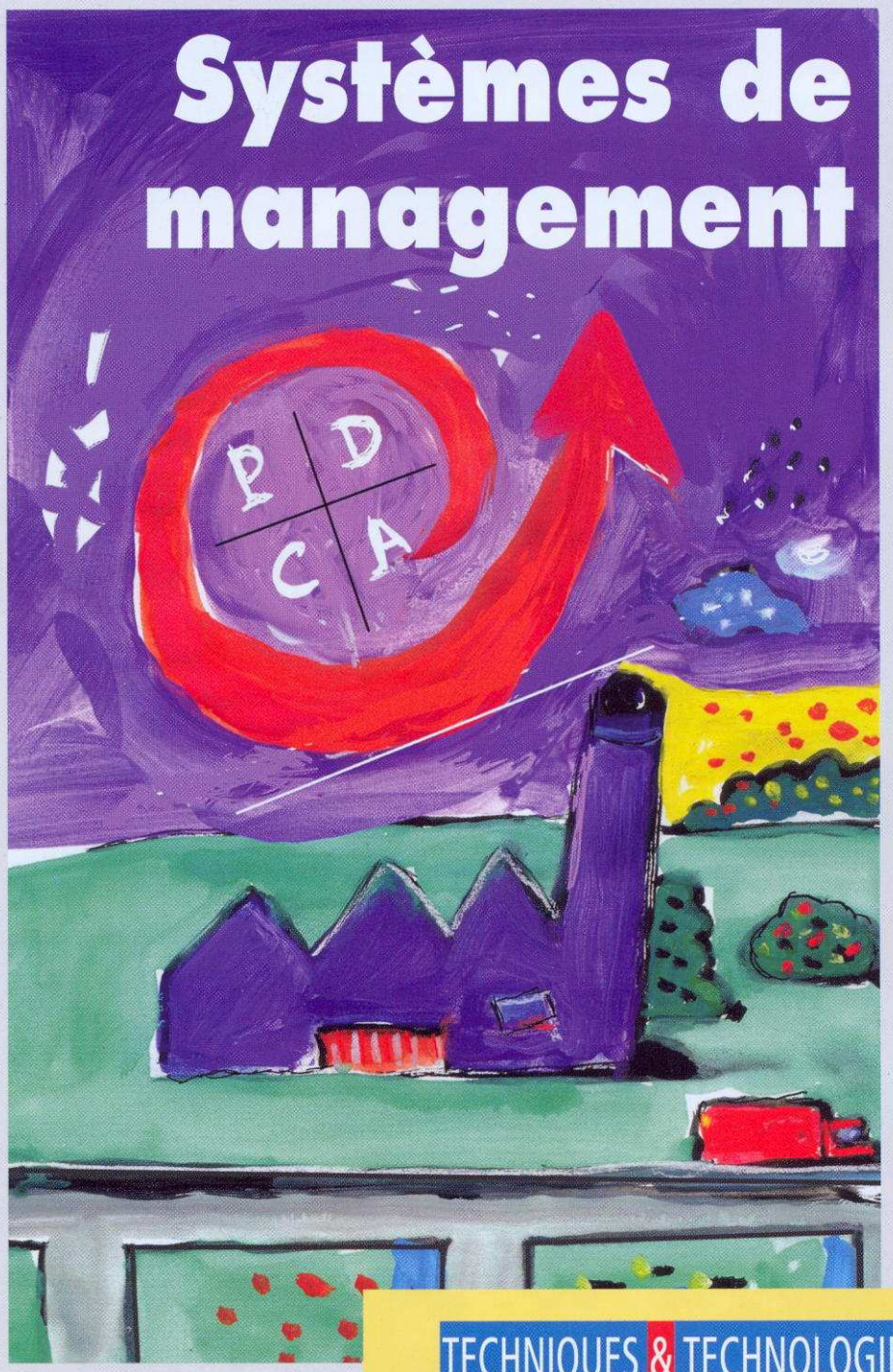
EXPOPROTECTION

FACE AU RISQUE

ISSN 0014-6269 - MENSUEL

LA RÉFÉRENCE DES ACTEURS DE LA MAÎTRISE DES RISQUES



L'approche processus

ISO 19011, les clés de l'audit

Manager le risque incendie

Les atouts de la certification

PORTRAIT
Préventionniste sapeur-pompier

ENVIRONNEMENT
Eco-construction à Lille

SYSTÈME DE SÉCURITÉ INCENDIE
Le métro marseillais

CHANTIER
Démantèlement au CEA Grenoble

MARCHÉ
La biométrie

TECHNIQUES & TECHNOLOGIES

Signalisation d'évacuation
Vidéosurveillance : analogique ou numérique ?
Protection contre la chaleur et les flammes

CNPP stand P110

CNPP

www.faceaurisque.com

RETOUR D'EXPÉRIENCE
Bleve d'un camion-citerne de GPL

Contrôle d'accès : la biométrie a le vent en poupe

A la différence du contrôle d'accès classique, les ventes basées sur des applications biométriques sont en plein essor grâce à des produits innovants. Des perspectives prometteuses qui expliquent la redistribution des cartes entre les acteurs à l'échelle mondiale

Le contrôle d'accès électronique « traditionnel » utilisant un lecteur de badges n'est plus un marché très dynamique. Après une progression annuelle d'environ 15 % dans les années 90 et un fléchissement régulier au cours de la dernière décennie, sa croissance est retombée autour de 2 % depuis l'année dernière. Les explications sont multiples : souci d'économie de la part des donneurs d'ordre qui ralentissent le rythme de renouvellement des produits, réduction des coûts de fabrication des matériels, pléthore d'acteurs qui se livrent une guerre des prix sans merci, crise du bâtiment, délocalisations et fermetures de sites qui suppriment des débouchés potentiels, etc. Dans un contexte économique toujours aussi morose, les perspectives ne sont pas franchement attrayantes.

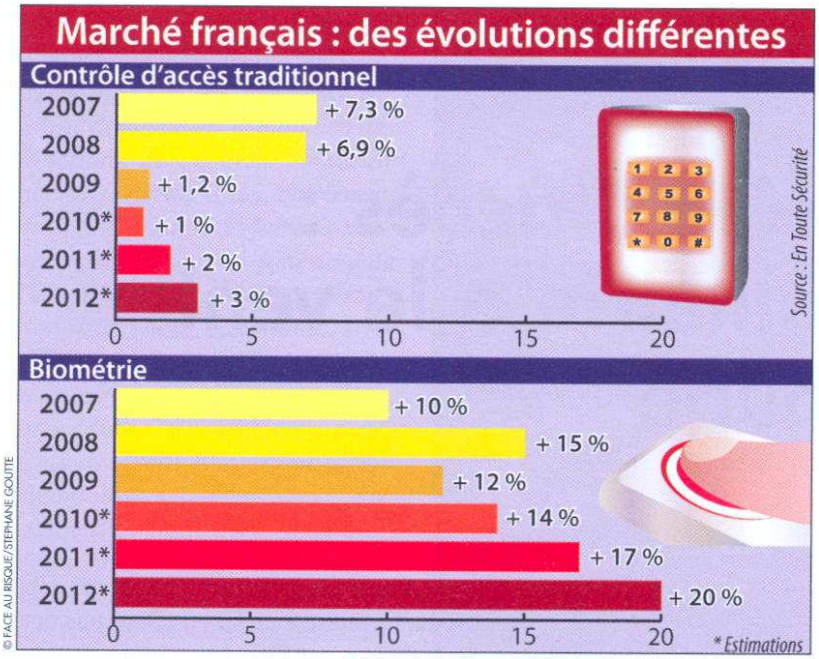
En revanche, un sous-segment de ce marché affiche une santé insolente : la biométrie. Jusque récemment réservée aux applications sensibles (contrôle d'accès de certaines zones sur des sites nucléaires ou pour des zones très protégées de laboratoires, d'usines, de bureaux ou d'infrastructures critiques), cette technologie s'est aujourd'hui fortement démocratisée au point d'envahir notre vie quotidienne. Elle est ainsi installée sur de simples portes de magasins ou d'hôpitaux, des vitrines de joaillers, des garages de maisons individuelles et même sur des ordinateurs ou des téléphones portables pour contrôler l'identité de l'utilisateur. On la voit aussi apparaître dans les cantines scolaires ou dans le vote électronique lors d'élections. Et l'on peut imaginer que le processus va encore prendre de l'ampleur. Le marché mondial est d'ailleurs estimé à la somme rondelette de quatre milliards de dollars, avec des perspectives de croissance de 20 % par an.

© SCIENCE PHOTO LIBRAR

La biométrie s'installe partout. Le marché mondial devrait connaître une croissance de 20 % en 2012

Protection des données personnelles

En fait, le développement de la biométrie résulte largement de la politique d'un pays. Les lois en vigueur sont plus ou moins souples



quant à son utilisation et son autorisation. La France a connu un certain retard dans la généralisation de la biométrie dû à des freins importants apparus dans le souci de protéger la vie privée des individus. Le recueil de données biométriques est ainsi soumis à l'autorisation préalable de la Cnil (Commission nationale informatique et libertés) qui se montre très vigilante sur d'éventuels dérapages. Elle préfère d'ailleurs les dispositifs sans traces (biométrie par reconnaissance du système veineux) que la reconnaissance d'empreintes digitales, car il est très facile de récupérer à son insu les empreintes laissées par un individu (voir encadré ci-contre). Tout comme pour la vidéosurveillance, les obstacles à une large diffusion de la biométrie tombent les uns après les autres dans l'Hexagone depuis deux ou trois ans. Les craintes du grand public pour les atteintes aux libertés individuelles s'estompent progressivement.

Aux États-Unis en revanche, la politique est totalement favorable à la biométrie, notamment depuis les attentats de septembre 2001. Les applications ne sont pas limitées à la lutte anti-terroriste mais aussi au fichage de trafiquants de drogue ou de fraudeurs à la carte bancaire. Les données sont transmises à l'ensemble des agences fédérales (FBI, CIA, NSA, Douanes, etc.) qui ont ainsi accès à de gigantesques fichiers.

Des technologies très évolutives

Très liée aux progrès de l'informatique, la biométrie bénéficie d'évolutions techniques permanentes. La capacité et la vitesse d'analyse des données se sont amplifiées, ce qui permet par exemple une reconnaissance faciale « à la volée », pratiquement en temps réel. Les bases de données peuvent traiter les informations de millions de personnes, voire de dizaines ou de centaines de millions d'individus : c'est ainsi que les cartes d'identité biométriques sont introduites dans des pays à forte population comme le Mexique ou l'Inde (voir *Face au Risque* n° 465 « Inde : de la bio à la crypto »). De plus, des croisements de fichiers avec comparaison des éléments communs ou divergents sont désormais très facilement possibles.

La biométrie multimodale (voir encadré page suivante) constitue la dernière tendance et connaît un fort engouement. Réduisant les erreurs d'analyse possibles avec une seule technologie, elle est actuellement appliquée pour l'accès à des zones sensibles. Elle commence néanmoins à apparaître pour des utilisations standardisées.

La biométrie se développera également sur la téléphonie mobile, car les terminaux intelligents permettent désormais un accès à l'Internet haut débit et à des fonctions de paiement. Il sera aussi bientôt possible de voter avec son téléphone mobile. Pour cela, ces appareils devront intégrer une puce RFID et un lecteur biométrique.

La Cnil veille

Dans les lieux de travail, aucun dispositif ne peut être mis en œuvre sans autorisation préalable de la Cnil. Les technologies à « trace » (empreinte digitale, par exemple) et celles qui reposent sur un système de conservation centralisée des données (par opposition à celles où les données sont conservées par le porteur) font l'objet de toutes les attentions. Pour la Commission, ces dispositifs ne se justifient que s'ils sont basés sur un fort impératif de sûreté et qu'ils répondent à quatre exigences :

- finalité (le but doit être légitime et dépasser l'intérêt de l'organisme demandeur) ;
- proportionnalité (en rapport avec son objectif) ;
- sécurité (fiable et éviter la divulgation des données) ;
- information (des différentes parties en respect des réglementations en vigueur).

Pour alléger ces formalités, il existe quatre cas (c'est-à-dire quatre technologies correspondant à quatre applications) où l'exploitant peut recourir à une simple déclaration de conformité, appelée « autorisation unique » :

- contour de la main pour le contrôle d'accès, la gestion des horaires et de la restauration pour les lieux de travail ;
- empreinte digitale exclusivement enregistrée sur support individuel pour l'accès aux locaux professionnels ;
- contour de la main pour assurer le contrôle d'accès au restaurant scolaire ;
- reconnaissance veineuse pour l'accès aux lieux de travail.

D. K.

Parallèlement, les prix de la biométrie connaissent une chute spectaculaire et il est probable que cette technologie s'imposera à terme dans la vie quotidienne des ménages, pour l'ouverture du réfrigérateur ou l'utilisation du téléviseur, par exemple.

Redistribution des cartes

Pour leur part, les entreprises de sécurité devront être capables d'intégrer ces technologies de pointe et de développer des logiciels évolutifs tout en conservant des configurations plus traditionnelles, comme les serrures biométriques autonomes, et en offrant des fonctionnalités étendues comme une interconnexion avec la vidéosurveillance et la détection incendie.

En raison de ces perspectives attrayantes, plusieurs acteurs se livrent à une course de vitesse pour se positionner clairement comme leader technologique ou pour atteindre une taille critique. Car le marché est totalement atomisé et aucun ténor ne se détache clairement à la différence de la concentration qui s'est déjà produite dans la sécurité incendie, le transport de fonds, les EPI (équipements de protection individuelle) ou la télésurveillance.

Dans cette redistribution des cartes à l'échelle mondiale, les groupes américains figurent nettement parmi les plus actifs. Les États-Unis représentent en effet près de 40 % du marché mondial et la demande y est très soutenue. Plusieurs entreprises ont émergé ces dernières années – essentiellement par l'acquisition de spécialistes du domaine – à l'instar de Tyco ou encore L1 Identity Solutions qui pèse plus de 650 M$ ou de Cogent Systems dont le chiffre d'affaires se situe à près de 150 M$. 3M a frappé un grand coup en septembre 2010 en lançant une OPA amicale sur Cogent et en s'emparant de la firme israélienne Attenti (voir *L'Hebdo* n° 547).

Dans ce panorama très mouvant, les européens ont également posé leurs jalons : Assa Abloy, leader mondial de la serrurerie, est en pointe, notamment après le rachat de l'Américain HID, tout comme Siemens, Kaba, Gieseke & Devrient ou Gemalto. Le français Morpho (anciennement Sagem Sécurité) est également très actif avec les rachats successifs d'Orga, de SDU-Identification, des activités biométriques de Motorola. Le groupe français a également conclu en septembre denier le rachat de L1 Identity Solutions, pour un montant de 834 M€. De nombreuses start-up et PME cohabitent à côté de ces ténors et il est donc probable que le mouvement de concentration ne fasse que commencer. ■

Patrick Haas

Étude réalisée par En Toute Sécurité

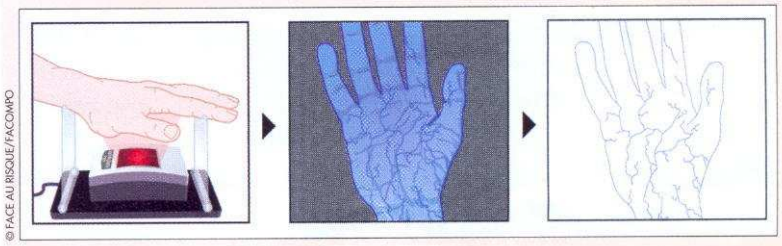
Quelles technologies ?

L'accès à une zone sous contrôle peut être réalisé selon trois modalités : ce que le demandeur possède (clé, badges…), ce qu'il sait (code), ce qu'il est. Dans cette dernière catégorie, se rangent les technologies biométriques et comportementales. Basées sur les caractéristiques anthropométriques, les technologies biométriques ne sont pas pour autant les plus fiables. La preuve, on leur attribue généralement un score, le taux d'égale erreur (TEE). Il s'agit d'un compromis entre le taux de faux rejets (TFR), c'est-à-dire les individus refusés à tort par le système et le taux de fausses acceptations (TFA), c'est-à-dire les individus acceptés par erreur.

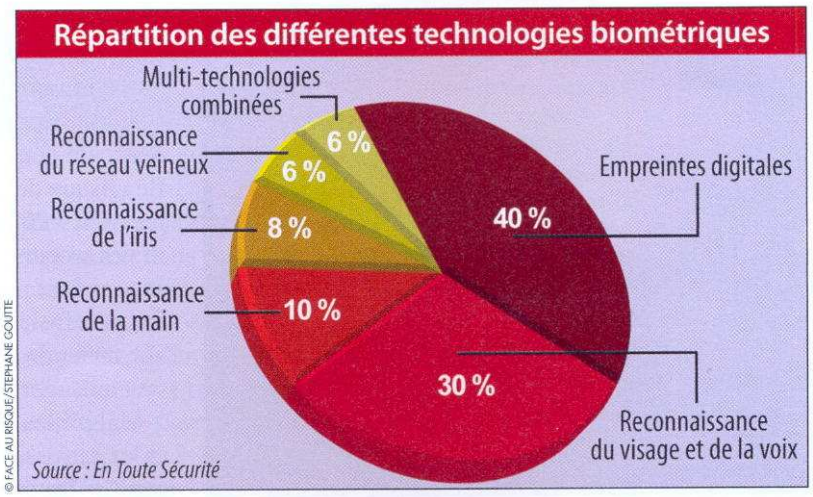
Les industriels du secteur ont donc développé les technologies multimodales. Il ne s'agit pas d'augmenter le niveau de sécurité mais de réduire les taux de faux rejets et permettre la cohabitation de plusieurs publics sans avoir à utiliser plusieurs lecteurs. Les technologies multimodales ne fonctionnent que très rarement de manière cumulative (iris + visage) mais plutôt de manière variable (empreinte digitale ou réseau veineux). C'est un peu comme si l'utilisateur est devant une porte et qu'il peut l'ouvrir avec une clé ou un badge sans contact. S'il échoue avec son badge, il utilise sa clé. Ainsi, la programmation de la séquence de reconnaissance a bien évidemment de l'importance dans la stratégie globale de sécurité.

D'ailleurs, c'est sur ce plan de la stratégie globale de sécurité, que la biométrie se révèle ou pas utile. A quoi sert un contrôle biométrique sur une porte en carton ondulé ?

D. K.



© FACE AU RISQUE/FACOMPO



© FACE AU RISQUE/STEPHANIE GOUITE