Yvon Avenel

Journaliste
Éditeur de
SmartcardsTrends

AUTHENTIFICATION

Biométrie : les technologies se banalisent

La biométrie, longtemps cantonnée à quelques domaines futuristes d'expérimentation, pourrait connaître prochainement de réels développements. Ces technologies se banalisent et leurs applications sont multiples : l'identification bien sûr, mais aussi une sécurité accrue, une meilleure connaissance des clients, voire de nouveaux moyens de paiement.

Un certain nombre de raisons nouvelles forcent, aujourd'hui, l'intérêt du secteur bancaire pour les technologies biométriques. Parmi celles-ci, une raison très générale : elles se banalisent. Et cette évolution est manifestement plus rapide que prévue. "*La biométrie devient un produit d'usage courant et les données biométriques, des données tout à fait standard*", soulignait récemment Philippe Dusautoir, directeur général de Thales Identification Systems, l'un des leaders mondiaux de la gestion d'identités, lors d'un colloque international sur ce sujet à Paris. "*L'image de science-fiction ou de technologies futuristes a complètement disparu*", confirme, de son côté, Nicolas Madinier, d'Unilog (LogicaCMG group), qui évoque l'actualité de l'intérêt que porte le secteur bancaire à ces technologies. Cette première raison, toute générale, n'est pas la moins importante, puisque cette banalisation repose au moins sur trois évolutions cruciales : une fiabilité désormais assez éprouvée des techniques et de leur mise en œuvre, une baisse de leurs coûts, et enfin un niveau d'acceptation dans le public qui n'a jamais été aussi élevé, en dépit de certains mouvements d'opinion qui s'élèvent ici et là. Mais il existe aussi des raisons plus particulières qui pourraient inciter les banques à adopter ces techniques ou, à dépasser le stade des réflexions et de travaux d'études qu'elles mènent pratiquement toutes aujourd'hui sur ce sujet. La lutte contre les fraudes de toute nature, dont l'origine est toujours un défaut d'identification ou d'authentification, un meilleur contrôle des accès aux données et sites sensibles, mais aussi des opportunités commerciales et marketing sont des raisons actuelles d'autant plus fortes qu'elles répondent à quelques grandes orientations du moment, comme la conformité réglementaire, assorties d'exigences de traçabilité et d'audit, d'une part, et l'attention renouvelée portée à la relation client, d'autre part.

PRÊTS À CHANGER POUR UNE MEILLEURE PROTECTION

Deux études récentes [1] le confirment : elles sont venues à quelques mois d'intervalles montrer que la biométrie allait rapidement représenter pour le secteur bancaire une source d'opportunités, mais aussi de risques. La première a été réalisée par Unisys. Elle a été annoncée lors du Bank Administration Institute's Retail Delivery Show qui s'est tenu en novembre dernier

1. LA RECONNAISSANCE DES VEINES POUR LES DISTRIBUTEURS DE BILLETS

Depuis octobre 2004, plusieurs banques japonaises, dont la Bank of Tokyo-Mitsubishi, la Bank of Ideka et la Suruga Bank, ont adopté pour leurs distributeurs de billets et guichets automatiques, une technologie basée sur la reconnaissance des veines de la main. Sur la base du volontariat (5 % des clients à ce jour), les clients ont été invités à s'enrôler dans ce système. Ils ont reçu une carte bancaire à puce qui contient soit un gabarit des formes caractéristiques de leurs veines, qui peut ainsi être comparé dans la carte à celui qui est reconnu par le système associé au distributeur de billets au moment où ils accèdent à ce service, soit un lien vers un serveur où se trouve stocké le gabarit de référence, et réalisé le matching. Développé par **Fujitsu**, ce système de reconnaissance qui fonctionne en éclairant fortement la main dans le proche infrarouge, et en analysant l'image avec une caméra adaptée, est annoncé comme très sûr : 0,00008 % de fausses acceptations pour un taux de 0,01 % de faux rejets. La banque Tokyo-Mistubishi prévoit 5 millions de cartes en 2008.

2. APPLICATION

Le contrôle d'accès logique et physique

■ La gestion des mots de passe ou des codes d'accès en interne est un domaine d'investigation pour les applications de la biométrie. Là où souvent le même mot de passe ne peut pas être utilisé pour accéder à des sites, des ressources ou des données différentes, l'utilisation d'une empreinte biométrique unique dans un système de SSO (*single sign on*) offre à la fois une solution de confort, de sécurité et d'économie, en supprimant le coût de la gestion des mots de passe. La Fireman's Fire Union, une institution financière américaine qui a opté pour un système biométrique (son personnel avait à mémoriser plus de 10 mots de passe différents), estime ce coût à quelque 300 dollars par mot de passe et par an. La Banque du Luxembourg, qui a adopté ce type de solution a étendu le domaine d'applications de la carte biométrique qu'elle a déployée pour ses 600 employés, et qui permet en plus de l'accès aux sites et données sensibles, l'accès au parking, aux ascenseurs, au restaurant de la banque, et à la gestion du temps de travail.

à Orlando aux États-Unis. Elle montre que l'inquiétude des Américains relative à la protection de leurs comptes en ligne croît : 73 % disent se soucier de cette question contre 51 % lors de l'étude précédente réalisée en 2004. Mais il y a plus, puisqu'ils sont 40 % à accepter l'idée de payer une protection supplémentaire (contre 27 % en 2004), et 50 % à se dire prêts à changer de banque pour un meilleur niveau de protection (contre 45 % il y a deux ans). Intéressant de noter qu'aux États-Unis, les services de La Poste (47 %) arrivent en tête en termes de confiance (un point devant les banques), et qu'en Europe ce sont les gouvernements (56 %) qui devancent les banques (44 %). Un résultat en partie confirmé par le choix de la carte d'identité, aux États-Unis (33 %) comme en Europe (45 %), comme premier moyen de contrôle de ses données personnelles d'identité pour accéder à des services, assez loin devant l'utilisation d'un système biométrique (26 % aux États-Unis, 21 % en Europe). Dommage que l'étude n'ait pas pris en compte le fait que les futurs documents d'identité feront aussi appel à des techniques de reconnaissance biométriques ! En tout état de cause, la carte d'identité et la biométrie conjuguées remportent une large majorité de suffrages (59 % aux États-Unis, et 66 % en Europe).

L'étude faite plus récemment par Logica-CMG enfonce encore le clou. 57 % des Européens se disent prêts à changer de comptes bancaires si on leur propose d'utiliser, pour s'identifier, une carte et un système basé sur une empreinte digitale plutôt que de fournir les documents d'identité usuels. Une réponse sans doute prévisible, mais qui met bien en évidence un point que l'étude d'Unisys avait déjà souligné : la motivation qui favorise l'adoption de l'usage de la biométrie chez les clients de la banque est bien le confort et la vitesse. Il est vrai que cette motivation est quand même soutenue par la conviction que la biométrie est un moyen fort et fiable d'authentification. Ils sont, en effet, 84 % en Europe à penser que cette technique est plus sûre que l'usage de la carte à puce associé à un code PIN. Cette étude souligne bien que l'adoption d'une nouvelle technologie se fait lorsque la valeur ajoutée des services offerts est patente pour les clients ou les consommateurs. Le système d'embarquement proposé à l'aéroport de Schipol en Hollande, qui est basé sur la reconnaissance de l'iris, est un bon exemple : 36 000 personnes se sont déjà inscrites à ce programme pour bénéficier d'un embarquement accéléré et, sans autres formalités que de se placer rapidement devant une machine équipée d'une caméra spéciale en présentant sa carte à puce [2].

> *« Ce sont les pays d'Europe du Sud qui se sont engagés le plus avant dans des pilotes pour explorer les possibilités offertes par le remplacement du PIN de la carte à puce bancaire (EMV) par une empreinte biométrique. »*

"C'est ce que nous disons aujourd'hui aux banques : vos clients sont prêts, ils adoptent ces technologies pour le confort qu'elles procurent. Et il y a là des opportunités d'attirer de nouveaux clients", ajoute Nicolas Madinier (Unilog).

MIEUX CONNAÎTRE LES CLIENTS

Les pistes d'investigation ne manquent pas. Tout comme les réflexions sur les technologies et les applications. Mais aussi sur ce qui fait ou pourrait faire encore obstacle à leur déploiement. Quelques grands domaines d'application se dégagent : celui des services clients à valeur ajoutée étroitement liés à des questions d'authentification ou d'identification, celui du paiement et des transactions effectuées notamment depuis les GAB ou DAB (*encadré 1*), et enfin celui plus spécifiquement lié, en interne, au contrôle d'accès physique et logique (*encadré 2*).

Les services clients à valeur ajoutée peuvent être très variés : utilisation de la reconnaissance vocale pour conditionner l'accès par téléphone aux différents comptes et titres, utilisation de *tokens* biométriques réclamant la reconnaissance d'empreinte digitale (à la place d'un code PIN) pour calculer un *challenge response* autorisant l'accès *on line* avec un PC à des transactions internationales importantes pour un segment de clientèle bien défini, système de reconnaissance faciale en agence de façon à permettre l'accès, voire à anticiper la préparation d'un dossier, etc. Qu'il s'agisse d'identifier (reconnaître une personne parmi d'autres) ou d'authentifier (vérifier que la personne est bien celle qu'elle prétend être), les techniques biométriques permettent d'accroître le confort et la sécurité. Le temps n'est sans doute pas si éloigné où les banques devront s'équiper de lecteurs d'empreintes digitales de façon à pouvoir lire les futurs documents d'identité biométriques de leurs clients au moment d'ouvrir un compte, par exemple, plutôt que de se contenter d'une photocopie de carte d'identité ou de fiche d'état civil. Restera à résoudre la question des ouvertures de compte sans présence physique du titulaire. Quoi qu'il en soit, il y a là des opportunités de développer de nouveaux services et d'apporter des réponses nouvelles à des questions comme celles que posent le blanchiment, la délinquance financière et le

financement du terrorisme qui s'appuient toujours sur un défaut d'identification, une mauvaise connaissance du client.
"Il faut noter que certains pays sautent plusieurs générations de technologies parce qu'ils sont obligés de tout inventer", souligne Bernard Didier, le directeur du développement Identité et Systèmes de sécurité chez Sagem. Et de citer l'exemple de la Reserve Bank of Malawi, amenée à déployer une carte à puce biométrique (Sagem en a livré à ce jour plus de 200 000) qui permet aux clients de la banque de retirer via des distributeurs de billets et des guichets de la banque le montant de leurs salaires ou pensions. Gemplus a livré l'an dernier à la Banco Azteca au Mexique, une carte d'identité bancaire du même type. Oberthur Card Systems a commencé depuis quelques mois la livraison de cartes bancaires biométriques à puce (plus de 500 000 cartes déjà livrées sur un objectif de 5 millions) en Côte d'Ivoire à la CECP (Caisse d'Épargne et de Chèques Postaux). Cette carte est aussi une carte d'identité bancaire. *"Nous avons en ce moment des demandes qui émanent de banques africaines pour des terminaux d'identité biométrique, parce que les nombreuses homonymies au niveau de l'état civil sont une source de difficultés et de conflits dans la gestion des comptes"*, explique Dominique Gauthier, le responsable marketing Software et Technologies chez Ingenico. Le numéro 2 mondial des terminaux de paiement travaille au développement d'un terminal biométrique qui embarque un capteur thermique d'empreinte à balayage. *"Pour ce type de terminal, les demandes sont de plusieurs natures et varient selon les pays : soit une combinaison de fonction de paiement par carte à puce et de contrôle d'identité biométrique – typiquement pour les services de police –, soit de paiement pur dans lequel le code PIN est remplacé par une empreinte digitale, soit une combinaison de paiement purement biométrique, et de paiement par carte bancaire classique, soit encore pour des fonctions d'identité purement bancaire."*

2,3 MILLIONS D'AMÉRICAINS PAYENT AVEC LE DOIGT

Le paiement est un domaine à part entière. Contrairement à quelques idées reçues, ce sont, aujourd'hui les pays d'Europe du Sud, comme l'Italie ou l'Espagne, qui se sont engagés le plus avant dans des pilotes pour explorer les possibilités offertes par le remplacement du PIN de la carte à puce bancaire (EMV) par une empreinte biométrique. Partout ailleurs, le sujet est à l'étude. L'impact sur l'infrastructure du réseau d'acceptation bancaire serait, semble-t-il, assez réduit, au moins sur la partie strictement EMV de la méthode d'authentification. La mise en œuvre à grande échelle des moyens d'enrôlement paraît par contre moins aisée. Les problèmes sont identifiés depuis longtemps. Mais plus que de stricts motifs de sécurité et de confort : réduction de la fraude, et résolution de problèmes de mémorisation pour des utilisateurs de plus en plus âgés, voire pour certains d'entre eux culturellement rétifs à cet exercice de mémoire, l'utilisation de l'empreinte digitale à la place du PIN, pourrait être remise en selle par le développement de nouveaux moyens de paiement.

On voit apparaître, depuis quelques années un autre modèle qui pourrait devenir une alternative à la carte bancaire classique – donc un risque pour les banques – parce qu'il s'apparente à une sorte de carte privative de paiement associé à son propre système de points de fidélité et de remises, et gratuite de surcroît. Ce modèle est promu par des chaînes de magasins, et bien évidemment n'est pas lié à un réseau interbancaire d'acceptation. Il s'agit d'un système de paiement purement biométrique : c'est le doigt qui est le seul "instrument" de paiement, utilisable après une procédure d'enrôlement. L'empreinte est en réalité associée à un code personnel qui est généralement un numéro de téléphone personnel. Plus de deux millions de personnes aux États-Unis – ce qui est loin d'être anecdotique – font leurs achats de cette façon dans plus de 7 000 magasins. Pay By Touch, la société américaine qui a développé ce système, est

3. EMPREINTE DIGITALE

Prime au capteur thermique à balayage

Les capteurs d'empreintes digitales ne font pas tous appel à la même technologie. Les capteurs optiques traditionnels (production d'une image) se sont vus concurrencés depuis une quinzaine d'années par des capteurs dits "silicium", construits à partir d'une puce capable de traiter directement les informations reçues en présence du doigt. Ces capteurs capacitifs (mesure des variations d'un champ électromagnétique) ou encore thermiques (mesure d'un profil thermique) sont beaucoup plus petits et moins chers que les capteurs optiques qui n'ont cessé par ailleurs de s'améliorer quand leur prix diminuait aussi.
Bien sûr, les performances de ces capteurs dépendent étroitement de la qualité des logiciels d'extraction (pour construire les gabarits), ou de reconstruction d'image (pour les capteurs silicium), et de reconnaissance (matching). Il semble pourtant que parmi ces capteurs silicium, les capteurs thermiques offrent des performances qui les placent parmi les tout premiers pour les utilisations "tout terrain" et dans les tests d'interopérabilité. L'un des principaux capteurs thermiques du marché, celui de la société française ID3 Semiconductors, est, par exemple, utilisé pour contrôler l'accès des mineurs (des doigts souvent abîmés) d'une mine de diamants en Afrique du sud, et il vient de remporter la première place (97 % de réussite sur 112 passeports différents) des capteurs industriels pour son interopérabilité (sur près de 50 autres lecteurs) dans le domaine des passeports biométriques. C'est en outre, le seul capteur à balayage, donc sans "trace" : le doigt glisse sur le capteur dont la largeur est de quelques millimètres.

issue de l'acquisition récente d'une autre société, Bio-Pay, qui lui a apporté pas loin de 2 millions de clients dans cette opération. La société IT-Werke en Allemagne a lancé avec la chaîne de supermarchés Edeka (28 % du marché allemand), un service similaire, basé sur le volontariat qui a permis d'enrôler 12 % des clients avec des gains de 40 % en temps sur le passage en caisse, et 90 % des utilisateurs satisfaits. Si la société allemande paraît se cantonner au marché allemand, Pay By Touch manifeste, quant à elle, des ambitions internationales. L'Américain a annoncé dans le courant du mois de juin sa première implantation en Europe via un accord avec la chaîne de magasins anglaise Midcounties Co-op et, par ailleurs, avec NCR pour la fourniture de kiosques d'enrôlement qui permettent aux clients du magasin de s'enregistrer et d'alimenter leur compte "porte-monnaie électronique" avant de faire leurs courses. Il se montre également très offensif dans le domaine du paiement en ligne sur Internet avec le lancement d'un service qui fait appel à un code PIN pour authentifier les paiements par cartes de débit.

DISTINGUER PERFORMANCES INTRINSÈQUES ET RÉSULTATS D'IMPLÉMENTATION

Deux grandes technologies biométriques sont en passe de s'imposer. Tout simplement parce que ce sont celles retenues par l'ICAO (International Civil Aviation Organization) pour les nouveaux passeports électroniques : il s'agit des empreintes digitales qui représentent à l'heure actuelle près de 44 % du marché global de la biométrie, et la reconnaissance du visage qui en représente 19 % (3). Pour Bernard Didier (Sagem), l'évaluation des "bonnes" techniques mérite d'être plus nuancée. *"Il importe de bien distinguer les performances intrinsèques d'une technique de son implémentation industrielle. La reconnaissance de l'iris pose aujourd'hui des problèmes de mise en œuvre (réglage de la profondeur de champ, de l'éclairage, problèmes liés à la présence de cheveu, à l'utilisation de lunettes ou de lentilles, etc.), mais on sait que cette technique pourra, à terme, grâce aux progrès escomptés dans sa mise en œuvre, apporter des résultats supérieurs à ceux des empreintes digitales, en tout cas bien meilleurs que ceux qu'il sera possible d'obtenir avec la reconnaissance faciale dont l'asymptote des performances intrinsèques est bien inférieure à celles des empreintes digitales et de l'iris. La reconnaissance faciale n'est vraiment efficace que si les utilisateurs se montrent coopératifs."*

RESPECTER LA PROTECTION DE LA VIE PRIVÉE

Le débat est loin d'être clos. Il n'y a pas de solution unique. D'une part, parce que certaines techniques se prêtent mieux que d'autres à tel ou tel type d'applications (les enquêtes policières peuvent prendre des mois d'analyse, le passage aux frontières suppose des traitements de quelques millisecondes), et qu'elles doivent obéir au principe de proportionnalité souvent mis en avant par la CNIL en France. Certaines techniques ou implémentations répondent plus que d'autres à certaines recommandations ou à des aspects réglementaires touchant la protection de la vie privée. La CNIL ne cache pas sa préférence pour les techniques qui ne laissent pas de traces (iris, géométrie de la main, etc.). Ce qui donne un avantage, pour les empreintes digitales, aux capteurs dits à balayage basés sur le défilement du doigt et la mesure d'un profil thermique, par rapport aux capteurs optiques qui laissent des traces (*encadré 3*). La CNIL apprécie, en outre, que les données biométriques soient sous le contrôle de la personne plutôt que stockées dans une base de données. Ce qui donne un avantage à l'utilisation combinée de la carte à puce et de la biométrie. Mais les évolutions récentes en matière de base de données (voir l'interview de Bernard Didier) laissent penser que le concept de base de données centrales toujours désigné comme l'arme fatale de "Big Brother" n'est pas loin d'avoir vécu. Le concept de base de données à liens faibles développé par Sagem offre des garanties inédites en matière de protection de la vie privée, et présente l'avantage d'éviter le chiffrement des liens entre gabarit d'empreinte et nom de la personne, chiffrement dont la robustesse ne repose que sur sa propre solidité et la confiance que l'on peut avoir dans l'organisme qui en détient les clés. ■

NOTES

[1] Unisys ID Fraud Research, publiée le 15 novembre dernier a été réalisée pendant l'été 2005 par Ponemon Institute. 2006 E-identity, European attitudes towards biometrics. LogicaCMG, mai 2006.

[2] Cette carte à puce de voyage délivrée par l'aéroport contient un gabarit de l'iris du propriétaire de la carte qui est comparé à celui qui est acquis au moment de son passage, devant une machine spéciale équipée d'une caméra. En France, un programme (projet Pegase) similaire, mais utilisant des empreintes digitales, est en train d'être testé à l'Aéroport Charles-de-Gaulle, également sur la base du volontariat.

[3] Pour un marché qui est évalué à 2,1 milliards de dollars cette année, et qui devrait atteindre 5,7 milliards en 2010 (selon IBG).

GLOSSAIRE

■ **Gabarit (ou *template*) :** ensemble d'informations qui résume la description (par extraction des éléments caractéristiques) de l'image d'une empreinte digitale ou d'une forme biométrique quelconque (iris, forme de la main, veines, fréquences vocales, signature…) et qui est utilisé pour établir la reconnaissance (*matching*).

■ **Minutae :** points caractéristiques qui définissent une empreinte digitale, et qui sont extraits de l'image acquise par un capteur grâce à un algorithme spécialisé. La façon dont ces données sont organisées et définies ont fait l'objet de travaux de standardisation (MIN : A et MIN : B).

■ **FRR (ou FMR pour *False Matching Rate*) :** taux de faux rejets. C'est la part des gabarits (*templates*) ou des images qui, au moment d'être comparés (*matching*), n'ont pas été identifiés comme étant les mêmes alors qu'ils étaient identiques. Très lié au FAR (cf. infra), si l'un varie l'autre varie également en sens inverse.

■ **FAR (ou FNMR pour *False Non Matching Rate*) :** taux de fausses acceptations. C'est la part des gabarits (*templates*) ou des images qui au moment d'être comparés (*matching*) ont été identifiés à tort comme identiques alors qu'ils étaient différents. Très lié au FRR, si l'un varie l'autre varie également en sens inverse.

■ **Matching :** opération de comparaison de deux images ou deux gabarits à partir de leurs éléments caractéristiques. Quand cette opération s'effectue dans la carte, on parle de *match-on-card* (l'opération la plus sécurisée), dans le lecteur ou le terminal, de *mach-on-board*, et sur un serveur distant disposant d'une base de données, de *match-on-server* (la plus sujette à réticence de la part de la CNIL).