Contrôle d'accès : Biométrie ou carte ?

L'info Expoprotection

D'un côté, le badge sans contact, support d'identification reconnu pour sa robustesse, sa simplicité de déploiement et sa capacité à concentrer les usages. De l'autre, la biométrie, technologie de pointe exigeante, capable d'assurer une sécurité de haut niveau, mais réservée à un champ d'applications strictement encadré. Alors, biométrie ou badge ? Difficile de les comparer. Encore plus de les opposer, tant leurs usages diffèrent, même si parfois ils convergent. Il est donc plus avantageux de les associer en tirant bénéfice de leurs performances respectives pour l'exploitation d'un système de contrôle d'accès.

Il est difficile de comparer la biométrie ou le badge en matière de contrôle d'accès : car, si leurs usages diffèrent, parfois ils convergent. © Thinkstock

Jamais l'un sans l'autre ?

Si le badge est largement rentré dans les usages et reste le support de prédilection du contrôle d'accès électronique, le marché de la biométrie est encore peu développé en France. D'abord parce que la Cnil veille, à juste titre, au bon usage des technologies d'identification du vivant. Ensuite, parce que la biométrie n'a pas pour vocation à concurrencer le badge sur tous les terrains. Contrairement à un badge multiapplication, la biométrie se limite en général à un seul usage. De fait, les situations où la biométrie se substitue au badge ne sont, en fin de compte, pas si variées : oui, un lecteur du contour de la main peut avantageusement remplacer le badge dans une entreprise, à l'entrée d'une salle de sport ou d'une cantine. Pour le pointage, c'est aussi une solution très conviviale et simple d'emploi.

ntégration réussie pour ce lecteur d'empreintes digitales Fingerprint, directement installé dans la porte ADS 60 DL de fabrication Batistyl.

Mais nombreuses sont les applications où la biométrie ne peut s'imposer sans l'usage d'un support associé, ne serait-ce que pour rester en conformité avec les exigences de la Cnil. Dès lors qu'on sort des petites installations autonomes pour des applications simples (un lecteur Biovein pour le contrôle d'accès d'une petite entreprise demeure une excellente solution), il semble difficile d'envisager la biométrie seule. Pour l'exploitation d'un système de contrôle d'accès et des usages plus développés (multiapplication), le badge reste un élément incontournable. Comme l'explique Pierre-Antoine Larrera de Morel (Stid), ce constat fournit l'occasion d'associer le meilleur des deux technologies : « A un moment ou à un autre, il y a de grandes chances pour que l'exploitant d'un site soit amené à utiliser des badges. Autant en profiter pour y intégrer de la biométrie, des empreintes digitales, par exemple. Les avantages sont évidents : les usagers disposent d'un moyen d'identification bien plus sécurisé, qui respecte les recommandations de la Cnil, dans la mesure où les données biométriques sont stockées sur un support individuel. »

« A un moment ou à un autre, il y a de grandes chances pour que l'exploitant d'un site soit amené à utiliser des badges »

Biométrie, les règles du jeu

En effet, on ne fait pas n'importe quoi avec la biométrie. En France, la Cnil applique un cadre strict à l'utilisation des technologies basées sur la reconnaissance du corps humain, de son comportement. Le nombre de modalités biométriques est vaste (iris, forme du visage, signature, voix, posture, etc.). Nous retiendrons les plus significatives en termes d'applications, à savoir l'empreinte digitale, le réseau veineux du doigt, la morphologie de la main. Pour rappel : sauf autorisation exceptionnelle, la Cnil impose d'associer l'empreinte digitale à un support individuel contenant les données personnelles de l'utilisateur pour le contrôle d'accès sur le lieu de travail. Les données relatives au réseau veineux du doigt sont, quant à elles, limitées à un stockage en local dans le lecteur biométrique, cette restriction imposant le déploiement de solutions autonomes. Seuls les gabarits du contour de la main peuvent être stockés dans une base de données pour une exploitation centralisée.

Tout projet d'exploitation d'une modalité biométrique dans un cadre professionnel doit donc faire l'objet d'une déclaration auprès de la Cnil, dans laquelle l'exploitant reconnaît avoir pris connaissance des règles d'utilisation et s'engage bien sûr à les respecter. En France, résume Pierre-Antoine Larrera de Morel, « dans le cadre d'applications de contrôle d'accès tertiaire ou industriel, la biométrie n'a pas toujours tous les atouts pour vivre seule ». Ce qui n'empêche pas de voir les usages évoluer : la Cnil a récemment étendu le champ des autorisations à la biométrie multimodale, empreinte + veine du doigt, technologie autorisée pour le contrôle d'accès sur le lieu de travail (l'usage de l'empreinte en technologie doigt seul étant toutefois soumis à une procédure d'autorisation spécifique, souvent lourde, auprès de l'organisme de régulation).

Lecteur Digitouch LDS, Vauban Systems : une solution biométrique sécurisée par Stid

Dédié aux applications haut de gamme, ce lecteur d'empreintes digitales conçu par Vauban Systems, le Digitouch LBS, intègre la technologie Stid de lecture sécurisée de badge DESFire EV1. Solution évolutive, le Digitouch offre plusieurs possibilités d'identification : empreinte + badge, empreinte seule, badge seul, code + empreinte, code seul. Le terminal dispose d'un écran couleur tactile permettant la saisie d'un code, ou encore l'affichage de la photo de l'utilisateur lorsqu'il s'identifie. Dans sa version autonome, le clavier affiche également le journal des événements.

« La biométrie n'a pas toujours tous les atouts pour vivre seule »

La sécurité avant tout ?

Cependant, et de manière un peu paradoxale, les conditions d'exploitation de la biométrie sont d'autant plus définies qu'il règne une certaine confusion dans ses usages. A quoi sert la biométrie ? En priorité, à augmenter le niveau de sécurité d'un accès en demandant à l'utilisateur une preuve irréfutable de son identité. « C'est son objectif premier, confirme Rodolphe Leiserson, de la société Vauban Systems. Toutefois, avec le développement de solutions d'identification autonomes « packagées », la biométrie est de plus en plus choisie pour ses qualités pratiques et son confort d'utilisation. D'où une confusion assez répandue entre la notion de confort et celle de sécurité. En conséquence, seule une petite fraction d'exploitants souhaitant s'équiper d'un système biométrique sait exactement pourquoi elle achète de la biométrie... » Plus de badge perdu ou volé, plus de code oublié...

Il faut reconnaître que la biométrie se présente comme une technologie d'identification idéale, et pour tout dire, très séduisante. « Avec la biométrie, la notion de confort est immédiatement perceptible, poursuit Rodolphe Leiserson : plus de contraintes, l'utilisateur passe son doigt ou sa main pour la lecture du réseau veineux ou du contour de la main, et il entre sans avoir besoin de sortir son badge. » L'utilisateur est son propre pass, en somme. Mais jusqu'où peut-on « rêver » ainsi la biométrie ? Un coût encore élevé (un lecteur biométrique est un produit de haute technologie), les restrictions de la Cnil et un certains nombre de contraintes de mise en œuvre limitent moins de restrictions. En effet, à partir du moment où on a la possibilité de centraliser des données biométriques, le champ des possibilités s'élargit. Mais, pour les raisons évoquées, il est conseillé d'employer la biométrie à des fins bien identifiées. A savoir, renforcer la sécurité d'un accès avec une procédure d'authentification forte. « Les contraintes d'exploitation de la biométrie donnent, en fin de compte, un véritable sens à l'application de ces technologies d'identification », en conclut Rodolphe Leiserson.

Lecteur d'empreintes digitales Digitouch NS, Vauban Systems

Ce lecteur biométrique d'empreintes digitales est compatible avec la technologie Natural Security. Il permet de mutualiser les applications de contrôle d'accès physique et logique, de paiement et de signature électronique. Capable de gérer jusqu'à 15 000 utilisateurs, il est équipé d'une liaison TCP/IP et fonctionne en mode autonome ou centralisé.

Le badge, cet incontournable

Le badge reste un support particulièrement adapté pour concentrer les usages, en sécurité et au-delà. Avec la multiapplication, les possibilités sont remarquables : on franchit des accès, on se paye un café, on y conserve ses gabarits d'empreintes... © Thinkstock

De son côté, le badge reste un support particulièrement adapté pour concentrer les usages, en sécurité et au-delà. Avec la multiapplication, les possibilités sont remarquables : on franchit des accès, on se paye un café, on y conserve ses gabarits d'empreintes, etc. Autant d'applications qui supposent de pouvoir centraliser les données d'un parc de badges. « Les systèmes de mise à jour dynamique, précise Pierre-Antoine Larrera de Morel, impliquent de pouvoir charger des droits sur un support doté de capacités de lecture-écriture. Ce support peut difficilement être autre chose qu'un badge équipé d'une puce à mémoire. » En conséquence, une technologie biométrique utilisée seule ne peut pas investir ce champ d'applications. Multi-usage, le badge est aussi un insigne qui indique l'appartenance de son porteur à une entreprise. Par sa présence, il permet de signaler qu'untel n'est pas un intrus. Le badge reste donc incontournable pour une quantité d'applications mais aussi d'environnements, de par sa robustesse et sa fiabilité. En extérieur, alors qu'un lecteur de badges ne pose pas, ou peu, de contraintes, l'installation d'un lecteur biométrique est beaucoup plus délicate. Les capteurs optiques utilisés pour la reconnaissance des empreintes digitales ou du réseau veineux sont sensibles aux rayonnements émis par le soleil, mais aussi aux rayures tracées sur la vitre de protection. Le froid peut nuire à la reconnaissance des veines du doigt, etc.

De plus, un lecteur biométrique est un équipement fragile. C'est un point à prendre en compte lors de l'installation : un lecteur biométrique est un dispositif de haute technologie qui nécessite d'être protégé des tentatives de vandalisme. Un lecteur de badge est un simple boîtier en plastique connecté à une centrale, elle-même abritée dans un local. Par ailleurs, le badge conserve l'avantage sur le plan de la fluidité de passage. Badger à la volée est quasi instantané. S'identifier devant un lecteur biométrique demande deux à trois secondes d'attente à l'utilisateur, le temps de procéder à la lecture du doigt, de la veine, du contour de la main, puis de procéder à sa comparaison avec un gabarit stocké sur un support individuel, en local ou dans une base de données suivant la modalité choisie. Difficile, le cas échéant, de déployer des équipements biométriques sur les accès principaux ou encore, à l'entrée d'un parking. Enfin, un badge sans contact passe, pour ainsi dire, à tous les coups devant un lecteur. Avec la biométrie, il faut s'attendre à des situations de faux rejets et de fausses acceptations. Même si son niveau de fiabilité est satisfaisant, la biométrie gagnerait encore à se hisser au niveau du badge.

« Beaucoup de lecteurs biométriques ne sont compatibles qu'avec la technologie Mifare Classic »

Biométrie et système : des contraintes à identifier

Pour des besoins simples et un nombre d'utilisateurs restreint, les systèmes biométriques autonomes représentent une bonne solution sécurisée qui ne pose pas de contraintes particulières de mise en œuvre.

Pour des besoins simples et un nombre d'utilisateurs restreint, les systèmes biométriques autonomes représentent une bonne solution sécurisée qui ne pose pas de contraintes particulières de mise en œuvre. Cependant, Laurent Rouyer, directeur des ventes Evolynx, a raison de préciser que « dès lors qu'on intègre de la biométrie dans des solutions systèmes, sur des sites étendus et/ou pour des applications sensibles, le déploiement se révèle vite plus complexe ». Installer et exploiter une solution d'identification biométrique dans un système de contrôle d'accès implique, en effet, de considérer plusieurs aspects. A commencer par l'investissement à effectuer : un lecteur biométrique reste plus cher qu'un lecteur de badges. Il est aussi plus complexe à mettre en œuvre. Du fait, principalement, des limitations imposées par la Cnil, en fonction de la modalité biométrique choisie. L'empreinte digitale, technologie la plus répandue en contrôle d'accès, suppose l'emploi de cartes sans contact à mémoire permettant de stocker un ou plusieurs gabarits d'empreintes. Il faudra donc opter a minima pour une technologie Mifare. Il faudra également tenir compte des étapes de mise en œuvre du support : mapping de la mémoire, définition des clés de cryptage, etc. Par ailleurs, pour une sécurité optimale, une technologie de puce sécurisée de dernière génération (DESFire EV1, Mifare +) est conseillée. C'est le point de vue défendu par la société Stid, qui recommande l'utilisation de puces sécurisées dans le cadre du développement d'applications biométriques. « Dès lors qu'on souhaite associer de la biométrie à un badge, il est essentiel d'adopter un support vraiment sécurisé, estime Pierre-Antoine Larrera de Morel. La technologie Mifare Classic, déployée sur de nombreux systèmes de contrôle d'accès, est peu ou pas sécurisée. Voilà pourquoi nous déployons des applications sur la base de la technologie DESFire EV1, qui permet de cumuler les meilleures performances en sécurité et en multiapplication. » Il y a cependant une contrainte à s'éloigner de la technologie dominante : « Beaucoup de lecteurs biométriques ne sont compatibles qu'avec la technologie Mifare Classic, nuance Laurent Rouyer. Dès qu'on s'éloigne de cette technologie, pour choisir des puces Legic par exemple, le nombre de lecteurs compatibles est beaucoup plus restreint. » Enfin, notons qu'une base de données d'empreintes n'est pas duplicable ni transférable. On peut transférer et réaffecter une base de données de badges à un nouveau système sans aucune contrainte, d'un simple copier-coller. Dans le cas de l'empreinte digitale, un changement ou un renouvellement de système obligera à enrôler à nouveau tous les utilisateurs.

Dans le domaine de la reconnaissance du réseau veineux, le déploiement de lecteurs autonomes est obligatoire. Un point à bien prendre en compte, dans la mesure où la mise à jour des droits des utilisateurs devra être effectuée sur chaque lecteur. C'est une procédure qui peut vite devenir fastidieuse si des dizaines de lecteurs sont installés. A limiter en nombre, donc. Pour le contour de la main, une gestion centralisée est possible et autorise plus de souplesse dans le déploiement et la mise à jour des équipements. Malgré cet avantage, les lecteurs du contour de la main, assez volumineux, réduisent les possibilités d'installation. Quelle que soit la modalité biométrique choisie, il faudra aussi considérer l'étape incontournable de l'enrôlement. Celui-ci impose la présence de l'utilisateur, dont la prise d'empreinte, du réseau veineux, de la forme de la main, nécessitera un lecteur et un logiciel spécifiques. Dans le cas où un badge est également utilisé, il faudra prévoir deux enrôlements. En général, les deux stations d'enrôlement sont distincts et rendent les procédures plus longues (une solution avantageuse consiste à intégrer l'enrôlement biométrique dans la solution logicielle de supervision : c'est le cas de certaines grosses installations équipées par Evolynx).

Fiabiliser l'identification biométrique...

La biométrie a donc ses contraintes. Elle n'en demeure pas moins une technologie performante et conviviale. Optimiser la fiabilité de l'identification, c'est l'enjeu de la biométrie multimodale, technologie combinant deux modalités comme l'empreinte et le réseau veineux du doigt. En effet, aucune biométrie n'étant fiable à 100 %, il y a un intérêt évident à associer deux biométries dans un lecteur pour réduire encore le taux de faux rejets. Car la biométrie reste une technologie exigeante pour l'utilisateur : des doigts sales ou blessés peuvent invalider l'identification de l'empreinte digitale. Certains individus ne possèdent pas, ou très peu, de sillons cutanés (ou minuties) au bout des doigts. Pour la reconnaissance du réseau veineux, une mauvaise circulation sanguine peut entraver l'identification. L'une ou l'autre technologie peut donc se révéler défaillante. Le lecteur MorphoAccess VP (empreinte + veine du doigt) développé par Morpho (groupe Safran) constitue la référence actuelle dans ce domaine *.

« De nouveaux champs d'application font leur apparition »

... et élargir les champs d'applications

Par ailleurs, comme nous l'avons vu, badge et biométrie sont souvent associés. Comment exploiter le meilleur de l'un et de l'autre ? Le concept développé par la société Natural Security apporte une réponse qui pourrait bien libérer les usages de la biométrie, tout en garantissant l'intégrité des données personnelles de l'utilisateur, dans n'importe quel environnement. Comme l'indique André Delaforge (Natural Security, Biometrics Alliance Initiative), « la biométrie s'est jusqu'à présent déployée principalement dans deux champs d'application : les applications gouvernementales et le contrôle d'accès physique. De nouveaux champs d'application font leur apparition. Dans un contexte transactionnel, la biométrie permet de prouver qu'un utilisateur est bien là au moment de la réalisation d'une opération ». Utilisée pour tous types d'opération de paiement, d'accès à des services, la biométrie peut donc être utilisée de manière plus transversale : en magasin, sur un automate bancaire, sur Internet, etc. C'est l'objectif du projet lancé par Natural Security qui travaille sur le développement d'un dispositif d'authentification forte, associant identification biométrique et technologie sans contact moyenne distance, au protocole Zigbee. « Natural Security a pour ambition de s'imposer comme le standard d'authentification de référence, utilisable à domicile ou en entreprise, en agence ou en magasin et sur automate, pour payer et accéder à des services », ajoute André Delaforge. L'utilisateur peut ainsi effectuer des paiements sur des terminaux dédiés, capables de reconnaître son badge à distance. Il lui suffit simplement de valider une transaction ou l'accès à un service, à l'aide de son doigt, en évitant toute manipulation de son support personnel lors de l'authentification.

Un dispositif simple et universel, qui supprime ou complète la saisie d'un code PIN. Un lecteur biométrique d'empreinte digitale supportant la technologie Natural Security est en cours de développement chez Vauban Systems. « La technologie de badge actif est au point. Il reste à finaliser un système permettant d'associer une carte à contact (une carte bleue, par exemple) à un étui RFID pour une utilisation à distance, précise Rodolphe Leiserson. D'ici fin 2012, l'ensemble de la solution sera opérationnelle. » Le standard Natural Security est adaptable sur de nombreux autres terminaux, comme le montre son intégration à la tablette biométrique Tazpad, depuis janvier dernier. Il en est de même pour les données de l'utilisateur qui, à l'avenir, pourront être déportées sur un smartphone utilisant la technologie NFC (Near Field Communication).

*** À noter qu'il s'agit du premier terminal biométrique multimodal à avoir obtenu, en juillet 2011, une autorisation de la Cnil pour le contrôle d'accès en entreprise. L'autorisation a été accordée pour une utilisation en mode identification, où les données biométriques sont conservées dans le terminal.**