Réponses aux questions les plus fréquemment posées
La Biométrie

La Biométrie

La biométrie se rapporte à l'identification automatique d'une personne, basée sur ses caractéristiques physiologiques ou comportementales. Cette méthode d'identification est préférée aux méthodes traditionnelles impliquant des mots de passe et des numéros de BORNE pour différentes raisons:
(i) La personne à identifier doit être physiquement présente au moment de l'identification
(ii) Les techniques biométriques éliminent la nécessité de se rappeler un mot de passe ou de porter un badge.
Avec une utilisation de plus en plus grande des ordinateurs comme véhicules de technologie de l'information, il est nécessaire de limiter l'accès aux données personnelles.
Les techniques biométriques peuvent potentiellement empêcher l'accès non autorisé ou l'utilisation frauduleuse de TPE, de téléphones cellulaires, de cartes à puce, de PC, de postes de travail, et de réseaux informatiques.

Les PINs et les mots de passe peuvent être oubliés, et des méthodes fondées sur des tokens d'identification comme des cartes d'accès, des passeports et des permis de conduire peuvent être dupliquées, falsifiées, volées, ou perdues. De ce fait les systèmes biométriques d'identification montrent un renouveau d'intérêt pour le grand public et les professionnels.
Divers types de systèmes biométriques sont employés pour l'identification en temps réel, les systèmes les plus populaires et les plus évolués étant basés sur la reconnaissance de l'empreinte digitale. Cependant, il y a d'autres systèmes biométriques comprenant le balayage d'iris, le balayage de la géométrie rétinienne, balayage de parole, faciale, et de la main…

Le mot Anglais "Biometric", utilisé pour définir "La mesure des éléments morphologiques des êtres humains", est fréquemment traduit en français par "Biométrie".
La définition de "Biométrie", est en fait (Petit Robert) : "Science qui étudie à l'aide de mathématiques (statistiques, probabilités) les variations biologiques à l'intérieur d'un groupe déterminé".
En français, le terme représentant "La mesure d'éléments de l'homme" est "Anthropométrie".
Par commodité (similitude avec la langue anglaise), le terme "Biométrie" est utilisé à la place du terme "Anthropométrie".

Pour prouver son identité il existe 3 possibilités :
- Ce que l'on possède (carte, badge, document) ;
- Ce que l'on sait (un mot de passe) ;
- Ce que l'on est - il s'agit de la biométrie.

Les 2 premiers moyens d'identification peuvent être utilisés par des fraudeurs pour usurper l'identité d'un tiers.
La biométrie permet l'identification d'une personne sur la base de caractères physiologiques ou de traits comportementaux automatiquement reconnaissables et vérifiables.

Il existe 2 catégories de technologies biométriques :
- Les techniques d'analyse du comportement :
  - La dynamique de la signature (la vitesse de déplacement du stylo, les accélérations, la pression exercée, l'inclinaison).
  - La façon d'utiliser un clavier d'ordinateur (la pression exercée, la vitesse de frappe).

Les techniques d'analyse de la morphologie humaine (empreintes digitales, forme de la main, traits du visage, dessin du réseau veineux de l'iris, la voix). Ces éléments ont l'avantage d'être stables dans la vie d'un individu et ne subissent pas autant les effets du stress par exemple, que l'on retrouve dans l'identification comportementale.

Pourquoi utiliser la biométrie ?

La biométrique est un domaine émergeant où la technologie améliore notre capacité à identifier une personne. La protection des consommateurs contre la fraude ou le vol est un des buts de la biométrie. L'avantage de l'identification biométrique est que chaque individu a ses propres caractéristiques physiques qui ne peuvent être changées, perdues ou volées. La méthode d'identification biométrique peut aussi être utilisée en complément ou remplacement de mots de passe. Plusieurs raisons peuvent motiver l'usage de la biométrie :

Une haute sécurité en l'associant à d'autres technologies comme le cryptage, le single sign-on...

Confort - En remplaçant juste le mot de passe, exemple pour l'ouverture d'un système d'exploitation, la biométrie permet de respecter les règles de base de la sécurité (ne pas inscrire son mot de passe à coté du PC, ne pas désactiver l'écran de veille pour éviter des saisies de mots de passe fréquentes). Et quand ces règles sont respectées, la biométrie évite aux administrateurs de réseaux d'avoir à répondre aux nombreux appels pour perte de mot de passe (que l'on donne parfois au téléphone, donc sans sécurité).

Sécurité / Psychologie - Dans certains cas, particulièrement pour le commerce électronique, l'usager n'a pas confiance. Il est important pour les acteurs de ce marché de convaincre le consommateur de faire des transactions. Un moyen d'authentification connu comme les empreintes digitales pourrait faire changer le comportement des consommateurs.

Performances des systèmes

Il est impossible d'obtenir une coïncidence absolue (100% de similitude) entre le fichier "signature" créé lors de l'enrôlement et le fichier "signature" créé lors de la vérification. Les éléments d'origine (une image, un son...) utilisés pour les traitements informatiques ne pouvant jamais être reproduit à l'identique. Les performances des systèmes d'authentifications biométriques s'expriment par :

T.F.R. - Taux de faux rejets : pourcentage de personnes rejetées par erreur.

T.F.A. - Taux de fausses acceptations : pourcentage d'acceptations qui n'auraient pas dû être retenues.

Ces taux vont dépendre de la qualité des systèmes, mais aussi du niveau de sécurité souhaité.

Comment choisir une technologie ?

Le principe de fonctionnement est le même pour tous :
- Capture de l'information à analyser (image en général).
- Traitement de l'information et création d'un fichier "signature" (éléments caractéristiques de l'image), puis mise en mémoire de ce fichier de référence sur un support (disque dur, carte à puce, code barre).
- Dans la phase de vérification, l'on procède comme pour la création du fichier "signature" de référence, ensuite on compare les deux fichiers pour déterminer leur taux de similitude et prendre la décision qui s'impose.

Plutôt que de comparer les performances de ces systèmes, il faut surtout tenir compte de l'environnement de leur usage. Chaque technologie possédant des avantages et des inconvénients, acceptables ou inacceptables suivant les applications. Ces solutions ne sont pas concurrentes, elles n'offrent ni les mêmes niveaux de sécurité ni les mêmes facilités d'emploi.

D'où vient cet engouement pour la biométrie ?

La technologie existe depuis de nombreuses années particulièrement pour les empreintes digitales.
La diffusion en masse était difficile car ces technologies ont besoin d'importantes puissances de calcul qui étaient trop onéreuses.
D'une manière générale, les besoins de solutions de sécurité forte sont en pleine croissance.
Pour les empreintes digitales il y a un autre facteur important concernant l'explosion de ce marché. En effet quelques sociétés (elles ne sont pas nombreuses car les investissements sont très lourds), dont Thomson CSF Semiconducteurs en France, SONY Biometrics au Japon, etc…, ont développé des capteurs silicium pour prendre l'image d'une empreinte digitale.
Leurs avantages par rapport aux lecteurs optiques sont nombreux :
Moins cher ;
Plus petit ;
Facile à intégrer dans toutes les applications.

L'usager craint-il la biométrie ?

Il y a encore quelques années la réponse était "oui". L'usager potentiel associait "empreintes digitales" à « police » et à « fichage ».
Dans un fichier caractérisant nos empreintes digitales, il n'y a pas d'information sur notre vie privée. C'est le fichier d'information sur notre personne qui est à mettre en cause, et là, même sans biométrie ce fichier peut exister.
Aujourd'hui, on se rend bien compte que c'est justement le moyen le plus efficace pour protéger notre bien, qu'il soit matériel ou sous la forme de données informatiques.

La biométrie est-elle concurrente de la carte à puce ?

Pas du tout, ces 2 technologies sont et seront souvent associées.
Les cartes à puce sont des produits de plus en plus fiables pour sécuriser des informations.
L'association de la biométrie et de la carte à puce permet d'être certain que l'on est bien le possesseur autorisé de cette carte et des informations qu'elle contient.
Dans un premier temps, on utilise la mémoire de la carte à puce pour enregistrer son empreinte (pas de base de données).
Dans le futur, les capteurs d'empreintes et une partie du logiciel de comparaison seront également sur la carte.

Mon empreinte digitale est-elle stockée?

Non, nos produits utilisent l'information d'identification unique produite quand le doigt est balayé. Ces données sont sauvées comme dossier numérique chiffré pour une authentification rapide. Cette approche est protégée et préserve votre intimité personnelle avec une plus grande certitude que pour les systèmes d'accès basés sur des badges. Il n'est pas possible de recréer des empreintes digitales d'utilisateurs de l'information stockée pour représenter les utilisateurs inscrits.

Qu'est ce que l'analyse des points de minutie?

Les arêtes d'empreinte digitale ne sont pas continues et droites. Au lieu de cela elles sont cassées, bifurquées, ou interrompues. Les points auxquels les arêtes finissent, bifurquent des points de minutie, et ces points de minutie uniques identifient l'information. Il y a différents types de points de minutie. Le premier type est une fin d'arête qui se produit quand une arête finit abruptement.

Une bifurcation d'arête est une arête qui se divise en deux branches ou plus. Un point est une arête qui n'apparaît pas en fait comme ligne , mais à la place comme point minuscule ou petite île.
Si une arête se sépare en deux et puis se reforme, on l'appellera clôture. Un autre type d'arête est une arête courte. Une arête courte se produit quand il y a une arête très petite, mais qui est encore plus grande qu'un point.

Un autre trait des points de minutie est leur orientation. La direction que prend le point de minutie est considérée comme son orientation relative.

Une troisième caractéristique est la fréquence spatiale. La fréquence spatiale se rapporte à la distance qui séparent chaque arête. La quatrième caractéristique est une courbure qui est le taux de l'orientation de l'arête. La caractéristique finale est la position du point de minutie. La position est prise en utilisant les axes des x et des y dans un sens absolu ou par rapport à un point fixe tel que le noyau et est employée pour l'analyse.

Vérification ou identification.

La vérification implique de confirmer ou de nier l'identité d'une personne (suis-je ce que je me réclame être - une comparaison 1 à 1).
Dans l'identification, on doit établir l'identité d'une personne (qui suis-je – une comparaison de 1 à n). Chacune de ces dernières approches a son ensemble d'avantages et d'inconvénients. Les clients accèdent aux besoins et les préférences détermineront la meilleure approche pour leur application.

Est-ce que les doigts "non vivant" doigt marchent?

La technologie Istec ne reconnaît que les doigts vivants, car les capteurs utilisés permettent d'identifier de la chaleur ou une pulsation cardiaque, voire d'autres critères de l 'élément vivant .

Que se passe t-il si j'endommage mon doigt?

Aucun problème, un administrateur peut vous inscrire avec un doigt différent. Nous suggérons d'enrôler deux doigts par personne (un doigt par main) afin réduire au minimum ce risque.

Peut-il s'intégrer dans mon système existant de sécurité?

Grâce aux SDK, Nous offrons les produits qui incluent les types multiples de possibilités d'intégration. En outre, nos produits qui utilisent Microsoft WINDOWS et autres systèmes centralisent les données en réseaux pour le stockage. Ces données peuvent être exportées dans un environnement existant si désiré.

Est-ce que cela fonctionne avec mon système Windows?

Nos produits d'accès logiques sont entièrement intégrés avec le modèle Windows NT et 2000 de sécurité et sur tous les autres OS MICROSOFT (95/98, XP…). Ceci élimine le besoin de reproduire des profils d'utilisateur et de maintenir les systèmes multiples.

Applications:

La biométrie est un secteur qui évolue rapidement avec un réel engouement de la part des entreprises. Des technologies biométriques peuvent être employées pour empêcher l'accès non autorisé aux équipements, ordinateurs individuels (laptop, desktop, PDAs), réseaux informatiques, serveurs de système, applications spécifiques et dossiers spécifiques. À l'avenir, la biométrie sera employée pour contrôler l'accès aux: TPE, téléphones cellulaires, smart card, transactions conduites par l'intermédiaire du téléphone et de l'Internet (commerce électronique et opérations bancaires électroniques). Dans un proche avenir vous mettrez en marche votre voiture ou entrerez dans votre maison sans souci et en évitant de vous rappeler où vous avez laissé vos clefs.

Quelle est la réglementation de la CNIL en France en rapport à la biométrie ?

La CNIL prescrit de ne pas stoker sur des supports fixes (disque) des empreintes pour des applications non essentielles, surtout sans l'autorisation de la personne concernée, au même titre que pour une photographie d'identité, etc…
Dans la mesure où ces données sont sécurisées et restent la possession de leur « émetteur », la CNIL ne voit pas d'objection à l'utilisation de tels systèmes.

Dans le cadre d'applications où ces données confidentielles sont stockées sur un support sécurisé (carte à puce sécurisée, données cryptées, utilisation de la signature de l'empreinte – qui ne permet pas la reconstitution du dessin de l'empreinte - et non pas son image informatique – permettant de refabriquer l'empreinte, etc…) et avec l'autorisation de leur émetteur les spécifications de la CNIL sont conservées.