

# Moyens de paiement et sécurité

## Jean-Claude Paillès Frédéric Baron

Jean-Claude Paillès, Supélec (1969), DEA de mathématiques, est spécialiste en télépaiement et en commerce électronique au Cnet (Branche Développement) et participe aux travaux de normalisation. Il a créé l'activité "paiement électronique, et monétique" au centre de Caen et animé le groupement correspondant. Auparavant, il a été chef de projet informatique à la société Jeumont Schneider.

Frédéric Baron, est responsable de l'activité Transactions Electroniques Sécurisées au sein de France Télécom (Branche Grand Public), pour les différents marchés français et internationaux dans les domaines du commerce électronique au sens large. Auparavant, il a participé à la création et à la direction d'une "start up" dans les services informatiques.

# Moyens de paiement et sécurité

**Le paiement en ligne est gouverné par une galaxie d'acteurs offrant un large éventail de prestations. A côté des établissements bancaires et des solutions traditionnelles, le commerce électronique ouvre la voie à des offres originales, du porte-monnaie électronique au terminal pour mobile et à des intermédiaires spécialisés du monde de l'Internet.**

## Paiement et sécurité

L'objectif du commerçant sur Internet est d'aboutir, pour chaque visite sur son site Internet à une transaction d'achat.

Dans la vie courante, l'acte d'achat est tellement banalisé que personne ne prête plus attention à la multitude de pré-supposés culturels et organisationnels mis en œuvre. Toute la difficulté du commerce en ligne est de trouver des substituts à la transaction de contact entre acheteur et vendeur du monde réel, qui, si possible, offre des avantages pour l'un et l'autre : ergonomie, simplicité, sécurité, auditabilité, coût réduit, universalité des usages, interopérabilité, ...

Il y aurait actuellement, plusieurs centaines de systèmes de paiement différents dans le monde. Cette prolifération est évidemment nuisible au développement du commerce électronique, et va à l'encontre de la demande de simplification et de transparence souhaitées par l'utilisateur.

On peut quand même dire qu'un nombre très limité de types de systèmes de paiement sur Internet se dégage : il s'agit de porte-monnaie électronique (réel ou virtuel), de systèmes dits de pièces ou jetons électroniques (cf. encart p. 70), et de systèmes basés sur les cartes bancaires, décrits ci-dessous.

## La carte bancaire de débit

Elle constitue le moyen de paiement universel par excellence. Son utilisation est possible dans tous les pays du monde, que ce soit pour du paiement de contact, chez les commerçants, ou pour du retrait d'argent dans les distributeurs.

Elle est donc utilisée en commerce électronique, suivant le même modèle de base que pour le commerce de contact : (cf. figure 1). Il décrit la cinématique d'une transaction par carte de débit, et fait apparaître les deux entités spécifiques au commerce électronique que sont l'autorité de certification et les plates-formes, qui sont décrites plus bas. En France, le réseau "carte bancaire" du GIE-CB\* permet le traitement des autorisations nationales ; le réseau SIT est utilisé pour les compensations ; pour des transactions transfrontières, les réseaux des grands opérateurs que sont Visa ou Mastercard sont utilisés.

## Les problèmes de sécurité liés au commerce électronique

Ils concernent les aspects suivants :

1. la protection des identifiants des cartes bancaires : l'espionnage sur le réseau, ou bien la réutilisation de ces numéros par un marchand indélicat sont des risques qui sont décuplés sur Internet, réseau ouvert à couverture mondiale ;

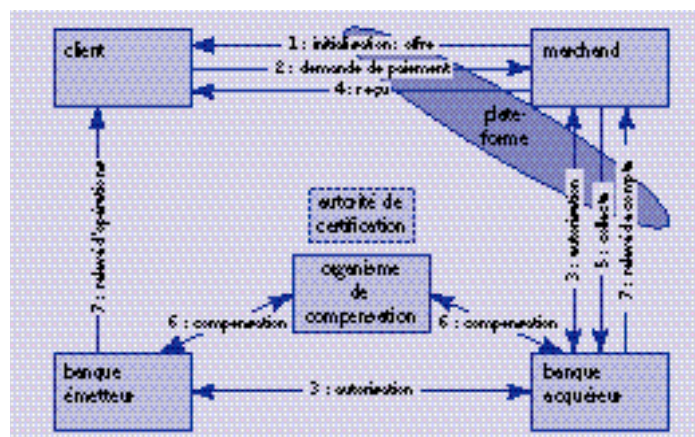


Figure 1 - Modèle générique d'un système de commerce électronique basé sur la carte bancaire.

2. la dématérialisation de la relation client-marchand dans le cas du commerce électronique peut inquiéter le client : ce marchand est-il sérieux, va-t-il livrer le bien que je suis en train de commander et payer ? Va-t-il livrer exactement ce que je pense avoir payé ? L'authentification du marchand, et des règles communes (pour obtenir l'interopérabilité) concernant la distribution des éléments permettant cette authentification (certificats) sont donc nécessaires ;

3. réciproquement, le problème de la répudiation par le client (1) se pose : si le client a les moyens de nier son achat. Sauf si un mécanisme fort de signature électronique reconnu permet d'engager réglementairement le client dans sa décision d'achat, il y a pour le marchand honnête un risque réel de non paiements, et un frein potentiel au développement du commerce électronique.

### Les start-up du paiement sur Internet n'ont pas eu un grand succès :

Une nuée de start-up sont nées du désir d'apparaître comme des intermédiaires incontournables du commerce électronique. Cybercash est une des plus connues: elle annonce des pertes importantes en 97, supérieures à son chiffre d'affaires.

First Virtual est dans une position encore plus critique, et ne doit son salut qu'à la prise de participation importante d'une banque japonaise.

Digicash et son originale technologie de "pièces électroniques" ne semble pas en meilleure forme : les percées effectuées aux USA donnent des résultats décevants, et Digicash se diversifie vers des activités plus traditionnelles de la carte à puce.

Les techniques actuellement utilisées sont les suivantes :

- l'envoi sans protection du numéro de carte sur le réseau concerne fort heureusement le passé ;
- actuellement, l'utilisation de SSL est très fréquente : le risque 1 est partiellement couvert (réutilisation des numéros encore possible), le risque 2 est couvert pour autant que l'on ait confiance à la façon dont a été attribuée le certificat au marchand ; le risque 3 reste entier !
- SET : le protocole SET est né en 96, des efforts conjugués de Visa, Mastercard, Europay, soutenus par de nombreux industriels dont IBM et Microsoft. Dans SET, clients et marchands sont certifiés par leurs banques respectives, elles-mêmes certifiées par des autorités nationales..., ceci jusqu'à une racine mondiale permettant donc une interopérabilité universelle des procédures de sécurité SET, et l'établissement d'une confiance mutuelle du fait d'une certaine homogénéité des règles d'attribution de ces certificats.

Les risques 1 à 3 sont tous résolus, du fait que clients et marchands s'authentifient réciproquement, et du fait aussi que le numéro de cartes n'est en principe pas connu du marchand : ils sont en effet chiffrés par le client, à destination d'une passerelle d'accès entre l'Internet et le monde bancaire (APG : Acquirer Payment Gateway). Le marchand ne peut donc accéder au message en clair.

## SET et son avenir

SET apparaît comme un plus évident. Cependant, des critiques, voire des doutes sur sa généralisation se font entendre.

– lourdeur de mise en place, notamment liée à la distribution de certificats aux clients,

– lourdeur des logiciels, complexité des protocoles, ce qui avec les progrès incessants des capacités des PC semble un peu exagéré ! En fait, il semble quand même qu'une dynamique SET soit en marche : Cybercash adopte SET, Microsoft est en train de faire tester, par l'organisme d'accréditation Setco (2), ses logiciels SET, IBM est un des grands supporters de SET à travers les logiciels clients, marchands, APG, ...

– aspects réglementaires : Visa et Mastercard ont annoncé aux USA une évolution de la réglementation, concernant les litiges de paiement, jusque-là très laxiste en faveur des clients. Cette évolution sera sans doute favorable à un développement du commerce électronique. Mais cette évolution, qui influe sur les relations contractuelles entre les différents acteurs du commerce électronique, prendra sans doute un certain temps.

Une autre critique sur SET est "quid de la carte à puce ?"

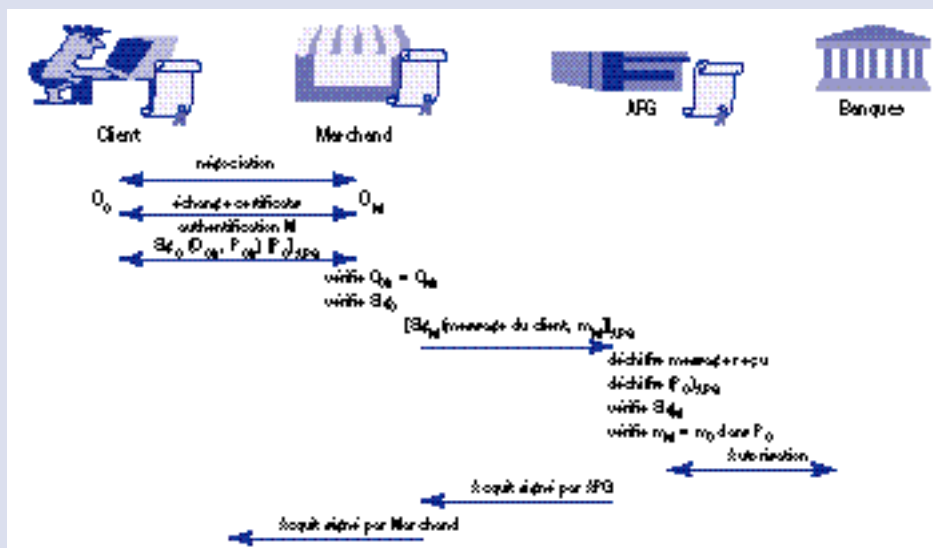
\* Voir abréviations en fin d'article.

(1) Il ne s'agit ici que du paiement, et non des règles relatives à la défense du consommateur qui effectue des achats en VPC, et qui a la capacité de renvoyer le bien avant un certain délai, s'il n'en est pas satisfait !

(2) Organisme en charge de l'accréditation SET, des évolutions, etc.

## Le protocole SET\*

Cet encart donne un aperçu très schématisé et simplificateur de ce protocole complexe, dont une description complète se trouve sur le site visa.com



### Notations du schéma :

- $Sig(X)$  représente l'information X et la signature de son condensé. Les signatures dans SET se conforment aux principes X509, avec un arbre de certification à 5 niveaux, dont les feuilles sont les clients et les marchands.
- L'APG est la passerelle entre le Net et le monde bancaire. C'est une infrastructure acqureur : CF le premier schéma sur le modèle général de transaction carte bancaire.
- $[X]_{APG}$  représente un message X chiffré à destination de l'APG. Il n'est déchiffrable que par l'APG.
- $X_h$  représente le condensé de l'information X (hashing).
- O : représente le bon de commande y compris le montant m et le numéro de transaction.
- P : représente les informations de paiement : notamment le numéro de la carte bancaire, les dates de validité, le montant et le numéro de transaction.
- m est le montant total de la transaction.  $m_M$  est le montant établi par le marchand, qui normalement doit être le même que celui pris en compte par le client dans  $O_C$  ou  $P_C$  !
- $O_C$  ou  $P_C$  sont les versions de O et P établies par le client.  $O_M$  est le bon de commande vu du marchand, qui si tout va bien doit être identique à  $O_C$  !
- APG : "Acquirer Payment Gateway" c'est-à-dire passerelle entre le Net et les réseaux bancaires.

### Principes généraux et justification du protocole :

La phase négociation (navigation du client sur le site du serveur) permet l'établissement des informations du bon de commande, et ne concerne pas SET, qui ne démarre qu'après un message d'un type particulier envoyé par le marchand, et l'activation d'un logiciel côté client appelé Wallet.

- L'APG doit s'assurer que le client et le marchand sont bien d'accord sur la prestation convenue et son prix, donc sur O et sur P, et ceci bien que O n'ait pas à être connu de l'APG (les Banques n'ont pas à connaître la nature des biens achetés par le client), et que P n'ait pas à être connu du marchand (le marchand n'a pas à connaître le numéro de la carte bancaire du client).
- Le client s'engage sur les informations de O et le P par une signature faite de façon à être vérifiable par M ou APG sans connaître in extenso les informations dans O et P. D'où la signature  $SIG_C$  sur les condensés de O et P. P doit être transmis à l'APG, mais doit rester confidentiel pour le marchand, d'où le chiffrement de P pour l'APG.
- Le marchand doit vérifier que le bon qu'il a établi est identique à celui du client, et que celui-ci a bien signé sa commande. Puis il contresigne le message reçu du client et le montant de la transaction tel qu'il l'a établi ( $m_M$ ) à l'APG, et chiffre le tout : le but est de préserver la confidentialité sur le NET de l'activité commerciale du marchand.
- L'APG doit alors vérifier que client et marchand sont bien d'accord sur les termes de la prestation :
  - elle vérifie l'identité entre le bon du client et celui du marchand, en vérifiant la valeur des hashes de  $O_C$  et  $O_M$ .
  - elle vérifie qu'il y a accord entre client et marchand sur le montant.
  - elle vérifie aussi bien sûr les signatures du client et du marchand.
- L'APG demande alors une autorisation via les réseaux d'autorisation habituels ; enfin, l'APG restitue un acquittement signé au marchand, puis au client, et contexte français.

\* Voir article de J. Traoré page 47.

## Le contexte français

SET dans sa définition actuelle tient peu compte des cartes bancaires à puce. On sait que les USA ne sont pas le terrain de prédilection de cette technologie. Mais il est vrai que dans SET, rien n'interdit que la signature électronique donnée par le client lors de sa demande de paiement soit produite par sa carte à puce, et non par son PC et les données (clés et certificats) stockées sur son disque dur, sous contrôle d'un mot de passe. Ceci nécessite donc qu'un lecteur de carte à puce soit connecté au PC. Des réalisations de cartes de ce type, aux limites des capacités technologiques actuelles, commencent à apparaître. Par contre SET dans sa version actuelle fait peu de cas des cartes bancaires à puce telles qu'il en existe essentiellement en France (30 millions de cartes, dites B0') et dans d'autres pays Européens, notamment en Allemagne avec la carte "Geldkarte" et sa fonction carte de débit, ou en Grande Bretagne où des pilotes importants sont en cours, et vont conduire à un déploiement généralisé en 2001. Par ailleurs, une importante spécification, qui a valeur de norme internationale, existe depuis 1995 : il s'agit d'"EMV" (du nom des 3 organismes qui l'ont développée : Europay, Mastercard, Visa). Par ailleurs, les cartes bancaires françaises vont migrer vers les EMV, avec un biseau allant de 2001 à 2003. Il y a donc dans les EMV un axe d'évolution important pour SET. En effet, il faut signaler que la carte à puce peut apporter un avantage évident en ce qui concerne la sécurité du commerce électronique.

### Les cartes bancaires débit/crédit à puce ; B0', EMV...

- Les chiffres de l'application CB françaises sont impressionnants :
  - 30 millions de cartes,
  - 26 000 distributeurs de billets,
  - 540 000 terminaux de paiement électronique,
  - 1 000 milliards de francs de paiement et retrait/an, pour 3 milliards d'opérations,
  - 0,02 % de fraudes, ce qui est le taux le plus bas dans le monde sur cette activité.
- Les fonctions de la puce B0' de la carte bancaire :
  - comme une carte magnétique, sa première fonction est bien sûr le support de l'identifiant du compte du porteur,
  - elle permet d'authentifier le porteur : contrôle du code confidentiel,
  - elle s'authentifie auprès du terminal de paiement, grâce à une valeur d'authentification, basée sur un algorithme à clé publique,
  - elle journalise les transactions,
  - elle permet au terminal une gestion du risque client : si par exemple le journal montre un flux de dépenses trop important sur la période en cours, le terminal doit demander une autorisation,
  - elle délivre une signature électronique de la transaction (calculée avec un algorithme à clé secrète) qui est une preuve de la véracité de la transaction enregistrée sur le ticket, et est utilisée en cas de litiges.
- La norme EMV  
Cette norme a une orientation nette multiapplication ; elle est en conformité avec les normes 7816-4, qui décrivent les commandes terminal-cartes. Elle est fonctionnellement proche de la carte B0', mais avec des avancées sur l'authentification par le terminal, et sur la gestion du risque client, qui est prise complètement en charge par la carte, afin que cette gestion ne dépende que de la banque émettrice et non du terminal sur laquelle cette carte est utilisée (et qui peut être dans un pays différent).  
En France, il est prévu que le passage de la carte bancaire aux EMV se fera entre 2000 et 2002.

Les solutions purement logicielles sont sensibles aux virus qui peuvent sévir dans le monde du PC, alors que la carte à puce y est complètement étanche.

Ces virus peuvent par exemple permettre de voler les clés, ce qui permet de réaliser de "fausses cartes virtuelles" utilisables pour des transactions sur le Net. Ou alors, ces virus pourraient modifier les paramètres de la transaction au bénéfice du marchand : par exemple augmenter le montant, ou modifier le descriptif du bien acheté, ou la quantité... Bref il y a là source potentielle de litiges commerciaux difficiles à gérer, et bien qu'aucune fraude de ce type n'ait été jamais mise en évidence, il vaut sans doute mieux parer à tout danger...

## Les initiatives de Banques françaises

Toutes ces considérations éclairent les initiatives des banques françaises dans les choix de protocoles de paiement sur le Net. Deux projets ont été lancés en 96, Cybercard et e-Comm. France Télécom est un des partenaires de e-Comm : les autres partenaires sont BNP, Société Générale, Crédit Lyonnais, Gemplus, et Visa international.

Ces deux projets visent, avec des approches différentes, à concilier SET et la carte B0'.

En avril 98, il a été décidé de faire converger ces deux approches vers une solution unique, Cybercomm et son protocole C-SET visant à :

- la compatibilité avec SET, mais sans certificats clients, puisque la carte B0' est utilisée ;

- la prise en compte dans les évolutions de SET de ce mode simplifié, assurant une totale interopérabilité ;
- la définition d'un concept de lecteur sécurisé, muni de plus d'un clavier et afficheur, pour contrer par exemple des fraudes de type modification du montant de la transaction.

## **Les atouts de l'approche française**

Cybercomm cherche donc à tirer avantage des investissements consentis par la communauté bancaire lors de la dernière décennie sur la carte à puce. Elle apporte un atout sécuritaire certain. Pour le client, la transaction, dans le cas du commerce de contact ou du commerce électronique, utilisera la même carte, et se déroulera de la même façon. Elle présente l'inconvénient de nécessiter un lecteur de cartes connecté au PC, muni des logiciels adéquats.

Le déploiement de Cybercomm est prévu pour mi-99, et les partenaires de Cybercomm semblent envisager une croissance rapide du parc de lecteurs de carte à puce. L'avenir dira si cette solution et ses caractéristiques réglementaires (non répudiation du client, garantie du commerçant) sera exclusive ou majoritaire par rapport à des solutions purement logicielles, et si elle constituera ou non un accélérateur du développement du commerce électronique, du fait des avantages décrits ci-dessus.

### **Les techniques de paiement à pièce ou à jeton électronique**

e-Cash comme Millicent se basent sur ces techniques :

- une pièce électronique est une donnée signée par l'émetteur de la pièce, pour qu'il soit le seul à pouvoir créer de la monnaie ;
- le marchand recevant une telle pièce en paiement, doit s'assurer qu'il ne s'agit pas d'un faux (contrôle de la signature) et aussi qu'elle n'a pas déjà été dépensée, puisque rien n'est plus facile que de dupliquer une donnée informatique ! Une base de données doit donc enregistrer chaque pièce dépensée, et doit être consultée à chaque paiement par le marchand.

Millicent résout ce problème en rendant les pièces spécifiques à un couple client/marchand (ou à un groupe de marchands qui fédèrent leur contrôle d'unicité). Le client doit donc gérer dans la "poche" virtuelle de son PC un grand nombre de monnaies différentes, s'il veut naviguer sur le Net.

L'approche e-Cash est plus radicale : elle se base sur une base de données unique et donc pose des problèmes d'ouverture évidents. De plus, e-Cash utilise une technique de délivrance des pièces aux utilisateurs autorisant un anonymat et une intrapçabilité comparable à ce que l'on a avec les pièces métalliques du monde réel. Il y a impossibilité (au sens cryptographique) d'associer tel client à telle transaction, ce qui n'est pas le cas dans, par exemple, les systèmes basés sur les cartes bancaires dont l'identifiant de compte permet aisément de remonter à la personne.

## **Le micropaiement sur le Net**

On trouve sur le Net des biens relevant plutôt de transactions de petits montants. Par exemple, certaines informations à valeur ajoutée importante, les jeux en ligne, certains logiciels, ...

Il est vrai aussi que sur le Net, la gratuité est un mode très répandu : les fournisseurs d'information couvrent leurs frais par la publicité, ou estiment que les économies faites avec le canal Internet sont suffisantes, ou que la notoriété acquise vaut la dépense ! Cependant, il est aussi clair que la gratuité peut être un frein au développement de certains services à forte valeur ajoutée, exigeant des coûts de développement et d'édition importants. Enfin en France, le Minitel a montré qu'il existe un marché solvable pour le commerce de l'information. Aux USA, le prévisionniste Jupiter Communication prévoit que le paiement de petits montants vont passer de 166 M\$ en 98 à 860 M\$ en 2000. (cf. [1]).

## **Coûts bancaires**

Le coût de traitement des transactions bancaires non Internet correspond au fonctionnement et à l'amortissement des moyens réseaux et informatiques bancaires afférents. Le commerce électronique malgré un développement rapide, ne représente qu'une charge marginale dans ces systèmes, et ne pousse donc pas à leur remise en cause. Le coût d'acquisition d'une transaction bancaire est estimé entre 1 et 2 FF (cf. [1]). Les banques disent qu'elles perdent de l'argent si les transactions font moins de 10 \$. Il n'est donc pas possible, en utilisant l'approche carte bancaire, de traiter économiquement le micropaiement, concernant des montants pouvant être inférieurs à 1 FF.

## Les solutions pour le micropaiement

L'abonnement aux services fournisseurs est une solution qui écarte tout

comportement impulsif du client, et trouve vite ses limites si le client doit avoir des dizaines d'abonnements !

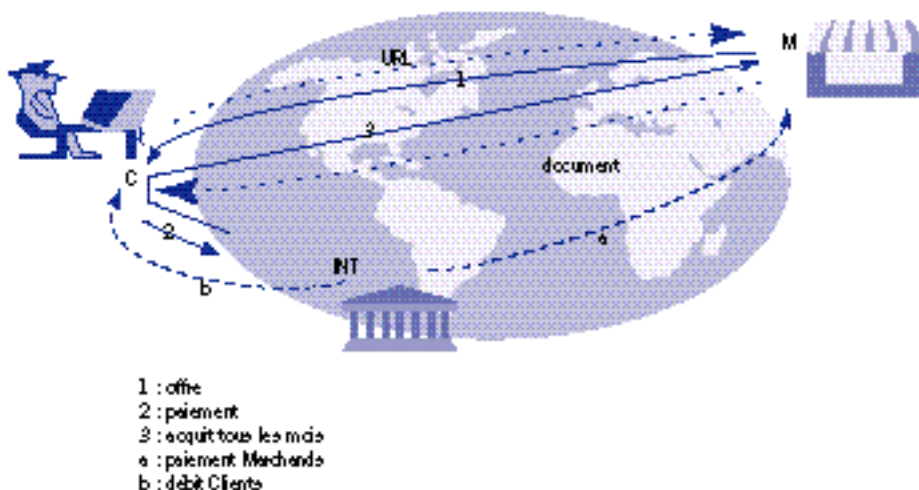
Le paiement à l'acte semble être mieux adapté aux besoins.

Le principe de tous les systèmes de micropaiement est d'agréger les petits montants, pour ne présenter aux banques que des montants significatifs.

Le client peut payer avant : il recharge une provision sur laquelle les micro-transactions s'imputent : on parle souvent de "porte-monnaie virtuel".

Le client peut payer l'addition après, tous les mois par exemple.

### Les micropaiement e-Comm



Les acteurs dans ce système micropaiement sont les suivants (cf. le schéma) :

- le client avec son PC : C ;
- le marchand sur Internet : M ;
- l'intermédiaire INT, constitué par une passerelle Internet, et un serveur du type Maxisim.

Le principe du fonctionnement est adapté au paiement à l'acte :

- le client choisit une information (ou télécharge un logiciel, ou un clip vidéo, ...) en cliquant sur une URL ;
- le marchand renvoie une offre (prix, description) : message offre : 1 ;
- le client paye : il donne son accord à l'intermédiaire ; message paiement : 2 ;
- l'intermédiaire renvoie un avis de paiement, que le client répercute au marchand ; message acquit : 3 ;
- le marchand contrôle l'acquit, et délivre le bien.

L'intermédiaire mémorise chaque demande de paiement (2), sans pour autant créer une opération de débit du compte bancaire du client, opération coûteuse qui pourrait revenir plus cher que le prix payé par le client ! Il gère le risque en comparant les cumuls de consommation de chaque client à un plafond autorisé. On parle donc d'un système de préautorisation/post-paiement.

L'intermédiaire, en fin de mois :

- cumule pour chaque client, les paiements élémentaires, et génère une seule opération de débit sur le compte bancaire de celui-ci (b) ;
- cumule pour chaque marchand, les paiements élémentaires qui lui reviennent, et génère une opération de crédit sur son compte bancaire (a).

Il s'agit donc d'une fonction proche de ce que fait Maxisim pour la publiphonie, où l'on retrouve aussi ces fonctions de contrôle en temps réel par rapport à des plafonds de consommation, de mémorisation des transactions et d'agrégation en fin de mois, ainsi que d'interfaçage avec les systèmes bancaires.

- Le nom générique de ces nouveaux systèmes à FT est Sigma pour la plate-forme, et MSET pour le protocole et ils sont issus du concept Maxisim.

## Les systèmes en lice

Les différentes techniques apparaissant dans ces systèmes correspondent à la façon dont la sécurité est traitée, ainsi que leur degré d'ouverture : capacité d'un tel système à traiter des paiements entre clients et marchands de pays différents : dans ce cas, l'utilisation de techniques à clé publique avec arbre de certification (comme SET) peut amener un plus : on retrouve ces choix dans e-Comm, Minipay et e-Cash (cf. encart micropaiement).

Dans une première catégorie, on trouve Keline, Cybercoin de Cybercash, Millicent de Dec, e-Cash de Digicash.

Dans une deuxième catégorie, on trouve le système de paiement à l'acte de Wanadoo, e-Comm (pour le sous projet micropaiement), et Minipay, d'IBM.

Une solution nouvelle pourrait venir du porte-monnaie électronique : ce nouveau moyen de paiement, conçu pour les petits paiements de la vie quotidienne (transports, publiphones, restauration rapide, petits commerces) pourrait, si son usage se généralise, devenir une bonne solution pour les petits paiements sur Internet.

---

## **Le paiement à l'acte de Wanadoo**

Le paiement dit "à la carte" est opérationnel, et permet de payer par exemple des articles de numéros anciens de certains journaux. Sa particularité est de faire payer le client par imputation sur sa facture Wanadoo, et non sur un compte bancaire. Ce système est donc limité aux marchands ayant un contrat avec Wanadoo.

## **Le porte-monnaie électronique (PME)**

Dans les systèmes de paiement à carte bancaire, l'argent reste sur le compte de la banque émettrice gestionnaire de ce compte, et la carte n'est qu'un moyen d'identification du titulaire de ce compte ; d'où, lors d'une transaction, des coûts incompressibles pour l'autorisation, puis la remise et compensation. Pour des paiements de petit montant, il convient de diminuer ces coûts : le principe du porte-monnaie électronique est donc d'enregistrer une valeur monétaire dans la carte (qui doit être à puce pour des raisons de sécurité), par exemple dans un compteur.

Une partie de cette valeur lors d'une transaction de paiement est envoyée dans le terminal (cf. encart).

## **Le développement du PME**

Le concept de PME a rencontré un grand succès dans différents pays du monde, et notamment en Europe : en Allemagne, il y a 40 millions de Geldkarte. La fonction PME coexiste sur certaines cartes avec la fonction carte bancaire de débit. En Belgique Banksys a développé le PME Proton, qui remporte un grand succès dans le pays et à l'exportation (80 millions de cartes). Les statistiques d'utilisation de ce nouveau moyen de paiement montrent cependant qu'il est loin d'être passé dans les mœurs (une utilisation par mois environ, contre une dizaine dans le cas de la carte bancaire française). En Espagne, au Portugal, en Australie, à Singapour, à Hong Kong, ..., des exemples de ce type pourraient être décrits. Visa défend l'approche Visacash, Mastercard a racheté Mondex en Grande-Bretagne. Il n'y a pas encore de normes mondiales sur le PME, mais des alliances se dessinent : Visa, Proton, ... Des normes européennes de l'ECBS existent. Beaucoup pensent que l'avènement de l'Euro en 2002 pour les particuliers pourrait pousser rapidement à la définition d'un système européen interopérable. Le rapport Lorentz (cf. [2]) identifie le développement d'un PME européen comme un axe important de développement du commerce électronique.

## **Le PME en France**

Paradoxalement, le PME ne s'est pas développé en France jusqu'à aujourd'hui. Mais trois projets apparaissent, pour mise en exploitation vers mi-99.

■ BMS (3) (billétique monétique services) est un consortium entre SNCF, RATP, Société Générale, Les Caisses d'Epargne, La Poste, et prépare un pilote de 50 000 cartes dans le quartier Montparnasse à Paris, pour mi-99. Les cartes seraient des cartes normales à contact, mais disposant aussi de l'interface sans contact, pour traiter rapidement la billétique et la monétique lors du passage dans les portillons de métro (Combi-Carte) .

■ Crédit Agricole et Banque Nationale de Paris préparent un pilote de 60 000 cartes à Tours aux mêmes échéances que BMS. La carte ne dispose pas d'interface sans contact, mais serait une combinaison de la Geldkarte (préparant ainsi l'avènement d'un PME européen), et de la carte bancaire française (autorisant ainsi les deux moyens de paiement en une seule carte).

■ Le Crédit Mutuel a décidé de lancer à Strasbourg son propre pilote. Il s'appuie sur la technologie Mondex, rachetée récemment par Mastercard, et sur l'"Operating system" appelé Multos, qui permet de gérer les cartes multiapplications.

---

(3) Rebaptisé récemment Modeus.

## Fonctionnement du porte-monnaie électronique :

### Principes

Echange sécurisé de valeur électronique entre le PME et le terminal.

Le Sam (abréviation de Secure Application Module) est l'organe qui, dans le terminal, reçoit la monnaie débitée dans les cartes porte-monnaie. On comprend aisément que cette "caisse électronique" présente donc une grande sensibilité du point de vue sécurité. D'autre part, la monnaie électronique est représentée par des messages électroniques, aisément modifiables, duplicables, et le processus d'échange de monnaie électronique entre le porte-monnaie (PME) et la caisse électronique "Sam", est donc hautement sensible. Souvent, dans les implémentations réelles de systèmes PME, le Sam prend la forme de cartes à puce : ce choix correspond à des besoins économiques – le Sam ne doit pas être coûteux – et sécuritaire : le Sam doit être sûr, donc non altérable ni duplicable, imitable, etc. Le choix de la carte à puce est donc particulièrement adapté à ces deux contraintes.

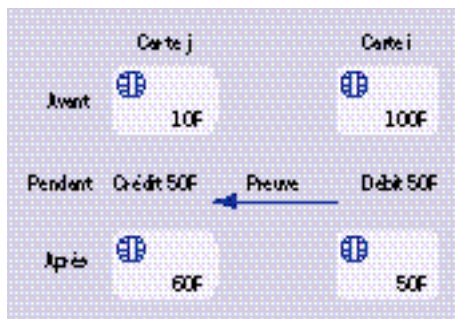


Figure 2 - Echange sécurisé de valeur électronique entre le PME et le terminal.

### Le principe de l'échange de monnaie sécurisé

La fonction cryptographique sur laquelle est basée le calcul de la preuve de débit implique l'utilisation de clés qui doivent être connues à la fois par la carte PME et le Sam. Ces clés sont identiques lorsque les algorithmes sont *symétriques*. Bien sûr les clés se trouvant dans les porte-monnaie des porteurs sont diversifiées à partir d'une clé de base. Mais le Sam, qui vérifie la preuve fournie par le PME, doit connaître cette clé de base et le mécanisme de diversification. Quoique cette clé soit bien protégée dans le "coffre-fort" que constitue la carte à microcalculateur sur laquelle le "Sam" est bâti, on comprend aisément le caractère sensible du "Sam" dans une application PME.

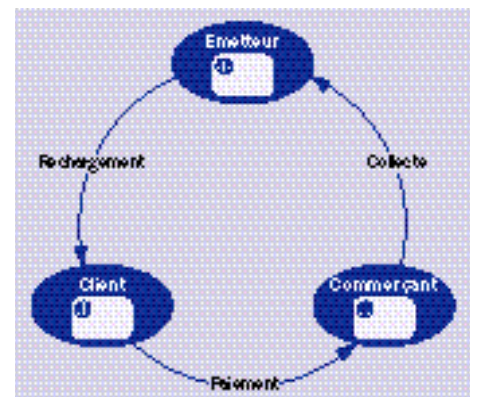
Dans le cas des algorithmes *asymétriques*, la situation est quelque peu différente. La clé utilisée pour le calcul de la preuve de débit, dans le PME, et la clé utilisée par le Sam pour vérifier la preuve, sont différentes. La connaissance de la clé de vérification, clé publique, n'implique pas la connaissance de la clé secrète de calcul de la preuve. Les algorithmes asymétriques apportent donc dans des applications de type PME un plus sécuritaire intéressant.

Figure 3 - La "ronde de la monnaie électronique" montre les flux d'échange de valeurs électroniques entre les acteurs d'un système PME.

### La ronde de la monnaie

Comme le montre de façon très simplifiée le schéma 2, il y a trois partenaires principaux (le client, le commerçant et les banques) et trois grandes catégories de transactions (le paiement, la collecte et le rechargement). L'approche de transfert sécurisé de monnaie électronique entre PME et Sam, pour le paiement, se généralise aux autres types de transaction. Il n'est donc pas nécessaire de conserver les traces des transactions, et ceci contribue à diminuer les coûts de fonctionnement d'un tel système, et donc à rendre économiquement viable le traitement de petits montants.

L'émetteur charge les PME des consommateurs en échange d'espèces ou après débit des comptes bancaires des clients. Les consommateurs vident leurs PME au fur et à mesure de leurs achats et remplissent parallèlement les Sam des prestataires. L'émetteur collecte les porte-monnaie des prestataires en échange du crédit du compte bancaire du prestataire. A chaque fois qu'une valeur électronique est transférée, des paiements conventionnels ou un échange de service sont donc réalisés dans l'autre sens (4).



(4) Cette description est schématique ; la réalité est souvent plus complexe, dans les systèmes actuellement opérationnels.

## Le mobile, dispositif de paiement ultime ?

Dès maintenant, le GSM apparaît à beaucoup, potentiellement, comme le terminal monétique "ultime" : ne contient-il pas, en effet tous les éléments utiles pour la monétique et sa sécurité : afficheur, clavier, liaison de données avec des serveurs (données DTMF dans le sens client-serveur, ou via des "short-messages" pouvant circuler dans les deux sens), cartes à puce (une seule, la carte Sim, pour les terminaux actuels ou deux pour les terminaux bifentes). Dans ces conditions il n'est pas étonnant de voir de nombreuses expériences pilotes se développer. Quelques exemples sont rappelés en annexe. A plus long terme, le portable peut se rapprocher encore plus près de l'ordinateur personnel, servant aussi bien de téléphone que d'organiseur ou de moyen d'accès à Internet, ...

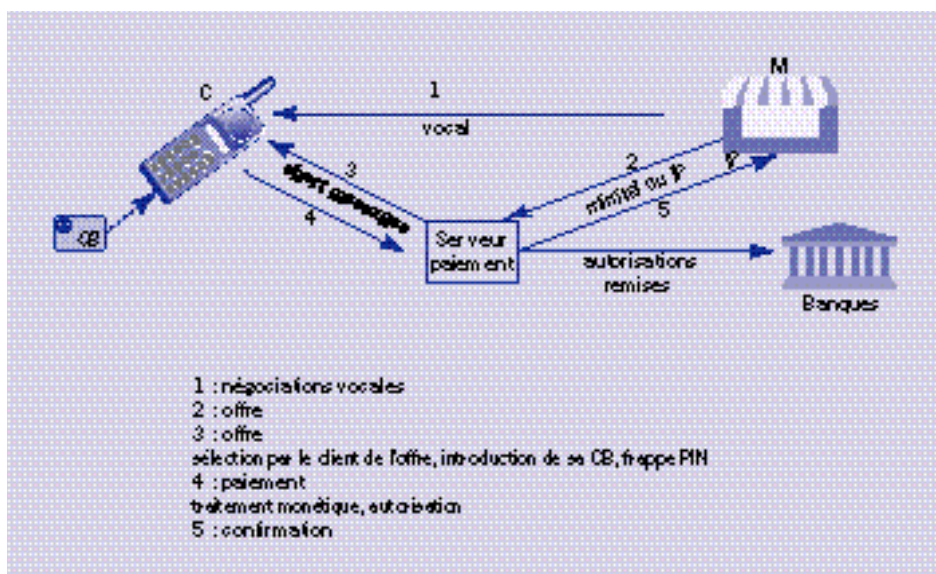


Figure 4 - Exemple de procédure de paiement avec un mobile GSM.

### Des exemples de services

Le portable étant actuellement avant tout un outil de communication vocale, le type de services envisagés avec les terminaux des générations actuelles concerne le paiement à distance entre un particulier et un commerçant, humain ou serveur vocal. Les "short messages" sont utilisés ensuite, pour officialiser l'accord entre le client et le vendeur sur les termes de la transaction, qui se traduit par une signature du client, calculée par sa carte. Ils remplacent par exemple la facture/devis papier et le chèque de la vie courante (figure 4).

Pour des générations futures de portables, qui sdeviennent de plus en plus d'assistants personnels, ou de PC, on pourrait également se rapprocher des services de commerce électronique sur Internet, grâce aux protocoles WAP ou HDML, qui rapprochent le portable d'un assistant personnel, voire d'un PC portable.

Sur ce sujet, FT et des instances bancaires coopèrent depuis avril 98, dans le but de définir des approches, des modes opératoires, des caractéristiques techniques adaptés.

### Porte-monnaie électronique

Des utilisations analogues à ce qui est décrit ci-dessus en télépaiement sont possibles ; certains pensent également à l'utilisation du PME pour payer les communications à l'opérateur Télécommunications ; cette possibilité est complexe sur un plan technique : elle requiert un contrôle par le réseau des paiements au fil de l'eau puisque rien ne permet de garantir la sécurité au niveau du Sim et du portable qui pourrait bloquer les demandes de débit du PME. Sur un plan marketing, l'anonymat de ce moyen de paiement ne va pas forcément dans le sens des intérêts de l'opérateur, qui ne gèrerait plus de relations clients ! Avec des mobiles bifentes, le rechargement du PME paraît par contre une fonctionnalité utile pour les usagers, et facile à réaliser !

## Les premiers pas du commerce électronique avec des mobiles

Voici quelques informations obtenues au "Global Mobile Commerce Forum" du 20/2/98 à Cannes. Il ne s'agit que de petits projets, qui explorent l'utilisation du mobile pour le paiement.

NB : de nombreux opérateurs offrent déjà des services à grande échelle, d'envoi d'informations d'une banque à son client, utilisant le mobile comme support, et les "short messages" comme vecteur. Il ne s'agit pas à proprement parler de commerce électronique, puisqu'il n'y a pas de paiement.

Mobi-Smart :

Ce projet est mis en œuvre par Téliat et PostGiro, en Suède ; il est réalisé sur portables Alcatel ou Ericson, phase 2+, avec un SIM gemplus contenant de plus une application SIM-Toolkit Mobi-smart. Le service offert concerne le virement du compte du client à un compte désigné (celui du prestataire que l'utilisateur veut payer). Le client choisit dans le menu du portable cette application, et compose le numéro de compte du prestataire, le montant, et un PIN spécifique ; le SIM calcule une signature de cet ordre, et l'envoi à un serveur. Le SIM reçoit un message (short message) de reçu de l'opération, qu'il peut stocker.

FSU-Powertel

FSU est la Florida State University ; Powertel est un opérateur US de mobiles GSM, sur 12 Etats du sud-est des USA. FSU opère, sur le campus de l'université (50 000 étudiants) un porte-monnaie électronique. Avec Powertel, ils sponsorisent une petite expérience associant le portable et ce PME. Le mobile Star-Tac de Motorola (Phase 2+) sert d'étui à une carte combinant la fonction Sim et PME, réalisée par Gemplus. La carte permet de payer des menus dépenses sur le campus, et de payer des services d'info sur Internet.

Avec le mobile, il est possible de charger un compte prépayé Powertel, et de recharger le PME. La taille du pilote est de seulement 50 personnes !

Nokia-Unisource

Ce consortium se base sur l'utilisation d'un mobile haut de gamme, un PDA, Nokia 9000, avec un lecteur de carte à puce externe, pour accueillir la carte PME Mondex. Les services offerts sont le rechargement du PME, et paiement de services d'information Internet. La taille du pilote serait d'une centaine de participants.

Moments

Il s'agit d'un projet européen mené par Nokia, et où l'un des participants est Gemplus. Comme dans le pilote FSU, on teste l'association sur une même carte à puce de la fonction Sim et d'une PME. De plus une plate-forme de services multimédia est accessible par les mobiles, et les informations consultées peuvent être payées par ce PME.

## Les plates-formes de commerce électronique

On constate que dans tous les systèmes de commerce électronique, basés sur des canaux tels que Internet, GSM, Minitel, avec des moyens de paiement carte bancaire, porte-monnaie électronique,... etc, un rôle central se crée naturellement, concernant des formes diverses de gestion des transactions électroniques. Les exemples précédents en attestent :

- Télécommerce et la plate-forme OMT,
- SET avec les passerelles appelées APG,

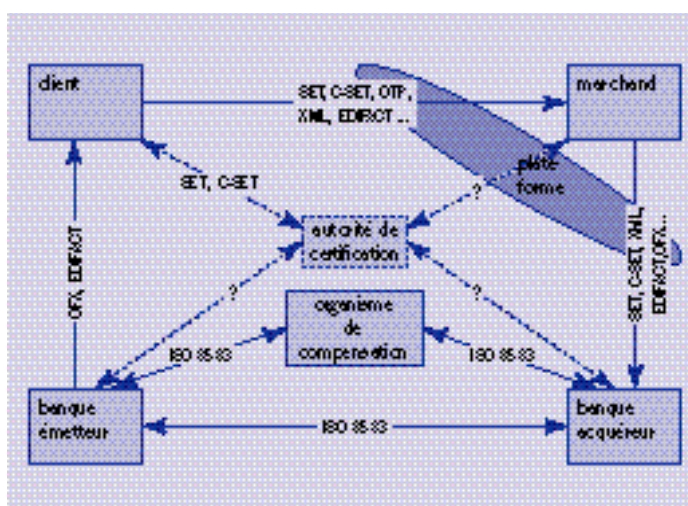


Figure 5 - Les protocoles du commerce électronique CF 8.

- le porte-monnaie électronique avec la nécessité d'un rôle de collecte et audit de la monnaie électronique.

Les fonctions rencontrées dans ces plates-formes informatiques dépendent du contexte considéré, mais on retrouve les caractéristiques ci-dessous :

- haute fiabilité, architecture "non stop" ;
- environnement sécurisé, firewalls... ; audit sécurité ;
- gestion technique de parcs de terminaux ou concentrateurs.
- gestion de base de clients, marchands, ...

Enfin, la variété des protocoles techniques utilisés est importante, mais des standards émergent, limitant un foisonnement qui risquerait d'être coûteux (cf. figures 5 et 6).

- France Télécom a été un artisan du développement de telles plates-formes, ces dernières années :

- Maccim est un serveur permettant d'agréger les paiements CB sur publiphone, et jouant le rôle de passerelle vers le monde "Bancaire" ;
- Sigma, dans le cadre du projet e-Comm micropaiement .

Apparaît donc une possible approche fédératrice du développement et de l'exploitation de ces plates-formes, couvrant (cf. figure 6) :

- les services offerts sur différents types de terminaux : "canaux de distribution" ;
- différents traitements de transactions, adaptés aux protocoles comme SET, C-SET, OFX, ... ;

- l'interfaçage avec les marchands, et la prise en compte de fonctions simplifiant sa tâche : fonctions logistiques, suivi de livraison, statistiques, ... ;

- les aspects sous-jacents aux traitement des transactions électroniques que sont la sécurité/gestion de clés/certificats/boîtes noires, l'archivage, le data mining, ... ;

- des fonctions d'exploitation de la plate-forme.

Cette approche, actuellement en évaluation, pourrait être génératrice d'économies, par la fédération d'investissements et de coûts de fonctionnement qu'elle pourrait sous-tendre. Elle pourrait également être prolongée par une offre tournée vers des besoins extérieurs à France Télécom.

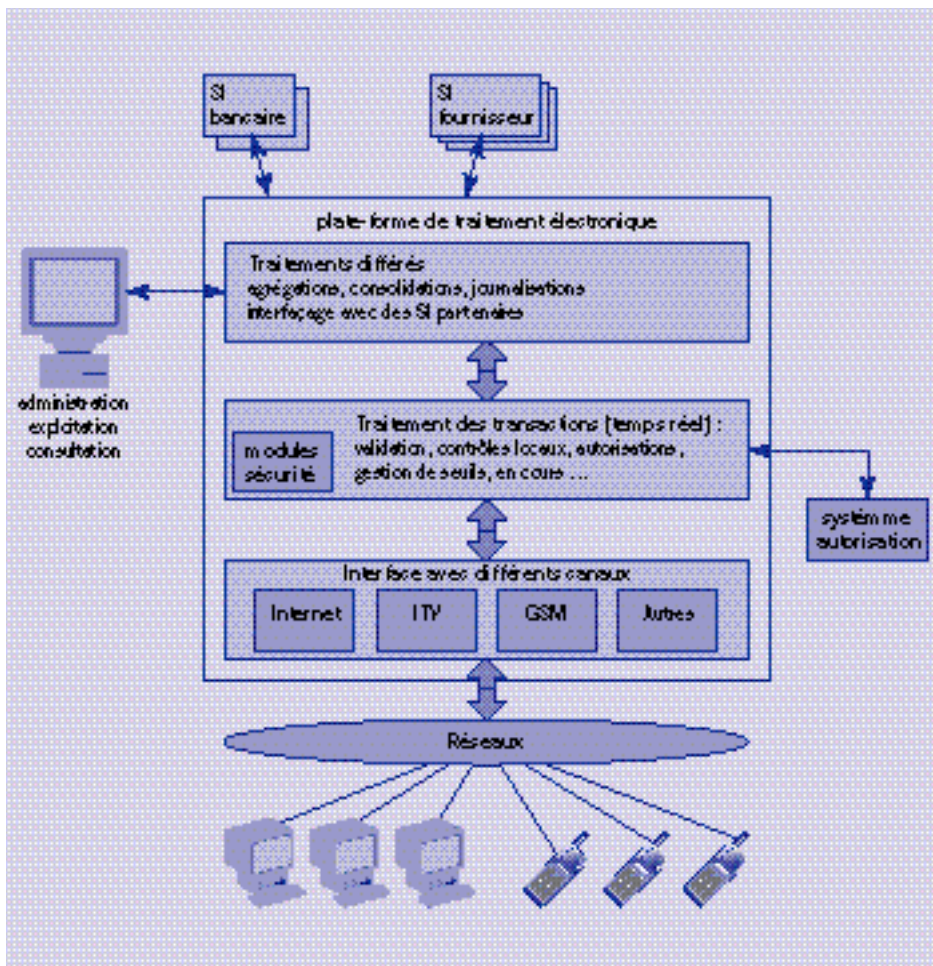


Figure 6 - Modèle généralisé de plate-forme de traitement des transactions électroniques.

---

## Références :

- [1] Electronic Payment International, juin 98, p. 10.
- [2] Rapport Lorentz.
- [3] Revue Times du 2/8/98.
- [4] XML : voir le site Web [w3.org/XML/](http://w3.org/XML/).
- [5] Etude Newscreen "le commerce électronique", juin 98.
- [6] Rapport Aftel "Internet , les enjeux pour la France" Edition 1998.
- [7] "Le commerce électronique : techniques et enjeux" P. Reboul et D. Xardel, , Editions Eyrolles, 1997.
- [8] CEN/TC 224 - ISO/TC 68/SC 6 : Group for Standardization on Electronic Commerce ; "Card-related secure commercial and financial transactions on open networks".
- [9] La lettre du commerce électronique et de l'E-Pub, n° 18, juin 98, p. 7.

## Abréviations

B to B ou B 2 B :	Business to Business
B to C ou B 2 C :	Business to consumer
CB :	carte bancaire
PME :	porte-monnaie électronique
VPC :	vente par correspondance
SET :	Secure Electronic Transaction
EMV :	Europay, Master-Card, Visa
OTP :	Open Trading Protocol
FT :	France Télécom
FTH :	France Télécom Hébergement
BNP :	Banque Nationale de Paris
CL :	Crédit Lyonnais
MF :	millions de francs
GF :	milliards de francs