

c) Carte de crédit EMV :

Il existe actuellement plusieurs types de carte bancaire, chacune utilisée dans un pays ou région mais ne peut pas être utilisée ailleurs. Par conséquence, ces cartes ne garantissent pas l'un des importants critères du e-commerce : l'universalité. Pour remédier à cet inconvénient, une solution a

été proposée par *Europay, MasterCard* et *Visa* pour donner naissance à un nouveau standard de paiement par carte.

EMV (Europay MasterCard Visa) est le standard international de carte bancaire à puce, fiable et bientôt universel (théoriquement, partout dans le monde dès 2008) [06]. Il résulte de l'harmonisation des processus de paiements et des principes sécuritaires d'authentification.

4.2. Chèques électroniques

Le chèque électronique (e-check) est basé sur l'idée que le papier peut être substitué par un document électronique et les signatures manuelles peuvent être remplacées par des signatures numériques [09]. Par conséquent, le chèque électronique peut remplacer le chèque de papier sans la nécessité de créer un nouveau moyen de paiement, accompagné par des nouvelles procédures juridiques, de nouvelle forme de contrôle, et des nouvelles procédures commerciales. Le chèque électronique convient très bien avec le système de chèque actuel et possède peu d'impact sur le payeur, le payé, la banque et le système financier.

4.2.1. Chèque électronique *FSTC* :

Le chèque électronique *FSTC* a été développé par *Financial Services Technology Consortium*. *FSTC* est composé de plus de 100 membres, comportant un grand nombre de banque, de laboratoires de recherche et d'universités [10].

Elaboré sur la base d'un outil financier largement diffusé et reconnu, le chèque *FSTC* s'apparente parfaitement à son homologue papier par l'utilisation des signatures numériques et la messagerie sécurisée sur Internet.

Le client disposera ainsi d'un livret de chèques électroniques. Les chèques *FSTC* pourront être délivrés au travers d'un site web ou attachés au courrier électronique. La signature manuelle sera remplacée par la signature électronique, que beaucoup considèrent comme étant plus fiable. L'impératif de sécurité serait ainsi satisfait. Facile d'utilisation, ce système devrait rencontrer un certain succès.

4.2.2. Cheque électronique *NetChex* :

De son côté, le système *NetChex* [11] fait intervenir un intermédiaire auprès duquel l'utilisateur et le commerçant devront s'enregistrer. *NetChex* permet au client de générer ses propres chèques sur son ordinateur personnel. *NetChex* est complètement compatible avec l'infrastructure

bancaire actuelle et ne remplace aucune des composantes des systèmes de transferts de monnaie inter-banques.

5. Monnaie électronique :

Selon la commission européenne, la monnaie électronique se définit comme « toute valeur monétaire représentant une créance qui est stockée sur un support électronique ; cette valeur monétaire doit être émise contre la remise de fonds d'un montant dont la valeur n'est pas inférieure à la valeur monétaire émise » [12].

5.1. Types de monnaie électronique :

Il existe principalement deux types de monnaies électroniques à usage multiple : le porte-monnaie électronique et le porte-monnaie virtuel [12] :

Le porte-monnaie électronique (*PME*) est une carte à puce permettant le règlement des petites sommes non assuré par les cartes bancaires. Le principe consiste à charger un certain montant d'argent dans la puce électronique (via un distributeur ou la machine d'un commerçant) puis de régler les petits achats (pain, journal, parking...) à l'aide de cette carte.

Le porte-monnaie virtuel (*PMV*) utilise comme support des signes monétaires, le disque dur d'un ordinateur. Les expériences en place sont encore mineures et sont souvent libellées dans une unité monétaire n'ayant pas cours légal, mais le *PMV*, grâce à ses caractéristiques et aux services qu'il offrira, est la forme de monnaie électronique ayant le plus grand potentiel.

6. Caractéristiques d'un mécanisme de paiement électronique :

Il existe actuellement une multitude de moyens de paiement électronique disponibles sur Internet. Bien que chaque entreprise prétende commercialiser le produit idéal, aucune d'entre elles ne convient parfaitement à l'ensemble des situations. Tous les mécanismes proposés possèdent des avantages et des inconvénients spécifiques et chaque commerçant doit choisir celui ou ceux qui paraissent convenir le mieux à sa situation. Il est donc important que le commerçant connaisse les différents éléments à considérer lors de cette prise de décision afin d'être en mesure d'effectuer un choix éclairé.

6.1- Universalité :

L'acceptation généralisée d'un mécanisme de paiement est l'un des éléments déterminants pour sa viabilité. Dans le contexte de l'internationalisation des échanges propre au commerce électronique, cette caractéristique redouble d'intérêt [09]. Aussi, du point de vue du

commerçant, le meilleur mécanisme n'est pas celui qui comble simplement ses propres besoins, mais plutôt celui qui répond aux attentes de l'ensemble de la communauté commerçante. Le système qui réussira à rassembler de nombreux commerçants attirera inévitablement de nombreux consommateurs, assurant ainsi son succès.

Pour y arriver, le mécanisme de paiement doit permettre un certain niveau de compatibilité entre les différents systèmes. En d'autres mots, il doit prévoir une standardisation essentielle aux communications sur un réseau hétérogène comme Internet. À ce niveau, il faut d'abord que les logiciels et le matériel nécessaires au fonctionnement du serveur de transaction puissent être utilisés sur de nombreuses plates-formes. De la même façon, du matériel à la fine pointe de la technologie ne doit pas être exigé du commerçant. Ensuite, si le système nécessite l'installation de logiciels clients, il est essentiel que ceux-ci soient disponibles pour un maximum de consommateurs, sans considération pour l'environnement matériel et logiciel qu'ils utilisent.

Dans la même optique, les mécanismes de paiement rattachés à une catégorie de transaction ou à un site en particulier doivent être évités. La compartimentation est dangereuse pour le commerçant qui prend alors le risque de s'isoler [13].

L'universalité doit également être respectée en ce qui a trait à l'accessibilité du mécanisme de paiement dans le temps. Sur Internet, les consommateurs s'attendent à un système de transaction disponible en tout temps. Le commerçant doit tenir compte du fait que sa clientèle se trouve dispersée dans plusieurs fuseaux horaires.

Finalement, l'universalité passe par la possibilité de transiger avec une pluralité de devises. Le mécanisme de paiement doit donc prévoir le recours à un système de conversion des devises qui informe le consommateur du taux de change offert.

6.2- Faibles coûts de transaction et rapidité d'exécution :

Pour que l'utilisation d'un mécanisme de paiement soit avantageuse, les frais relatifs à son utilisation doivent être peu élevés. Parmi les facteurs contribuant à faire augmenter les coûts de transaction, le principal consiste à recourir à un tiers afin de compléter le processus de paiement. Il n'est pas difficile de comprendre que les frais augmentent rapidement lorsque les parties doivent rémunérer une personne supplémentaire pour prendre le paiement en charge. Le degré d'automatisation influence également les coûts

de transaction. Lorsque la supervision de personnes physiques est nécessaire au bon déroulement du processus, les coûts augmentent inévitablement. De la même façon, les systèmes basés sur l'utilisation de matériel (carte, lecteur, puces électroniques, etc.) engendrent des coûts plus élevés que les systèmes reposant sur l'utilisation de logiciels. Toutefois, il est possible qu'une solution matérielle soit avantageuse dans la mesure où celle-ci est largement utilisée.

Dans tous les cas, le coût d'utilisation d'un mécanisme de paiement électronique doit être proportionnel à la valeur de la transaction. Ainsi, les commerçants misant sur des transactions de faibles valeurs ont souvent avantage à opter pour des systèmes dont les coûts sont calculés au pourcentage. D'un autre côté, les commerçants dont les transactions atteignent des sommes importantes recherchent plutôt les mécanismes de paiement établissant un coût fixe pour toutes les transactions.

Le temps passé par le consommateur à effectuer le paiement est un autre type de coût pour l'utilisateur d'un mécanisme de paiement électronique. L'exécution du paiement doit être rapide sinon ce dernier risque d'abandonner l'opération ou chercher un autre commerçant pour ses futurs achats. Comme la partie la plus longue du processus de paiement en ligne concerne la saisie des données par le consommateur, le commerçant devrait lui faciliter cette tâche. Pour y arriver, le commerçant doit être en mesure de conserver les données du consommateur, lui évitant ainsi d'avoir à remplir un nouveau formulaire pour chaque achat. L'utilisation de fichiers témoins peut également être envisagée afin de permettre au consommateur de personnaliser le processus de paiement en fonction de ses propres besoins, dans la mesure où les considérations ayant trait au respect de la vie privée sont prises en compte [09].

6.3- Facilité d'utilisation :

Pour que les consommateurs acceptent d'utiliser un mécanisme de paiement électronique, celui-ci doit avant tout être simple. Actuellement, une majorité d'Internautes estiment que les méthodes proposées sont difficiles à utiliser [14]. Le commerçant doit donc porter une attention particulière aux systèmes qui ne requièrent aucune expertise particulière de la part des consommateurs.

Les mécanismes de paiement les plus simples sont évidemment ceux qui ne nécessitent pas d'installation de logiciels clients. Malheureusement ceux-ci sont plutôt rares. Lorsque l'installation de logiciels est inévitable, le recours à des plugiciels (plug-in) est souhaitable puisqu'elle permet au

consommateur de continuer à utiliser un logiciel dont il connaît déjà les fonctionnalités. De plus, une fois le processus d'installation complété, le logiciel de paiement électronique doit nécessiter le moins d'interventions possibles de la part de l'utilisateur. Le mécanisme de la transaction devrait être transparent pour lui dans la mesure où il en comprend les implications. Enfin, il est très important que l'entreprise qui met de l'avant le mécanisme de paiement offre un support technique efficace au consommateur.

6.4- Anonymat :

Pour des raisons de discrétion, les consommateurs ne désirent pas qu'un organisme ou qu'un commerçant puisse accéder à leur identité ou retracer l'ensemble de leurs paiements. Il s'agira de faire en sorte que les transactions effectuées au moyen d'unité de paiement électroniques répondent aux caractéristiques de la monnaie fiduciaire, dont l'utilisation demeure anonyme.

6.5- Vérification de l'authenticité de l'argent :

Tout moyen de paiement doit être en mesure de garantir au créancier la valeur de ce qui lui est remis en guise de paiement. Les mécanismes de paiement électronique doivent donc être capables d'authentifier l'argent transmis afin d'obtenir la confiance des différents acteurs. Cette exigence est particulièrement pertinente pour les systèmes reposant sur l'utilisation de monnaies électroniques. Puisque celle-ci est composée de données informatiques, elle est théoriquement facile à reproduire. Comme la copie informatique est impossible à distinguer de l'originale, la contrefaçon serait alors impossible à détecter. S'il en était ainsi, toute personne disposant d'une pièce de monnaie électronique pourrait devenir millionnaire en quelques minutes. Pour être viable, les mécanismes de paiement électronique doivent donc éliminer ce problème de la double utilisation (double spending) [15].

Pour les systèmes en ligne, la solution consiste à communiquer avec la banque émettrice à chaque fois qu'une transaction a lieu. Cette dernière, en maintenant une base de données des pièces utilisées, indique au commerçant si la monnaie qui lui est proposée a déjà été dépensée. Si la réponse est positive, la transaction est annulée, alors que si la réponse est négative, la transaction peut être complétée. Cette façon de faire ressemble en partie à la méthode actuellement utilisée pour vérifier les cartes de crédit [09].

Pour ce qui est des systèmes hors ligne, il existe principalement deux méthodes pour régler le problème de la double utilisation [15]. La première consiste à doter les cartes d'une puce qui tient un compte exact des pièces de monnaie dépensées. Si le propriétaire de cette carte tente d'utiliser une pièce

déjà dépensée, la puce n'autorise pas la transaction. Ces puces sont conçues de façon à ce que la carte devienne inutilisable après toute tentative de modification des données qui s'y trouvent. La seconde méthode repose sur la cryptographie. En structurant le protocole cryptographique, il est possible de s'assurer que l'identité du double utilisateur soit révélée lorsqu'une pièce de monnaie retourne à la banque. En principe les utilisateurs ne devraient pas dépenser deux fois leurs pièces s'ils sont certains d'être pris en peu de temps. L'avantage de cette deuxième solution est qu'elle ne nécessite pas l'utilisation de puces spéciales et qu'elle peut donc reposer entièrement sur des logiciels.

6.6- Assurance de l'intégrité du paiement :

Pour qu'un mécanisme de paiement gagne la confiance des acteurs du commerce électronique, il doit aussi assurer l'intégrité des communications ayant lieu lors de la transaction. Il s'agit du principal élément de sécurité en matière de commerce sur Internet.

Cela signifie premièrement que les tiers ne doivent pas être en mesure de modifier les messages transmis. Deuxièmement, il faut que l'intégrité du paiement soit aussi protégée contre la fraude de l'une ou l'autre des parties. De plus, dans le cas de la monnaie électronique, l'hypothèse de la collusion entre le consommateur et le commerçant dans le but de tromper la banque émettrice doit être envisagée. Lorsque ces exigences ne sont pas respectées, un grand nombre de transactions courent le risque d'être répudiées, ce qui affecterait la stabilité du commerce électronique en général.

Pratiquement, l'intégrité du paiement est assurée par le recours à la cryptographie. Les procédés utilisés pour une transaction d'une faible valeur sont les mêmes que ceux qui servent pour les transferts importants entre banque ou pour la défense nationale. Cependant, comme aucun procédé cryptographique n'est totalement inviolable, le commerçant doit tout de même être vigilant en ce qui a trait à la sécurité de son système.

6.7- Identification adéquate des parties :

Très souvent, il sera important pour une partie d'être en mesure d'identifier exactement son co-contractant au moment du paiement. En étant certain de l'identité du commerçant, le consommateur a la certitude de ne pas se faire escroquer par un usurpateur et se réserve des éléments de preuve qui lui seront utiles en cas de litige. De son côté le commerçant s'assure que le consommateur est le véritable détenteur du mode de paiement utilisé, ce qui lui confirme la validité du paiement. En fait, l'identification des parties est avantageuse dès lors que la transaction possède un élément non instantané. Il peut s'agir, par exemple, d'une garantie, de la possibilité de poursuites en responsabilité, de la possibilité que possède l'une des parties de répudier le

paiement, etc. En conséquence, un mécanisme efficace de paiement électronique doit donner aux parties la possibilité de s'identifier mutuellement.

Toutefois, la simple utilisation de procédés cryptographiques ne garantit aucunement que la personne à l'origine d'une communication n'est bel et bien celle qu'elle prétend être [09]. Heureusement, d'autres techniques peuvent être utilisées pour établir un mécanisme d'identification efficace. Ainsi, certains mécanismes de paiement électronique prévoient l'enregistrement des participants qui doivent alors fournir des informations sur leur identité. Ces informations sont ensuite rendues disponibles aux co-contractants. D'autres systèmes reposent sur les certificats d'identification émis par des autorités de certification. Ceci permet aux parties de s'assurer que la clé de chiffrement utilisée émane effectivement de la bonne personne. En utilisant un tel certificat de concert avec un mécanisme de signatures électroniques, le consommateur et le commerçant obtiennent un niveau de confiance élevé quant à l'identité de l'autre partie à la transaction. Cette façon de procéder ne permet pas de certifier hors de tout doute l'identité du contractant, mais il s'agit définitivement de la méthode la plus efficace disponible actuellement [16].

6.8- Confidentialité :

Finalement, le niveau de confidentialité offert par un mécanisme de paiement électronique est un autre élément dont le commerçant doit tenir compte. En effet, le paiement suppose la communication de nombreux renseignements de la part du consommateur. Ce sont justement ces renseignements, récoltés lors de l'utilisation d'un service, qui sont les plus prisés par les entreprises. Il s'agit, entre autres, de l'adresse physique du consommateur, de ses renseignements bancaires, du mode de paiement utilisé, du contexte du paiement (date, heure, provenance ...), etc. Ces données ont une valeur économique élevée et permettent un contrôle social important. Il n'est donc pas étonnant que plusieurs entreprises les accumulent afin de dresser des portraits extrêmement détaillés des consommateurs. C'est, entre autres, le cas de certains mécanismes de paiement électronique [09].

Les commerçants doivent toutefois apprendre à se méfier de ces systèmes. Premièrement, il est fort possible que les pratiques de ceux-ci soient illégales dans plusieurs juridictions. Comme beaucoup d'États se sont dotés de législations sur la protection des renseignements personnels au cours des dernières années, la collecte en est souvent limitée [02].

Deuxièmement, les entreprises accumulant ces données tentent généralement de les vendre par la suite [03]. Il peut être extrêmement nuisible pour un commerçant d'être associé à ce type de comportement. Sa réputation peut être définitivement entachée. Troisièmement, les consommateurs n'accorderont pas leur confiance à un système qui permet de récolter des renseignements à outrance. Peu importe la méthode utilisée (base de donnée centrale ou carte à puce), s'il existe un doute quant au contenu des données accumulées lors du paiement, cela peut être suffisant pour freiner l'utilisation d'un système.

D'un autre côté, les mécanismes de paiement électronique totalement anonymes ne représentent pas une meilleure solution. En effet, plusieurs Etats envisagent de les interdire à cause du risque qu'ils représentent pour le blanchiment d'argent, l'évasion fiscale et l'achat de produits et services illégaux [09]. Il faut comprendre que le contexte des environnements dématérialisés permet d'atteindre un niveau d'anonymat encore inégalé dans le monde physique. Si la monnaie classique ne laisse aucune trace, le commerçant traditionnel peut toujours identifier le consommateur visuellement. Le commerce électronique élimine ce dernier élément d'identification. A cela s'ajoute le fait que plusieurs législations exigent des institutions financières qu'elles suivent le déroulement de certaines transactions électroniques et en conservent des traces.

Conclusion :

Le mécanisme de paiement idéal doit donc constituer une solution intermédiaire à ces deux extrêmes. Sans accorder l'anonymat complet, il doit assurer au consommateur que seuls les renseignements nécessaires au paiement seront emmagasinés et que ceux-ci seront utilisés à cette unique fin. De plus, il doit assurer la majorité des caractéristiques vues précédemment.

BIBLIOGRAPHIE

Ouvrages et articles :

[01] OCDE© : Commerce électronique : Organisation de Coopération et de Développement Économique 2002.

[02] P. Doyon, F. Bégin, A. El Zaïm et O. Ureche : Rapport de veille stratégique - les systèmes de paiement électronique sur internet. Centre de recherche informatique de Montréal 1999.

[03] Jean-Pierre VIERLING : Le paiement en ligne: Des moyens techniques et juridiques pour la sécurisation du e-commerce. Avril 2000 Chambre de commerce et d'industrie Paris.

[04] Donal O'mahony, Michael Pierce, Hitesh Tewari: Electronic Payment Systems for E-Commerce. 2001 ARTECH HOUSE INC.

[07] Corinne LAMOUCSIÈRE-POUVREAU : Vos droits - La carte bancaire. INC Hebdo juillet 2003

[08] Cristian Radu: Implementing Electronic Card Payment Systems. 2001 ARTECH HOUSE INC.

[09] Pierre-Paul LEMYRE : Le guide juridique du commerçant électronique - Chapitre 8 – Le paiement électronique.

[10] VISA: 3-D Secure System Overview. Version 1.0.2, May 01, 2003.

[12] Donal O'mahony, Michael Pierce, Hitesh Tewari: Electronic Payment Systems for E-Commerce. 2001 ARTECH HOUSE INC.

[13] Marloye CONDE, Ranaivo Mahaleo RAZAKANIRINA : Réseaux et Sécurité - Pratique de la sécurité Paiement sur Internet. Université de Genève janvier 2005.

[14] - Florence Labasque : Le paiement en ligne : l'état du droit face à la technique

[15] David Bounie – Sébastien Soriano : La monnaie électronique-Principes, fonctionnement et organisation. La finance électronique LCN, n° 1-2003.

[16] Jean-François Blanchette : Les procédés cryptographiques de monnaie électronique - Design, fonctionnalités et usages. Université de Montréal octobre 1997.

[17] Milton M.Anderson: The Electronic Check Architecture. Version 1.0.2 – September 29, 1998.

Sites Web:

[05] <http://www.SecuriteInfo.com>

[06] <http://www.Wikipédia.com>

[18] [http://www.guideinformatique.com/dossier-banque assurance finance- 3.html](http://www.guideinformatique.com/dossier-banque_assurance_finance-3.html).

[11] <http://www.netchex.com/>