Paiements à distance : les solutions sont multiples !

Il n'existe pas de solution unique pour sécuriser les paiements à distance. A court terme, les cartes virtuelles dynamiques sont un bon compromis pour relancer le commerce électronique. Mais la recherche d'une authentification forte devrait réhabiliter les solutions fondées sur la carte à puce.

BERNARD VAGINAY
Directeur marketing
Setib

En matière de vente à distance, il y a longtemps que les banquiers ont trouvé des solutions qui permettent de concilier les impératifs d'un acheteur qui ne veut pas payer avant d'être livré, et d'un vendeur qui ne veut pas expédier la marchandise avant d'avoir reçu le paiement. C'est ainsi que sont nés les crédits documentaires et autres lettres de crédit. La généralisation (il y a bientôt 9 ans !) de la diffusion des cartes bancaires à puce allait dans ce sens et a propulsé la France en tête du palmarès de la sécurité des paiements avec le taux de fraude sur les opérations par carte le plus bas du monde. La confiance de tous les acteurs (commerçants, acheteurs, banquiers) explique dans une large mesure la progression à deux chiffres du volume des opérations par carte en France, et ceci de façon constante depuis des années.

INTERNET, LE TALON D'ACHILLE DE LA VENTE À DISTANCE

Avec l'arrivée d'internet, il a fallu rapidement considérer que le potentiel du cybercommerce, qui utilise des procédures VAD (vente à distance) ne mettant pas en œuvre les dispositifs sécuritaires qu'offre la puce, allait immanquablement générer un nombre important de malversations et de litiges et faire trembler tout l'édifice. Le constat est là : les incidents se multiplient, largement relayés par les médias, et la défiance vis-à-vis du paiement on-line augmente rapidement. Conséquence : au moins trois internautes sur quatre abandonnent, en France comme ailleurs, leurs achats en ligne au moment de compléter la zone dans laquelle il faut saisir le numéro de carte, Talon d'Achille de tout le système de paiement. Et le commerce électronique ne décolle que très lentement.

MOINS DE RISQUE AVEC LES CARTES DE CRÉDIT

Le problème a pris une acuité particulière en France due à la conjonction de deux aspects. Les commerçants restent toujours les premières victimes de la répudiation des achats, ce qui ne les encourage pas à promouvoir les ventes par internet, mais de plus l'utilisation majoritaire de cartes de débit augmente aussi le risque sur les acheteurs. Alors que l'Américain du Nord possède 2,5

cartes de crédit en moyenne, le ratio est inférieur à 1 en France. En cas de fraude, avec une carte de débit, le porteur est devant le fait accompli. Avec une carte de crédit, au contraire, il décide s'il paie et comment il paie.

Cybercomm : un haut niveau technique mais un business model discutable

Il fallait donc trouver des solutions qui restaurent la confiance sur les transactions de e-paiement en conciliant les impératifs des commerçants comme ceux des acheteurs. Les banques françaises n'ont pas tardé à réagir puisque dés 1996, des structures étaient mises en place pour trouver une parade, mais ce n'est qu'en 2000 que la solution de convergence Cybercomm a vu le jour : un lecteur sécurisé permettant une authentification forte de la carte et de son propriétaire. Cette solution reste néanmoins contestée : elle affiche un haut niveau technique mais un *business model* discutable. Résultat : le marché national pourtant demandeur a sanctionné cette offre dont la diffusion reste confidentielle. Il peut paraître étonnant que cette solution, qui est actuellement la seule permettant d'appliquer toutes les clauses de garantie du contrat carte, n'ait pas trouvé sa dynamique. Elle recrée ainsi les conditions sécuritaires de l'achat de proximité qui avaient fait recette. Mais il faut croire que le marché a trouvé que ces conditions n'étaient pas suffisantes si elles n'apportaient pas, en plus simplicité, universalité et gratuité.

«Il existe aujourd'hui sur le marché mondial près de 400 solutions de paiement électronique sécurisé.»

Il n'existe pas de solution unique…

Ce rendez-vous manqué permet un examen de la gestion du risque transactionnel sous un angle différent. Le renforcement du «blindage» autour de l'instrument de paiement lui-même est-il la meilleure et la seule solution ? Un début de réponse vient du marché : il existe aujourd'hui sur le marché mondial prés de 400 solutions de paiement électronique sécurisé. Le spectre va certes du professionnel au folklorique, mais c'est aussi la preuve qu'une seule solution pour tous et pour tout est utopique.

Pour le court terme, la lutte globale contre la fraude utilisera une série de protections dédiées et complémentaires, c'est un peu le système des frappes chirurgicales des militaires d'aujourd'hui.

Si on positionne ces offres sur les trois dimensions du marché, du support et du risque, une panoplie de possibilités répond à une problématique donnée.

… du PME au cryptogramme visuel…

Les micro-paiements, par exemple, sont traités par un porte-monnaie électronique ou une carte prépayée si un support physique est requis. Dans le cas contraire, ce sera par un porte-monnaie virtuel. L'offre pour les paiements, à côté des solutions sur SSLv2 largement prédominantes, se divise en deux branches : les solutions orientées «commerçants» et celle orientées «clients». Pour les secondes, l'objectif est plutôt quantitatif et répond au souci d'augmenter le nombre d'acheteurs en ligne en restaurant la confiance. Il faut donc répondre à la demande de protection de l'information sensible qu'est le

numéro de carte afin de faire échec aux acheteurs indélicats en possession de numéros de cartes récupérés sur un site de «*carding*», détournés d'une boutique virtuelle ou recopiés d'une facturette… Les premiers exemples de solution sont les cryptogrammes visuels. Imprimés au verso des cartes et ne figurant nulle par ailleurs, ils garantissent contre les achats pour lesquels l'auteur n'est pas en possession physique de la carte. Les cartes disposant de ces cryptogrammes visuels sont déjà largement diffusées.

… POUR ABOUTIR À LA CARTE VIRTUELLE DYNAMIQUE

En suivant la logique, les banques et les réseaux émetteurs ont étudié un dispositif complémentaire : la carte virtuelle dynamique (CVD). Là encore le but n'est pas de traiter globalement la lutte contre la fraude mais de rassurer les internautes afin qu'ils augmentent leurs achats dans les boutiques virtuelles. Le concept est simple : pour qu'un numéro de carte ne soit plus détourné, il suffit de ne plus le transmettre et de le remplacer par une information à validité conditionnelle. A chaque achat en ligne (*encadré*), le porteur demande à sa banque de lui générer un numéro de carte virtuelle qui sera transmis au commerçant et qui lui permettra de faire toutes les vérifications habituelles sans que le numéro de sa carte réelle ne transite sur le réseau et ne puisse donc être stocké. Le numéro de carte virtuelle n'est valable qu'une fois et son détournement n'a plus aucun effet pour le porteur.

UN PROCÉDÉ OPÉRATIONNEL

Dans les systèmes les plus avancés, comme celui que le GIE Carte Bleue lance dans le courant de cet été, l'acheteur en ligne peut activer des options qui restreignent ou étendent son champ d'application (numéro de CVD restant valable n jours pour ce commerçant, par exemple, validité jusqu'à un seuil, etc.). Ce procédé est opérationnel depuis plus d'un an et a fait ses preuves dans plusieurs pays anglo-saxons (en Irlande notamment). Il semble promis à un réel succès dans la mesure où, à côté des solutions disponibles, il en existe plusieurs autres au stade d'annonce.

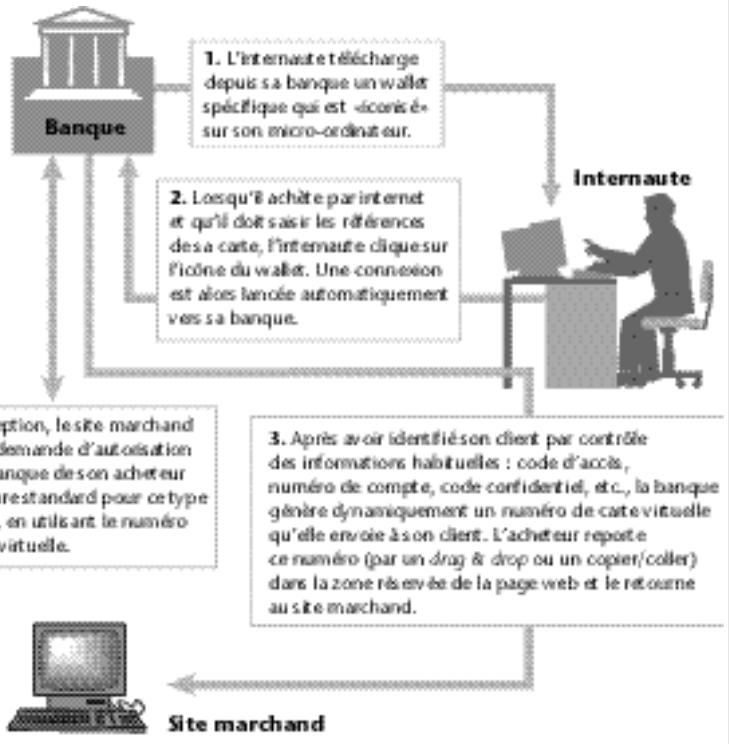
Aucun des promoteurs de ce type de solution ne prétend disposer de la solution miracle, en particulier pour les transactions venant d'un pays tiers. Pour le commerçant en particulier, il n'y a pas d'effet novatoire : on reste dans un système de VAD dans lequel la vente peut être répudiée. Mais la CVD, en plus de son bon compromis sécuritaire, dispose des critères d'acceptation que nous évoquions : simplicité, universalité et gratuité qui la positionne bien comme une solution alternative réaliste.

POUR UNE AUTHENTIFICATION FORTE, LA CARTE À PUCE RESTE EN COURSE

Il reste aux banques et réseaux émetteurs à en faire la promotion auprès de leurs clients internautes afin qu'elle trouve sa dynamique et que son succès stimule la recherche d'une nouvelle solution.

A cette occasion, on peut penser que le problème de l'authentification forte du client reviendra sur le devant de la scène et que la carte à puce sera à nouveau considérée comme une excellente solution d'identification, à condition de pouvoir l'exploiter. Dans cette perspective, il faut d'ores et déjà souligner que plus de 50 % de la population de l'UE possède un terminal capable de cela (et qui sert aussi à téléphoner). ●

Schéma d'ensemble d'un paiement par carte virtuelle dynamique



A aucun moment, le numéro de la carte réelle n'aura circulé sur le réseau internet. Il ne sera donc pas stocké sur un site marchand.