Yvon Avenel
Journaliste
Éditeur de
SmartcardsTrends

SÉCURITÉ

La banque et le paiement en ligne préparent un Internet plus sûr

Les banques françaises s'apprêtent à déployer des solutions d'authentification forte pour leurs services en ligne. La suite logique de la mise en place de 3D Secure, de l'essor du *e*-commerce et de la lutte engagée depuis de longue date contre la fraude sur Internet.

La décision des banques françaises de généraliser la mise en œuvre de 3D Secure pour les opérations de paiement sur Internet depuis le 1er octobre dernier sera sans doute à marquer d'une pierre blanche. Même si cette décision, dans sa phase initiale, ne réalise pas encore pleinement sa promesse – authentifier fortement et formellement le porteur de la carte (*voir plus loin*) en ligne – elle figure désormais comme une étape importante d'un processus déjà très actif en Europe, et désormais en France. Il conduira tôt ou tard à la constitution d'un ou de modèles d'authentification des clients de la banque en ligne et du *e*-commerce, qui pourront préfigurer celui d'un Internet dont l'accès et les services seront plus sûrs et fonctionnellement encore plus riches.

LA FRANCE RATTRAPE SON RETARD EN EUROPE

Comment ce ou ces modèles vont-ils se constituer, se déployer et se généraliser en France ? Comment l'expérience acquise ailleurs sera-t-elle valorisée ? Verra-t-on, à l'instar de ce qui s'est produit dans le domaine du paiement avec EMV puis avec les normes PCI pour la sécurité des données, émerger un standard bancaire, voire "universel" d'authentification en ligne ? Toutes ces questions mettront sans doute encore quelques années à trouver leurs réponses. Pour l'heure, force est de constater qu'elles sont au cœur des réflexions et, déjà, des prochaines mises en œuvre des banques françaises dont la maturité dans ce domaine tardait paradoxalement à se manifester, alors que ces banques mêmes s'étaient, dans le domaine du paiement et de la lutte contre la fraude, montrées par le passé aux avant-postes en Europe et dans le monde. Marc Andries, le chef du service des moyens de paiements scripturaux (*voir l'interview en page 51*) de la Banque de France dont le rôle incitatif dans ce mouvement aura été aussi décisif, qui prédit l'imminence des premiers déploiements "massifs" dans notre pays de solutions d'authentification forte pour accéder aux services de banque en ligne, souligne par ailleurs que "*la mise en œuvre par les banques françaises de ces solutions leur permettra de se situer au meilleur niveau des pays européens en ce domaine*". Avec le SEPA, l'émergence d'une Europe des paiements unifiée et plus concurrentielle apparaît avec la lutte contre la fraude – et notamment la mise en œuvre de 3D Secure – l'essor du *e*-commerce, comme l'un des facteurs clés des évolutions que l'on constate aujourd'hui en faveur de solutions d'authentification forte en ligne pour les clients de la banque. Benoît Grangé, en charge des développements logiciels chez Vasco Data Security International, l'un des plus importants fournisseurs mondiaux de solutions d'authentification "tout terrain", rappelle en effet incidemment que les banques du Benelux, et de certains pays nordiques en sont déjà à leur troisième génération de déploiements de ce type de solutions, alors que d'autres pays n'ont pas encore sauté le pas. La Grande-Bretagne s'est lancée, il y a un plus d'un an, dans le déploiement de plusieurs millions de lecteurs de cartes EMV-CAP fortement recommandés par l'APACS, sur la base d'une spécification que l'association professionnelle des industries du paiement a elle-même développée [1]. Mais la différence traditionnelle entre les pays du nord de l'Europe, précurseurs du *sweet-home banking* – peut-être tout simplement

[1] L'APACS a développé une spécification d'authentification pour la banque en ligne et le *e*-commerce, basée sur celle de MasterCard (CAP), également adoptée par Visa (DPA), qui fait donc appel à des secrets présents dans la carte EMV.

SOLUTIONS LOGICIELLES OU MATÉRIELLES

Vers un standard pour l'authentification en ligne ?

■ Le marché de l'authentification est devenu en quelques années, comme celui de la carte à puce, un marché de volume. Ce marché est largement dominé par une offre de solutions logicielles. Selon Vasco Data Security International, on devrait compter cette année dans le monde un peu plus de 1,5 milliard d'utilisateurs qui font appel, pour plus de 85 % d'entre eux, à ces solutions logicielles pour contrôler et gérer des identifiants et des mots de passe. Dans environ 70 % des cas, ces solutions sont mises en œuvre dans des applications d'entreprises (accès logique). Pour 25 % des cas, elles sont appliquées à l'accès à des services de banque en ligne. Le restant concerne des applications souvent très sensibles de B2B.

En valeur, la part des solutions à base d'équipement matériel (calculette, clés USB, lecteurs de cartes) était, en 2008, de l'ordre de 700 à 750 millions de dollars, pour un marché global estimé à 1,5 milliard de dollars. En dépit d'une part de marché encore faible en unités, les solutions matérielles représentent donc un marché qui est en valeur quasiment égal à celui des solutions logicielles. Vasco prévoit que ce marché dépassera, dès l'an prochain, celui des solutions logicielles pour atteindre en 2013, une valeur supérieure à 2,5 milliards de dollars en adressant pas loin de 3 milliards d'utilisateurs qui seront encore majoritairement des entreprises (un marché de plus de 1,8 milliard, soit 41 % du marché global de l'authentification forte, tandis que le marché strictement bancaire approcherait alors le milliard de dollars (22 % du marché).

La montée en puissance des solutions matérielles et la diversification des applications qui requiert des moyens d'authentification forts ne signifient pas la fin des solutions logicielles, mais un redéploiement de l'ensemble de ces solutions sous la forme de plateformes de services. La généralisation dans le domaine du paiement d'un standard comme EMV, devrait favoriser l'émergence d'un standard que CAP (Chip Authentication Program) est peut-être en train de devenir*. L'APACS en Grande-Bretagne a créé sans doute un précédent en Europe en construisant sa spécification nationale sur ce standard. Des travaux dans le droit fil de ceux menés outre-Manche sont menés en France par le groupement Cartes Bancaires et, au niveau européen, le sujet a déjà été abordé au sein de l'EPC, mais sans véritable conclusion.

*** Xiring estime qu'à l'horizon 2013, on devrait compter 60 millions d'utilisateurs de solutions EMV-CAP en Europe. On estime aujourd'hui le potentiel du marché européen des utilisateurs de services de banque en ligne à 100-110 millions de personnes (13 millions en France).**

En valeur, la part des solutions à base d'équipement matériel (calculettes, clés USB, lecteurs de cartes) représentait en 2008 environ 50 % du marché global de l'authentification en ligne. Elle devrait dépasser dès 2009 la part des solutions logicielles.

pour des raisons climatiques – et les pays du sud – très attachés à leur agence bancaire – est donc manifestement en train de s'estomper sous la pression du développement des services Web et du *e*-commerce. L'Italie a déjà déployé plusieurs centaines de milliers de lecteurs sécurisés [2], et l'Espagne suit le mouvement. Reste la France et, dans une certaine mesure, l'Allemagne. On sait que dans l'Hexagone, au moins deux grandes banques sont sur le point de mettre en place ces solutions et que toutes les autres poursuivent leurs campagnes de tests. "*La France est en train de combler son retard en Europe. Nous avons signé un contrat pour la livraison de 400 000 lecteurs de cartes qui sont passe d'être déployés. Comme d'habitude, certaines banques sont un peu plus en avance que les autres et créent le mouvement*", confirme de son côté Laurent Maître, en charge du *business development* de Xiring, le premier fournisseur en Europe de solutions d'authentification à base de CAP-EMV. "*Le marché français va démarrer cette année et nous verrons vraisemblablement des déploiements plus importants en 2010*", corrobore Cédric Collomb, *senior* vice-president Identité et gestion d'accès chez Gemalto, le premier fabricant mondial de cartes à puce. Cédric Collomb pointe néanmoins quelques incertitudes qui demeurent sur les types de solutions qui seront finalement adoptés.

LA FRAUDE, MAIS SURTOUT LE *E*-COMMERCE

Les banques françaises ne découvrent pas aujourd'hui les solutions d'authentification forte déjà déployées dans d'autres pays : calculettes (*tokens*), lecteurs de cartes à puce, clés USB... Ces supports, dont les évolutions techniques sont testées régulièrement, ont déjà été mis en œuvre pour des clients "entreprise", et bien souvent pour des opérations beaucoup plus sensibles que le simple accès aux données d'un compte en ligne. Ce qui est nouveau, c'est leur extension annoncée à la banque de détail pour laquelle, jusqu'ici, les efforts ont principalement consisté à protéger les identifiants et mots de passe statiques de façon à rendre de plus en plus diffici-

[2] La Poste Italienne s'est récemment équipée de 700 000 lecteurs Xi-Sign 4 000 de Xiring.

les leur capture par d'éventuels fraudeurs. Les raisons de cette évolution fortement encouragée par la Banque de France et les institutions de régulation sont multiples. L'évolution des techniques de fraude (le *phishing*, le *pharming* et les *keyloggers* et autres chevaux de Troie) a montré les limites [3] de ces solutions tout en soulignant que les données bancaires (numéros de carte de paiement, de compte et codes d'accès) restent les principales cibles des organisations cyber-criminelles et sont en nombre et en valeur les premières données qui soient "commercialisées" et exploitées par ces organisations. Mais ce n'est pas la seule raison. L'importance de la fraude liée à des usurpations d'identité sur les sites de banques en ligne ne fait pas encore l'objet de mesures spécifiques de la part de l'Observatoire de la sécurité des paiements et ne figure pas, semble-t-il, parmi les domaines les plus sensibles. Cependant, les liens avec la fraude qui touche le paiement plus directement (les virements) créent des contraintes qui se traduisent par des restrictions de services, qui font, du coup, aussi partie des contre-mesures nécessaires. La limitation des comptes de destinations pour les virements ou le temps mis pour référencer un compte à virer en sont les principales illustrations. "*On a bien vu lors des déploiements de Barclays en Grande-Bretagne que l'offre de lecteurs d'authentification dynamique a permis de nouveaux services qui se sont traduits par de nouveaux clients*", rappelle Cédric Collomb (Gemalto). "*Le niveau de service apporté par le système Faster Payment* [4] *en Grande-Bretagne a été rendu possible par le niveau de sécurité atteint dans les opérations de virements grâce aux nouveaux lecteurs. En France, c'est encore plus nettement le développement du e-commerce qui est le ressort principal de ces évolutions*, souligne Laurent Maître (Xiring), *et 3D Secure s'inscrit lui parfaitement dans ce mouvement*".

[3] Les identifiants et mots de passe statiques peuvent être renouvelés souvent, protégés par des techniques de clavier virtuel, ou des systèmes de listes de mots de passe unique, mais ils sont toujours exposés aux risques d'être capturés par *phishing* via de faux sites Web.

[4] Le Faster Payments Service lancé en mai 2008 en Grande-Bretagne permet de réaliser des paiements (virements et paiements par cartes à distance) avec des délais de l'ordre de l'heure. Du coup, les livraisons sont accélérées. En six mois, 63 millions d'opérations ont été enregistrées pour une valeur de 26 milliards de livres.

On voit qu'en poussant la logique 3D Secure jusqu'au bout – il faut authentifier formellement le porteur de la carte –, ce sont les mêmes conclusions qui s'imposent à la fois pour le paiement et pour la banque en ligne : il faut éliminer les mots de passe statiques et généraliser les mots de passe non rejouables : des mots de passe qui ne

> *"Les banques du Benelux, et de certains pays nordiques en sont déjà à leur troisième génération de déploiements de solutions d'authentification forte en ligne pour les clients, alors que d'autres pays n'ont pas encore sauté le pas."*

puissent pas être utilisés par des fraudeurs qui auraient pu d'une façon ou d'une autre s'en emparer. On sait, pour cette raison, que le choix des banques d'utiliser une donnée de leurs clients facilement disponible (statique) [5] pour servir de mot de passe 3D Secure n'est que provisoire. Cette nécessité renforce encore celle de faire d'une pierre deux coups en choisissant pour authentifier les clients et les transactions réalisées sur un site de banque en ligne, la même solution ou des solutions faisant appel à des techniques similaires à celles utilisées pour générer sur 3D Secure un mot de passe dynamique.

DES SOLUTIONS COMPLÈTES

L'une des caractéristiques des solutions d'authentification forte capables de générer des mots de passe dynamiques, qu'il s'agisse d'ailleurs de celui du contrôle d'accès en entreprise ou celui du contrôle d'accès aux services de banque en ligne et de paiement, est d'abord leur nombre et la variété des procédés – tous plus ingénieux que les autres – auxquels elles font appel. Les principaux fournisseurs comme Vasco, Xiring et Gemalto ont développé des familles complètes de lecteurs ou de calculettes, mais également des solutions de *back-office* lorsque les solutions clients les imposent. Ils interviennent tous avec des offres de produits, mais aussi de services de conseil, de *packaging*, de *marketing*, de communication et de logistique. Vasco, qui compte déjà dans le monde de très nombreuses références bancaires, se positionne désormais comme un éditeur de solutions logicielles et plus du tout comme un fournisseur de tokens. "*Nous avons développé un portfolio de solutions logicielles et matérielles autour de notre serveur de façon à rendre transparente leur intégration dans les infrastructures bancaires existantes : serveur, base de données HSM*", souligne Benoit Grangé. Gemalto met également en avant son *leadership* dans le domaine de la "sécurité numérique" pour proposer une offre complète – de la fourniture de lecteurs à la campagne de *marketing* et de communication – qui "*permet aussi de traiter la sécurité des employés de la banque avec notamment des solutions pour le* trading floor", comme l'indique Cédric Collomb.

En choisissant de focaliser son offre sur des calculettes et des lecteurs de cartes EMV-CAP, Xiring, qui a déjà livré près de 5 millions de lecteurs pour les banques anglaises, table à la fois sur le bénéfice que peut présenter ce type de solutions – la carte EMV est déjà déployée – et sur son intégration facile et transparente dans les infrastructures existantes de serveurs monétiques.

DU CLAVIER VIRTUEL À LA SIGNATURE ÉLECTRONIQUE

La simplicité des recommandations de la Banque de France, qui s'est aussi accompagnée d'un agnosticisme affiché sur les techniques et des différentes solutions utilisées pour parvenir à cet objectif, ne résume pourtant pas la complexité des enjeux que représentent les choix que sont en train de faire les banques. La fin du couple "identifiant/mot de passe" (ou sa redéfinition) utilisé pour identifier et authentifier les clients de la banque en ligne n'est pas seulement une question de choix technique, même si cet aspect reste assez primordial, imposant études et tests approfondis. En publiant, dès 2004, un profil de protection pour établir un référentiel complet destiné aux maîtres d'ouvrage et aux équipes d'exploitation et de maintenance des sites de banque en ligne, la Banque de France et le CFONB ont bien montré la complexité de la mise en œuvre d'un site Web soumis à

[5] Le choix s'est porté dans un premier temps sur la date de naissance du client.

QUELQUES EXEMPLES DE SOLUTIONS D'AUTHENTIFICATION POUR L'ACCÈS ET LES SERVICES DE BANQUE EN LIGNE

Type d'équipement client	Nom/société	Fonctions	Équipement serveur	Commentaires
Logiciel (Applet Java)	Digipass for Mobile/Vasco	OTP/CR/*e*-signature	Vacman Controller	Téléchargeable *over-the-air* sur le téléphone mobile depuis un serveur bancaire (via SMS).
Logiciel (Applet Java)	Digipass for Web/Vasco	OTP/CR/*e*-signature	Vacman Controller	Téléchargeable *via* Internet sur le PC depuis un serveur bancaire.
Token USB	Plug&Seal/Gemalto	OTP/CR/signature PKI (transaction et document)	PKI Plug-in	Intégrable sur tous types de plateformes bancaires.
Token USB	Digipass 860/Vasco	OTP/signature PKI	Vacman Controller	Équipé d'un petit afficheur et d'un bouton.
Token USB	Digipass Key1/Vasco	OTP/CR/PKI signature	Vacman Controller	Peut être utilisé avec Digipass CertID, logiciel de signature électronique. Conforme à Global Platform et Javacard 2.1 et 2.
Calculette (non connectée)	Digipass GO (3 à 7)/Vasco	OTP (Basé sur le temps)/ Authentification mutuelle	Vacman Controller	Équipé d'un bouton et d'un afficheur. Une famille de calculettes personnalisables
Calculette (non connectée)	Ezio Token/Gemalto	OTP (Basé sur le temps ou sur des événements)	Ezio Server	Équipé d'un bouton et d'un afficheur.
Calculette PINpad (non connectée)	Digipass PRO (250-700)	OTP/CR/e-signature	Vacman Controller	Équipé d'un clavier et d'un afficheur.
Calculette PINpad (non connectée)	Ezio PIN Token/Gemalto	OTP/CR/Signature PKI (transaction)	Ezio Server	Le serveur supporte CAP, OATH, TAN. Intégrable sur tous types de plateformes bancaires.
Lecteur de cartes à puce (non connecté)	Ezio Reader/Gemalto	OTP/CR/Signature PKI (CAP-DPA-TAN-OATH)	Ezio Server	Existe en 5 versions dont une optque et une ultra-fine.
Lecteur de cartes à puce (non connecté)	Xi-Sign 1000-2000/Xiring	OTP/CR/e-signature (CAP-DPA)	Serveur monétique existant	Équipé d'un bouton et d'un afficheur. Utilise une carte EMV au format SIM (boîtier scellé).
Lecteur de cartes à puce (non connecté)	Xi-Sign 4000/Xiring	OTP/CR/e-signature (CAP-DPA)	Serveur monétique existant	Intégrable dans 3D secure.
Lecteur de cartes à puce (non connecté)	Xi-Sign 4100/Xiring	OTP/CR/e-signature(CAP-DPA)	Serveur monétique existant	Équipé d'un clavier et d'un tiroir SIM (EMV-CAP) optionnel. Modèle APACS.
Lecteur de cartes à puce (non connecté)	Xi-Sign 4400/Xiring	OTP/CR/e-signature(CAP-DPA)	Serveur monétique existant	Avec une fonction de restitution sonore et un grand afficheur pour les malvoyants.
Lecteur de cartes à puce (non connecté)	Digpass 840 Comfort Voice/ Vasco	OTP/CR/e-signature (CAP-DPA-TAN)	Vacman Controller	Équipé d'un clavier, et d'une fonction restitution sonore pour les malvoyants. Conforme 3D secure et avec la carte d'identité belge.
Lecteur de cartes à puce (connecté)	Xi-Sign 6000/Xiring	OTP/CR/e-signature PKI (CAP-DPA)	Serveur monétique existant	Lecteur de carte à puce PC/SC intégrant la technologie Xiring Secure Pin Entry.
Lecteur de cartes à puce (connecté)	Xi-Sign PKI/Xiring	OTP/CR/e-signature PKI (CAP-DPA)	Serveur monétique existant	Avec gestion sécurisée du code PIN.
Lecteur de cartes à puce (connecté)	Digipass Secure Reader 850/ Vasco	OTP/CR/e-signature PKI	Vacman Controller	Peut être mis à jour pour CAP.
Lecteur de cartes à puce (hybride)	Digipass 865/Vasco	OTP/CR/e-signature PKI (CAP-DPA-TAN)	Vacman Controller	Peut-être utilisé en mode connecté ou non connecté. Fonction "vous signez ce que vous voyez".

Légendes :
OTP (One Time Password), mot de passe unique, authentification dynamique, soit basée sur des intervalles de temps soit sur un compteur.
CR (Challenge-Response), mot de passe dynamique, basé sur un jeu de questions et réponses pour vérifier des secrets partagés.
CAP (Chip Authentification Program), spécification développée par MasterCard pour le calcul d'un OTP, d'un CR et d'une signature à partir de clés présentes dans la carte EMV. Son équivalent chez Visa s'appelle DPA (Dynamic Passcode Authentication).
TAN (Temporary Account Number), standard des banques allemandes pour l'authentification.
OATH (Open AuTHentication) est une initiative de l'industrie pour spécifier une architecture pour l'authentification par OTP.

des objectifs et des exigences de sécurité qui répondent à un éventail très étendu de risques. Les choix supposent des arbitrages et des stratégies *marketing*. Les coûts de déploiement, le niveau de sécurité, le confort d'utilisation de la solution, les nouveaux services, et la campagne de communication qui doit préparer ces évolutions, sont chacun pris en compte. Les banques anglaises n'ont pas toutes adopté les mêmes options techniques. Certaines ayant maintenu le recours du mot de passe pour l'accès au site et l'authentification CAP (Chip Authentication Program) pour les virements. Les niveaux de sécurité offerts aujourd'hui s'adaptent à la nature des services offerts et la sensibilité des opérations. L'authentification simple des calculettes OTP (One Time Password) offre un premier niveau de sécurité qui lui-même peut être modulé selon le type de génération du mot de passe (base de temps, compteur et liste), tandis que l'authentification obtenue par un Challenge-Response [6]offre encore un niveau supérieur en coupant court à toute possibilité de capturer un OTP et de l'utiliser pendant la durée de sa validité.

Enfin, la signature électronique offre le meilleur niveau de sécurité et de non-répudiation, en déjouant en particulier les attaques de type *man-in-the-middle*. Les implémentations de ces solutions sont également sujettes à des options comme l'utilisation du téléphone mobile pour envoyer les OTP sous forme de SMS, utiliser son clavier pour taper un code PIN comme sur un terminal de paiement ou encore son afficheur pour vérifier les données d'une opération de paiement. D'autres solutions encore ont été implémentées sur des clés USB qui permettent d'intégrer de façon sécurisée l'URL de la banque de façon à déjouer toutes les tentatives de *phishing*. Autant de solutions qui visent à terme à reproduire en ligne – quelques années après les cuisants insuccès de SET et de Cybercom – la sécurité et le confort d'utilisation que permet le paiement par carte dans le monde bien physique du commerce de proximité. ■

[6] Vasco a développé une solution de challenge response dans laquelle le challenge envoyé par la banque permet au client d'authentifier cette dernière.