Yvon Avenel

Journaliste
Éditeur de
SmartcardsTrends

SERVICES FINANCIERS

Banque en ligne entre confort et sécurité

L'essor de la banque en ligne est une réalité. Reste à savoir quelle offre proposer sur ce canal : services de masse ou approche marketing plus de créative. La sécurité est également un paramètre important : la profusion des méthodes d'authentification disponibles n'aura sans doute qu'un temps. Le marché tranchera et, dans ce domaine le choix des banques sera déterminant.

L'essor de la banque en ligne n'est plus un sujet de prospective. Les chiffres le montrent : les services bancaires accessibles via Internet depuis un PC – et dans une moindre mesure grâce au téléphone mobile ou à l'utilisation d'un décodeur de TV numérique – sont devenus sans doute aujourd'hui le premier service de e-commerce au monde. Selon une étude récente de Datamonitor, 58 millions de titulaires de comptes en ligne en Europe cette année, soit environ 36 % des utilisateurs d'Internet; 53 millions d'Américains, selon le Pew Internet & American Life Project, soit 44 % des utilisateurs d'Internet. La croissance a été depuis 2000, en moyenne de 24 % par an en Europe, et un peu plus forte aux États-Unis, de l'ordre de 34 % de moyenne annuelle. IDC prévoit qu'elle devrait être encore plus importante au cours des deux ou trois ans à venir, particulièrement en Asie où le taux de croissance d'ici 2007 est annoncé autour de 300% ! Les chiffres le montrent aussi : la principale raison de ce succès tient à la facilité d'accès et d'utilisation des services en ligne, au confort qu'ils procurent. La "convenience" disent les Anglo-Saxons. Cette raison est d'ailleurs nommément citée (79 %) avant le gain de temps (71 %), et la capacité à mieux gérer ses comptes (52 %) dans un sondage effectué en février dernier par Pew qui dissèquent les motifs de l'utilisation des services bancaires en ligne. D'où également le lien direct naturel qui existe entre les utilisateurs d'Internet qui disposent d'un accès large bande (ADSL), et les titulaires d'un compte bancaire en ligne. Selon Pew, ils sont en effet 63 % à disposer d'un compte en ligne parmi les utilisateurs d'un accès large bande, contre 32 % parmi les utilisateurs d'une simple liaison RTC. Le PC reste par ailleurs le moyen d'accès privilégié à ces services également pour des raisons de confort d'utilisation, bien que le téléphone mobile représente déjà quelque 27 millions d'utilisateurs en Europe, et connaît une croissance moyenne annuelle de 124,3 %, selon l'étude déjà citée de Datamonitor. L'émergence des technologies 3G (3e génération de téléphones) et un peu plus tard 4G, offrant des débits de type large bande en sans fil, avec des appareils de type PDA (Pocket PC, et autres ordinateurs de poche), pourraient au cours des prochaines années apporter un confort similaire à celui des PC d'aujourd'hui, mais avec en plus la mobilité. L'utilisation des décodeurs de TV numérique pour accéder à des services bancaires en ligne connaît elle aussi, en Europe une forte croissance (90,5 % en moyenne par an depuis cinq ans). Le nombre de titulaires de comptes bancaires en ligne utilisant ce moyen en Europe atteint 9,8 millions cette année, selon Datamonitor. Dont une bonne part (environ un demi-million) en Grande-Bretagne.

DES DISPARITÉS SELON LES PAYS, LES CLASSES D'ÂGE, LES REVENUS…

La croissance du nombre d'utilisateurs de services bancaires en ligne cache des disparités qui peuvent être importantes selon les pays, mais aussi selon les classes d'âges et les niveaux de revenus. L'ergonomie, le confort d'accès et d'utilisation sont, certes, des motifs d'adhésion largement partagés, mais ils se composent aussi avec d'autres raisons, des contextes différents où les taux d'équipement et la culture jouent aussi leur rôle. Comme le soulignait en septembre dernier lors d'une conférence de l'Atelier [1], Laurent Cornu, responsable CRM chez IBM Consulting, *"les Anglais ont en Europe, deux fois plus recours aux services d'assurances en ligne que la moyenne."* Questions de culture et de tradition de services. L'étude Datamonitor souligne de son côté des grandes différences entre les marchés fran-

> *« Les internautes ont deux fois plus confiance sur un site bancaire que sur un autre site. Il faut utiliser ce capital pour développer des services, voire vendre des produits non financiers, comme des voyages, des loisirs, des abonnements à des journaux. »*

çais, italien, allemand et scandinave dans le développement de la banque en ligne. Les pays nordiques où le taux d'équipement en PC et accès Internet (et en téléphones mobiles), et le développement des services en ligne bancaire sont très élevés, connaissent bien sûr un taux de croissance de ces services plutôt faible, de l'ordre de 5 %, alors que la France et l'Allemagne suivent une évolution comparable entre 28 et et 25 %, et que l'Italie connaît-elle sans doute la plus forte croissance en Europe (55,3 %).

Le confort d'utilisation, c'est aussi la sécurité. Au moins si l'on considère que la sécurité, ou la confiance dans les services que l'on utilise sont une partie essentielle du confort de leur utilisation. Quels services en ligne ? Quelle sécurité ? La réponse à ces deux questions impose souvent des compromis. La sécurité est une partie du confort d'utilisation des services en ligne, mais elle peut être aussi parfois un motif de restreindre la richesse fonctionnelle et l'intérêt de ces services. L'impossibilité, par exemple, sur certains sites bancaires de

> *« Les services Internet ont besoin d'être segmentés, même s'il apparaît, sur Internet comme ailleurs que ces services, peu importe leur contenu, ont d'abord à voir avec la mise en place d'une chaîne de confiance. »*

pouvoir effectuer des virements de comptes à comptes si ces derniers ne sont pas associés – une contre-mesure *antiphishing* –, en est un exemple. Des études montrent parfois de façon contradictoire, l'impact des problèmes de sécurité sur le développement de la banque en ligne. Une étude de Gartner parue en juin dernier, et portant sur les comportements d'achats de 5 000 internautes américains révèle que les trois-quarts des personnes interrogées se disent plus méfiantes qu'il y a un an. Des résultats confirmés par une autre étude réalisée au même moment par The Conference Board signale que 54 % des personnes interrogées se disent également moins confiantes qu'il y a un an dans la façon dont sont protégées leurs données personnelles. Mais une troisième étude, parue encore au même moment, et conduite cette fois-ci par Yahoo plus précisément sur l'utilisation des services bancaires, montre que deux tiers des personnes interrogées (2 687 personnes) ne se sentent pas concernées par les risques d'usurpation d'identité signalés sur Internet. Parmi celles-ci, 64 % d'entre elles disent consulter leurs comptes bancaires le plus souvent sur Internet, et 56 % ont recours à Internet pour gérer et contrôler leur portefeuille d'investissements. Elles étaient 20 % à affirmer que les risques de fraude ne les avaient pas dissuadées d'utiliser leurs services financiers en ligne. Une étude, conduite cette année par Forester Research, était pourtant parvenue à des conclusions opposées en affirmant que 14 % des personnes interrogées avaient cessé toute utilisation de leurs comptes en ligne, suite aux informations publiées sur les risques de fraude liées aux techniques d'usurpation d'identité sur Internet (*phishing*).

Chez Vasco Data Security, une société belge fournisseur de solutions d'authentification forte pour les banques en ligne, leader dans ce domaine avec 17 millions de *tokens* (certificat d'authentification) déployés à ce jour, a vu son chiffre d'affaires décoller en 2003, précisément au moment où le phishing connaissait un essor sans précédent. *"Indéniablement, il s'est produit à ce moment-là un déclic, mais nous nous attendons dès cette année à un boom du marché encore plus fort que les années précédentes"*, souligne Jochem Binst, l'un des responsables de la société qui voit également dans la migration EMV, l'un des moteurs de cette évolution.

SÉCURITÉ PERÇUE : UN ÉLÉMENT DE CONFORT

"La sécurité est un facteur clé, mais il convient de faire la différence entre la sécurité effective et la sécurité perçue", souligne Jérôme Ajdenbaum, responsable marketing à la Business Unit services financier de Gemplus, et contributeur de la spécification CAP (*Chip Authentication Program*). La réalité de la fraude due au *phishing* et à ses variantes comme le *pharming* (*voir glossaire*), et aux attaques diverses de virus de type *keylogger*, doit être distinguée des craintes et des sentiments de méfiance que ces menaces inspirent aux internautes. Comme dans bien des domaines, la menace est souvent plus forte que sa réalisation. *"Globalement, les internautes ont deux fois plus confiance sur un site bancaire que sur un autre site. Il faut utiliser ce capital pour développer des services, voire vendre des produits non financiers, comme des voyages, des loisirs, des abonnements à des journaux, etc."*, remarquait Laurent Cornu, lors de la conférence de l'Atelier, déjà citée. Mais le capital confiance n'est jamais vraiment acquis. Il faut l'entretenir.

À l'heure où les banques – et notamment les banques françaises – redéploient leur réseau d'agences avec une vision désormais multicanal, le développement de la banque en ligne se trouve confronté à de nouvelles opportunités, mais aussi à des défis inédits. Qui sont tout à la fois économiques, marketing, techniques et organisationnels.

QUELS SERVICES ? POUR QUELS CLIENTS ?

Le succès et l'avenir des services en ligne sont imprévisibles. La déclaration d'impôt sur Internet a surpris par son ampleur (environ 4 millions de transactions cette année contre 1,3 million en 2004). Tout est donc ouvert. Faut-il réserver à l'agence tous les services à forte valeur ajoutée, et confier à la banque en ligne tous les services simples qui réclament peu d'interactivité, mais permettent d'économiser sur les coûts administratifs ? L'approche économique a de quoi convaincre avec des gains de coûts significatifs (par exemple sur la dématérialisation des extraits ou des comptes mensuels, de l'ordre de 60 centimes d'euros avec une version pdf), mais l'approche marketing peut inviter à plus de créativité. *"Autant l'Internet donne en termes d'achat de produits, des taux de succès très faible, autant il est un bon levier pour capitaliser sur l'enchaînement des cycles de réachats. On peut ainsi via des pop-up, au moment de la consultation du compte, proposer de nouveaux produits très ciblés"*, souligne Joël Nadjar, Partner Accenture pour la banque de détail. Mais cela suppose aussi une bonne connaissance du client, et des outils de CRM bien intégrés à la plateforme Web. La SSII travaille ainsi en phase avancée depuis plusieurs années sur les évolutions combinées des différents canaux de la relation client dans la banque de détail. En 2002, son étude sur ce sujet avait mis en évidence plusieurs catégories de clients (6 profils) parmi lesquels ceux qui réclamaient avant tout de la disponibilité des services et manifestaient la volonté de garder le contrôle de la relation avec leur banque pour les conseils étaient ceux qui privilégiaient bien évidemment les services via le Web et les alertes ou communications par e-mails. Mais ils n'étaient que 8 %... Dans ce panel, un autre profil, représentant 17 % de la population interrogée, était décrit comme plutôt pro-Internet : il s'agissait de ceux qui recherchaient l'utilisation des canaux les plus économiques (GAB, téléphone, Internet), pour de simples services et très peu de conseils. On le voit les services Internet ont aussi besoin d'être segmentés, même s'il apparaît, sur Internet comme ailleurs que ces services, peu importe leur contenu, ont d'abord à voir avec la mise en place d'une chaîne de confiance.

SOLUTIONS D'AUTHENTIFICATION

■ **RSA Security** et **Aladdin Knowledge** proposent des solutions d'authentification forte qui font appels à des tokens (calculettes). **Vasco Data Security** et **Xiring** montrent des solutions avec des lecteurs de cartes à puce qui utilisent les secrets de la carte pour calculer le mot de passe.

LE COFFRE-FORT ÉLECTRONIQUE : UNE PREMIÈRE ET UN EXEMPLE

L'un des services les plus inédits et les plus emblématiques qui ait été mis en œuvre à ce jour est celui de coffre-électronique, développé par la banque OBC (Groupe ABN AMRO), une banque d'affaires et de gestion de patrimoine. Cette réalisation a d'ailleurs reçu le Trophée de l'innovation de la FNTC (Fédération nationale des tiers de confiance) l'an dernier. De quoi s'agit-il ? D'une réplique électronique et télématique des services de location de coffres-forts bien physiques ? Un peu plus. Ce service en effet tire toutes les conséquences du cadre juridique et réglementaire sur la signature électronique et la dématérialisation des documents réclamant traçabilité et partage de preuve (voir l'interview de Jean-Pierre Doussot, le directeur adjoint de la banque OBC). Il répond notamment au décret du 16 février 2005-137, qui stipule que toute facture dématérialisée d'un montant supérieur à 120 euros doit être conservée pendant dix ans. Il confirme en outre la banque dans son rôle de tiers de confiance. *"C'est presque une mission d'État, au fort caractère notarial"*, souligne Jean-Pierre Doussot. Grâce à une interface Web développée par la société Avallone, un éditeur de solutions pour la banque, spécialisée dans la sécurisation des transactions, une entreprise ou un particulier peut stocker ses factures, ses polices d'assurance, l'estimation de ses biens, ses fiches de salaires, ses messages vocaux, ses disques durs, ses photos, etc., avec des garanties de conservation de cinq, dix ou trente ans [2]. La signature électronique et l'authentification forte se font grâce à l'utilisation de cartes à puce dans laquelle est stocké un certificat numérique acquis par le titulaire de la carte auprès d'une autorité de certification. Ce service présente du coup l'intérêt de proposer un modèle pour l'authentification forte. Et pas seulement un modèle technique, mais aussi organisationnel, puisqu'il est construit comme un service monétique, et qu'il invite, pour son implémentation et sa maintenance, à passer la main, au sein des banques, aux "monéticiens" plutôt qu'aux informaticiens, jusque-là plutôt promoteurs des solutions login/mot de passe encore largement déployées dans le monde du PC. Enfin, il apporte une réponse économique – c'est viable et productif - et réglementaire vis-à-vis des recommandations de Bâle II sur la maîtrise du risque opérationnel. La traçabilité et le partage de la preuve – l'opération n'est ni copiable ni rejouable – sont assurées.

AUTHENTIFICATION : LE MODÈLE "MONÉTIQUE"

À l'instar des services de coffre-fort électronique, le déploiement de services de banque en ligne implique la mise en œuvre conjuguée de moyens d'authentification qui permettent à l'utilisateur d'être reconnu et identifié par sa banque, mais aussi à ce dernier d'avoir l'assurance qu'il est bien sûr le site Web de sa banque, et qu'il y est en sécurité. Après des années d'utilisation de login/mot de passe, les banques françaises sont peut-être en train d'adopter un modèle "monétique" à base de carte à puce. La très grande majorité d'entre elles ont récemment passé en effet des appels d'offres pour des solutions d'authentification à base de CAP (*voir le glossaire*) basée sur l'utilisation d'un lecteur non connecté de carte EMV. Il y a à cela plusieurs raisons dont la plus évidente est la migration EMV. Le "retour" de la carte à puce comme moyen

> *« Le "retour" de la carte à puce comme moyen d'authentification fort se fait cette fois-ci en douceur. »*

d'authentification fort se fait cette fois-ci en douceur. Tous les obstacles qui avaient, en leur temps, fait trébucher lourdement l'opération Cybercomm [3] sont maintenant écartés. La problématique du lecteur connecté, associé à la mise en place d'une hot-line coûteuse, et sans doute souvent impuissante à régler tous les caprices de l'univers Windows, est résolue : la solution d'authentification associée à la carte EMV peut utiliser un lecteur non connecté de type "transparent", bon marché. La problématique du coût est également résolue deux fois : une fois parce que le coût de ce lecteur "connecteur" n'a plus rien à voir avec celui du lecteur Cybercomm, intelligent certes et très sécurisé, mais cher à

faire fabriquer (autour de 400 francs à l'époque). Une seconde fois, puisque la carte à puce utilisée est déjà "payée" dans le processus de son émission (fabrication, personnalisation et logistique) normale en tant que carte de débit/crédit classique. Enfin, la problématique des spécifications trop franco-françaises et de leur compatibilité avec les standards internationaux (à l'époque, il s'agissait d'une lourde architecture de paiement sécurisée baptisée SET avec sa version C-SET pour la carte BO') est résolue. Les spécifications de CAP (*Chip Authentification Program*), définies depuis 2001 par Visa et MasterCard avec le concours d'experts de l'industrie de la carte à puce, sont des spécifications internationales que l'on peut qualifier de "légères". Il s'agit en fait d'une application (applet) ou de réglages de certains paramètres qui n'ont pas d'incidence sur la capacité mémoire des cartes à puce EMV ni sur leurs prix. Une mémoire de 4 Ko suffit.

TOKEN OTP, MATRIX OU CARTE AVEC CERTIFICAT

CAP n'est pas, bien sûr, à ce jour la seule solution d'authentification pour accéder aux services de banque en ligne. Des sociétés comme RSA Security, Aladdin Knowledge, ou Rainbow – aujourd'hui Safenet – ont aussi des solutions d'authentification forte (à deux facteurs) qui font appel à des *tokens* (calculettes), utilisant souvent des microcontrôleurs de cartes à puce pour calculer des OTP (*One Time Password*) à partir d'un secret contenu dans la carte, d'un aléa et d'un PIN code. Une solution assez similaire à celle proposée avec CAP, mais sans EMV et sans carte à puce dans la plupart des cas. Vasco Data Security et Xiring ont pourtant montré depuis plus d'un an des solutions à base de *tokens*, lecteurs de cartes à puce, qui utilisent les secrets de la carte pour calculer le mot de passe. Le niveau de sécurité atteint de cette façon est bien supérieur à celui des mots de passe statiques (copiables et rejouables) utilisés encore en majorité pour accéder aux sites bancaires. Des sociétés proposent également des grilles de papier ou cartes plastiques (Matrix) sur lesquelles sont imprimées des séquences utilisables de façon pseudo-aléatoire comme mots de passe (une sorte de OTP pré-calculés), et qu'il faut réimprimer lorsqu'elles ont été complètement utilisées. Un ingénieur de Vasco a montré que cette méthode permettait à des hackers un peu exercés de trouver rapidement tous les chiffres de la grille par la simple écoute d'un certain nombre de réponses et des challenges échangés sur Internet. Enfin, il existe des *tokens* plus "faibles" que les *tokens* OTP, dont l'objet est surtout d'offrir un service de confort par rapport à l'utilisation de mots de passe classiques qu'il faut mémoriser, en permettant de stocker ces mots de passe dans la mémoire flash de *token* dont l'accès est généralement contrôlé par un mot de passe unique. Certainement mieux que le post-it collé sur l'écran de l'ordinateur, mais encore vulnérable aux attaques des logiciels de type *keylogger* puisque les mots de passe sont statiques, donc copiables et rejouables. Enfin, il existe enfin des solutions à base de cartes à puce et de lecteurs avec clavier et afficheur sécurisés utilisant des certificats dont le niveau de sécurité est des plus élevés. Contrairement à l'utilisation de certificats stockés dans un PC et géré par Windows, aucune entorse à la validité ou la pseudo-authenticité des certificats n'est alors permise. La biométrie fait également son apparition dans les *tokens* (chez Giesecke & Devrient) qui peuvent intégrer un capteur d'empreintes digitales en remplaçant du coup, le besoin de lecteur équipé de clavier. L'empreinte remplace la frappe du code PIN.

La profusion des méthodes et des moyens d'authentification forte ou faible disponibles sur le marché n'aura sans doute qu'un temps. Le marché va trancher et, dans ce domaine le choix des banques sera déterminant. Par ailleurs, des travaux sont en cours pour assurer une forme d'interopérabilité des moyens d'authentification par-delà les types de moyens utilisés. L'OATH (*Open AUThentication Initiative*) est ainsi en train de proposer à l'IETF, un algorithme standard (HOTP) pour générer des OTP. Et la façon de les calculer, de les vérifier, les mécanismes, les commandes et les messages qui doivent être implémentés et mis en œuvre font également l'objet de travaux de standardisation autour de la spécification PKCS#11. Les OTP, tout comme CAP, supposent des serveurs (et des HSM dédiés) spécialisés qui à l'avenir auront besoin de communiquer. Les offres complètes (cartes ou *tokens*, avec les serveurs) se multiplient en ce moment, signe que le marché est sur le point de décoller. ■

GLOSSAIRE

■ **CAP** (*Chip Authentication Program*) : méthode d'authentification spécifiée par Visa et Mastercard basée sur l'utilisation de lecteur non connecté (une version connectée est néanmoins possible) et de clés spécifiques stockées dans la carte EMV et distinctes des clés utilisées pour le paiement avec les méthodes SDA ou DDA/CDA. À l'insertion de la carte, l'utilisateur est invité à entrer son code PIN. La carte calcule alors un mot de passe numérique (de 4 à 12 chiffres, ce paramètre est réglable) que l'utilisateur entre au clavier de son PC et qui est vérifié par un serveur distant, synchronisé dans le temps.

■ **OTP** (*One Time Password*) : une méthode d'authentification basée un algorithme de type SHA-1, MD4 ou MD5 (hachage) et qui permet de calculer à partir des mêmes secrets, des mots de passe à chaque fois différents (par un système de compteur), qui sont reconnus par un serveur distant synchronisé dans le temps.

■ **Phishing sécurisé :** Cette attaque de phishing est basée sur l'utilisation d'un "vrai-faux" certificat numérique SSL qui force Windows à ouvrir la boite de dialogue de contrôle du certificat pour indiquer que le visiteur est sur un site Web soi-disant sécurisé mais qu'il peut néanmoins accepter de continuer en cliquant sur OK. Ce que font généralement la plupart des utilisateurs.

■ **Le pharming** utilise les techniques de phishing combinées à des attaques sur les caches des serveurs DNS en agissant sur le lien faible entre l'adresse IP et le nom de domaine d'un site web.

■ **Keylogger :** logiciel espion capable de tracer sur un PC l'activité d'un utilisateur à son insu, et le cas échéant de reconnaître la frappe d'un mot de passe, et de le capter pour le réutiliser.

NOTES

[1] L'intégration du "cyber-client" dans les services bancaires en partenariat avec IBM et Siebel.
[2] Le stockage est assuré par la société IX Europe dans des "data centers" régis par une réglementation très sévère (redondance des lieux de stockage dont la distance est suffisante pour diviser les risques, etc.)
[2] Projet lancé dans les années 1998-2000 qui avait spécifié un lecteur de cartes à puce pour effectuer des paiements sécurisés sur Internet et qui répondait au standard SET développé par Visa et Mastercard. Ce lecteur était en fait conforme à la spécification C-SET, compatible à l'époque avec la version SET logicielle et la carte bancaire française BO'.