Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DES FINANCES ET DE L'INDUSTRIE

RAPPORT DU GROUPE DE TRAVAIL N° 5

présenté au comité d'orientation du
15 novembre 2001

« Les services financiers en ligne»

Rapporteur :
Carlos MARTIN - Banque de France
carlos.martin@banque-france.fr

Animateur :
Denis BEAU - Banque de France
denis.beau@banque-france.fr

Mission pour l'économie Numérique

Rapport du sous-groupe « les paiements et leur sécurité»

Animateur : Denis BEAU (Banque de France)

Rapporteur : Carlos MARTIN (Banque de France)

SYNTHESE

Le gouvernement a confié à la Mission pour l'Économie Numérique l'analyse de l'impact des technologies de l'information et de la communication sur l'ensemble de l'économie. Dans ce cadre, une étude plus particulière a été réalisée sur les services financiers. Ainsi, le sous-groupe «les paiements et leur sécurité» a-t-il été mandaté pour dresser un état de l'art en matière de solutions techniques de paiement sécurisé en ligne afin de formuler des recommandations sur la sécurité que devraient offrir les moyens de paiement électroniques.

Un moyen de paiement électronique, de par son caractère technologique, est soumis à des risques d'ordre technique, qui se traduisent par des menaces dont la vitesse de propagation est très élevée. Pour contrer ces menaces, il est opportun que le gestionnaire du moyen de paiement électronique définisse des **objectifs de sécurité** qui prennent en compte d'une part les étapes du cycle de vie du moyen de paiement (conception, validation, surveillance) et, d'autre part, les caractéristiques opérationnelles concernant le fonctionnement du dispositif. La définition de ces objectifs doit conduire à la mise en œuvre d'un ensemble de mesures (organisationnelles, techniques…) dont la cohérence doit être assurée. Ces mesures doivent viser sur un plan opérationnel à protéger la communication, à permettre la vérification de l'identité des parties impliquées dans la transaction, à garantir la sécurité des composants du système (serveurs, réseaux, …) et à assurer une bonne protection des utilisateurs. *(Chapitre 2)*

Le sous-groupe a réalisé un état des lieux non exhaustif des moyens de paiement électroniques actuellement disponibles en ligne ou en cours de développement *(Chapitre 3)*. Du point de vue des utilisateurs, les moyens de paiement offerts présentent un degré de différenciation élevé. Sur un plan technique ils se distinguent par le recours à une technologie de type matériel (cartes à puce) ou logiciel («wallet»). On peut également observer que tous les moyens de paiement électroniques n'ont pas vocation à couvrir l'ensemble du marché du commerce électronique. Leur utilisation est fonction de leur coût d'utilisation et du montant moyen des paiements à effectuer. En outre, ils ne présentent pas tous la même flexibilité. Certains sont des moyens de paiement simplement adaptés à Internet, tandis que d'autres ont été spécialement conçus pour ce réseau. Enfin, les niveaux de sécurité offerts sont inégaux. Les observations faites sur le plan sécuritaire ont conduit le sous-groupe à formuler un ensemble de recommandations *(Chapitre 4)* dont les principales sont les suivantes :

(1). La définition d'un référentiel de sécurité spécifique à chaque type de moyen de paiement électronique. Ce référentiel de sécurité à définir par les entités concernées en concertation avec la Banque de France, chargée de veiller à la sécurité des instruments de paiement, devrait s'adapter à la nature et à l'utilisation envisagée du moyen de paiement et ne pas entraver l'innovation nécessaire au développement de ces nouveaux services. Il pourrait servir de guide dans toutes les étapes du cycle de vie du moyen de paiement, aussi bien dans l'expression des besoins de sécurité, la validation que la maintenance de la sécurité.

(2). La création d'un label de sécurité permettant aux utilisateurs d'avoir des garanties sur le niveau de sécurité offert par le service, les fournisseurs de ce dernier pouvant s'en prévaloir dans leur politique commerciale.

(3). **La vérification forte de l'identité des parties impliquées dans la transaction.** Cette vérification est souvent inexistante (paiement par utilisation du numéro de carte). La plupart des nouveaux moyens de paiement utilisent un mécanisme de mot de passe pour authentifier le client. Quoique présentant une amélioration par rapport à la communication du numéro de carte bancaire, le niveau de sécurité offert reste élémentaire. L'authentification des parties impliquées (personnes ou systèmes informatiques les représentant) dans la transaction devrait être **mutuelle et forte**, grâce par exemple à des techniques de type «défi-réponse» (non communication des secrets sur le réseau).

(4). Parmi les solutions disponibles sur le marché, les infrastructures à clé publiques (signature électronique) présentent des garanties de sécurité appropriées. Ces infrastructures permettent de lier une valeur numérique (certificat) à l'identité d'une personne physique ou morale. **Le sous-groupe encourage fortement le développement de telles infrastructures.** Au plan pratique, une infrastructure à clé publique repose sur deux types d'entités :

- Une autorité d'enregistrement qui effectue la vérification d'un certain nombre d'informations concernant la personne morale ou physique demandant l'octroi d'un certificat, notamment son identité, et envoie ces informations à l'autorité de certification.
- Une autorité de certification qui définit la politique de certification, conserve la clé secrète servant à signer les certificats et assure ou sous-traite la gestion des certificats (fabrication à partir du message envoyé par l'autorité d'enregistrement, publication, révocation, …) .

Le sous-groupe recommande que l'autorité d'enregistrement soit assurée par l'État afin d'homogénéiser la distribution des certificats et de promouvoir l'utilisation de la signature électronique.

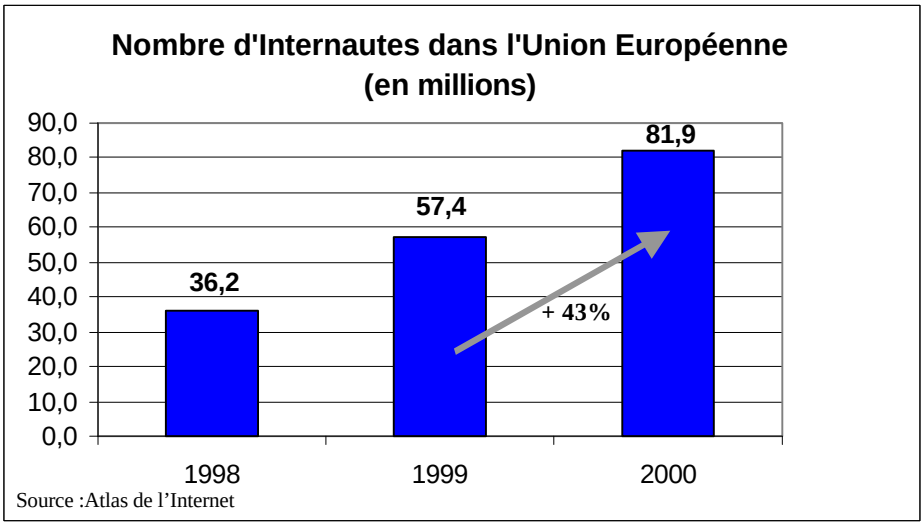
(5). **L'intégration de la sécurité des composants dans la politique de sécurité,** ce qui implique la mise en œuvre de nombreuses mesures dont les plus importantes sont le confinement des réseaux, le contrôle d'accès au système, la sécurité des serveurs, la sûreté des systèmes d'information et l'utilisation de boîtiers de sécurité.

(6). **Le renforcement de la protection des utilisateurs.** Celle-ci est peu prise en compte sur Internet. La pertinence, la qualité et l'ergonomie du produit distribué à l'internaute doivent être vérifiées. Celui-ci doit disposer d'une information suffisante, facilement accessible et simple, quant aux modalités d'utilisation du moyen de paiement. A cette fin le sous-groupe recommande que soit précisé à l'internaute, afin de le responsabiliser, les règles minimales de sécurité qu'il doit respecter (conformité aux recommandations de sécurité, sauvegarde des données, protection contre les virus, stockage des clés d'accès au service, …).

SOMMAIRE

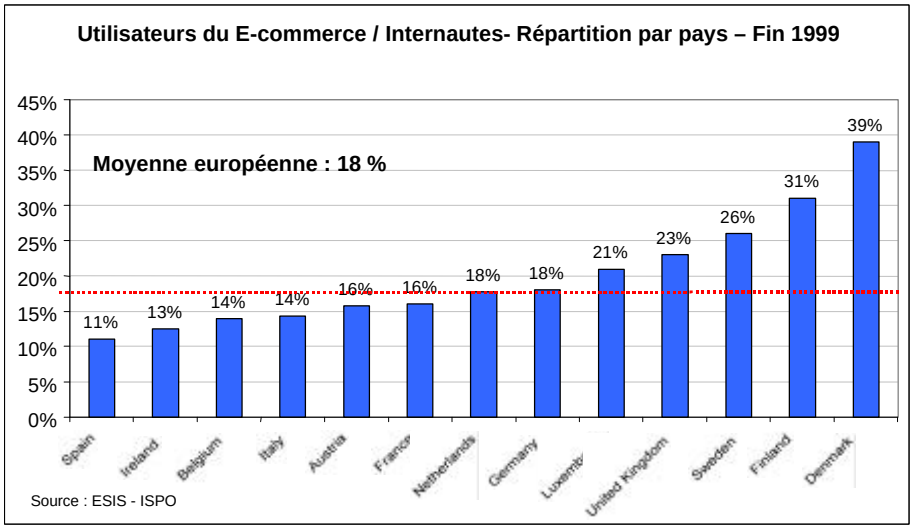
INTRODUCTION

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'usage d'Internet est en pleine expansion en Europe et de même le commerce électronique, comme le montrent les graphiques ci-dessous.



Le marché du commerce électronique est évalué à 218 milliards d'euros en 2000, selon Gartner Group et IDC. Les données comprennent le Business to Business (B to B) qui représente la majeure partie du marché (environ 209 milliards d'euros).

Dans l'Union européenne, en 1999, 18% des internautes effectuaient des achats en ligne. Comme le montre le graphique suivant, les pays nordiques (Danemark, Finlande et Suède) ainsi que le Royaume-Uni sont les plus avancés en ce domaine. Les pays au développement intermédiaire sont l'Allemagne, les Pays-Bas et la France[1]. Le commerce électronique est peu répandu en Espagne et au Portugal.



[1] Ces statistiques ne tiennent pas compte de l'utilisation du Minitel qui plaçait en 1999 la France loin devant tous les autres pays européens en terme de volume des paiements à distance (source : étude ACSEL).

Selon les données publiées par Europrofile[2], une forte croissance du commerce électronique en Europe est prévue pour les années à venir. Selon ces prévisions, le marché du commerce électronique passerait d'environ 14Md d'euros à 500Md d'euros en 2004. Cette croissance du commerce électronique devrait s'accompagner d'une croissance parallèle des paiements en ligne. Selon Europrofile, ceux-ci devraient représenter en 2004 10% du commerce électronique, soit environ 50Md d'euros.

Une condition importante de réalisation de ces perspectives est que les consommateurs disposent de moyens de paiement adaptés aux échanges électroniques. En effet, Internet n'a pas été développé pour le transfert d'informations sensibles (telles que les données associées à une transaction de paiement) et son utilisation dans un moyen de paiement sans des mesures de sécurité additionnelles est une source de risques sécuritaires très importante. Sur ces marchés en forte croissance, des acteurs spécialisés dans ces nouvelles technologies apparaissent et offrent de nouvelles possibilités quant aux paiements. Cette surenchère en matière de solutions techniques implique des niveaux de sécurité disparates.

C'est pourquoi, dans le cadre de la Mission pour l'Economie Numérique, le sous-groupe «les paiements et leur sécurité» (voir composition en annexe 1) a été chargé d'étudier les conditions d'apparition de nouveaux moyens de paiement adaptés à l'économie numérique et d'en recenser les conséquences juridiques, commerciales et macroéconomiques.
Le rapport qui suit présente le résultat des travaux menés qui ont visé à définir les concepts concernant le commerce électronique, recenser les exigences minimales de sécurité, dresser un état des lieux critique sur le plan sécuritaire des moyens de paiement électroniques et enfin établir des recommandations à promouvoir.

Des offres d'assurance destinées aux particuliers et aux commerçants peuvent constituer un complément utile aux solutions techniques de paiement sécurisé en vue de renforcer la confiance des acteurs et accélérer le démarrage du commerce électronique. Cependant, l'examen de ces offres ne relève pas du mandat du sous-groupe.

[2] Europrofile est une entreprise qui fournit des statistiques sur le commerce électronique sur Internet ; (http://www.europeprofile.com/).

CHAPITRE 1 : LES PRINCIPES

La procédure de paiement est une étape de l'achat par voie électronique, comme le choix du produit, sa commande et sa livraison. La problématique des paiements sur Internet peut donc se résumer à la question : comment payer d'une manière sûre sur un réseau ouvert qui par construction n'offre aucune sécurité.
Ce chapitre vise à définir les principes fondamentaux permettant de comprendre les enjeux liés aux paiements sur Internet.

1.1. Le commerce électronique

Le commerce électronique se réfère à toute transaction commerciale dans laquelle une ou plusieurs des étapes suivantes est effectuée de manière électronique : le conseil ou la promotion d'un produit, le choix du produit, la commande, le paiement, la livraison et le service après vente. Comme le commerce traditionnel, le commerce électronique peut être ainsi divisé en cinq phases : l'information ou l'offre, la commande, le paiement, la livraison et l'après-vente.

Une distinction claire doit être faite entre les produits immatériels (information, logiciels, images, musiques…) et les produits physiques (livres, CDs…). Le commerce électronique de ces deux types de produits se différencie par la procédure de livraison : la livraison de produits immatériels peut se faire en temps réel alors que celle des biens physiques nécessite un délai. La nature du lien avec la procédure de paiement est donc différente. En effet, de manière assez générale pour le commerçant, la sécurisation de la commande pour les biens matériels repose sur la sécurisation préalable du paiement ce qui n'est pas forcément le cas pour les biens immatériels.

Le commerce électronique se caractérise par des transactions électroniques, dont plusieurs types peuvent être relevés :

- les transactions entre l'acheteur et la banque (banque à domicile, banque par téléphone …) dont l'objectif est la gestion des comptes bancaires mais aussi d'établir un contact direct entre la banque et son client ;
- les transactions entre l'acheteur et le vendeur : il s'agit d'un contrat aux termes duquel le vendeur fournit un service au consommateur et reçoit en contrepartie un paiement ou un ordre de paiement (paiement par téléphone, paiement sur Internet …) ;
- les transactions entre l'acheteur, le vendeur et un intermédiaire qui est généralement une banque.

Les achats qui sont initiés de manière électronique (consultation d'une offre et/ou commande), mais dont le paiement ne s'initie ou ne s'effectue pas par ce biais ne rentrent pas dans le cadre d'une transaction électronique. Ainsi, les instruments de paiements traditionnels comme le paiement par chèque soit par envoi postal soit lors de la livraison, l'envoi d'un fax comportant le numéro de carte de paiement, ne sont pas considérés comme des transactions électroniques.

Le transfert des activités de commerce traditionnel vers le monde virtuel introduit un certain nombre d'interrogations concernant la sécurité offerte par le commerce électronique. La suite du document tente de clarifier ces points.

1.2. Les moyens de paiement électroniques

Pour les besoins de ce rapport, le terme «moyen de paiement électronique» recouvre :

- un instrument de paiement (chèque, carte de paiement, virement, porte-monnaie électronique, logiciel téléchargé sur le poste de l'utilisateur…) qui permet à l'utilisateur de générer l'ordre de paiement,
- le dispositif technique qui permet de traiter l'ordre de paiement.

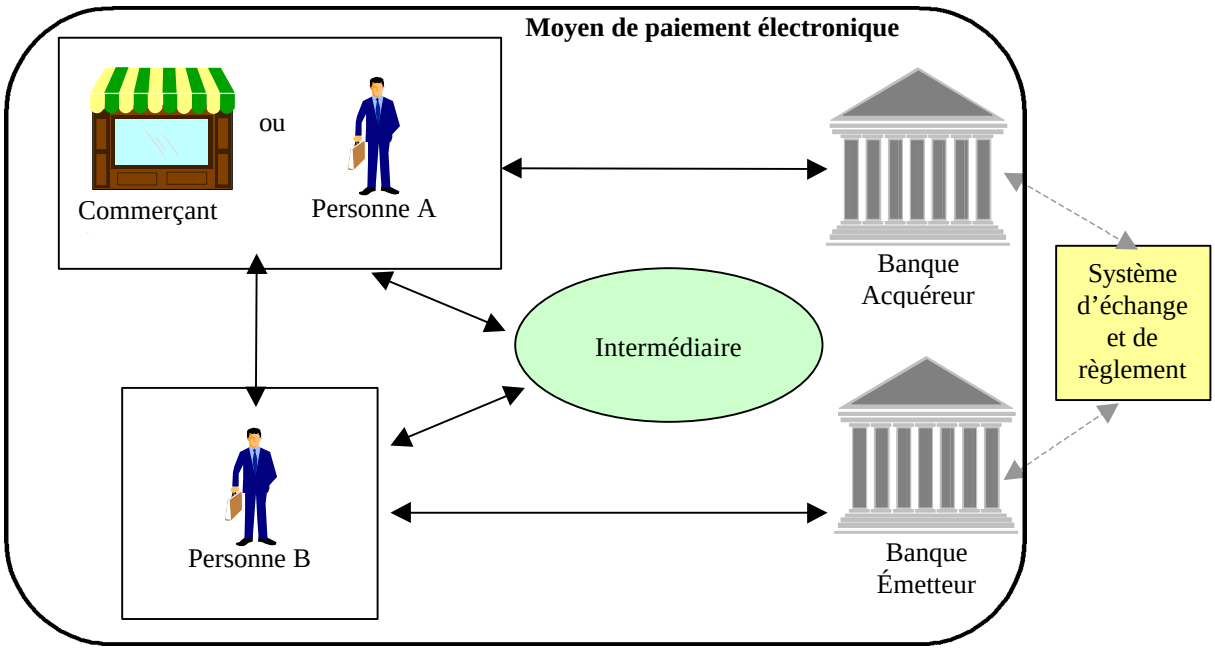
Dans le cadre de cette définition, un moyen de paiement ne comprend pas les systèmes d'échange et de règlement entre les banques.

De nombreux acteurs sont impliqués dans l'échange d'ordre de paiement ou la circulation de monnaie virtuelle. Pour l'essentiel, ces acteurs comprennent l'acheteur, le vendeur et des intermédiaires. Ces intermédiaires sont traditionnellement des banques mais de nouvelles sociétés apparaissent dont la principale activité est associée au nouveau moyen de paiement qu'elles développent.

Dans ce rapport, ces différents acteurs seront modélisés de la manière suivante :

- l'entité qui passe la commande,
- la banque émetteur, en référence à la banque qui émet l'instrument de paiement,
- l'entité qui reçoit la commande et demande à être payée (personne ou commerçant),
- la banque acquéreur,
- et éventuellement un intermédiaire qui peut intervenir entre ces quatre premiers acteurs.

Un moyen de paiement électronique est donc le résultat du choix d'un instrument de paiement par l'entité qui initie le paiement et des flux entre les différents acteurs de ce moyen de paiement. De manière générale, la circulation des flux est spécifique à chaque moyen de paiement.



On notera que les premiers moyens de paiement proposés sur Internet se sont appuyés sur des instruments de paiement existants. C’est en particulier le cas avec l’emploi des cartes de paiement. Pour les paiements à distance, la carte de paiement est utilisée en communiquant seulement son numéro et sa date de validité. Cette pratique a conduit notamment à une forte augmentation du taux de fraude sur les cartes bancaires. Ainsi, la fraude sur les rechargements des téléphones par cartes bancaires a atteint un taux supérieur à 5% pour certains opérateurs de téléphonie mobile.

CHAPITRE 2 : LES EXIGENCES DE SECURITE DES MOYENS DE PAIEMENT ELECTRONIQUES

La sécurité d'un moyen de paiement, dépend des trois facteurs suivants :

- la solidité du gestionnaire de ce moyen de paiement : Le gestionnaire est confronté à un ensemble de risques dont la réalisation est susceptible de menacer sa pérennité, et ce faisant d'entraîner des effets systémiques négatifs au sein du système financier et une perte de confiance dans les instruments de paiement. Parmi ces risques figurent en particulier un risque de liquidité et un risque opérationnel. Le gestionnaire doit donc disposer d'une structure financière solide et d'un système de contrôle des risques performant ;
- la solidité des accords contractuels entre les acteurs : Celle-ci détermine notamment la protection des utilisateurs contre le risque de perte financière, le risque d'inexécution des transactions dans les conditions attendues, et le risque de fraude. Les accords contractuels doivent ainsi définir précisément et de façon transparente les obligations et les risques de chacune des parties, et en particulier les modalités de répartition des pertes consécutives à un dysfonctionnement du système ;
- la sécurité technique et organisationnelle du système : Celle-ci a trait à la protection du moyen de paiement contre des menaces qui peuvent porter sur les applications ou sur les moyens techniques employés. Dans le domaine de la sécurité, une attention particulière est accordée aux menaces liées à des activités humaines malveillantes.

La suite de ce chapitre traite plus spécifiquement des mesures de sécurité qui peuvent être mises en œuvre pour assurer une protection efficace contre les menaces de nature technique ou organisationnelle des moyens de paiement électroniques.
Ces mesures de sécurité visent à réduire les vulnérabilités et à satisfaire les politiques de sécurité des gestionnaires des moyens de paiement. Des vulnérabilités résiduelles peuvent persister après la mise en œuvre de ces mesures. De telles vulnérabilités peuvent être exploitées par des attaquants, constituant ainsi un niveau de risque résiduel à l'encontre des systèmes à protéger. Ce risque résiduel peut être minimisé par l'adoption de mesures d'ordre organisationnel.

2.1. Les menaces

Le caractère hautement technologique des moyens de paiements crée :

- *un risque de perte de maîtrise de l'outil informatique* par les émetteurs qui ne seraient plus en mesure de s'assurer que les systèmes d'information associés au moyen de paiement offrent le niveau de sécurité et de service garanti à l'utilisateur ;
- *un risque financier*, les dysfonctionnements intentionnels ou non d'un moyen de paiement peuvent conduire à des pertes financières pour l'ensemble des parties impliquées dans la transaction ;
- *un risque de blanchiment* facilité par la nature dématérialisée de la relation entre les parties impliquées dans la transaction électronique qui rend plus difficile la vérification de l'identité ;
- et enfin, *un risque d'image* qui peut engendrer une défiance de l'utilisateur dont la propagation à l'ensemble des moyens de paiement électroniques et aux institutions qui les gèrent est porteuse de risques systémiques et de perte de confiance dans la monnaie.

Ces risques d'ordre générique traduisent l'existence de menaces, de nature traditionnelle et liées à l'émergence des nouvelles technologies des systèmes d'information, qui peuvent se classer dans les principales catégories suivantes :

- la perte d'intégrité des flux d'information (transactions, poste utilisateur, serveur),
- la répudiation d'une transaction,
- l'usurpation d'identité d'un utilisateur autorisé,
- l'atteinte à la vie privée,
- le déni de service,
- le détournement de sites,
- …

Une autre particularité des menaces dans le domaine des transactions électroniques est la vitesse de propagation des attaques associées. La réactivité face à de telles menaces est donc un facteur majeur pour entraver aussi bien l'extension que l'aggravation des conséquences.

Une liste détaillée des menaces spécifiques aux transactions électroniques est jointe en annexe 2 et s'articule autour des menaces qui concernent les applications (canal de communication, serveur, poste client) et les menaces liées aux techniques utilisées (composants, cryptographie…).

2.2. Les objectifs de sécurité

Des mesures doivent donc être adoptées pour prévenir, détecter les menaces et minimiser leurs conséquences éventuelles. Ces mesures ne peuvent être liées aux seules caractéristiques opérationnelles du moyen de paiement concernant le fonctionnement du dispositif. Elles doivent également et en premier lieu tenir compte de son cycle de vie.

2.2.1. Le cycle de vie

Le cycle de vie d'un moyen de paiement peut être décomposé suivant trois phases.

a. La phase de conception

Lors de la conception d'un nouveau moyen de paiement électronique, un nombre important de menaces doit être pris en compte. Il en résulte que des mesures de sécurité de nature différente peuvent être implémentées, dont la cohérence doit être assurée. Cet objectif peut être atteint par la définition d'un modèle de sécurité. Il s'agit de modéliser l'ensemble de règles ou de principes qui permettent d'atteindre les objectifs de sécurité qu'une analyse de risque préalable a définis.
Ce modèle doit considérer chaque composant du moyen de paiement pris individuellement et leurs interactions éventuelles. En fonction de la nature de ces composants, des mesures d'ordre organisationnel ou technique, relatives aux personnels ou aux infrastructures devront être mises en œuvre pour atteindre les objectifs de sécurité souhaités. Dans ce contexte, le concepteur doit s'assurer du respect des principes décrits ci-après.

1. Mécanismes de contrôle

Tout moyen de paiement doit prévoir des mécanismes de détection des attaques et les réactions appropriées.

2. Cryptographie

La grande majorité des moyens de paiement électroniques utilisent des techniques cryptographiques. La validation du système cryptographique utilisé doit être effectuée au fur et

à mesure de sa conception. La cryptographie est une science qui évolue rapidement, il convient que la conception du système cryptographique prenne en compte l'évolution des techniques.
Par ailleurs, seuls des algorithmes cryptographiques, dont la résistance a été confirmée, doivent être utilisés. Par exemple, il faut préférer un triple DES à un simple DES ; si l'algorithme RSA est utilisé, la longueur des clés ne doit pas être inférieure à 768 bits, une longueur de 1024 bits serait un meilleur choix.

3. Logiciel et dispositif matériel fournis aux utilisateurs

Pour utiliser des moyens de paiement électroniques, des composants logiciels ou matériels sont fournis à l'utilisateur. Le niveau de protection offert par ces composants doit être adapté au risque identifié. Si des données sensibles doivent être conservées par l'utilisateur, elles devront être stockées dans des dispositifs matériels résistants aux attaques comme une carte à puce ou une carte PC. Les composants logiciels doivent disposer de la capacité de vérifier leur intégrité.

4. Protection des données de sécurité

Toutes les données de sécurité (par exemple les mots de passe) doivent être correctement protégées contre la modification ou un accès non autorisé dans tous les composants du moyen de paiement (pas seulement pendant leur transmission).

b. La phase de validation

La réalisation des objectifs de sécurité exige non seulement que des mesures de sécurité adaptées soient sélectionnées mais aussi que ces mesures soient correctement mises en œuvre et vérifiées à intervalles réguliers. Il est vital que ces vérifications soient effectuées par des organismes indépendants dont la compétence technique est reconnue.

c. La phase de surveillance

La sécurité d'un moyen de paiement peut subir des dégradations du fait de la découverte de nouvelles failles de sécurité, failles propagées rapidement dans les forums de discussion en ligne. La description de la faille est souvent accompagnée des outils pour la mettre en œuvre (script, programme, logiciel…). La mise en place d'une veille technologique pour collecter régulièrement l'information pertinente auprès des sources connues et fiables est indispensable. Tout moyen de paiement doit faire l'objet d'un suivi régulier en matière de sécurité.

2.2.2. Le fonctionnement du dispositif

Indépendamment des mesures de protection techniques ou organisationnelles qu'il convient de prendre à chaque phase du cycle de vie, l'ensemble des moyens de paiement électroniques partage des caractéristiques opérationnelles concernant le fonctionnement du dispositif qui appellent des mesures visant à :

- protéger la communication,
- vérifier l'identité des parties impliquées dans la transaction,
- assurer la sécurité des composants techniques utilisés,
- protéger les utilisateurs.

a. La protection de la communication

Pour protéger correctement la communication associée à une transaction électronique, les objectifs de sécurité ci-après doivent être respectés :

- *rejet d'une transaction* : toute transaction dont les données transférées, spécialement dans le domaine de la commande, du paiement et éventuellement de la livraison, ont été modifiées doit être rejetée ;
- *confidentialité des données* : la confidentialité des données transmises doit être garantie, spécialement les données associées aux individus participant à la transaction ;
- *non rejeu* : il doit être impossible de rejouer une transaction ;
- *non-répudiation* : il doit être impossible de répudier une commande, un paiement et éventuellement une livraison.

b. La vérification de l'identité de parties impliquées dans la transaction

La vérification de l'identité est un point fondamental pour la sécurité des transactions électroniques. Dans des réseaux ouverts comme Internet, il convient de ne pas se fier à une simple vérification d'identité des parties impliquées dans la transaction. Une authentification mutuelle de chaque composant du système est nécessaire.

Pour assurer une bonne authentification, la procédure classiquement utilisée est la technique du «défi réponse» dont le principe est le suivant : si la personne A doit s'authentifier auprès de la personne B, B doit connaître une caractéristique de A que seule A possède : «le secret». Par exemple, il peut s'agir d'une clé symétrique qui n'est connue que de A et de B. A peut également, dans le cadre d'un système de chiffrement à clé asymétrique, utiliser sa clé privée, B ayant le certificat contenant la clé publique associée.
Sur un plan opérationnel, la procédure est la suivante : B envoie à A un nombre aléatoire. A effectue une opération convenue avec B qui utilise le nombre aléatoire et le secret puis retourne le résultat à B. B effectue le même type d'opération et compare le résultat obtenu au résultat envoyé par A. Si les résultats sont concordants, alors B est assuré qu'il est réellement en communication avec A car seul A est en possession des informations nécessaires pour effectuer l'opération.

c. La sécurité des composants

Une société qui offre des services de commerce électronique doit disposer d'un système d'information ouvert sur l'Internet dont la disponibilité est assurée. L'architecture du système d'information doit être conçue pour permettre de distinguer différents niveaux d'exposition aux risques et de mettre en œuvre des moyens de défense adaptés. Pour jouer pleinement son rôle, le système d'information doit respecter les objectifs de sécurité suivants :
- La disponibilité du service et du système informatique qui fournit ces services doit être assurée conformément aux règles d'exploitation ;
- Toutes les opérations effectuées sur le système d'information doivent être enregistrées. Ces enregistrements doivent permettre une traçabilité de ces opérations ;
- Le système d'information doit être protégé contre des intrusions internes ou externes ;
- L'intégrité et la confidentialité des données associées au service doivent être assurées.

d. La protection des utilisateurs

Le consommateur souhaite utiliser Internet sans restriction mais dans la plupart des cas, il n'a pas connaissance des risques associés. Toutefois, il reste le seul responsable de son poste de travail et du niveau de sécurité qu'il offre. Toute solution de paiement qui utilise comme support le poste du travail du consommateur devrait prendre en compte les exigences suivantes :

- les logiciels installés sur le poste de travail du consommateur doivent offrir un niveau de sécurité adapté aux caractéristiques du moyen de paiement concerné ;
- le système doit être le plus simple possible pour l'utilisateur final. Toute solution qui nécessite l'intervention d'un tiers doit être rejetée ;
- toutes les transactions doivent rester sous le contrôle de l'utilisateur et des preuves doivent être enregistrées ;
- le logiciel installé doit être résistant aux erreurs et offrir une bonne protection contre les pertes financières : une défaillance du système ou une perte de la connexion ne doivent pas aboutir à une perte financière pour l'utilisateur ;
- le système doit être conçu pour assurer une bonne protection des données associées à l'utilisateur lors de leur transmission et de leur stockage. Il est recommandé que les informations relatives à l'utilisateur ne soient transmises que si elles sont strictement nécessaires à la réalisation de la transaction.

Les solutions purement logicielles ne permettent pas toujours d'atteindre le niveau de sécurité requis. Si un moyen de paiement exige que des données sensibles telles que des clés cryptographiques, des codes confidentiels ou encore de la monnaie virtuelle soient conservés par l'utilisateur, il est probable que des dispositifs matériel résistants aux attaques devront être fournis aux utilisateurs. Ces dispositifs peuvent prendre la forme d'une carte à puce, d'un boîtier électronique…

De manière générale, les dispositifs logiciels et matériels mis à la disposition de l'utilisateur devraient satisfaire les exigences de sécurité suivantes :

- ils ne peuvent pas être utilisés sans le consentement de l'utilisateur. Ce consentement peut prendre la forme d'un mot de passe, d'une caractéristique personnelle (biométrie) ou encore d'une carte à puce ;
- il doit être extrêmement difficile de modifier les données liées à une transaction au moyen d'un programme malicieux (virus, cheval de Troie…) En particulier, il est doit être impossible que des logiciels chargés de manière licite ou illicite à partir d'Internet modifient les transactions sans que l'utilisateur en soit averti ;
- pour limiter les conséquences d'une défaillance du système, celui-ci doit prévoir un moyen simple pour restaurer les données associées à un paiement ;
- les informations sensibles comme les clés cryptographiques, les mots de passe doivent être conservées de manière sûre afin que seuls les utilisateurs autorisés puissent les utiliser ;
- pendant la transaction de paiement, l'utilisateur ne doit pas être trompé sur les montants financiers échangés. L'intégrité des données échangées doit être assurée ;
- l'ensemble des transactions doit être imputé afin d'assurer une traçabilité des paiements.

CHAPITRE 3 : UN ETAT DES LIEUX DES MOYENS DE PAIEMENT ELECTRONIQUES EN LIGNE

Ce chapitre dresse un état des lieux non exhaustif des moyens de paiements électroniques sur Internet. Chaque moyen de paiement fait l'objet d'une description de son principe de fonctionnement, de son champ commercial de déploiement et enfin d'une analyse de la sécurité qu'il offre, sur la base des informations auxquelles le sous-groupe a pu avoir accès.

Les différents moyens de paiement ont été classés d'un point de vue de l'utilisateur qui a recours à un instrument de paiement utilisant principalement une technologie de type logiciel ou matériel. Le domaine de la banque à domicile n'a pas été inclus dans ces deux catégories car il offre des services beaucoup plus larges que le seul accès à un moyen de paiement (consultation de comptes, virements, opérations de bourse…).

3.1. Les instruments à base de dispositif matériel

3.1.1. Authentification par «calculatrice»

- **Principe :**
- Un commerçant souhaite authentifier le client qui lui a passé commande. Il lui envoie un défi sous forme d'aléa, c'est-à-dire une série de chiffres pris au hasard. Le client tape le défi sur sa «calculatrice» qui par l'intermédiaire d'un algorithme transforme cet aléa en une autre série de chiffres. Il transmet cette réponse au commerçant qui vérifie l'exactitude de cette série de chiffre en utilisant le même algorithme.
- **Déploiement :**
- Ce procédé d'authentification est utilisé principalement en Europe du Nord.
- **Analyse sécuritaire :**
  Cycle de vie : Pas d'information disponible.
  Protection de la communication : Non pertinent.
  Vérification de l'identité des parties impliquées dans la transaction : Par «défi réponse» pour l'utilisateur, pas d'information disponible pour le commerçant.
  Sécurité des composants : Dépend de la résistance des boîtiers aux intrusions.
  Protection des utilisateurs : Pas d'information disponible.

3.1.2. Boîtiers électroniques associés à une carte à puce

Diverses solutions reposent sur l'utilisation de boîtiers avec la carte de paiement.

a. Cyber-COMM

- **Principe :**
  La société Cyber-COMM a développé une application de paiement utilisant le lecteur de carte à puce, permettant l'authentification de la carte, ainsi que du porteur par la saisie du code confidentiel. Elle utilise les moyens de signature embarqués dans la carte à puce CB pour signer les transactions dans un environnement matériel sécurisé – le lecteur de carte - et non dans l'ordinateur personnel du consommateur. Cette application s'appuie sur le protocole international SET (Secure Electronic Transaction) dont une description est donnée en annexe 3. La combinaison du lecteur, de la carte à puce et du protocole SET permet d'assurer la non-répudiation des paiements et la garantie de paiement aux

commerçants. Cyber-COMM est une initiative des banques françaises auxquelles se sont associés quelques industriels.

D'autres applications sont envisageables : soit pour le paiement (par exemple l'utilisation du lecteur et de la carte bancaire à puce pour renforcer l'authentification de solutions de paiement moins sécurisées, telle que les Cartes Virtuelles Dynamiques), soit en dehors du paiement (l'authentification d'accès à des services bancaires, le rechargement des cartes Porte-Monnaie Electronique, etc...).

- **Déploiement des lecteurs Cyber-COMM :**

  20 000 lecteurs ont été distribués aux porteurs de cartes CB. 140 commerçants avaient signé avec 4 banques à mi-juillet 2001.

  Une description détaillée du dispositif de Cyber-COMM pour le paiement figure en annexe 4.

  Cependant, l'avenir du protocole de paiement SET étant incertain, la société Cyber-COMM procède actuellement à un repositionnement stratégique autour du lecteur pour d'autres applications que le paiement : notamment l'authentification d'accès pour les services de Banque à Domicile, et le rechargement des cartes Porte-Monnaie Electronique.

- **Analyse sécuritaire des lecteurs Cyber-COMM :**

  Cycle de vie : Evaluation des cartes bancaires mais pas des lecteurs.

  Protection de la communication : Basée sur le protocole SET.

  Vérification de l'identité des parties impliquées dans la transaction :

  Utilisateur : Authentification par carte à puce.

  Commerçant : Protocole SET.

  Sécurité des composants : L'hébergement du serveur est sécurisé, les opérations sont traçables au niveau du lecteur et du Serveur Acquéreur, la génération des secrets s'effectue dans une boîte noire.

  Protection des utilisateurs : Le lecteur est isolé pendant le dialogue avec la carte bancaire. L'affichage sur le lecteur est contrôlé. Les secrets sont stockés dans la carte à puce.

b. Téléphones portables bi-fentes

- **Principe :**

  Un utilisateur consulte un site marchand et décide de commander un produit. Le commerçant confirme la commande de l'utilisateur en envoyant un message SMS sur le téléphone portable de ce dernier. Celui-ci insère sa carte bancaire dans son téléphone portable et saisit son code confidentiel. La demande est alors envoyée à la banque par SMS. Cette solution assure la non-répudiation des paiements, d'où la garantie des paiements accordée au commerçant.

- **Déploiement :**

  Des projets basés sur le commerce électronique par les téléphones portables sont en cours. Ces projets utilisent des protocoles WLS (SSL pour WAP). En France, ce type de solution est actuellement développé par France Télécom (ItiAchat).

  La solution proposée par France Télécom Mobiles pour ce type de moyen de paiement est décrite en annexe 4.

- **Analyse sécuritaire : ItiAchat**

  Cycle de vie : Evaluation des cartes bancaires mais pas des téléphones.

  Protection de la communication : Dépend du protocole SMS utilisé, il n'y a pas confidentialité des données.

Vérification de l'identité des parties impliquées dans la transaction :

Utilisateur : Authentification par carte à puce.

Commerçant : Aucune.

Sécurité des composants : Le réseau GSM n'offre pas de garantie de disponibilité de service. C'est le SMS de confirmation qui sert de reçu à l'utilisateur.

Protection des utilisateurs : Les données de la carte bancaire ne sont pas transmises. L'affichage sur le portable n'est pas contrôlé.

c. Télévision à péage

- **Principe :**

  Un poste de télévision est muni d'un lecteur de carte à puces (fourni souvent conjointement à un décodeur pour avoir accès à des chaînes privées). L'utilisateur peut effectuer des achats (films, accès à des sites marchands particuliers, Internet) en insérant sa carte de paiement dans le lecteur.

- **Déploiement :**

  La solution proposée par Canal+ pour ce type de moyen de paiement est décrite en annexe 4.

  Canal + avec 14 millions d'abonnés en Europe est le 3ème groupe mondial de télévision à péage. Il existe actuellement 2 millions de décodeurs numériques acceptant la carte bancaire en France. Avec l'arrivée du numérique terrestre, 7 millions de décodeurs numériques acceptant les cartes de paiement à la norme EMV sont attendus en Europe pour 2004.

- **Analyse sécuritaire : Lecteur Canal +**

  Cycle de vie : Evaluation des cartes bancaires mais pas des décodeurs.

  Protection de la communication : Il n'y a pas confidentialité des données.

  Vérification de l'identité des parties impliquées dans la transaction :

  Utilisateur : Authentification par carte à puce.

  Commerçant : Pas d'information disponible.

  Sécurité des composants : Pas d'information disponible.

  Protection des utilisateurs : Les données de la carte bancaire ne sont pas transmises. L'affichage sur le lecteur n'est pas contrôlé.

d. Minitel

- **Principe :**

  Des minitels de type Magis peuvent être munis de lecteur de cartes à puce. Après avoir effectué sa commande sur Minitel, le client insère sa carte de paiement dans le lecteur et règle ses achats.

- **Déploiement :**

  Le Minitel rassemble 8000 éditeurs de service et génère un chiffre d'affaire de 12 milliards de francs.

- **Analyse sécuritaire : Minitel Magis**

  Cycle de vie : Evaluation des cartes bancaires mais pas du Minitel.

  Protection de la communication : Liaison de type X25.

  Vérification de l'identité des parties impliquées dans la transaction :

  Utilisateur : Authentification par carte à puce.

  Commerçant : Pas d'information disponible.

  Sécurité des composants : Pas d'information disponible.

Protection des utilisateurs : Les données de la carte bancaire ne sont pas transmises.

e. Porte-monnaie Electronique (PME)

- **Principe :**
  Le porteur est muni d'une carte à puce qu'il peut charger en monnaie électronique. Il insère sa carte dans le lecteur pour effectuer le paiement. A la différence de ce qui se passe pour les paiements de proximité, le commerçant est muni d'un lecteur comprenant une puce (SAM : Secure Access Module) ou d'un logiciel ayant les mêmes fonctionnalités.
  Le système fonctionne donc comme pour les paiements de proximité, la différence résidant dans la communication qui passe par Internet.
- **Déploiement :**
  Banksys a adapté la technologie Proton pour le paiement sur Internet mais son utilisation reste marginale.
- **Analyse sécuritaire :**
  Pas d'information disponible.

3.2. Les instruments à base d'un dispositif logiciel

3.2.1. Utilisation de l'image de la carte de paiement

a. Communication du numéro de carte de paiement en ligne

- **Principe :**
  La solution prédominante de paiement en ligne par carte de paiement s'appuie sur le protocole SSL (Secure Socket Layer) dont un descriptif est fourni en annexe 3. Lors du paiement, l'acheteur communique son numéro de carte de paiement ainsi que la date de validité de sa carte au commerçant via le protocole de communication SSL qui permet d'établir un canal sécurisé (confidentialité) pour la transmission des données. Le commerçant a ensuite la charge de gérer la transaction avec la banque.
  Une variante de cette solution technique, qui paraît préférable en termes de sécurité et de protection du client du point de vue de ses informations personnelles, est le passage par un intermédiaire. Ces intermédiaires ou «tiers de confiance» sont des hébergeurs qui assurent la gestion pour compte d'autrui des clés SSL et le stockage sécurisé des numéros de carte bancaire.
- **Déploiement :**
  De nombreux intermédiaires se sont développés. En France, les principaux sont repris dans le tableau suivant :

Nom	*Promoteur*	*Etat*
Cybermut	Crédit Mutuel	500 sites commerçants
Payline	Experian	400 sites commerçants
Télécommerce	France Télécom	300 sites commerçants

- **Analyse sécuritaire :**
  Cycle de vie : Pas d'information disponible.
  Protection de la communication : Majoritairement du SSL 128 bits. L'authentification des serveurs n'est pas toujours existante.
  Vérification de l'identité des parties impliquées dans la transaction :
  Utilisateur : Repose sur les informations de la carte.

Commerçant : Pas d'information disponible.

Sécurité des composants : Variable selon les plates-formes de paiement.

Protection des utilisateurs : Variable selon les plates-formes de paiement. Le client n'est pas protégé contre des attaques sur son poste de travail.

b. Cartes virtuelles

- **Principe :**

Pour régler un achat, l'internaute se voit attribuer par sa banque un numéro qui peut être à usage unique, dédié à un même commerçant, plafonné, ou à durée déterminée. Ce numéro est obtenu soit en se connectant au site de la banque, soit en utilisant un logiciel téléchargé sur son ordinateur personnel.

Cette solution ne peut être utilisée pour certains types de transaction : elle n'autorise pas les micro paiements car les paiements passent par les réseaux classiques de cartes de paiement dont les coûts de traitement sont élevés. De plus, elle ne garantit pas le paiement.

- **Déploiement :**

Un certain nombre de projets sont en cours de déploiement :

Nom	*Promoteur*	*Etat*	*Caractéristiques*
PCN (Pseudo Card Number)	Maestro	Lancement en 2001	Numéro de carte en clair ou chiffré par le protocole SET
e Carte Bleue	Carte Bleue	Disponible en France fin 2001. Banque pilote : Caisses d'Epargne	Technologie Orbiscom
Private Payments	American Express	Etats-Unis, serait disponible auprès des accepteurs d'Amex	Destiné aux utilisateurs BtoC d'Amex

La solution proposée par Carte Bleue pour ce type de moyen de paiement est décrite en annexe 4.

- **Analyse sécuritaire : Carte Bleue**

Cycle de vie : Pas d'information disponible.

Protection de la communication : SSL 128 bits. L'authentification des serveurs n'est pas toujours existante.

Vérification de l'identité des parties impliquées dans la transaction :

Utilisateur : Identifiant / mot de passe

Commerçant : Pas d'information disponible.

Sécurité des composants : Pas d'information disponible.

Protection des utilisateurs : Il n'y a pas de stockage sécurisé de données prévu pour l'utilisateur, si le numéro virtuel n'est pas à usage unique. Le client n'est pas protégé contre des attaques sur son poste de travail.

3.2.2. Porte-monnaie virtuel

- **Principe :**

  Les paiements de petit montant posent un problème spécifique, lié au rapport entre les montants unitaires et les coûts de traitement. Les systèmes de monnaie électronique offrent une solution adaptée.

  Des porte-monnaie virtuels (PMV) sont disponibles sur Internet. Ceux-ci prennent la forme de points de fidélité ou de cartes prépayées.

- **Déploiement :**

  De multiples initiatives apparaissent, mais peu atteignent un déploiement important.

Nom	*Promoteur*	*Etat*	*Caractéristiques*
Beenz	Beenz.com	Implanté dans plus de 15 pays, dont la France	Les Beenz sont des points de fidélité échangeables contre des biens et des services pré-déterminés.
Ecupocket	Réseau des Caisses d'Epargne	Pilote en France	Carte physique prépayée qui porte un numéro de 16 chiffres caché au dos, achetée auprès d'une agence Caisse d'Epargne, d'un montant maximal de 20 euros. Ce numéro, uniquement connu du porteur, sert à régler les achats sur le site marchand.
Odysseo	Blue Line International		Portefeuille virtuel composé d'une partie porte-cartes (l'internaute peut y référencer ses cartes de paiement) et d'une partie porte-monnaie (alimenté dans la devise de son choix, à partir de l'une des cartes référencées dans son portefeuille) pour effectuer des micro paiements. La solution utilise une PKI et introduit la signature électronique (3DES). Elle garantit la non-répudiation des achats.
Splash plastic	Consortium anglais	Royaume-Uni	Rechargeable dans 7400 Paypoints, utilisé pour acheter chez une centaine de commerçants en ligne (60 000 attendus fin 2001).
UK Smart	Smart Creds	Royaume-Uni	Carte prépayée vendue 20£ dans les bureaux de Poste.

- **Analyse sécuritaire :**

  Dépend des systèmes mis en place. Peu d'informations disponibles.

3.2.3. Les techniques de paiement PtoP (de personne à personne)

- **Principe :**

  Le paiement PtoP permet à chacun d'envoyer et de recevoir de l'argent par courrier électronique. L'internaute s'inscrit sur un site de «paiement par courrier» en fournissant un numéro de compte bancaire ou de carte de paiement. Il indique ensuite l'e-mail de la personne à qui il veut envoyer de l'argent (ami, parent, marchand,…) en précisant la somme voulue. Le correspondant reçoit un e-mail contenant un lien URL qui le guide

vers le site sécurisé où il ouvrira à son tour un compte en indiquant son compte bancaire habituel afin de percevoir l'argent. Ces solutions s'appuient majoritairement sur le protocole SSL lors des communications utilisateur – serveur.

- **Déploiement :**

  Cette solution rencontre un important succès aux Etats-Unis et au Royaume-Uni. 42 millions de paiements online PtoP ont eu lieu en 2000 aux Etats-Unis.

  Le tableau ci-dessous reprend les principales initiatives en matière de paiement PtoP aux Etats-Unis.

Nom	*Promoteur*	*Caractéristiques*
Billpoint	eBay.com et Wells Fargo	Développé initialement pour les utilisateurs d'eBay, autorise les paiements par cartes de paiement.
eMoneyMail	BankOne	Même système que Paypal. Il n'est pas nécessaire d'avoir un compte ouvert chez BankOne.
Paypal	Paypal	La politique de gestion du risque est basée sur la vérification des coordonnées bancaires des utilisateurs par des virements blancs effectués par Paypal sur leurs comptes bancaires.
Propay	Yahoo	Offre également la possibilité de payer ses factures en ligne.

  La solution MinutePay, proposée en France par BNP Paribas, est décrite en annexe 4.

- **Analyse sécuritaire : MinutePay**

  Cycle de vie : Un audit interne a été réalisé. Des tests d'intrusion sont prévus.

  Protection de la communication : SSL 128 bits, les mots de passe sont stockés chiffrés sur le serveur de base de données.

  Vérification de l'identité des parties impliquées dans la transaction : Mot de passe pour l'utilisateur. Le système peut s'adapter facilement à une infrastructure à clé publique.

  Sécurité des composants : Architecture bancaire classique, redondance, firewall…

  Protection des utilisateurs : Les coordonnées bancaires sont entrées une seule fois sur le site de MinutePay. Le produit prévoit quelques mesures de protection contre des attaques dirigées sur le poste de travail de l'utilisateur.

3.2.4. Systèmes avec intermédiaire

a. Séquestre

- **Principe :**

  i-Escrow est un système de règlement entre un client et un acheteur, fondé sur le principe de la mise en séquestre. Après commande d'un produit par l'acheteur, ce dernier envoie à i-Escrow les fonds, qui sont déposés sur un compte non rémunéré. Dès réception des fonds, i-Escrow autorise l'envoi de la marchandise à l'acheteur qui dispose d'un délai de rétractation de 15 jours. Au terme de ce délai, i-Escrow règle le vendeur.

- **Déploiement :**

  i-Escrow, filiale de Tradenable, est opérationnel aux Etats-Unis.

- **Analyse sécuritaire :**

  Pas d'information disponible.

b. Agrégateur

- **Principe :**

i-Pin permet à un internaute de régler les biens immatériels et les services qu'il aura consommés sur les sites Internet des commerçants ou prestataires par l'intermédiaire par exemple, de son fournisseur d'accès à Internet. i-Pin collecte le détail des opérations effectuées par chacun des utilisateurs et communique le total au fournisseur. i-Pin est crédité par le fournisseur d'accès puis il reverse les sommes reçus aux différents commerçants et prestataires.

- **Déploiement :**
  La technologie i-Pin est opérationnelle dans différents pays : aux Etat-Unis dont le promoteur est Wells Fargo, au Royaume Uni par British Telecom, en Israël par Internet Gold.
  Pour la France, on trouvera en annexe 4, une présentation détaillée du moyen de paiement w-HA qui utilise la technologie i-Pin.
- **Analyse sécuritaire : w-HA**
  Cycle de vie : Des tests d'intrusion et des audits par des organismes extérieurs sont prévus. Une maintenance de la sécurité est mise en place en lien avec i-Pin et France Télécom.
  Protection de la communication : SSL 128 bits. L'authentification des serveurs n'est pas toujours existante.
  Vérification de l'identité des parties impliquées dans la transaction : pour l'utilisateur un identifiant plus mot de passe ou série de mots de passe.
  Sécurité des composants : redondance du système, firewalls, sondes, OS durcis, hébergement sécurisé…
  Protection des utilisateurs : Le client n'est pas protégé contre des attaques sur son poste de travail. Des sauvegardes de la base de données de w-HA sont effectuées régulièrement.

3.3. La banque à domicile

- **Principe :**
  Les banques proposent des services par téléphone (fixe ou portable) permettant à leurs clients de consulter leurs comptes.
  Elles offrent également la possibilité de consulter des comptes en ligne (vidéotext, Internet, Banque par télévision), mais également d'effectuer des virements ou des achats boursiers. Dans une grande majorité des sites bancaires existants, la validité des transactions effectuées repose sur l'authentification de l'utilisateur par un simple mot de passe. Les liaisons entre le poste client et le serveur bancaire s'effectuent majoritairement par un protocole SSL.
- **Déploiement :**
  La plupart des banques offrent ce type de services à leurs clients : consultation de comptes, virements intrabancaires et interbancaires, ordres de bourse…
- **Analyse sécuritaire :**
  Cycle de vie : Pas d'information disponible.
  Protection de la communication : SSL 40 bits ou 128 bits majoritairement. L'authentification des serveurs n'est pas toujours existante.
  Vérification de l'identité des parties impliquées dans la transaction :
  Utilisateur : Identifiant / mot de passe.
  Banque : Dans les applications «banque en ligne», la protection globale des services offerts dépend du niveau de sécurité des deux entités communicantes, à savoir les systèmes informatiques de la banque et le poste de travail de

l’utilisateur. Les données sensibles, notamment les mots de passe, qui sont généralement stockées sur le poste de travail (dont le niveau de protection est insuffisant) ou qui circulent sur Internet, ne sont pas réellement protégées et donc sujettes à de nombreuses attaques (détournement de site, capture du mot de passe sur le réseau ou dans le poste de l’utilisateur, …).

Sécurité des composants : Infrastructures bancaires classiques, redondance, firewall…

Protection des utilisateurs : Des informations fonctionnelles sur le site peuvent être envoyées aux utilisateurs, mais elles ne comportent pas en général de conseil quant à la sécurité à adopter par les utilisateurs.

CHAPITRE 4 : LES RECOMMANDATIONS

L'état des lieux dressé au chapitre 3, conduit à formuler un certain nombre de recommandations qui visent à améliorer le niveau de sécurité actuellement offert par les différents moyens de paiement disponibles sur Internet.

4.1. Les recommandations concernant le cycle de vie

4.1.1. Un référentiel de sécurité

La vocation première d'un tel référentiel de sécurité serait de garantir, de façon publique, la conformité d'un moyen de paiement au regard d'un ensemble de critères élaborés et reconnus par la communauté concernée (par exemple au niveau du CFONB) et approuvés par la Banque de France dans le cadre de ses missions de surveillance de la sécurité des instruments de paiement. Afin d'en faciliter la conception et la validation, il serait nécessaire de définir un référentiel de sécurité spécifique à chaque moyen de paiement. Il convient cependant de tenir compte de la nature et de l'utilisation envisagée du moyen de paiement dans la définition de ce référentiel de sécurité et de faire en sorte qu'il ne constitue pas un frein à l'innovation et au développement de nouveaux services.

Ce référentiel pourrait prendre différentes formes. La rédaction d'un «profil de protection» au sens des Critères Communs[3], fondé sur l'analyse des menaces qui peuvent porter atteinte aux utilisateurs et au service pourrait être retenu. Conçu pour être reconnu au niveau international, le profil de protection revêt un caractère souple et s'adapte aux différentes technologies utilisées. Il est également possible de se référer à d'autres normes particulières telles que ITSEC, BS 7799, GMITS ou encore à des processus spécifiques.

4.1.2. L'expression des besoins de sécurité

Une démarche consistant à prendre en compte systématiquement la sécurité dès les premières phases de la conception d'un moyen de paiement est souhaitable. Le résultat d'une telle démarche pourrait prendre la forme d'une expression des besoins de sécurité contenant les éléments suivants :

- *la politique de sécurité* : il s'agit d'exposer les motivations de la politique de sécurité à partir de la stratégie de l'entreprise et des textes réglementaires applicables (conformité à un éventuel référentiel) et d'en identifier les contours de façon sommaire :
  - quels sont les actifs, autrement dit les données, qui doivent être protégées ?
  - pourquoi (confidentialité, intégrité, disponibilité, etc.) ?
  - contre quoi (acteurs malveillants, incidents de fonctionnement, etc.) ?
  - sur quel périmètre ?
  - comment ?
- *la modélisation du moyen de paiement* ou encore du système d'information sous-jacent : la complexité croissante de ces systèmes, la multiplicité des intervenants justifient que la nature des flux d'information entre les acteurs du système soit étudiée et les rôles (responsabilités) des uns et des autres clarifiés ;

[3] Il s'agit de la norme ISO 15408 (Critères d'évaluation pour la sécurité des technologies de l'information). Cette norme définit de façon standardisée, d'une part, des exigences fonctionnelles de sécurité visant des produits ou des systèmes utilisant les technologies de l'information et d'autres part des exigences d'assurance de sécurité, ie les moyens que l'on se donne pour vérifier la conformité de ces produits ou systèmes aux exigences fonctionnelles de sécurité. Les Critères Communs fournissent également un outil appelé «Profil de Protection» permettant aux utilisateurs de préciser de façon générique leurs exigences de sécurité relatives à une famille de produits ou de systèmes.

- *l'analyse des risques* : il s'agit d'évaluer le degré de gravité des conséquences possibles d'attaques du système d'information visant les actifs identifiés dans la politique de sécurité ; l'objectif étant ensuite de restreindre l'analyse aux scénarios d'attaque qui peuvent emporter des conséquences dites «insurmontables» pour l'entreprise ou contraires à la réglementation en vigueur ;
- *la liste des scénarios d'attaque* (ou des menaces) : les menaces associées aux scénarios identifiés dans l'analyse de risques sont énumérées, avec pour chacune une indication des facteurs qui peuvent concourir à augmenter la probabilité de leur réalisation ou aggraver leurs conséquences ;
- *les objectifs de sécurité* : pour chaque menace identifiée, des objectifs de sécurité sont proposés afin de prévenir la réalisation de la menace, en détecter la réalisation, en dépit des mesures de prévention, et en limiter les conséquences ;
- *l'architecture technique* retenue qui doit :
  - identifier les composants du système affectés par les différents objectifs de sécurité,
  - proposer au niveau de ces différents composants des mesures sécuritaires susceptibles de remplir les objectifs annoncés,
  - faire une étude des risques résiduels (non couverts par ces mesures).

4.1.3. La validation de la sécurité

Il revient à l'émetteur de s'assurer que le moyen de paiement satisfait aux exigences définies dans le référentiel de sécurité applicable.

La vérification de la conformité d'un moyen de paiement doit être conduite par un organisme indépendant, aux compétences reconnues et suivant une méthodologie adaptée et reconnue. Comme pour le référentiel de sécurité, le processus de validation choisi doit tenir compte de la nature et de l'utilisation envisagée du moyen de paiement (montant moyen, risques encourus…) dans la définition de ce référentiel de sécurité et faire en sorte qu'il ne constitue pas un frein à l'innovation et au développement de nouveaux services.

En outre, une politique active de coopération au niveau européen et international doit être engagée pour réduire les risques de distorsion de concurrence liés à des opérateurs de paiement non localisés sur le territoire français.

Les investigations de sécurité peuvent être notamment conduites en utilisant la méthodologie définie dans les Critères Communs. Les organisations mises en place (souvent appelées schéma d'évaluation et de certification de la sécurité des technologies de l'information) pour l'application de ces critères apportent l'assurance que les travaux de vérification sont effectués par des experts indépendants, spécialisés en sécurité des technologies de l'information et dont la compétence technique est régulièrement vérifiée. Les méthodes d'évaluation système sont encore en cours d'amélioration. Quelques certificats systèmes ont d'ores et déjà été publiés par le schéma français d'évaluation et de certification.

4.1.4. La maintenance de la sécurité

Étant donné l'évolution de la technologie et des modes de mise en œuvre des menaces, la vérification de la sécurité ne doit pas se limiter à la seule validation initiale. Il apparaît nécessaire d'assurer un suivi du niveau de sécurité réellement offert par le moyen de paiement.

Ce suivi doit permettre une bonne traçabilité de toutes les modifications effectuées et de l'évolution du moyen de paiement. En outre, la maintenance ne doit pas être que réactive : elle doit être planifiée et comporter un volet préventif suffisant pour permettre au moyen de paiement de s'adapter à l'évolution des technologies, qui est en grande partie prévisible, et à l'évolution des menaces moins prévisible.

Le schéma français d'évaluation et de certification de la sécurité des technologies de l'information propose de tels programmes de maintenance de la sécurité.

4.1.5. Une labellisation

La création d'un **label de sécurité** visible par l'utilisateur répondrait à l'objectif d'offrir une assurance complémentaire, tout en constituant un argument commercial pour les émetteurs qui l'adopteraient. Ce label pourrait être défini au sein des organisations professionnelles. Des réflexions supplémentaires devraient être menées afin de permettre une graduation des labels, qui selon les diverses exigences de sécurité couvertes et les usages, peuvent être par nature différents.

4.2. Les recommandations concernant le fonctionnement du dispositif

Les recommandations propres aux caractéristiques opérationnelles concernant le fonctionnement du dispositif, développées au chapitre 2, sont présentées selon les quatre mêmes axes :

- protection de la communication,
- vérification de l'identité des parties impliquées dans la transaction,
- sécurité des composants utilisés,
- protection des utilisateurs.

4.2.1. La protection de la communication

La protection de la communication (intégrité et confidentialité) est souvent assurée par l'utilisation du protocole SSL. Le niveau d'intégrité et de confidentialité ainsi obtenu est satisfaisant à condition d'utiliser la version SSL 128 bits avec authentification mutuelle des serveurs en charge de la communication.

La prévention du rejeu d'une transaction est aussi une propriété fondamentale que tout moyen de paiement doit satisfaire. Des clés cryptographiques dynamiques, des numéros de transactions et de l'horodatage peuvent être utilisés pour garantir que les messages rejoués seront rejetés.

4.2.2. La vérification de l'identité des parties impliquées dans la transaction

Un constat s'impose pour la grande majorité des nouveaux moyens de paiement électroniques : lorsqu'elle existe, la vérification de l'identité des parties impliquées dans une transaction électronique se fait par le biais d'un (ou d'une série de) mot(s) de passe. Cependant, l'utilisation de mots de passe est un mécanisme qui laisse place à un risque de fraude important, même si l'ampleur de cette fraude n'a pas été mesurée. De plus, dans la plupart des cas, seul l'utilisateur s'authentifie vis-à-vis du serveur.

L'authentification des parties impliquées dans la transaction doit être mutuelle. Pour assurer une bonne authentification, la technique du «défi réponse» qui évite la transmission des éléments d'authentification sur le réseau est fortement recommandée. Cette procédure utilise une cryptographie symétrique ou asymétrique.

Cependant, les marchés de masse, qui touchent de nombreux clients, peuvent représenter une situation particulière vis-à-vis de cette recommandation. Une authentification moins forte que dans d'autres moyens de paiement peut être tolérée.

Pour les solutions à base d'une cryptographie asymétrique, la mise en place d'une infrastructure à clé publique (PKI : Public Key Infrastructure) est souhaitable afin de permettre une authentification forte mais également d'assurer la non-répudiation de la commande, du paiement ou éventuellement de la livraison. En effet, dans une telle infrastructure, dont une description est donnée en annexe 3, chaque participant possède un certificat et acquiert ainsi la possibilité de signer la transaction électronique.
La mise en œuvre d'une infrastructure à clé publique repose sur deux types d'entités :

- une autorité d'enregistrement : elle effectue la vérification d'un certain nombre d'informations concernant la personne morale ou physique demandant l'octroi d'un certificat, notamment son identité, et envoie ces informations à l'autorité de certification ;
- une autorité de certification : elle définit la politique de certification, conserve la clé secrète servant à signer les certificats et assure ou sous-traite la gestion des certificats (fabrication à partir du message envoyé par l'autorité d'enregistrement, publication, révocation, …) .

Le développement de la signature électronique est limité par les investissements nécessaires à la création de l'infrastructure à clé publique et tout particulièrement par ceux relatifs à l'autorité d'enregistrement. Une autorité d'enregistrement de référence ou «racine» devrait être mise en place afin de vérifier l'identité de chaque personne physique ou morale pour la création d'un certificat d'identité. **Cette autorité d'enregistrement, qui correspond essentiellement à une mission publique, devrait être assurée par l'État**. Il s'agirait donc, en quelque sorte, de fournir à chaque personne physique ou morale une identité électronique simple, sans droits attachés, un « état-civil électronique ». Sur la base d'une telle structure, de nombreuses applications pourraient voir le jour notamment dans le domaine des moyens de paiement où la vérification de l'identité des parties impliquées est une nécessité. Les certificats initiaux pourraient ainsi être complétés en fonction des applications développées et tout en permettant la mise en place de structures d'enregistrement allégées pour les banques. Par ailleurs, cette autorité d'enregistrement «racine» permettrait d'obtenir une certaine homogénéité dans la distribution des certificats et ainsi faciliterait l'interopérabilité entre les différentes autorités de certification.

4.2.3. La sécurité des composants

L'état des lieux révèle la difficulté d'obtenir des informations concernant la sécurité des composants.

Cependant, afin de satisfaire les objectifs de sécurité liés à ce domaine, il est apparu nécessaire de mettre en place un nombre important de mesures de sécurité qui ne peuvent pas toutes être décrites dans ce document. Les principales mesures sont présentées ci-après :

- *confinement* : un sous-réseau (souvent appelé «zone démilitarisée») doit être intercalé entre l'extérieur (Internet) et le réseau interne à protéger. La communication entre cette zone

démilitarisée et le système d'information est contrôlée par des dispositifs de sécurité (firewalls …). L'administration du système d'information doit être effectuée localement ou à distance par un accès dédié à partir du réseau protégé et suivant des plages de temps déterminées.

- *contrôle d'accès* : il est vital pour une exploitation sûre du système d'information que l'accès aux locaux, serveurs et données soit contrôlé. Seuls les administrateurs du système d'information doivent avoir accès aux différents serveurs le constituant. Les règles de gestion des mots de passe (péremption, complexité, renouvellement, …) doivent être définies.
- *sécurité des serveurs* : les serveurs constituant le système d'information doivent utiliser des versions de systèmes d'exploitation durcies. Seuls les services du système d'exploitation nécessaire au bon fonctionnement des applications de paiement doivent être installés. En particulier, tous les services réseau non utilisés doivent être supprimés. Il est aussi recommandé d'installer des programmes pour vérifier périodiquement l'intégrité des logiciels installés, pour détecter des attaques virales et pour analyser automatiquement les enregistrements d'audit.
- *sûreté du système d'information* : les services de commerce électronique doivent être en général disponibles 24 heures sur 24 heures. Il faut prendre en considération des défaillances technologiques ou des sabotages mais aussi les attaques venant d'Internet dont l'objectif est de bloquer l'accès au serveur. Il est possible de se protéger contre ce type de problèmes en installant des systèmes redondants.
- *boîtiers de sécurité* : comme le système d'information sera amené à manipuler des clés cryptographiques pour effectuer les opérations nécessitant ce type de technologie, il est recommandé d'équiper les serveurs de dispositifs matériels indépendants en charge des opérations cryptographiques. Cela procure un bon niveau de protection contre des attaques internes mais aussi contre les pirates informatiques.
- *veille sécurité* : la sécurité d'un système d'information peut subir des dégradations du fait de la découverte de failles de sécurité par des utilisateurs internes ou externes. La diffusion des alertes de sécurité et les procédures pour mettre en place les parades doivent être clairement définies. Cette veille doit être assurée de façon durable et tenir compte de la durée de service.
- *audit* : l'enregistrement de l'état ou de l'activité des différents serveurs dans des traces est le principal moyen de couvrir les objectifs de traçabilité de l'activité et d'imputabilité des actions. Les traces doivent être analysées régulièrement pour détecter toute tentative d'attaque.
- *personnel* : le personnel en contact direct avec le système d'information doit satisfaire à de forts critères de probité et de compétences (ces personnels doivent se tenir informés des derniers développements en matière de sécurité).

4.2.4. La protection des utilisateurs

La protection des utilisateurs est dans l'ensemble peu prise en compte.

Il est donc important que les solutions proposées par les fournisseurs de moyens de paiement satisfassent les mesures suivantes :

- *pertinence du produit* : pour les produits logiciels, il est probable que l'utilisateur devra observer un nombre important de procédures de sécurité (installation, configuration…). Si la solution prévoit un dispositif matériel, les informations sensibles (clés cryptographiques,

valeur électronique pour la monnaie électronique…) peuvent y être stockées afin d'en assurer une bonne protection ;

- *qualité du produit* : le niveau de sécurité du produit fourni doit être vérifié par un organisme indépendant. Il est souhaitable que le niveau de qualité du produit soit visible par l'utilisateur (voir section sur l labellisation) qui aura ainsi l'assurance que le produit a un niveau de sécurité suffisant et qu'il a été correctement testé ;
- *ergonomie du produit* : les moyens de paiement électroniques doivent présenter une interface ergonomique pour l'utilisateur.

De plus, le consommateur doit être informé :

- des règles d'utilisation qui sont nécessaires à la protection des transactions de paiement et qui engagent la responsabilité du consommateur dans l'utilisation du moyen de paiement dont il dispose ; en cas de doute sur ces règles, il doit avoir la possibilité de contacter le fournisseur pour avoir les éclaircissements nécessaires . Parmi ces règles devront sans doute figurer au minimum :
  - conformité aux recommandations de sécurité : l'utilisateur doit utiliser le moyen de paiement dans les conditions de sécurité définies par le fournisseur ;
  - sauvegarde des données : l'utilisateur doit faire des sauvegardes régulières au minimum des données financières ;
  - stockage des clés d'accès au service : les mots de passe, les codes confidentiels ou encore les cartes à puce doivent être conservés de manière sûre. Lorsqu'il s'agit de biens immatériels, il faut éviter de les conserver sur son poste dans la mesure du possible.

  Ces règles doivent être claires, simples et raisonnables (proportionnées au risque et à l'assurance sur le risque), de manière que l'utilisateur ne soit pas dissuadé de les suivre en pratique (ce qui aurait pour effet de les invalider).
- des recommandations nécessaires à l'installation et au fonctionnement du moyen de paiement mis à sa disposition. A titre d'exemple, des recommandations sur une utilisation sûre d'un navigateur ou sur les risques de télécharger des programmes à partir d'Internet ou d'utiliser des contrôles ActiveX peuvent être fournies. Enfin, l'utilisateur doit être informé des risques associés à l'usage des codes confidentiels ou des clés cryptographiques ;
- des précautions et des conseils permettant d'améliorer la sécurité, par exemple, protéger son poste contre des attaques virales, ne pas charger de programmes d'origine inconnue ou de type suspect sans s'assurer de son origine, etc.

ANNEXE 1 : LE SOUS-GROUPE

Jean-Luc BARÇON-MAURIN	MINEFI - DGCCRF
Denis BEAU, animateur	Banque de France
Patrick de CANECAUDE	Ministère de la Justice
Gaëtan DALIGAULT	Cyber-Comm
Nadia DOMEC	Canal +
Jean-François DUCHER	BNP Paribas
Bernard DUTREUIL	BNP Paribas
Elisabeth GARREAU	France Télécom Mobile
Jean-Christophe HAMMOND	w-HA
Cécile JANICOT	Banque de France
Michèle JAVEL	MINEFI - DECAS
Benoît JOLIVET	CNCT
Gilles KREMER	Magicaxess
Martin LAFON	Magicaxess
Carlos MARTIN, rapporteur	Banque de France
Jacques PANTIN	Certplus
Laurent PERDIOLAT	MINEFI – DIGITIP
Guillaume POUPARD	DCSSI
Cédric SARAZIN	GIE des Cartes Bancaires
Marc SIRVEN	DCSSI
Jacques SCHUHMACHER	CNCE
Frédéric TATOUT	MINEFI - DIGITIP
Frédéric TOUMELIN	Carte Bleue

ANNEXE 2 : LES MENACES ASSOCIEES AU COMMERCE ELECTRONIQUE

Le commerce électronique doit faire face à un certain nombre de menaces qui portent sur les applications ou qui sont de nature purement technique.

2.1. Les menaces au niveau des applications

Ces menaces se divisent en deux grandes catégories : celles qui visent le canal de communication et celles qui visent le poste client ou le serveur.

2.1.1. Sur le canal de communication

- perte de confidentialité des données transmises (mot de passe, données liées à la transaction…),
- perte d'intégrité des données transmises (dysfonctionnement du système ou malveillance),
- perte de disponibilité (dysfonctionnement du système ou manipulation),
- rejeu des données d'une vieille transaction,
- répudiation du paiement ou de la commande,
- usurpation d'identité,
- clonage de site Internet : l'internaute est ainsi détourné vers un site qu'il croît être la plate-forme du moyen de paiement qu'il désire utiliser. Ses informations confidentielles (telles que son mot de passe) peuvent ainsi être récupérées et utilisées à des fins frauduleuses.

2.1.2. Sur le poste de travail (client ou serveur)

- attaques de l'extérieur : ces attaques peuvent être basées sur l'utilisation des failles de sécurité publiées dans les forums de discussion sur Internet pour prendre le contrôle de la machine,
- attaques internes : elles peuvent être un accès illicite au serveur, dans le contexte familial, ou une utilisation illicite des droits associés à un individu, …
- sabotage (type déni de service),
- dysfonctionnement du système : au niveau des logiciels (bug) mais aussi au niveau des données stockées dans des moyens informatiques (les clés cryptographiques),
- virus,
- chargement de logiciel non contrôlé à partir d'Internet (Contrôle ActiveX ou Applets Java).

2.2. Les menaces techniques

Ces menaces sont relatives principalement aux composants techniques employés, à la communication, à la transaction de paiement, et à la cryptographie.

2.2.1. Relatives aux composants techniques

- perte de confidentialité du code source,
- modification des composants logiciels,
- faille de sécurité dans le logiciel ou le matériel,
- dysfonctionnement d'un composant,
- perte de données enregistrées,
- modification des données enregistrées,

- incohérence des données enregistrées,
- vol d'un composant,
- perte d'information lorsqu'un moyen de stockage est saturé,
- duplication des unités monétaires,
- déni de service,
- mauvaise séparation des utilisateurs.

2.2.2. Relatives à la communication

- rejeu des messages,
- ecoute des communications,
- usurpation des identités,
- modification non autorisée des messages,
- erreur de transmission,
- répudiation du message,
- détournement des messages,
- utilisation non autorisée des accès dédiés à la maintenance,
- incohérences dues à une mauvaise exécution de la transaction.

2.2.3. Relatives à la transaction de paiement

- transaction illicite,
- création de profils utilisateur,
- blanchiment,
- insolvabilité.

2.2.4. Relatives à la cryptographie

- découverte des clés cryptographiques,
- utilisation d'une méthode de chiffrement non sûre,
- utilisation d'une fonction de hachage non sûre,
- générateur de nombre aléatoire déficient,
- utilisation des clés cryptographiques de test après la mise en service du système,
- génération et gestion non sûre des clés cryptographiques,
- clés cryptographiques faibles,
- perte des clés enregistrées.

2.2.5. Divers

- contrôle inadapté des mesures de sécurité des technologies de l'information,
- accès non-autorisé de personne aux locaux soumis à protection,
- exercice illicite des droits,
- plan inadapté des urgences.

ANNEXE 3 : LA DESCRIPTION DE DIFFERENTS PROTOCOLES SUR INTERNET

Cette annexe présente le principe de la cryptographie à clés publiques et également différents protocoles utilisés sur Internet comme SSL et SET.

3.1. Les infrastructures à clé publique

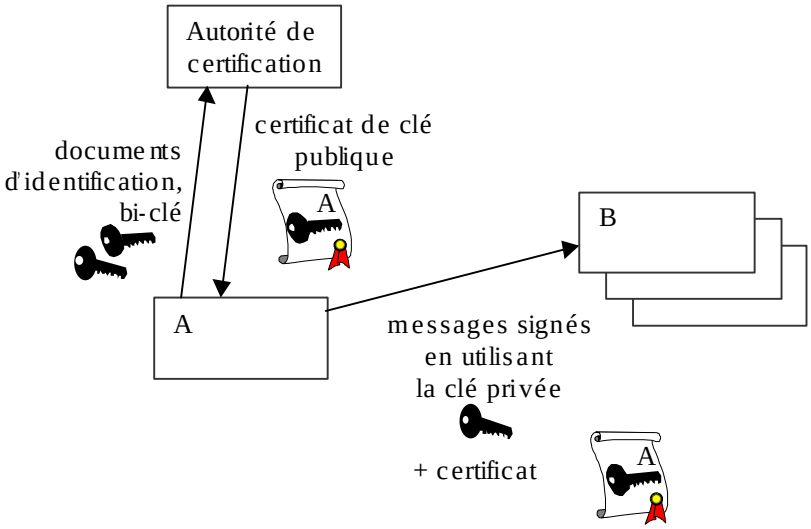
3.1.1. Le principe

On génère pour chaque internaute (personne physique ou morale) un couple de clés indissociables :

- La première clé est un **secret** qui est seulement connu de l'internaute,
- La seconde clé, au contraire, est une donnée **publique** qui peut être diffusée à tous ses interlocuteurs[4].

Ce couple de clés ou **bi-clé** est conçu de telle sorte qu'un message crypté en utilisant l'une des clés **peut être décrypté en utilisant l'autre, et seulement l'autre**.

Exemple d'utilisation, pour remplir le besoin d'identification :



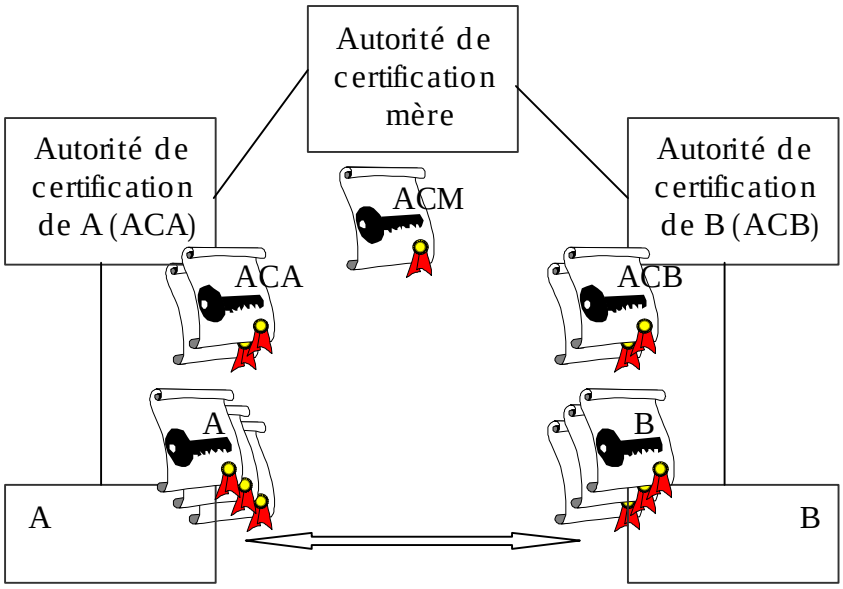
Pour s'identifier lors de l'envoi d'un message, un internaute A va crypter ce message en utilisant sa clé privée ; tout détenteur B de la clé publique de A saura décrypter le message envoyé par A et le lui attribuer. Il y a une condition à cela **: que B puisse faire le lien de façon sûre entre la clé publique de A et l'identité de A**. C'est le rôle d'une **tierce partie de confiance** que d'apporter cette assurance à B en délivrant un **certificat établissant le lien entre la clé publique de A et son identité** : on parle **d'autorité de certification pour qualifier ce service rendu à la communauté des internautes.**

3.1.2. Chaîne de confiance et interopérabilité

Pour éviter que des fraudeurs fabriquent de faux certificats de clés publiques, les certificats de clés publiques émis par l'autorité de certification sont signés à leur tour par celle-ci avec sa clé

[4] L'algorithme de génération des clés est tel que bien sûr il est impossible de retrouver la clé privée à partir de la clé publique correspondante.

privée. Le destinataire peut donc vérifier le certificat qu'il reçoit en utilisant la clé publique de l'autorité de certification, laquelle est diffusée par tous moyens utiles (publication officielle, etc.). Dès lors que deux internautes certifiés par deux autorités de certification différentes chercheront à communiquer de façon sûre, se pose la question de la reconnaissance mutuelle de leurs certificats de clés publiques.
On pourrait imaginer que les autorités de certification passent entre elles des accords bilatéraux de reconnaissance mutuelle ; mais la complexité exponentielle d'un tel système serait ingérable. On voit en fait apparaître des architectures arborescentes d'autorités de certification au niveau mondial avec des autorités mères (ex. GTA) et des autorités filles qui évitent la conclusion d'un grand nombre d'accords bilatéraux entre les autorités de certification locales.



3.1.3. La politique de certification

La politique de certification est l'ensemble des procédures et règles de sécurité appliquées par une autorité de certification (ou exigées de ses prestataires) pour une catégorie donnée de certificats.
En effet, on peut avoir des politiques différentes pour des certificats destinés à des transactions de nature différente : les exigences sécuritaires au niveau de la fabrication et la délivrance des certificats seront renforcées pour des échanges d'informations sensibles ou des transactions de gros montant.

3.1.4. Les métiers de la certification

Les métiers de la certification se segmentent autour de trois grandes composantes :

- **l'autorité d'enregistrement** : Elle effectue la vérification d'un certain nombre d'informations concernant la personne demandant l'octroi d'un certificat de clé publique, notamment son identité, et adresse un message normalisé à l'opérateur de certification "encapsulant" ces informations,
- **l'opérateur de certification** : il fabrique le certificat de clé publique à partir du message envoyé par l'autorité d'enregistrement, le signe, en assure la publication, gère sa révocation éventuelle,

- **l'autorité de certification** : c'est le donneur d'ordre des prestataires précédents, qui assume la responsabilité finale vis-à-vis des tiers ; il définit la politique de certification, gère éventuellement la marque associée à son activité, les problèmes d'interopérabilité, conserve la clé secrète servant à signer les certificats, etc.

Suivant les cas, certains des trois métiers peuvent être exercés par la même entité.

3.1.5. La signature électronique en France

Pour être conforme à la réglementation en vigueur sur la signature électronique, une solution technique envisageable pour signer électroniquement est l'utilisation d'une infrastructure à clé publique telle que décrite précédemment.

a. Une évolution juridique notable

Les techniques de signature électronique sont pratiquées depuis une décennie dans plusieurs domaines, par exemple au sein de certaines grandes entreprises ou entre elles, dans le système de paiement par carte bancaire, et dans le cadre de la procédure de télé-déclaration de TVA, par 17 000 grandes entreprises. Cette pratique s'appuyait sur des conventions de preuve ou des règlements privés. Sur le plan juridique, l'article 1341 du code civil consacrait en effet la prééminence de la preuve écrite sauf pour les transactions entre commerçants et celles n'excédant pas 5000 F ou sauf convention privée expresse.

La loi du 13 mars 2000 modifie cet article en consacrant la force probante de la signature sous forme électronique et la possibilité pour celle-ci d'avoir la même force que la signature manuscrite sur du papier, ainsi que l'acte authentique électronique (un décret spécifique est en cours de préparation). Le décret d'application du 30 mars 2001 fixe les conditions par lesquelles un procédé de signature électronique possède cette force probante et est présumé fiable jusqu'à preuve du contraire.

Ces nouveaux instruments adaptent au droit national la Directive 1999/93/CE du 13 décembre 1999, en reprenant ses exigences sur la signature électronique pour qu'elle ait même force vis à vis d'un document électronique qu'une signature manuscrite sur un texte sur papier, directive qui offre également un cadre à la reconnaissance juridique de la signature électronique entre les membres de la Communauté européenne.

La loi du 13 mars 2000 et le décret du 30 mars 2001 permettent donc de se passer de convention de preuve et de simplifier le règlement des litiges, donnant ainsi un cadre juridique propice à ce que l'usage de la signature électronique se développe largement dans un réseau ouvert tel qu'Internet dans toute l'Europe. Le cadre juridique institué va de pair avec la libéralisation totale de l'usage des moyens de cryptographie, et l'encadrement juridique du commerce électronique, qui sont en cours de préparation dans le cadre de la future Loi sur la Société de l'Information.

b. Les prochaines étapes en France

Le décret du 30 mars 2001 précise l'organisation d'un schéma national de qualification volontaire des prestataires de services de certification électronique. Ce schéma sera appliqué à deux niveaux :

- la certification du système technique du prestataire par un CESTI, selon une procédure animée par la DCSSI (les normes utilisées seront précisées dans un arrêté) ;
- la certification du prestataire résultant d'un audit sur des critères d'organisation et de qualité, selon un schéma défini par le Ministre de l'Industrie (un arrêté précisera le centre d'accréditation, les normes utilisées et certaines modalités).

La qualification dans le cadre du schéma national vaudra présomption de conformité aux exigences techniques du décret, ce qui constitue une incitation à l'obtenir.

Le contrôle des prestataires sera effectué suivant une procédure en cours de définition par les services du Premier Ministre (DCSSI).

c. Les apports du nouveau cadre juridique, les usages et le marché de la signature électronique

Ainsi, la télé-déclaration sera élargie par Internet aux entreprises de plus de 100 MF de chiffre d'affaire. La carte professionnelle de santé, diffusée à 1,5 millions d'exemplaires, permettra probablement la signature électronique en réseau ouvert. La procédure de référencement des produits et des prestataires associés à ces services s'intégrera progressivement dans le schéma de certification national.
Le système de paiement par carte bancaire connaîtra probablement une évolution semblable, peut-être dans le cadre de sa migration vers le standard EMV.

Une dizaine de prestataires de services liés à la signature électronique existent ou sont en formation.
Les certificats d'un niveau inférieur à celui exprimé par le décret seront d'un coût très faible et pourront être utilisés pour des transferts de biens ou de messages de petite importance. Les certificats d'un niveau plus élevé sont actuellement en général chers (de l'ordre 2000 F par an).

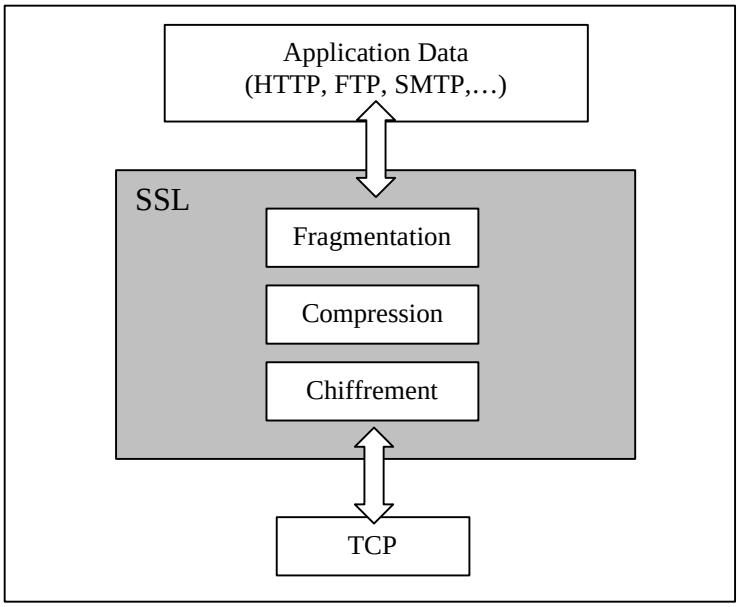
Le marché de la signature électronique sera donc probablement ouvert par les applications B to B et de l'état vers les entreprises. Les applications citoyennes qui se généraliseront dans le cadre du Programme d'Action Gouvernemental pour la Société de l'Information contribueront au décollage du marché vers le grand public en faisant baisser les prix du marché.

3.2. Le protocole SSL

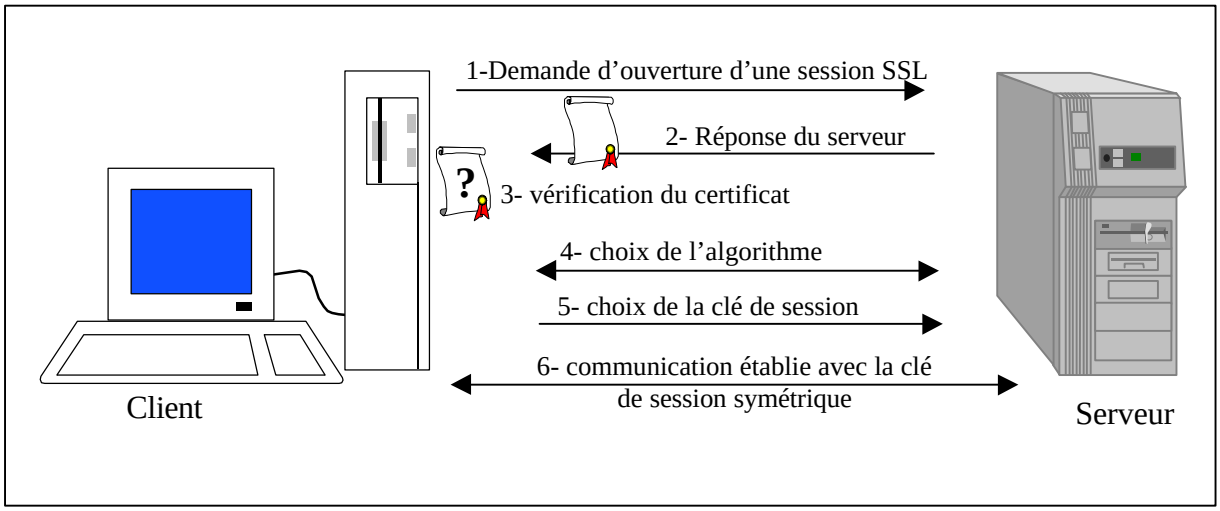
Développé par la société Netscape, le protocole SSL (Secure Socket Layer) a été accepté de manière universelle sur le Web pour assurer la confidentialité et l'intégrité des messages échangés entre ordinateurs. Dans ses versions les plus récentes, SSL permet également l'authentification mutuelle des clients.

Ce protocole se situe entre la couche transport (TCP) et les protocoles de la couche application (HTTP, SMTP, FTP…). Il combine cryptographie à clé publique et symétrique.
SSL est composé de 2 niveaux :

- SSL record layer protocol permet l'encapsulation des protocoles de plus haut niveau au-dessus du protocole de transport (fragmentation + compression + chiffrement),



- Un niveau supérieur permet notamment l'authentification des intervenants, la négociation des paramètres de chiffrement.

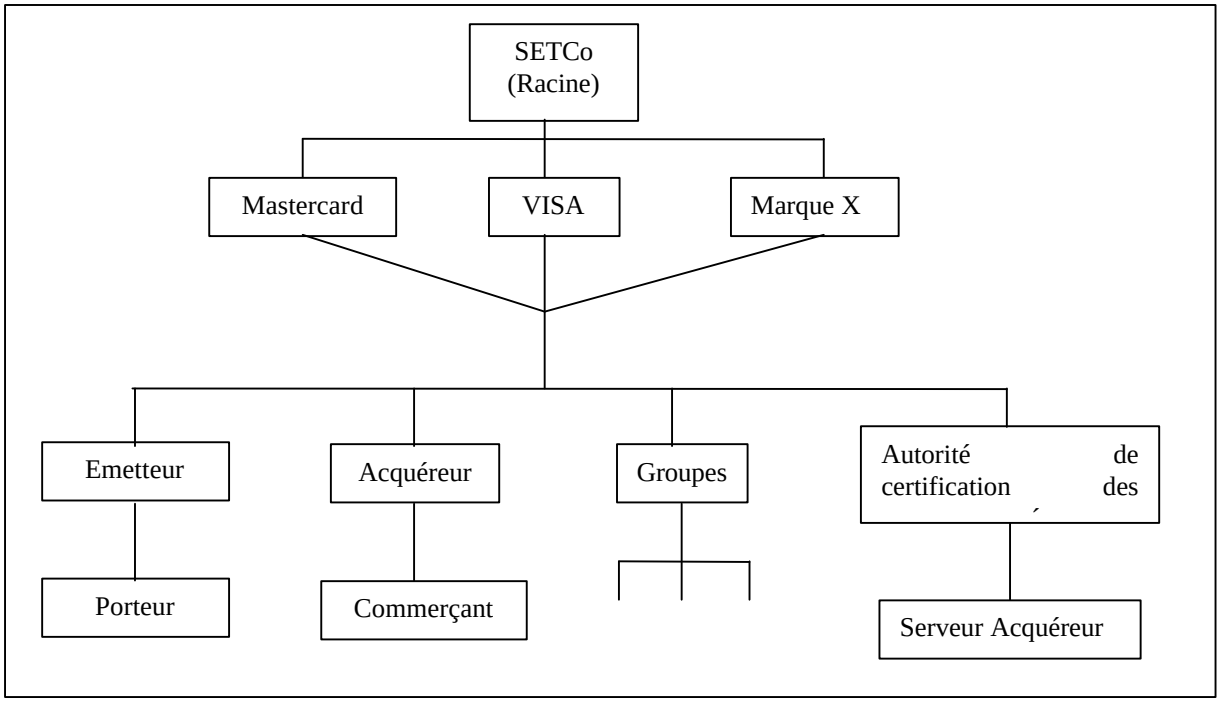


Cependant, SSL n'est pas accompagné d'une organisation de distribution des clés et des certificats. Le client n'a aucune raison de faire a priori confiance à la clé publique du serveur et inversement.
Même s'il est mis en œuvre avec tiers certificateur, SSL ne garantit pas, lorsqu'il est utilisé dans le cadre d'un moyen de paiement, le commerçant contre le risque de répudiation du paiement par le client. Enfin, des informations sensibles (clés, certificats…) sont gérées dans l'ordinateur personnel du client, environnement perméable aux virus et chevaux de Troie. De même, le protocole n'assure pas la confidentialité des données stockées chez le commerçant.

3.3. Le protocole SET

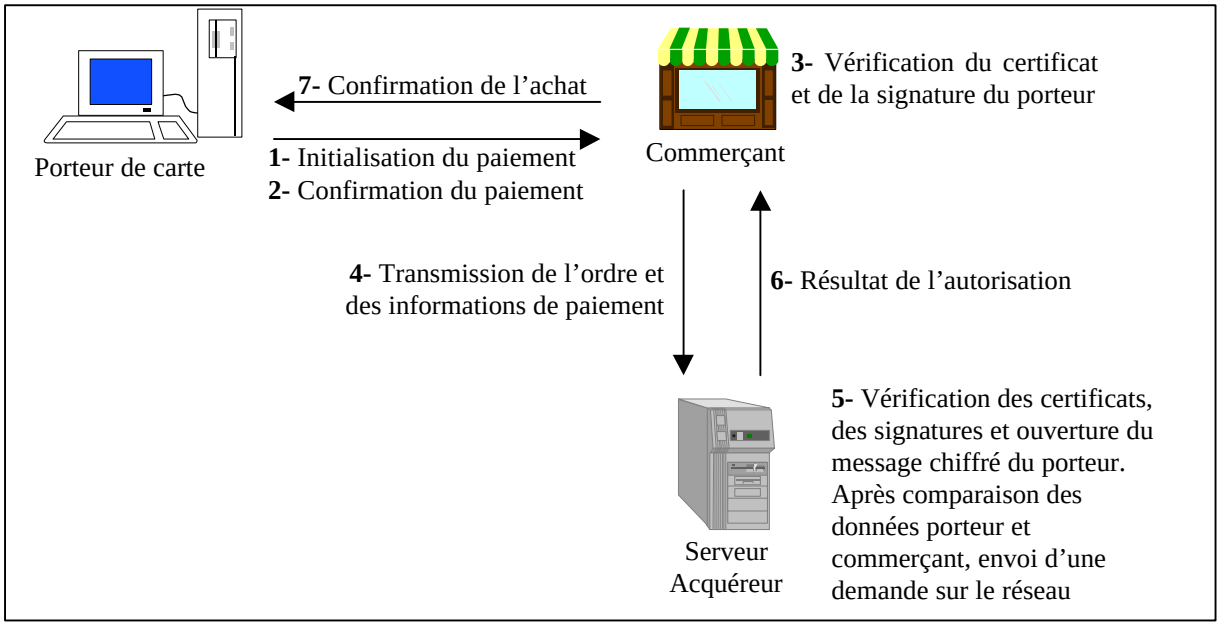
Développé sur l'initiative de Visa et Mastercard, SET (Secure Electronic Transaction) est un protocole de sécurité au niveau applicatif.
SET connaît trois acteurs : le porteur de carte (ou Cardholder), le commerçant (ou Merchant) et le serveur acquéreur (ou Payment Gateway). Les relations entre l'acquéreur et l'émetteur sont hors du champ de SET : ces relations sont normalement assurées par les réseaux d'autorisation et de remise.

SET assure la confidentialité et l'intégrité des informations échangées, l'identification et l'authentification des parties (par le biais de certificats numériques).
Le protocole s'accompagne d'une organisation bancaire de certificats (chaîne de confiance), avec une hiérarchie remontant jusqu'à une clé racine unique, détenue par SETco (voir schéma ci-dessous).
Chacun des participants reçoit un certificat émis par sa banque de rattachement (le porteur de carte par sa banque émetteur, le commerçant par sa banque acquéreur et le serveur acquéreur par la marque de carte)



Hiérarchie des certificats SET

Les transactions utilisant SET se déroule comme suit :



Toutes les transmissions sont signées par les différents acteurs concernés.
Dans ce processus, le commerçant ne peut pas lire les informations qui ne lui sont pas destinées (informations de paiement dont numéro de carte). Il les joint à la demande d'autorisation qu'il envoie au serveur acquéreur, accompagnée de ses propres données, de sa signature et de sa chaîne de certificats. Le porteur de carte, de ce fait, conserve un anonymat partiel.

SET reste peu utilisé dans le monde car il est complexe à mettre en œuvre (distribution par les banques de certificats à l'ensemble de leur clientèle).
En outre, la faiblesse majeure de SET réside dans l'aspect logiciel du dispositif client. Il s'agit, en effet, d'un logiciel installé sur un ordinateur à architecture ouverte, vulnérable aux virus et chevaux de Troie, sans que l'utilisateur ait forcément les compétences nécessaires pour mesurer les risques encourus.

Des solutions, telles que celle mise en œuvre par Cyber-COMM, à base de cartes à puce bancaires et de lecteurs sécurisés, permettent cependant de remédier à la fois à la complexité de distribution des certificats SET (le certificat est remplacé par la carte à puce déjà diffusée par ailleurs par la banque) et à la vulnérabilité aux chevaux de Troie (le lecteur est sécurisé). Par contre elles nécessitent de déployer massivement des lecteurs auprès des internautes, ce qui pose d'autres types de problèmes (problèmes financiers, marketing, commerciaux et industriels).

ANNEXE 4 : LES MOYENS DE PAIEMENT EXAMINES

Au préalable, il est nécessaire de relever un certain nombre de critères qui permettront ensuite de caractériser les différents moyens de paiement.

4.1. Critères de différenciation

Les différents moyens de paiement peuvent être différenciés par les caractéristiques suivantes :

- Mode de transaction :
  - En ligne,
  - Local.
- Type de transaction :
  - Non-signée,
  - Signée.
- Type de paiement :
  - Pré-payé (comme les valeurs stockées dans une carte),
  - Payé lors de la transaction (comme le fiduciaire),
  - Post-payé (comme avec les cartes de paiement ou le chèque).
- Instrument de paiement :
  - Similaire au fiduciaire,
  - Type chèque ou carte de paiement,
  - Virement,
  - Autres.
- Anonymat :
  - Totalement anonyme,
  - Partiellement anonyme,
  - Totalement transparent.
- Adéquation :
  - Aux paiements de petits montants,
  - Aux paiements de gros montants,
  - Aux informations, programmes ou services disponibles sur Internet,
  - Aux commandes par courrier.
- Mobilité (utilisation possible dans plusieurs terminaux)
- Utilisation :
  - Local,
  - National,
  - International.
- Flexibilité :
  - Transaction sans intermédiaire,
  - Transaction avec intermédiaire.
- Mode de livraison :
  - Immatériel,
  - Matériel.

4.2. Cyber-COMM

Intervenant : Gaëtan DALIGAULT (Cyber-COMM)

Cyber-COMM, issu de la réunion entre 3 projets pilotes (CyberCard, e-Comm et SEC France) a été officiellement lancé en avril 2000.
La société Cyber-COMM a pour actionnaires des banques (1/2 du capital), des organismes interbancaires (1/4 du capital), comme Visa, Europay et enfin des industriels (1/4 du capital) tels que France Télécom et Bull.

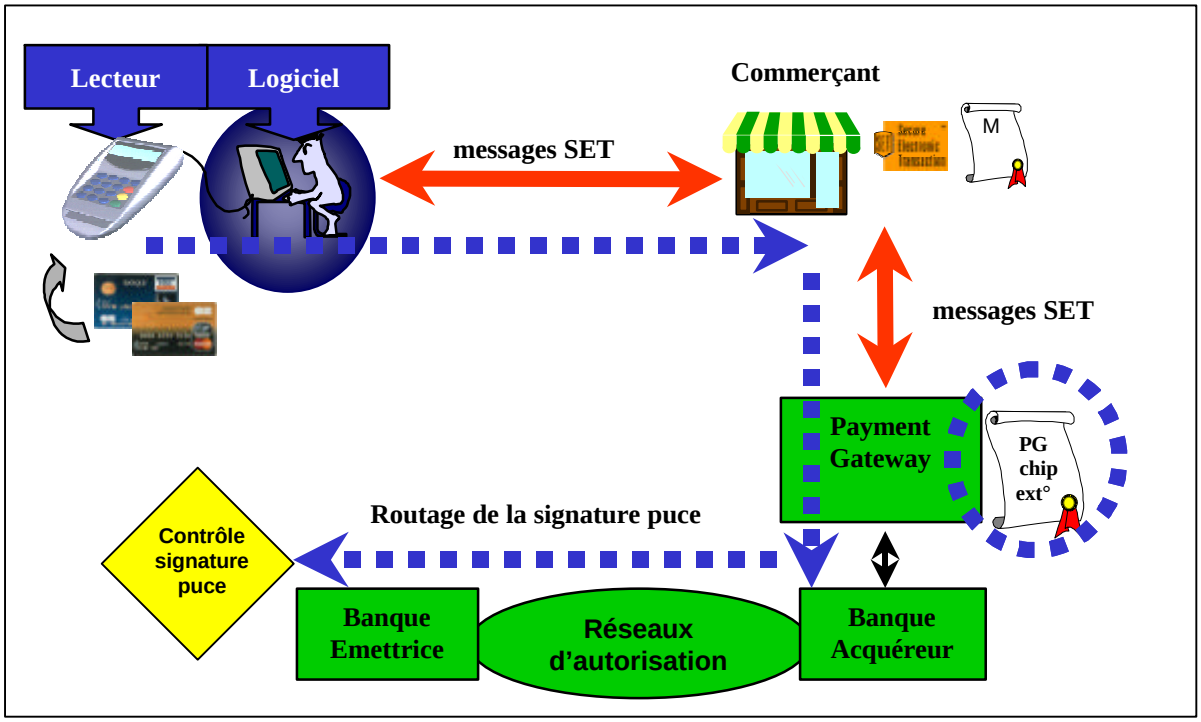
4.2.1. Principe

Ce système permet le paiement par carte bancaire à distance grâce à un lecteur relié au PC du client.
Ce système repose sur :

- l'utilisation physique de la carte à puce,
- la composition du code confidentiel pour valider le montant tout en s'assurant d'une légitimité du porteur de la carte,
- le remplacement de l'authentification visuelle de la carte par une authentification dynamique virtuelle, sur la base d'une signature par la puce,
- le remplacement de la reconnaissance visuelle d'un commerçant CB par la vérification automatique d'un certificat virtuel.

La solution Cyber-COMM peut être utilisée dans différents services :

1. L'accès à la banque à domicile,
2. Le rechargement à domicile des PME Monéo,
3. L'authentification forte pour les Cartes Virtuelles Dynamiques,
4. Le paiement,
5. Autres (courtage en ligne,…).



Le paiement avec Cyber-COMM

4.2.2. Critères fonctionnels

- Mode de transaction : En ligne,
- Type de transaction : Signée,
- Type de paiement : Post-payé,
- Instrument de paiement : Carte de paiement,
- Anonymat : Totalement transparent,
- Adéquation : Aux paiements de gros montants,
- Mobilité (utilisation possible dans plusieurs terminaux),
- Utilisation : International,
- Flexibilité : Transaction avec intermédiaire,
- Mode de livraison : Immatériel et matériel.

4.2.3. Déploiement

La distribution devrait se faire par l'intermédiaire de différents canaux :

- Par les banques (Banque à Domicile + PME) : 20.000 distribués,
- Par des distributeurs : CSD, Surcouf, PC City, Boulanger,
- Via des offres packagées de constructeurs.

140 commerçants avaient signé avec une banque à la mi-juillet 2001. 27 de ces 140 commerçants, dont Darty et Leroy Merlin, ont un site opérationnel. Les autres (Conforama, Décathlon,..) sont en cours de migration.

Cependant, l'avenir du protocole SET étant incertain, la société Cyber-COMM opère un repositionnement stratégique autour du lecteur. Les modalités de ce repositionnement pourraient être arrêtées cet été par le Conseil d'Administration de Cyber-COMM, et devrait donner à Cyber-COMM un rôle de promotion autour du lecteur et des applications qui l'utiliseront. Le Groupement des Cartes Bancaires pourrait prendre en charge les aspects spécifications et homologation du lecteur et des applications bancaires associées. Le marché (fabricants, SSII, ...) pourrait être mis plus largement à contribution pour accroître les différents types de lecteurs déjà existants, pour les intégrer plus largement dans les terminaux d'accès à Internet (dans des claviers ou autres), et pour développer les applications répondant aux besoins de sécurité renforcée des banques et des autres acteurs. Cette répartition des missions actuelles de Cyber-COMM sur le Groupement des Cartes Bancaires, le marché, et une société de promotion Cyber-COMM, devrait contribuer à diffuser et promouvoir plus largement et rapidement les lecteurs personnels auprès du grand public.

4.2.4. Sécurité

Le lecteur a les caractéristiques suivantes :

- Afficheur (montant + devise, ou autres données),
- Clavier numérique (code confidentiel, …),
- Algorithmes DES, RSA, SET/OAEP (clés RSA de 1024 bits),
- Applications internes téléchargeables sous forme sécurisée (vérification de la signature),
- Le lecteur peut être authentifié à distance (identifiant + clé privée interne au lecteur).

Un Profil de Protection SCSSI n°9902 a été développé pour les lecteurs de type Cyber-COMM.

Les plates-formes de Cyber-COMM sont exploitées par les sociétés Certplus (flux SET) et Experian (flux monétiques)

Les mesures de sécurité physique des plates-formes sont les suivantes :

- Une salle dédiée dans locaux sécurisés, avec accès contrôlé, avec identification individuelle, digicode, cartes d'accès, caméras,
- Des locaux agréés par autorités de certification, avec audits annuels (CB, VISA, MasterCard),
- Un personnel d'exploitation autorisé.

La sécurité des échanges et la conservation des données sensibles sont assurées par :

- Des logiciels agréés et une administration dédiée à l'exploitation,
- Un double firewall,
- La génération et la conservation des secrets dans boîte noire,
- L'intégrité et la confidentialité des données par un serveur sécurisé et un protocole avec une clé RSA de 1024 bits (+root-key à 2048 bits),
- Des tests d'intrusion périodiques et un reporting courant.

4.3. France Télécom Mobile

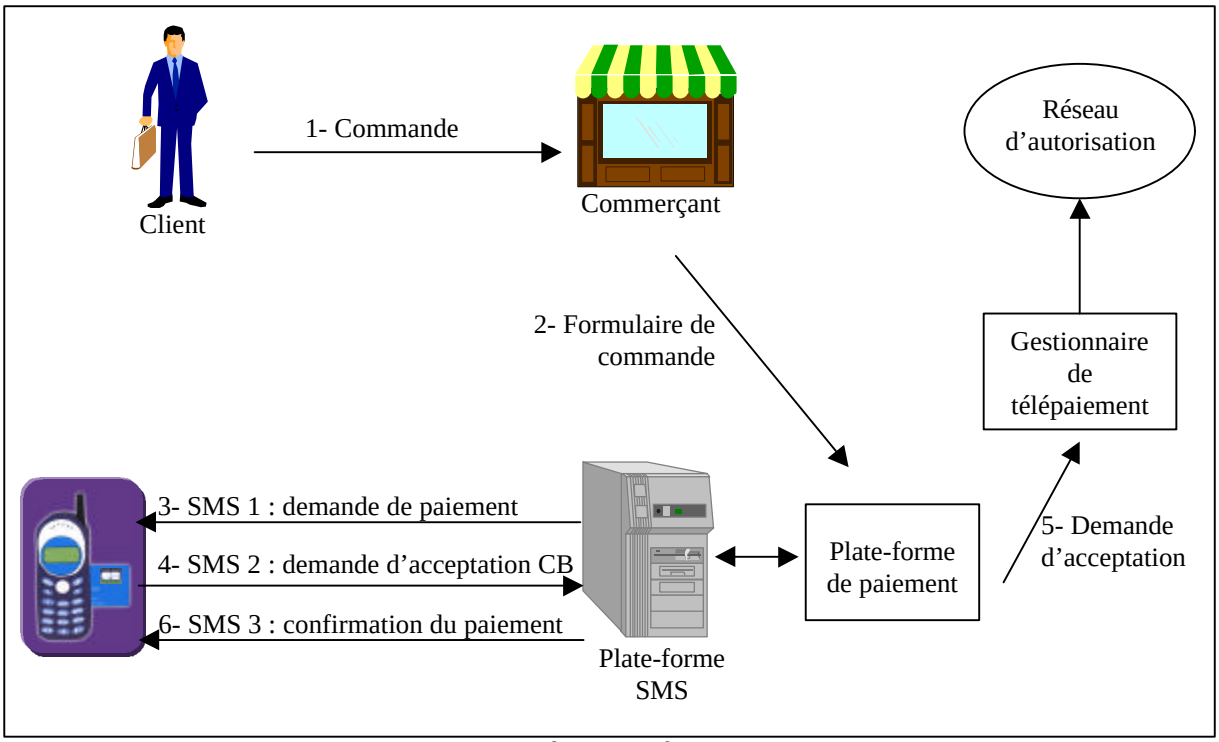
Intervenant : Elisabeth GARREAU (France Télécom Mobile)

4.3.1. Principe

France Télécom Mobile propose une solution de paiement par carte bancaire «CB» sur téléphone portable. Pour ce faire, le téléphone portable est muni d'un lecteur de carte à puce additionnel (téléphone bi-fente).

Cette solution de paiement vise les commandes à distance (par correspondance, téléphone, minitel, internet, portail Wap). Après avoir effectué sa commande, le client communique son numéro de téléphone portable au commerçant. Le client reçoit un SMS (ou mini-message) de demande de paiement qui précise le montant et la désignation de l'article. Il insère sa carte de paiement et saisit son code confidentiel. Son code est vérifié en local, il n'est pas stocké sur le téléphone portable et ne circule pas sur la carte SIM ou sur le réseau GSM. Le client reçoit ensuite un SMS de confirmation.

Le client peut conserver 5 SMS de confirmation sur son téléphone portable qui lui servent de reçus.



Détail des flux

Les principaux commerçants intéressés sont les commerçants de la Vente à Distance (VAD) classique, les commerçants sur Internet et enfin les facturiers (paiement de factures type EDF,…).

L'intégration d'un nouveau commerçant se fait en trois étapes :
- La signature d'un contrat bancaire spécifique de télépaiement,
- La signature d'un contrat avec une plate-forme de mini-message,
- L'intégration de la solution à l'environnement marchand (logo CB, interface automatique).

4.3.2. Critères fonctionnels

- Mode de transaction : En ligne,
- Type de transaction : Signée,
- Type de paiement : Post-payé,
- Instrument de paiement : Carte de paiement,
- Anonymat : Totalement transparent,
- Adéquation : Aux paiements de gros montants,
- Mobilité (utilisation possible dans plusieurs terminaux),
- Utilisation : International,
- Flexibilité : Transaction avec intermédiaire,
- Mode de livraison : Immatériel et matériel.

4.3.3. Déploiement

La phase de déploiement a débuté le 30 juin 2000 et concerne les marques Itineris, Ola et Mobicarte. 300 000 terminaux bi-fentes sont actuellement commercialisés. Le client ne voit aucun surcoût quant au prix du terminal bi-fente. Il lui est facturé au même prix qu'un terminal classique.

Il y a environ 2000 transactions par jour pour le rechargement de Mobicarte.
La cible visée de commerçants est actuellement limitée à la France. 40 commerçants sont actuellement partenaires de France Télécom Mobile, dont Alapage, les 3 suisses, EDF-GDF, Hertz, Interflora. 100 autres commerçants sont en cours d'intégration.
Le coût d'une transaction pour le commerçant dépend de sa banque acquéreur. Il est de l'ordre de 2 à 3 francs. Le client paye un SMS au cours de la transaction soit 1 franc.

4.3.4. Sécurité

L'application de paiement est gérée par une carte SIM Toolkit 32 Ko qui assure le dialogue entre la carte bancaire et le mobile.
Des spécifications ont été émises par le Groupement Cartes Bancaires.

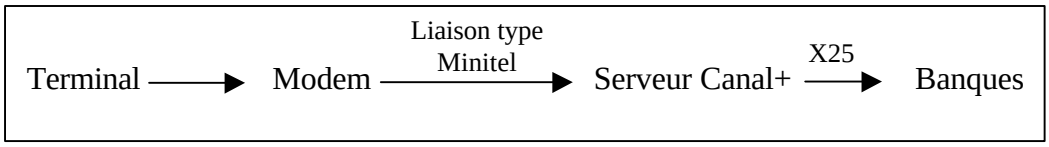
4.4. Canal +

Intervenant : Nadia DOMEC (Canal+)

4.4.1. Principe

Il existe une première génération de décodeurs numériques et une nouvelle est en cours de développement. Depuis 1996, ces terminaux sont dotés de lecteurs de cartes. La carte à puce permet l'authentification des abonnés à distance ainsi que le rechargement de cette carte en jetons prépayés.
Les applications développées sont le Pay per View, la boutique (FNAC,…), le PMU et la banque à domicile.

La première génération de décodeurs fonctionne comme suit :



Les décodeurs de la nouvelle génération peuvent être mis à jour par satellite. Ils permettent l'accès à Internet et ont tous un lecteur de cartes de paiement et de carte d'accès.
L'abonné Canal Satellite pourra avoir accès à trois types de commerçants :
1. les commerçants de Canal Satellite,
2. les commerçants réunis en un réseau sécurisé (VPN),
3. les commerçants sur l'internet ouvert.

4.4.2. Critères fonctionnels des décodeurs 2nde génération

- Mode de transaction : En ligne,
- Type de transaction : Signée,
- Délai de paiement : Post-payé,
- Instrument de paiement : Carte de paiement,
- Anonymat : Totalement transparent,
- Adéquation : Aux paiements de gros montants,
- Mobilité (utilisation possible dans plusieurs terminaux),
- Utilisation : International,
- Flexibilité : Transaction avec intermédiaire,

- Mode de livraison : Immatériel et matériel.

4.4.3. Déploiement

Canal + a 14 millions d'abonnés en Europe dont 7 millions en France. C'est le 3ème groupe mondial de télévision à péage. Il existe actuellement 2 millions de décodeurs numériques acceptant la Carte Bancaire en France.
Ces 2 millions de décodeurs génèrent (en tenant compte d'une seule banque acquéreur) environ 150 millions de transactions par an (dont 50 millions pour le PMU).
Avec l'arrivée du numérique terrestre, 7 millions de décodeurs numériques acceptant les cartes de paiement à la norme EMV sont attendus en Europe pour 2004.
Le prix d'un décodeur de 2ème génération est de 2000 francs environ, soit la moitié d'un TPE (Terminal de Paiement Electronique).

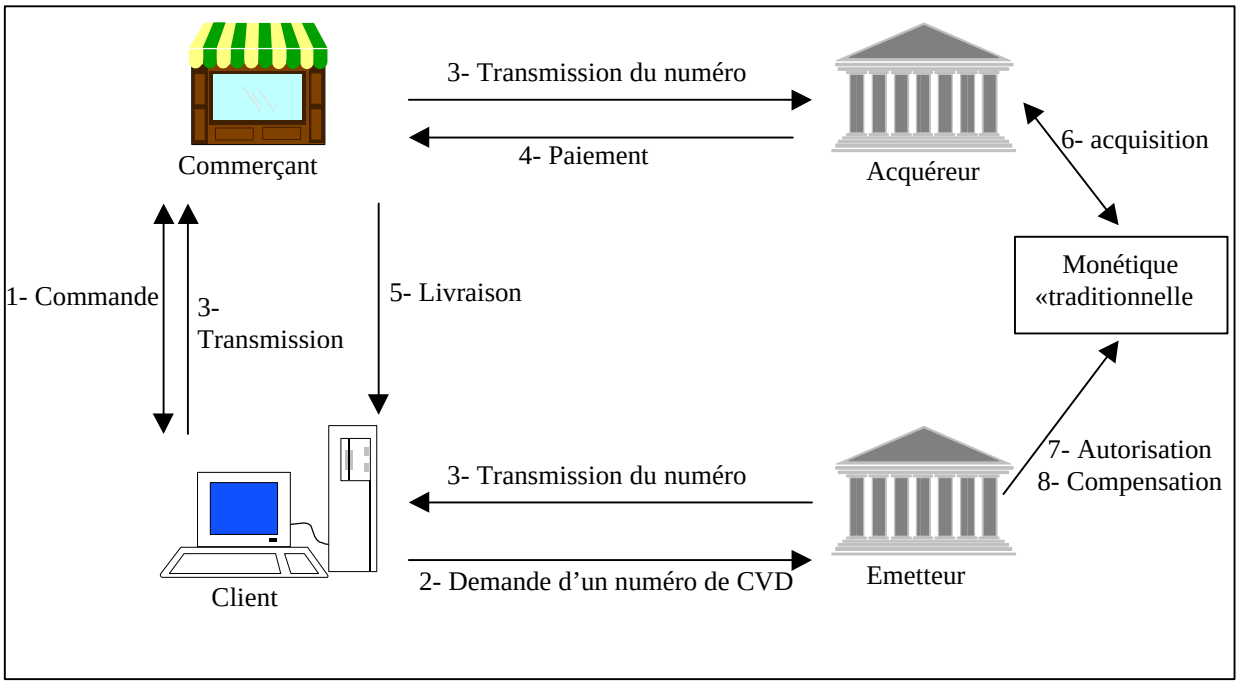
4.5. Carte Virtuelle Dynamique

Intervenants : Jacques SCHUHMACHER (CNCE), Frédéric TOUMELIN (Carte Bleue)

Carte Virtuelle Dynamique (CVD) est un produit développé par le Groupement Carte Bleue.

4.5.1. Principe de la Carte Virtuelle Dynamique

L'objectif de ce moyen de paiement est de permettre de cesser la diffusion des numéros réels de cartes en vente à distance. Le client s'inscrit au préalable auprès de son émetteur. La transaction se déroule comme suit :



Le client, après avoir validé sa commande auprès du commerçant, se connecte sur le site de son émetteur. L'émetteur lui transmet un numéro de CVD avec une durée de validité déterminée et un montant d'utilisation maximum.

Ce système, qui ne garantit pas le paiement, fonctionne auprès de tous les commerçants. Ceux-ci ne voient aucun changement par rapport au système actuel de communication du numéro de carte de paiement.

Ce moyen de paiement ne modifie pas le système Acquéreur. Le numéro de CVD suit le circuit classique des paiements Carte Bleue. C'est le serveur de CVD qui récupère les demandes d'autorisation et effectue les contrôles (durée de validité, restriction en montant) et qui recherche le numéro de carte réel associé.

4.5.2. Critères fonctionnels

- Mode de transaction : En ligne,
- Type de transaction : Non-signée,
- Délai de paiement : Post-payé,
- Instrument de paiement : Carte de paiement,
- Anonymat : Totalement transparent,
- Adéquation : Aux paiements de gros montants,
- Mobilité (utilisation possible dans plusieurs terminaux),
- Utilisation : International,
- Flexibilité : Transaction avec intermédiaire bancaire,
- Mode de livraison : Matériel et immatériel.

4.5.3. Déploiement

Le lancement sera annoncé en juin 2001. Les Caisses d'Epargne est la banque pilote du système. Des accords de coopération spécifiques ont été passés avec France Télécom et Orbiscom. La tarification pour l'utilisateur n'a pas encore été arrêtée.
Cette solution est déjà déployée et utilisée dans le monde (AIB, Discover, MBNA).

4.5.4. Sécurité

Les numéros de cartes virtuelles sont de vrais numéros de cartes bancaires.
Les relations entre le client et l'émetteur sont de la responsabilité de l'émetteur qui choisit les moyens de sécurité adéquats (identifiant / mot de passe, signature électronique).

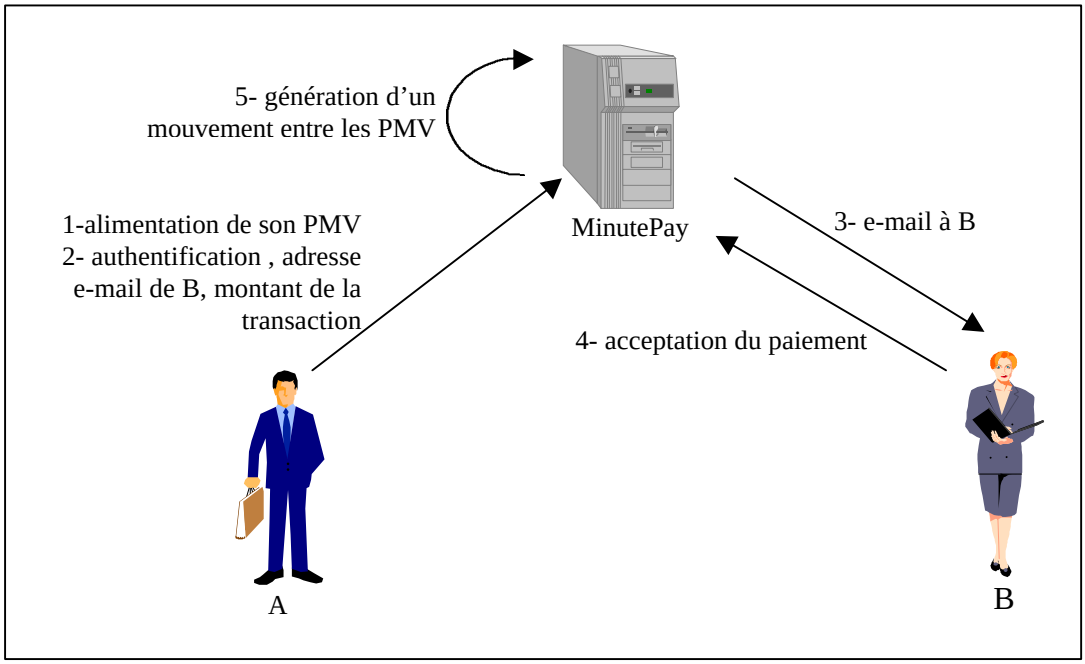
4.6. MinutePay

Intervenant : Jean-François DUCHER (BNP Paribas)

MinutePay est un moyen de paiement proposé par Banque Directe (filiale de BNP Paribas).

4.6.1. Principe

Ce système permet le paiement «par e-mail» entre deux personnes (P to P ou Person-to-Person), grâce à une technologie basée sur un porte-monnaie virtuel (PMV). Cette solution pourra, à terme, être utilisée pour les transactions C to B (Consumer-to-Business). Le paiement via MinutePay se déroule de la manière suivante.



L'e-mail n'est que le vecteur pour informer le bénéficiaire du paiement. Il n'a aucun effet sur les flux de paiement.
Le PMV peut être alimenté par tous les moyens scripturaux. Cependant, dans une première phase, le virement est privilégié. Le remboursement du PMV s'effectue seulement par virement sur le compte bancaire du bénéficiaire.
Le système distingue deux types d'utilisateurs : l'utilisateur de base et l'utilisateur vérifié. Un utilisateur est dit vérifié quand un lien univoque a pu être effectué entre son compte bancaire et son PMV MinutePay. Un utilisateur de base (découvrant généralement MinutePay par le principe de viralité) a de fortes limitations quant à l'utilisation du système. Il ne peut en particulier ni entrer ni sortir de l'argent du système.
Banque Directe est responsable de la relation client, elle gère le «float». Elle est également le point d'entrée dans le système interbancaire (SIT, RCB). MinutePay, quant à lui, effectue la prestation technique sous mandat.

4.6.2. Critères fonctionnels

- Mode de transaction : En ligne,
- Type de transaction : Non-signée,
- Type de paiement : Pré-payé,
- Instrument de paiement : Virement,
- Anonymat : Totalement transparent,
- Adéquation : A tous les paiements dans les limites fixées par MinutePay,
- Mobilité (utilisation possible dans plusieurs terminaux),
- Utilisation : National,
- Flexibilité : Transaction avec intermédiaire,
- Mode de livraison : Immatériel et matériel.

4.6.3. Déploiement

MinutePay sera lancé en juin.
Ce type de moyen de paiement connaît déjà un fort développement aux Etats-Unis et au Royaume-Uni avec notamment Paypal, Billpoint, Earthport,… Ainsi Paypal, en 18 mois, possède 7 millions d'utilisateurs et en gagne 30 000 nouveaux par jour.
Le moyen de propagation de ce type de système est principalement viral (une personne inscrite sur le site de paiement PtoP envoie de l'argent à une personne qui n'est pas inscrite et qui à son tour peut s'inscrire sur MinutePay).
Le service devrait être payant pour les utilisateurs les plus actifs.

4.6.4. Sécurité

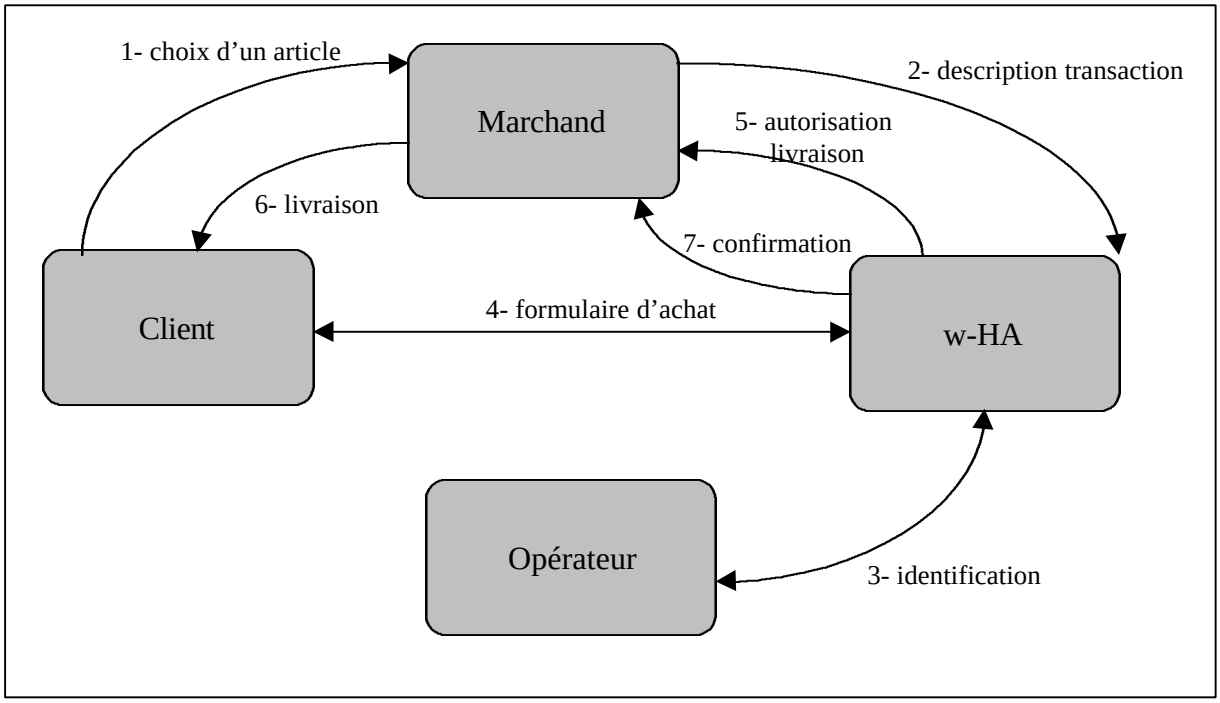
La technologie de ce système de paiement a été développée par Digineer et Valoris. Digineer a déjà développé un système équivalent chez Bank One, eMoneymail qui est opérationnel depuis 2 ans.
La plate-forme technique est hébergée par France Télécom Hébergement.
Des tests et des audits sécuritaires seront effectués régulièrement. Un audit a été réalisé par la BNP Paribas (RSI). Des tests d'intrusion seront faits avant le lancement puis tous les 3 mois par deux sociétés indépendantes.
L'architecture est classique (de type bancaire). Les serveurs sont redondants avec 2 couches de firewalls, la surveillance physique et logique se fait 7j/7, 24h/24.
Les données sont chiffrées et l'utilisateur ne rentre qu'une seule fois ses informations bancaires.
Les communications s'effectuent avec l'utilisateur avec le protocole SSL 128 bits, dans le système par IPSEC, et avec chiffrement hardware sur le routeur sur la ligne spécialisée.
La connexion au site sécurisée de MinutePay s'effectue pour l'utilisateur par identifiant / mot de passe. Cette authentification évoluera, par exemple avec la mise en œuvre de PKI, en fonction des moyens recommandés par la communauté bancaire française et répandus sur le marché.
Le produit prévoit une protection contre certaines attaques dirigées sur le poste de travail du client, notamment le détournement sur des faux sites visant à lui extorquer ses mots de passe ; lors de sa connexion au site MinutePay un certain nombre de données personnelles connues seulement de MinutePay (nom, dernière connexion, solde de son porte-monnaie) lui sont présentées ; des efforts d'éducation des utilisateurs seront effectués sur le site dès lors que les risques de fraude sont avérés.

4.7. w-HA

Intervenant : Jean-Christophe HAMMOND (w-HA)

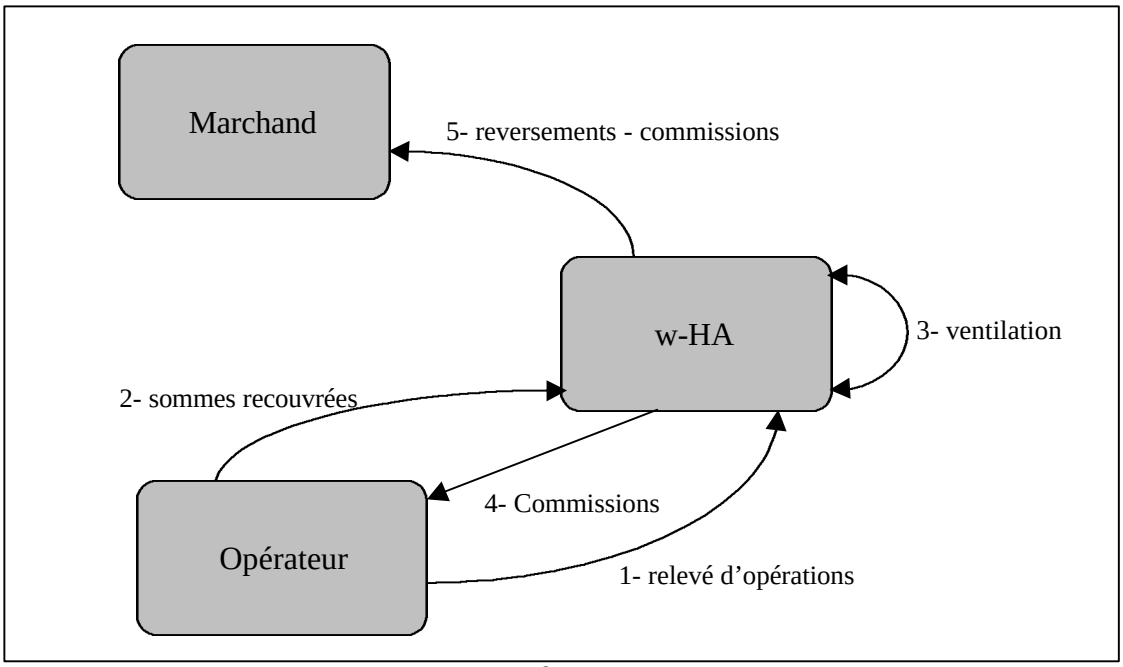
La société w-HA est une filiale de France Télécom.
w-HA a développé un moyen de paiement, basée sur la technologie iPin, pour l'achat de biens immatériels (publications, services en ligne, biens numériques (images, musique), dons) de faibles montants (maximum 15 euros).
w-HA s'appuie sur des partenaires («facturiers»), les Opérateurs Clients qui peuvent être des fournisseurs d'accès à Internet (FAI), des opérateurs de téléphonie mobile ou des banques en ligne.

4.7.1. Principe



Cinématique d'une transaction

Le client choisit un service proposé par un Marchand (sur Internet ou sur le Wap). Celui-ci envoie une demande d'autorisation de vente à la plate-forme w-HA. La plate-forme w-HA s'adresse à l'Opérateur Client pour identifier le client. Après identification, l'Opérateur Client adresse une autorisation de transaction à la plate-forme w-HA, qui est répercutée au Marchand. Le Marchand peut alors fournir le service au client.



Flux financiers

w-HA transmet à l'Opérateur Client un récapitulatif de l'ensemble des transactions réalisées par les clients de l'Opérateur Client concerné. L'Opérateur Client indique sur sa facture

envoyée à ses clients un relevé d'opérations w-HA réalisées. L'Opérateur Client reverse à w-HA les sommes recouvrées au titre des transactions w-HA réalisées par ses clients. w-HA reverse ces sommes moins les commissions prélevées aux Marchands. Il reverse une partie de ces commissions à l'Opérateur Client.

Pour les Marchands, il n'y a pas de garantie de paiement. Ce moyen de paiement repose sur la confiance qu'a le client en son Opérateur Client.

4.7.2. Critères fonctionnels

- Mode de transaction : En ligne,
- Type de transaction : Non-signée,
- Délai de paiement :
  - Post-payé (si les opérateurs clients sont des FAI ou des opérateurs de téléphonie mobile),
  - Possibilité de gérer du pré-payé (si les opérateurs clients sont des banques),
- Instrument de paiement :
  - Traditionnels,
  - Porte-monnaie virtuel (si les opérateurs clients sont des banques),
- Anonymat : Totalement transparent pour w-HA,
- Adéquation : Aux paiements de petits montants pour des biens immatériels disponibles sur Internet,
- Mobilité,
- Utilisation : nationale (au démarrage avec possibilité de passer à l'international),
- Flexibilité : transaction avec intermédiaire non bancaire. w-HA a été agréé par le CECEI,
- Mode de livraison : Immatériel.

4.7.3. Déploiement

w-HA n'a pas encore été lancé. Les premiers Opérateurs Clients qui devraient proposer w-HA sont Club Internet, Wanadoo et Itinéris.
L'équilibre d'exploitation est envisagé pour 2003.
Cette solution s'inscrit en continuité des kiosques France Télécom (Minitel, Audiotel…). La cible visée est notamment celle du Minitel qui regroupe 8 000 éditeurs de service avec un chiffre d'affaire généré de 12 Mds de Francs par an.

La solution iPin fonctionne déjà aux Etats-Unis (Wells Fargo), en Israël (Internet Gold).

4.7.4. Sécurité

Les informations échangées sont sécurisées par l'utilisation du protocole SSL 128 bits.
La sécurité de la plate-forme informatique est assurée par l'existence de 2 réseaux d'accès, d'une architecture 3 tiers avec zonage avec utilisation de 2 types de firewalls. Sur le réseau de production, l'accent est mis sur la lutte anti-intrusion. Le réseau d'administration utilise une ligne louée avec un fort niveau d'authentification.

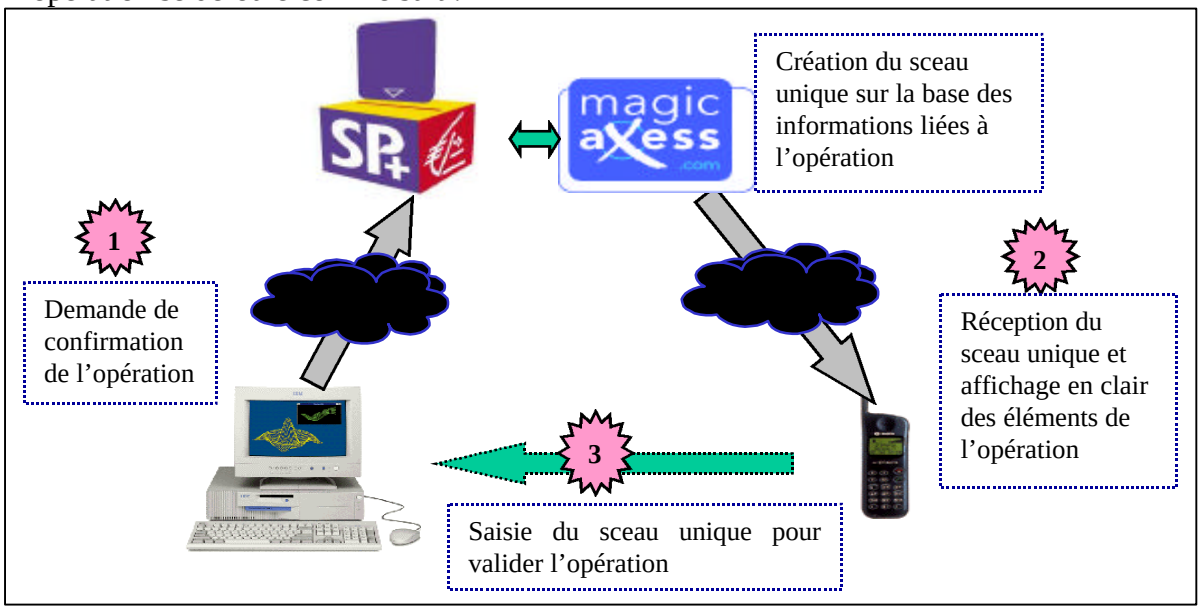
4.8. Magicaxess

Intervenants : Gilles KREMER (Magicaxess) et Martin LAFON (Magicaxess)

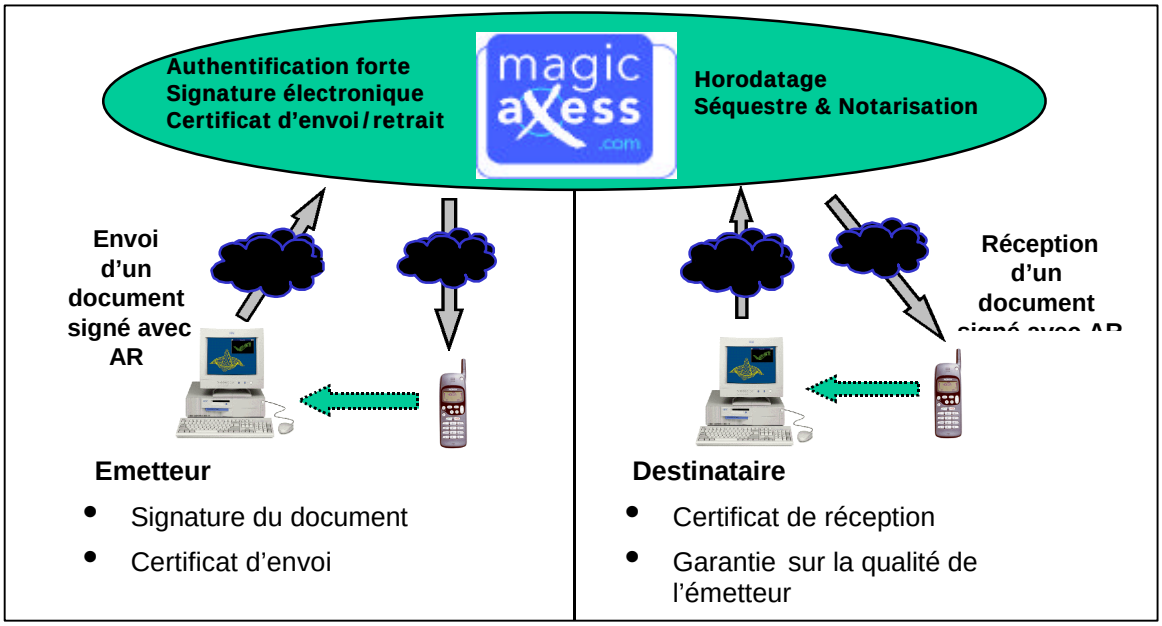
4.8.1. Principe

Magicaxess est un procédé de signature électronique. Il est basé sur l'utilisation d'un téléphone portable.
Le client doit au préalable s'enregistrer auprès d'une banque (et/ou par correspondance).

L'opération se déroule comme suit :



Ce procédé de signature peut s'appliquer dans diverses possibilités : envois d'un «e-mail recommandé», identification du client lors d'une transaction, envoi de devis…



Exemple d'application : «E-mail recommandé»

Moyen de paiement :
Lors d'un achat en ligne, ce procédé peut permettre l'authentification du client et la signature de la commande. A la demande du commerçant, le client se connecte sur SP Plus et demande

la confirmation de son opération en cours. Il retransmet sur le site du commerçant son sceau unique pour valider la transaction.

4.8.2. Déploiement

Magicaxess sera intégré à SP Plus à la fin de mai 2001. Des pilotes BtoB (Business to Business) et BtoC (Business to Consumer) sont prévus en juin 2001.

4.8.3. Sécurité

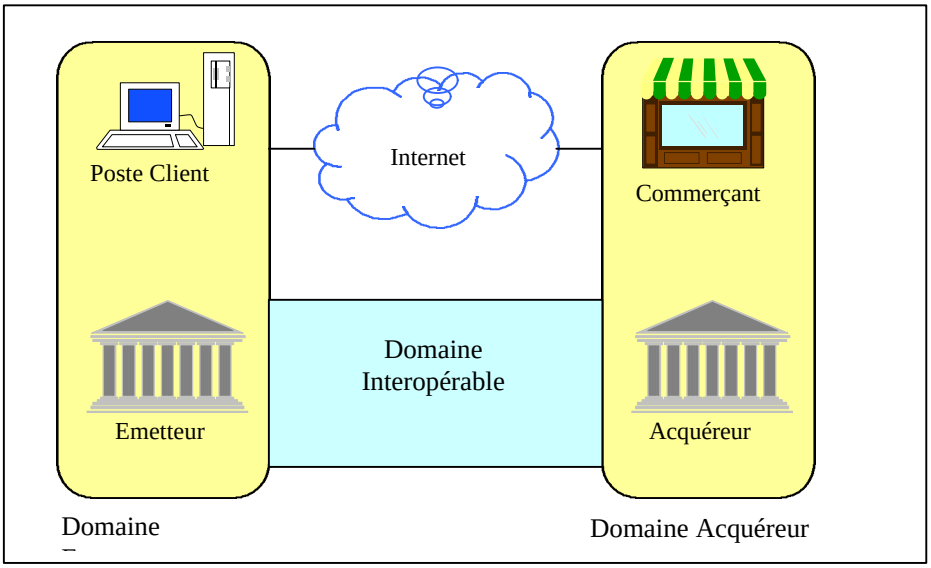
Lors de la connexion sur le site de Magicaxess par le client, le protocole SSL 128 bits est utilisé. Un défi/réponse a lieu lors de l'ouverture de la session.
Des évaluations sécurité sont en cours.

4.9. Concept 3 Domaines

Intervenant : Jacques SCHUMACHER (CNCE).

Ce concept a été développé par VISA. Cette solution 3D (Three Domains) vise à identifier et certifier les acheteurs et les vendeurs sur Internet.
Ce programme permet de gérer d'une manière souple chacune des étapes de la relation :

- entre le porteur et sa banque (Domaine Emetteur) pour la sécurisation de sa carte avant toute transaction,
- entre le marchand et sa banque (Domaine Acquéreur),
- entre la banque du porteur et la banque du marchand lors de la transaction (Domaine Interopérable) pour que le numéro de la carte ne transite plus sur le réseau pendant la transaction.



Modèle 3D

Ce modèle repose sur le protocole SET (3D SET), obligatoire pour le Domaine Interopérable. Les Domaines Acquéreur et Emetteur sont de la responsabilité des banques.

Il est prévu qu’en octobre 2001, toutes les banques VISA devront avoir déployé un système d’authentification utilisant 3D SET. Cette solution 3D (Three Domains) vise à identifier et certifier les acheteurs et les vendeurs sur Internet.