DOSSIER TECHNIQUE

TECHNIQUES DE CONTROLE D'ACCES PAR BIOMETRIE

Juin 2003

Commission Techniques de Sécurité Physique

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, Rue Pierre Semard
Téléphone : 01 53 25 08 80 Fax : 01 53 25 08 88
Mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.fr

Table des Matières

1 Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la conception de ce document, tout particulièrement :

Thierry	AUTRET	Ernst & Young
Robert	BERGERON	Cap Gemini Ernst & Young
Muriel	COLLIGNON	IBM
Marie-Agnès	COUWEZ	Clusif
André	DENIS	André Denis Consultants
Jean-Claude	GANDOIS	Legrand
Guy	KHOUBERMAN	Acoss
Michel	LECLERC	Jerlaure
Jean-Yves	MARTIN	Ares Global Service

2 Préambule

La sécurité est une préoccupation de plus en plus importante au sein des entreprises et commence par l'accès à l'information. Pour se prémunir contre d'éventuelles personnes indélicates, une nouvelle technique de contrôle d'accès a fait son apparition et ne cesse de croître depuis 1997 : il s'agit des contrôles d'accès par les systèmes biométriques. Ces systèmes sont utilisés aussi bien pour des contrôles d'accès physiques que pour des contrôles d'accès logiques. Depuis 2001, sont organisés des salons professionnels entièrement consacrés à ce type de technique.

Les techniques de contrôle d'accès sont basées sur les critères suivants :

- Ce que l'on sait.
- Ce que l'on possède.
- Ce que l'on est.

ou sur une combinaison de ces critères.

L'objet de ce document est de traiter le troisième point.

Dans le cadre de cette étude, les personnes qui font l'objet d'un contrôle d'accès ont volontairement déposé leurs caractéristiques biométriques (cf : le badge dans les entreprises)

Exemples :
Dans le domaine judiciaire : recherche de candidats probables dans une base de données afin de trouver l'identité correspondant à des caractéristiques biométriques. (Identification)

Dans le domaine du contrôle d'accès : stockage d'une empreinte digitale dans une carte à puce (1 pour 1) et vérification que l'empreinte du demandeur de droits est bien la même que celle qui est dans la carte. (Authentification)

D'autres utilisations de la biométrie sont possibles : recherche (ADN, dentition, oreille, battement du cœur…), contrôle horaire, tests de présence, preuves au cours d'une enquête, mais leur étude ne fait pas partie du présent document.

3 Pourquoi la biométrie

3.1 Définitions

Un système de contrôle biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à un individu : physique, comportement…

Le mot "biométrie" utilisé dans le domaine de la sécurité est une traduction de l'anglais "biométrics" qui correspond en fait à notre mot anthropométrie.

Le mot français biométrie définit "l'étude mathématique des variations biologiques à l'intérieur d'un groupe déterminé".

Dans la suite du document pour plus de clarté, nous utiliserons la définition "franglaise" du terme qui est passée dans le langage "sécurité" courant : biométrie.

La biométrie est basée sur l'analyse de données liées à l'individu et peut être classée en trois grandes catégories :

- Analyse basée sur l'analyse morphologiques. (empreinte digitale, forme de la main, traits du visage, réseau veineux de la rétine, iris de l'œil, voix, etc.)
- Analyse de traces biologiques. (odeur, salive, urine, sang, ADN, etc.)
- Analyse basée sur l'analyse comportementale. (dynamique du tracé de signature, frappe sur un clavier d'ordinateur).

Tout d'abord il est important de définir les termes employés.

Il est rappelé que l'identité d'un individu est l'ensemble des données de fait et de droit qui permettent d'individualiser quelqu'un. De là :

- la vérification de l'identité conduit à l'**identification**,
- la preuve de l'identité conduit à l'**authentification.**

Identification
La vérification de l'identité est faite à partir d'une pièce d'identité (document officiel) : ni l'iris de l'œil, ni l'empreinte, ni la voix ne peut donner l'identité. Les personnes faisant l'objet d'une identification ont volontairement déposé leur identité.
La vérification de l'identité demande une base de référence et le but est de vérifier que l'identité de l'individu qui se présente existe bien dans la base de référence.

Authentification
L'authentification est réalisée en deux temps :
vérification de l'identité

La personne déclare son identité en se présentant au contrôle d'accès.
preuve de l'identité
Les éléments biométriques (empreintes, voix, visage, iris…) de la personne sont comparés avec le gabarit de cette (soi-disant) personne, afin de vérifier si son identité est bien la bonne (1 parmi 1).

3.2 Caractéristiques communes des systèmes biométriques

3.2.1 L'unicité.

Pour identifier ou authentifier une personne au sein d'une population donnée, il est nécessaire que la donnée biométrique utilisée soit unique à cette personne. L'empreinte digitale, la rétine et l'iris sont réputés pour présenter des caractéristiques uniques au sein de très larges populations. En particulier, ces techniques permettent de distinguer les vrais jumeaux, et l'empreinte digitale est reconnue juridiquement comme identifiant un individu. Ces caractéristiques uniques tiennent autant à l'environnement aléatoire de leur formation qu'au patrimoine génétique. Cette formation aléatoire est illustrée par exemple par les variations de robe des animaux clonés. D'autres techniques biométriques sont beaucoup plus liées au patrimoine génétique. C'est le cas de la forme de la main ou du visage qui n'ont pas vraiment la capacité de distinguer de vrais jumeaux.

3.2.2 Caractère public d'une donnée biométrique.

Un code personnel (PIN) est secret et doit le rester pour qu'un système de contrôle d'accès fonctionne. Une caractéristique biométrique n'est pas secrète. Elle peut être plus ou moins facilement capturée et imitée. Un système de contrôle d'accès biométrique doit donc prendre en compte cette menace et éliminer les artefacts construits pour le tromper.

3.2.3 Mesure d'un système biométrique.

Un système biométrique n'utilise pas toute l'information contenue dans l'image ou le signal capté. Il en extrait certaines caractéristiques, ce qui réduit la quantité d'information, donc la capacité du système à reconnaître l'unicité d'une donnée. Puis il effectue un calcul et obtient un résultat à partir des données recueillies.
Sa robustesse dépend du nombre de critères retenus et de la méthode de modélisation (ou de calcul) utilisée.

Un système biométrique est alors mesuré par deux paramètres :

- Le taux de fausse acceptation, qui est la probabilité de confusion d'identité (FAR)

- Le taux de faux rejet, qui est la probabilité de ne pas reconnaître une identité lors d'un essai (FRR)

Un troisième paramètre mesure l'utilité du système. C'est le taux d'échec à l'enrôlement, qui traduit la probabilité d'absence d'une caractéristique biométrique pour un individu dans une population (FER).

3.3 Types d'application

Les types d'application les plus courants sont :

- Accès à des locaux sensibles. (équipements techniques, archives, stocks, laboratoires, casino, coffres des banques, etc.)
- Gestion d'horaire, etc.
- Contrôles d'accès logiques.

L'ensemble des secteurs d'activité ayant un besoin d'authentification forte est susceptible de recourir aux contrôles d'accès biométriques.

4 Présentation des techniques

4.1 Morphologie

4.1.1 Empreintes digitales

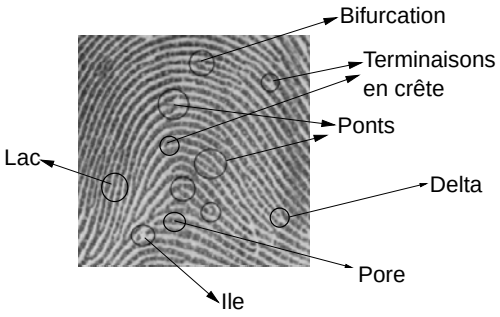
4.1.1.1 introduction

La technique des empreintes digitales est une des techniques les plus anciennes, elle a été développée vers la fin du 19ème siècle par Alphonse Bertillon, fondateur de la police scientifique en France. A cette époque et jusqu'à récemment, une tablette et un encreur sont le matériel utilisé pour la capture d'empreinte. Le premier système automatique d'authentification a été commercialisé au début des années 1960.

4.1.1.2 Définitions

Les minuties : codifiées à la fin des années 1800 en « caractéristiques de Galton[1] », les minuties sont composées, de façon rudimentaire, de terminaisons en crêtes, soit le point où la crête s'arrête, et de bifurcations, soit le point où la crête se divise en deux.
Le noyau est le point intérieur, situé en général au milieu de l'empreinte. Il sert souvent de point de repère pour situer les autres minuties. D'autres termes sont également rencontrés : le lac, l'île, le pont, le croisement, le delta, la vallée, le pore…

Notons que dans l'analyse des minuties, une douzaine de variables doivent être prises en compte.



(source : les dossiers de l'Atica)

[1] Du nom de Sir Francis Galton.

4.1.1.3 Principe de fonctionnement

L'authentification par les empreintes digitales repose sur la concordance entre le fichier d'enregistrement, ou « signature », obtenu lors de l'enrôlement et le fichier obtenu lors de l'authentification.

Ces deux fonctions se décomposent chacune en plusieurs étapes :

Enrôlement

- Capture de l'image de l'empreinte. Les données d'un doigt sont en principe suffisantes à l'enrôlement, mais la plupart des systèmes enregistrent au moins deux doigts (un par main par exemple) pour parer l'indisponibilité résultant de petites blessures.
- Numérisation de l'image afin d'extraire les minuties, ou éléments caractéristiques.
- Enregistrement sur un support. (carte à puce, disque dur…)

Authentification

- Capture de l'image de l'empreinte.
- Numérisation de l'image afin d'extraire les minuties, ou éléments caractéristiques.
- Comparaison entre l'échantillon et le gabarit « signature ».
- Prise de décision.

Lors de la capture de l'image, celle-ci est toujours constituée à partir des points de contact du doigt sur le capteur.

Etapes de traitement

- Lorsque la capture de l'image est réalisée, elle doit être convertie dans un format approprié. L'extraction des minuties est réalisée grâce à différents algorithmes. Il s'agit ensuite par une technique mathématique (segmentation) d'éliminer les informations non utiles au système : niveau de bruit trop élevé (image sale, doigt mal placé).
- L'image est numérisée. Afin de localiser précisément les terminaisons et les bifurcations, les crêtes sont affinées de 5 à 8 pixels à 1 pixel.
  A ce stade, l'image a des distorsions et de fausses minuties, qui peuvent être dues à des cicatrices, de la sueur, un défaut de propreté du doigt comme du capteur. Les minuties vont être filtrées afin de ne conserver que les plus fiables.

Les avis divergent sur le rapport de proportion entre minuties extraites pour l'enrôlement et minuties suffisamment fiables pour la vérification. A partir de 31 minuties extraites, seulement 10 pourront correspondre lors de l'authentification.

A titre informatif, une empreinte numérisée occupe en moyenne entre 250 et 1000 octets.

4.1.1.4 La technique optique

C'est, après l'encre, la technique la plus ancienne et qui a fait ses preuves.
Le principe physique utilisé est celui de « la réflexion totale frustrée[2] » : Le doigt est placé sur un capteur éclairé par une lampe. Une caméra CMDs (Charge Modulation Device) avec CCD (Charged Coupled Device / en français : DTC : Dispositif à Transfert de Charge) convertit l'image, composée de crêtes foncées et de vallées claires, en un signal vidéo retraité afin d'obtenir une image utilisable.
Nous pouvons différencier les terminaux en lumière visible à fenêtre sèche et à fenêtre à film liquide (la fenêtre est l'emplacement où l'utilisateur pose le doigt). Dans ce dernier cas, la fenêtre est nettoyée avant chaque prise de vue par un mélange d'eau et d'éthanol injecté sous le doigt. Des terminaux à image infra-rouge par capteur linéaire intégré sont parfois utilisés, mais présentent les mêmes inconvénients que ceux à lumière visible.

Avantages	Inconvénients
• Son ancienneté et sa mise à l'épreuve.	• Il est possible que l'empreinte d'utilisateurs précédents reste latente, d'où une possibilité de dégradation de l'image par sur-impression.
• Sa résistance aux changements de température, jusqu'à un certain point.	• Apparition possible de rayures sur la fenêtre.
• Son coût abordable.	• D'autre part, le dispositif CCD peut s'user avec le temps et devenir moins fiable.
• Sa capacité à fournir des résolutions de plus de 500 dpi.	• Problèmes de contrastes (doigt propre et sec devient trop clair tandis qu'un doigt humide et recouvert d'un film gras devient très foncé), problème résolu grâce au film liquide mais système mal accepté. (mouille le doigt !)

4.1.1.5 La technique silicium

Cette technique est apparue à la fin des années 90. Le doigt est placé sur un capteur CMDS. L'image est transférée à un convertisseur analogique-numérique, l'intégration se faisant en une seule puce.
Cette technique produit des images de meilleure qualité avec une surface de contact moindre que pour la technique optique. Les données fournies sont très détaillées. Elle possède une bonne résistance dans des conditions non-optimales.
Cette technique est adaptée à un développement de masse, notamment par ses coûts réduits.

[2] Dans la préface du livre collectif sur le Champ Proche Optique [3]J. M. Vigoureux rappelle l'expérience de la réflexion totale frustrée de Newton. Un prisme est éclairé selon une incidence correspondant à la réflexion totale. En posant une lentille sur la face du prisme, Newton s'aperçoit qu'une partie de la lumière est transmise à travers la lentille dans le second milieu. Ce phénomène, maintenant parfaitement décrit par la théorie ondulatoire de la lumière, résulte de l'existence d'une onde évanescente à la surface du prisme.

Avantages	Inconvénients
• Coût assez bas.	• Capteur vulnérable aux attaques extérieures fortuites ou volontaires.

4.1.1.6 La technique ultrason

Très peu utilisée à ce jour, elle repose sur la transmission d'ondes acoustiques et mesure l'impédance entre le doigt, le capteur et l'air.
Cette technique permet de dépasser les problèmes liés à des résidus sur le doigt ou sur le capteur.
Cette technique peut aussi être utilisée par des scanners à ultrasons qui construisent par échographie une image ultra sonore. Elle est considérée comme la plus fiable.

Avantages	Inconvénients
• Facilité d'usage avec de grandes plaques	• Aucun inconvénient technique significatif n'a pu être identifié à ce jour au travers des textes et des témoignages des experts.
• Capacité à surmonter des conditions de lecture non optimales (les poussières sont souvent transparentes aux ultrasons)	• Coût élevé.

4.1.2 Main

La reconnaissance s'effectue à partir de la géométrie de la main dans l'espace (3D) : longueur des doigts, largeur et épaisseur de la paume, dessins des lignes de la main.

Avantages	Inconvénients
• Le résultat est indépendant de l'humidité des doigts et de souillures éventuelles car il n'y a pas de contact direct avec le capteur ou une fenêtre, donc pas de risque d'encrassement. • Facilité de l'enrôlement du point de vue de l'usager et bonne acceptation psychologique. • Faible volume de stockage par fichier.	• Système encombrant. • Risque élevé du taux de fausses acceptations et faux rejets, par exemple à cause d'une blessure ou pour les jumeaux ou les membres d'une même famille. • Cette technique n'a pas évoluée depuis plusieurs années. • Le lecteur est plus cher que pour les autres types de capture de données physiques.

Pour la capture de l'image, la personne pose sa main sur une platine où les emplacements du pouce, de l'index et du majeur sont matérialisés.

Une caméra CCD (Charged Coupled Device / en français : DTC : Dispositif à Transfert de Charge) prend l'image, reliée à un lecteur où sont enregistrées les informations. Ce lecteur inclut des logiciels de traitement et de codage.

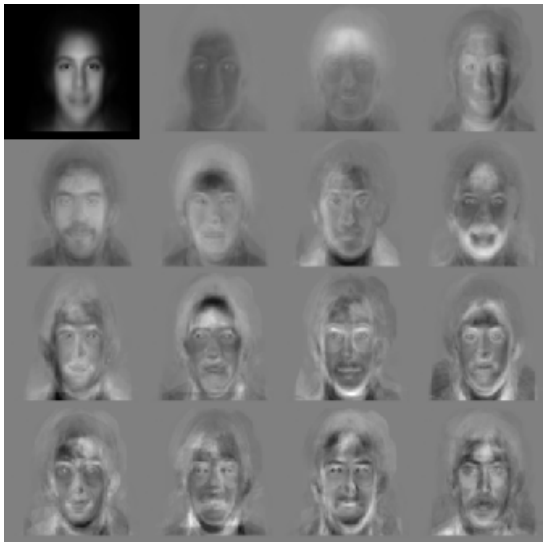
(source : mccccm.free.fr)

Quatre vingt dix caractéristiques sont examinées parmi lesquelles la forme tridimensionnelle de la main, la longueur et la largeur des doigts ainsi que la forme des articulations, et constituent un fichier d'environ neuf octets de mémoire.
Cette technique, très répandue aux USA, a été utilisée lors des J.O. d'Atlanta.

4.1.3 Visage

La reconnaissance à partir du visage se base sur les caractéristiques jugées significatives comme l'écart entre les yeux, la forme de la bouche, le tour du visage, la position des oreilles.
Il existe plus de 60 critères fondamentaux.

Une méthode consiste à décomposer le visage selon plusieurs images en différentes nuances de gris : chaque image met en évidence une caractéristique particulière comme le montre l'image ci-après.



(Source : MIT Face Recognition Demo Page)

D'autres méthodes dérivent de la méthode précédente et ajoutent des informations telles que l'écart entre les yeux, etc.

La plupart des systèmes d'identification du visage utilisent du matériel classique du marché : un ordinateur et une caméra pour capturer l'image. L'image est enregistrée dans une base de données exigeant approximativement 100 octets de mémoire par image.

Avantages	Inconvénients
• Technique peu coûteuse, peu encombrante • Absence de contact avec le capteur, méthode non intrusive pour la personne ; pas de risques pour la santé.	• Les vrais jumeaux ne sont pas différenciés. • Psychologiquement, certaines personnes rejettent leur image photographique (refus de son image, ajout d'accessoires, rôle, religion, critique de la qualité de la caméra, etc.). L'image est considérée comme trop personnelle pour être utilisée. • En tant que contrôle d'accès, le visage n'est pas, traditionnellement, reconnu comme un mécanisme fiable d'authentification. (Peut être dupé par l'utilisation de maquillage ou d'un masque en silicone) • Dans l'état des systèmes actuels, technique trop sensible au changement d'éclairage, changement d'échelle (taille du visage ou distance de la caméra), présence d'arrière plan non stationnaire, changement de position lors de l'acquisition de l'image (inclinaison de la tête ou expression). • Tout élément tel que lunettes de soleil, chapeau, moustache, barbe, percing, blessure peut causer des anomalies avec des systèmes d'identification du visage.

Comme pour tous les contrôles biométriques, cette méthode nécessite quatre étapes :

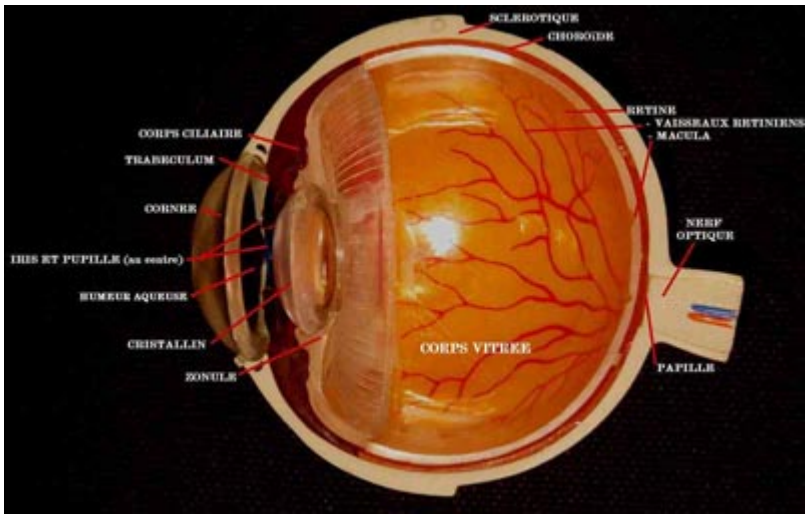
- Capture de l'image.
- Extraction des traits caractéristiques.
- Comparaison avec l'existant.
- Prise de décision.

La capture de l'image s'effectue à partir d'une caméra CCD (Charged Coupled Device / en français : DTC : Dispositif à Transfert de Charge). Chaque image enregistrée nécessite environ 100 octets de mémoire.

L'utilisation de cette technique dans les aéroports, les casinos, certains grands magasins, sort du cadre de cette étude, orientée contrôle d'accès.

4.1.4 Examen de l'œil

4.1.4.1 La rétine



(source :www.institutdelamyopie.com)

La lecture des caractéristiques de la rétine est une technologie utilisée pour des applications de sécurité très élevée : par exemple, des systèmes de balayage de rétine ont été employés dans des applications militaires ou nucléaires.

Les caractéristiques de la rétine sont liées à la configuration géométrique des vaisseaux sanguins. La technologie utilise du matériel spécialisé et un rayon illumine le fond de l'œil. Les systèmes identifient jusqu'à cent quatre vingt douze points de repères. Quelques risques pour la santé ont été révélés et limitent l'utilisation de cette technique à des locaux de haute sensibilité.

Avantages	Inconvénients
• Résistant à la fraude, difficile et long à imiter. • Unicité même chez les vrais jumeaux. • Technique fiable. • La cartographie de la rétine est la même tout au long de la vie, en l'absence de maladie spécifique.	• Nécessité de placer ses yeux à très faible distance du capteur, donc système intrusif mal accepté psychologiquement. • Coût. • Difficile à utiliser en cas de contrôle d'une population importante (temps important). • Installation délicate (hauteur..)

4.1.4.2 L'iris

(source : securiteinfo.com)

Dès 1950, il est fait mention de l'utilisation de l'iris comme moyen d'authentification, mais les travaux de J. Daugmann de 1980 basés sur les ondelettes de Gabor[3] vont conduire à son développement. Il a été démontré que la probabilité de trouver deux iris identiques est inférieur à l'inverse du nombre d'humains ayant vécu sur terre.

Le traitement relativement rapide exige que la personne soit très proche de l'objectif qui doit être un objectif macro.

Le traitement s'effectue en trois phases :

- Recherche de la position de l'iris dans l'image de l'œil.
- Extraction des paramètres caractéristiques.
- Comparaison avec les éléments connus.

Avantages	Inconvénients
• Fiable. • Pas de risque identifié pour la santé.	• Système intrusif mal accepté psychologiquement. (hygiène, proximité de l'objectif) • Contraintes d'éclairage.

4.1.5 Reconnaissance vocale

4.1.5.1 Définitions

La reconnaissance de la voix n'est pas intrusive pour la personne et n'exige aucun contact physique avec le lecteur du système. Le logiciel de reconnaissance peut être centralisé et la voix transmise par le réseau, d'où un impact de réduction des coûts. Le dispositif nécessite un micro en source de capture.

Les systèmes d'identification de la voix sont basés sur les caractéristiques de voix, uniques pour chaque individu. Ces caractéristiques de la parole sont constituées par une combinaison

[3] Dennis Gabor (Prix Nobel de Physique en 1971) a mis au point en 1948 l'holographie, méthode d'enregistrement et de reproduction de l'image d'un objet tridimensionnel.

des facteurs comportementaux (vitesse, rythme, etc…) et physiologiques. (tonalité, âge, sexe, fréquence, accent, harmoniques, …).

4.1.5.2 Principe de fonctionnement

Pour être stockée, la voix est numérisée puis segmentée par unités échantillonnées. Les méthodes sont basées sur des algorithmes mathématiques (Shannon).

Les systèmes d'identification de la voix utilisent soit un texte libre, soit un texte imposé, les mots devant être lus devant un micro.

Avantages	Inconvénients
• Disponible via le réseau téléphonique. • Les imitateurs utilisent les caractéristiques vocales sensibles au système auditif humain, mais ne sont pas capables de récréer les harmoniques de la voix, servant de base à l'identification. Il est quasi impossible d'imiter la voix stockée dans la base de données. • Non intrusif.	• L'utilisation d'un micro nécessite un dispositif adapté présent sur l'environnement. • Sensibilité à l'état physique et émotionnel d'un individu. • Sensibilité aux conditions d'enregistrement du signal de parole : bruit ambiant, parasites, qualité du microphone utilisé, qualité de l'équipement, lignes de transmission. • Fraude possible en utilisant un enregistrement de la voix de la personne autorisée, facilitée dans le cas de système basé sur la lecture d'un texte fixe.

Remarque :
Les inconvénients signalés montrent que ce système est vulnérable et doit être utilisé couplé avec un système d'identification (lecteur de badges).

4.1.6 Exemple de parades

Fondamentalement, quatre parades sont, à ce jour, utilisées pour lutter contre les attaques : texture, température, mouvement, provoquer une réaction de l'utilisateur.

- Texture
  - Ce contrôle est utilisable pour les doigts, les mains et la reconnaissance du visage et permet de vérifier qu'il s'agit bien de la peau et non d'une autre matière (plastique, résine,…).
  - Ce contrôle a de bonnes performances et de faibles coûts.
- Température

- Ce contrôle est utilisable pour les doigts, les mains et la reconnaissance du visage
- Ce contrôle peut être trompé par l'utilisation de source de chaleur annexe (tests positifs réalisés à Milipol : salon (MILItaire et POLice) ayant lieu en France tous les deux ans et présentant de nombreux outils de lutte contre les agressions).

- Mouvement
  - Ce contrôle est uniquement utilisable pour la reconnaissance du visage et de l'iris.
  - Ce contrôle a de bonnes performances et de faibles coûts
- Réaction de l'utilisateur
  - C'est une bonne méthode, mais consommatrice de temps.
  - Impédance caractéristique (doigt vivant,…)

La meilleure chose est sans doute de combiner ces différentes parades.

4.2 Comportement

4.2.1 Signature dynamique

(source : mccccm.free.fr)

Principe de fonctionnement
Ce système fonctionne avec un capteur et un crayon lecteur ou stylo.

Le capteur utilisé est une table à digitaliser électromagnétique « du commerce », dimensions 20 cm x 20 cm. Ce capteur est relié à un PC, qui commande une ouverture de porte, l'accès à une base de données,…Tout mouvement du stylo est pris en compte, en écriture mais aussi jusqu'à environ 2 cm au dessus de la tablette. (vitesse de la signature, variation du rythme du stylo, accélération, pression, calcul de la distance pendant laquelle la plume est suspendue entre deux lettres au dessus de la table à digitaliser, etc.)

Enrôlement
Trois signatures minimum sont demandées pour l'enregistrement d'une nouvelle personne. La cohérence de ces signatures est vérifiée par le logiciel, qui en déduit une « signature de référence moyenne ».
La référence est stockée en mémoire, ou sur une carte à puce.

Ensuite il s'agit de fixer le taux d'acception de la signature appelé seuil. Si ce taux est trop élevé il y a risque d'acceptation de fausse signature et s'il est trop bas, risque de refus de signature valide…

Reconnaissance
La signature faite est comparée à la signature de référence. Si la cohérence est reconnue (système à seuil), l'authentification est acceptée.
Etapes du traitement
Le logiciel ne prend pas en compte la position du stylo, mais bien sa dynamique vectorielle. (vitesse, direction, etc.)

Chaque signature est comparée par échantillonnage aux références enregistrées. Une fourchette d'incertitude est laissée : la note de cohérence est donnée selon le nombre de points dans la fourchette et ceux en dehors. Pour la sévérité du contrôle, la dimension de la marge d'incertitude est paramétrable. (seuil)

La durée du traitement dépend du nombre de signatures en mémoire, par exemple, pour cent signatures, elle est évaluée à moins d'une demie seconde.
La reconnaissance est instantanée si la signature est stockée sur une carte à puce.

Avantages	Inconvénients
• Geste naturel qui responsabilise le signataire.	• Détermination d'un seuil. • Dépendance de l'état émotionnel de la personne. • Utilisation à l'intérieur de bâtiment uniquement.

Exemple :
Le moyen biométrique d'authentification décrit ci-dessous a été utilisé pendant trois ans à l'entrée d'une zone de bureaux traitant de prestations de nature confidentielle. Il commandait l'ouverture de la porte blindée.

4.2.2 Dynamique de la frappe au clavier

La dynamique de la frappe au clavier est caractéristique de l'individu, c'est en quelque sorte la transposition de la graphologie aux moyens électroniques.

Les paramètres suivants sont généralement pris en compte :

- Vitesse de frappe
- Suite de lettres
- Mesure des temps de frappe
- Pause entre chaque mot
- Reconnaissance de mot(s) précis

Avantages	Inconvénients
• Moyen non intrusif qui exploite un geste naturel.	• Dépendance de l'état physique de la personne. (âge, maladies,…)

4.3 Biologie

La biologie est essentiellement utilisée dans le cadre de recherche d'individus à partir de données biologiques, et sort du cadre de ce document.

4.4 Comparatif

La colonne "Physique /Logique" précise l'usage le plus courant de chaque technique.

Techniques	Avantages	Inconvénients	Physique/ Logique
Empreintes digitales	Coût. Ergonomie moyenne. Facilité de mise en place. Taille du capteur.	Qualité optimale des appareils de mesure (fiabilité). Acceptabilité moyenne. Possibilité d'attaque. (rémanence de l'empreinte...)	P/L
Forme de la main	Très ergonomique. Bonne acceptabilité.	Système encombrant. Coût. Perturbation possible par des blessures et l'authentification des membres d'une même famille.	P
Visage	Coût. Peu encombrant. Bonne acceptabilité.	Jumeaux. Psychologie, religion. Déguisement… Vulnérable aux attaques.	P
Rétine	Fiabilité. Pérennité.	Coût. Acceptabilité faible. Installation difficile.	P
Iris	Fiabilité.	Acceptabilité très faible. Contrainte d'éclairage.	P
Voix	Facile.	Vulnérable aux attaques.	P/L
Signature	Ergonomie.	Dépendance de l'état émotionnel de la personne. Fiabilité.	L
Frappe au clavier	Ergonomie.	Dépendant de l'état physique de la personne	L

5 Contraintes techniques et organisationnelles

5.1 Introduction

5.1.1 Problématique liée à l'environnement

La mise en place d'un système de contrôle d'accès biométrique doit prendre en compte des éléments propres au facteur humain pour que les contrôles fonctionnent efficacement.
En particulier, il convient de prendre en compte les éléments suivants :

- Appareils communs à toute une population.
- Capteur : problèmes d'hygiène.
- Durée du contrôle.

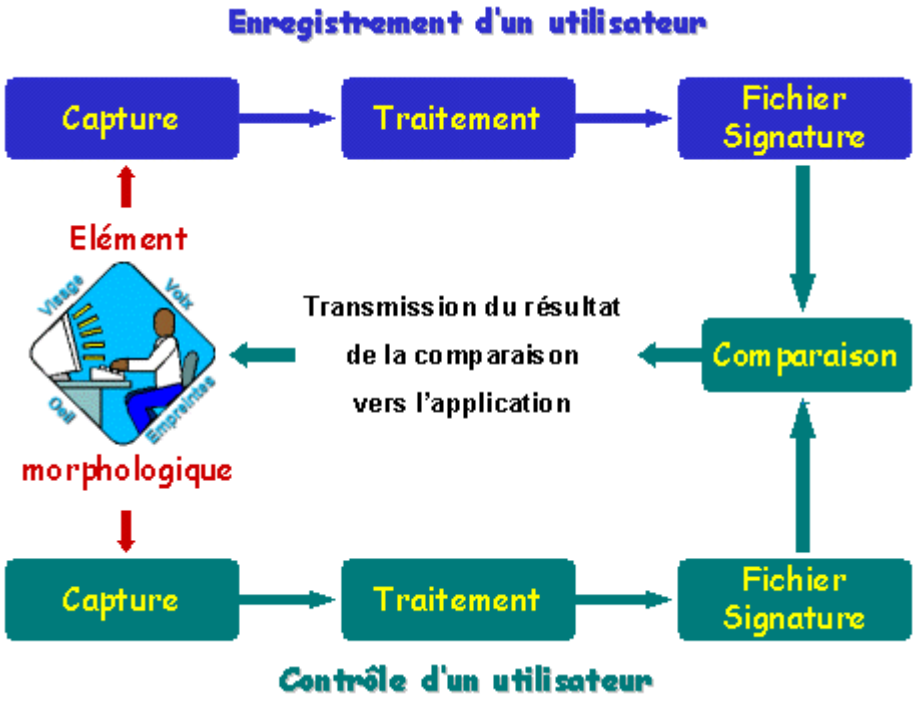
5.1.2 Consentement

Dans le cadre de cette étude l'ensemble des contrôles sont réalisés avec l'autorisation formelle de la personne.

5.2 Cycle de vie d'un processus d'identification biométrique

5.2.1 Processus macroscopique

Le cycle macroscopique d'un processus d'identification biométrique se décompose en deux grandes étapes l'enrôlement et le contrôle.



(source : www.biometrie.online.fr)

Enrôlement :
L'enrôlement des personnes est la phase initiale de création du gabarit biométrique et de son stockage en liaison avec une identité déclarée. Les caractéristiques physiques sont transformées en un gabarit représentatif de la personne et propre au système de reconnaissance.
Durant cette phase, des données additionnelles propres à la personne qui s'enrôle sont enregistrées comme par exemple ses nom et prénom et un identifiant personnel (PIN).
Cette étape n'est effectuée qu'une seule fois.

Contrôle (vérification / identification) :
C'est l'action de contrôle des données d'une personne afin de procéder à la vérification de son identité déclarée ou, dans une investigation, à la recherche de l'identité de cette personne. Cette étape se déroule à chaque fois qu'une personne se présente devant le système.

La vérification consiste à confirmer l'identité prétendue d'une personne (authentifier) par le contrôle de ses caractéristiques physiques. Des données d'identification (nom, PIN, identifiant, etc.) sont présentées par la personne au système en même temps que ses caractéristiques physiques.
C'est une comparaison « *un-pour-un* » dans laquelle le gabarit biométrique saisi est comparé au gabarit de référence correspondant dans une carte (ou autre dispositif physique personnel équivalent) ou dans une base de données. Dans le cas d'une carte, le gabarit saisi est directement rapproché du gabarit stocké dans la carte. La réponse est donnée par le terminal

biométrique. Elle peut aussi être donnée par la carte moyennant l'emploi de protocoles cryptographiques garantissant l'authenticité de la réponse.
Dans le cas du stockage des gabarits dans une base de données, l'accès au gabarit de référence se fait par accès direct sur l'index de l'identifiant déclaré de la personne.
L'identification consiste à identifier une personne à l'aide de ses seules caractéristiques physiques au sein d'une population préalablement enregistrée. C'est une comparaison « *un-pour-plusieurs* » dans laquelle le gabarit biométrique saisi est comparé à tous les gabarits stockés dans une base de données.

À ces deux processus s'ajoutent souvent les deux processus suivants :

- Le rafraîchissement ou actualisation : le système biométrique peut périodiquement corriger le gabarit de référence lors d'un contrôle de façon à prendre en compte des évolutions des données personnelles de la personne, en particulier pour des systèmes comportementaux (dynamique de signature) ;
- La fin de vie : le gabarit et autres données de références propres à la personne sont détruites pour prendre en compte la suppression de la personne du système de contrôle.

5.2.2 Processus détaillés

Chaque système biométrique utilise des spécificités liées à la caractéristique physique analysée (empreinte, iris, forme de la main, etc.) et également liées à la technologie du système. Il est néanmoins possible d'identifier une série d'étapes ou de composantes génériques au processus.

Note : Nous ne présentons ici que le macro-processus de contrôle (hors enrôlement).

5.2.2.1 Collecte [capture] des données d'identification

C'est l'étape de saisie des données d'identification de la personne et en particulier de ses caractéristiques physiques par l'intermédiaire d'un capteur spécialisé correspondant à la caractéristique physique analysée.

Les données saisies peuvent être selon le système :

- Les données sur l'identité prétendue (PIN, nom, identifiant, etc..). La collecte des données d'identité se fait à l'aide d'un lecteur approprié (PINpad, clavier, lecteur de carte, etc.).
- Les données physiques personnelles (biologiques, morphologiques, comportementales). La collecte des données physiques se fait à l'aide d'un capteur approprié.

5.2.2.2 Système de transmission

Le système de transmission sert à transporter les données entre les différents sous-systèmes du système biométrique. En particulier il est possible que le sous-système de collecte et le sous-système de comparaison, voire celui de transformation soient distants l'un de l'autre. Le système de transmission qui peut être local (interne à un boîtier) ou distant (liaison Ethernet, réseau ouvert, etc.) doit être clairement identifié afin d'en assurer la protection contre des écoutes ou des manipulations de données.

Que ce soit dans le processus initial d'enrôlement ou dans celui de capture, il faut que l' identification et l'authentification soient garanties en terme d'intégrité.
Le premier type de transmission intéresse la partie capteur : généralement cette partie capteur comprend une partie analogique (empreinte, voix, morphologie signature ..) qui est digitalisée par la suite. Dans ce schéma nous trouvons des signaux optiques, sons, vidéo...
Ces signaux se trouvent généralement très proche du système de numérisation. Le problème est principalement un problème d'intégrité : cette intégrité est obtenue par un échantillonnage du signal adéquat. Le cas le plus général est la transmission entre le capteur et la base de données où se trouve le gabarit de référence.

Si la transmission utilise un réseau (local ou public) des mesures de sécurité adéquates doivent être utilisées afin de protéger les données échangées en intégrité (des données et des flux).

Les données véhiculées sont des données personnelles. A ce titre elles doivent également être protégées en confidentialité.

5.2.2.3 Transformation en un gabarit biométrique

Le capteur des caractéristiques physiques transmet les données capturées à un système d'analyse qui a pour rôle de les transformer en un gabarit, selon un algorithme approprié à la caractéristique physique analysée. (empreinte, iris, forme de la main, etc.)

5.2.2.4 Comparaison à une référence

Le gabarit calculé doit être ensuite rapproché du gabarit de référence afin de vérifier l'identité de la personne ou de l'identifier.

Ce processus se compose de :

- La recherche de la référence pour la comparaison :
  - Via les données d'identification pour accès à la référence stockée pour une vérification ;
  - Via la comparaison directe du gabarit calculé à la valeur de référence stockée pour une identification ;

- La comparaison du gabarit calculé à une valeur de référence : à cette étape intervient une analyse qui est propre à la technologie du système développé. La comparaison fait généralement intervenir un calcul de score qui permet de considérer la comparaison en succès ou en échec selon que le score calculé est à l'intérieur ou à l'extérieur d'une plage d'acceptation.

5.2.2.5 Prise de décision

Le sous-système de décision reçoit le résultat du score calculé de rapprochement au gabarit stocké. En fonction d'une politique de décision lié à une analyse de risque propre à l'application utilisatrice du système biométrique, le sous-système de décision décide des actions à suivre.

Le sous-système de décision peut considérer la vérification ou l'identification :

- En succès et rendre une réponse positive au système applicatif utilisateur ;
- En échec complet et rendre une réponse négative au système applicatif utilisateur ;
- En indécision : dans certains cas de systèmes plus sophistiqués, le système peut demander une re-saisie voire la saisie d'une autre caractéristique physique (ex : autre doigt pour l'analyse d'empreinte).

En cas d'échec le système peut offrir la possibilité de recommencer le processus à l'étape de collecte ou alors comptabiliser le nombre de contrôle en échec de la même personne et décider d'un blocage du contrôle pour la personne considérée.
La réponse est rendue au système applicatif qui utilise le système biométrique. C'est ensuite à l'application de décider des droits qu'elle accorde à la personne identifiée. En particulier, dans un contrôle par rapport à un fichier dit « *négatif* », le fait de ne pas être reconnu par le système biométrique peut être aussi important que l'inverse.

5.2.3 Système de stockage

Le système de stockage permet de maintenir le gabarit de référence des personnes enregistrées dans le système. Il permet de créer, modifier, supprimer des gabarits dans le système en relation avec des données d'identification de la personne.
Ce système est principalement lié à l'application utilisatrice. En particulier, selon que le but final de l'application est de vérifier l'identité d'une personne ou au contraire de l'identifier au sein d'une population, le mode de stockage sera différent.
Dans le premier cas, en raison de la réglementation sur la protection des personnes et des données personnelles, le système pourra mettre en oeuvre un contrôle *un-pour-un*, le gabarit de référence étant stocké dans un support portable en possession de l'utilisateur.
Dans le second cas, seul un stockage centralisé dans une base de données peut répondre au besoin. Là encore, la réglementation nationale peut ou non permettre une telle utilisation.

5.2.4 Système de rafraîchissement [d'actualisation]

La plupart des caractéristiques physiques sont stables dans le temps (empreintes, iris, forme de la main, etc.). En revanche, des caractéristiques physiques comportementales comme la dynamique de la signature, le rythme de la frappe au clavier, etc. peuvent évoluer dans le temps. Il peut alors être nécessaire d'actualiser le gabarit de référence de la personne selon une procédure propre au dispositif technologique.
Si un tel rafraîchissement est opéré, le système devra garder des traces d'audit des mises à jour afin d'éviter toute fraude sur le système.

5.3 Choix des paramètres (seuil d'acceptabilité)

Quel que soit le procédé biométrique utilisé, la coïncidence à 100 % entre les deux fichiers signatures, celui établi lors de l'enrôlement et celui établi lors de l'authentification est impossible.
La performance et la fiabilité d'un système s'expriment donc par le taux de faux rejets (T.F.R.) et le taux de fausses acceptations (T.F.A.). Un système émet un faux rejet lorsqu'il rejette par erreur un vrai utilisateur. A l'inverse, un système émettra une fausse acceptation en donnant accès à quelqu'un qui n'a pas de droit.
Le seuil de décision doit être estimé en fonction du niveau de sécurité souhaité.

5.4 Contraintes ergonomiques

Le temps d'utilisation du système doit être le plus court possible car il est généralement admis que le temps d'attente pour accéder à un lieu doit être de l'ordre de quelques secondes.
En cas d'utilisation pour un contrôle d'accès logique, ce temps doit être révisé à la baisse par rapport aux contrôles d'accès physique.
Un système biométrique est d'autant plus toléré qu'il est moins intrusif.
Les personnes sont sensibles aux aspects "hygiène" dans l'utilisation des systèmes.

6 CNIL

6.1 Point de vue de la CNIL.

La biométrie dans ses fonctions d'authentification des individus à partir de caractéristiques physiques suppose à la fois la transmission des données physiques concernant des individus mais aussi leur stockage.
De sorte que, si la biométrie peut sécuriser un accès ou un échange, la contrepartie sera une aliénation de liberté.

La CNIL s'en est par conséquent émue et a consacré une partie importante de son 22ième rapport annuel d'activité, présenté le 10 juillet 2002. Elle considère que les technologies biométriques révèlent deux enjeux :

- la systématisation de la "logique des traces" (ADN, empreintes digitales, empreintes vocales...), qui conduirait au développement, à des fins plus ou moins avouables, de méthodes de recherche et d'identification des traces humaines à grande échelle ;
- le risque d'atteinte aux libertés fondamentales et notamment le risque de création de « l'identité biologique » unique.

6.2 Identification des risques juridiques liés à l'utilisation des techniques de biométrie

*** S'agissant de la technologie de reconnaissance des visages,** la CNIL considère que celle-ci comporte deux risques sérieux :

- le premier serait la tentation des services de police de ficher non seulement des personnes recherchées, mais également des personnes non suspectes mais connues de leurs services, à des fins de prévention. (En ce sens se référer aussi aux positions de la CNIL sur les fichiers d'empreintes génétiques).
- le second risque, lié au premier, serait l'augmentation du nombre des caméras de vidéo surveillance dans les lieux publics. (voir en ce sens la loi Pasqua, loi n° 95-73 d'orientation et de programmation relative à la sécurité ainsi que la délibération de la CNIL n°94-056 du 21 juin 1994, in 15ième rapport annuel d'activité).

* **S'agissant de la conservation des bases de données d'éléments biométriques** :

- le détournement de la finalité du traitement et, notamment, à d'autres fins que celles ayant justifié sa création est un risque important. Force est de constater que la création

de fichier "ADN", d'empreinte digitale, de photo ou caractéristique du visage, en permettant la mise en place de procédé d'authentification, offrirait aussi des moyens tout à fait considérables d'investigation policière.

- à contrario la CNIL va considérer que le "**risque social**" est bien moindre lorsque l'élément constitutif de la reconnaissance biométrique n'est pas stocké dans une base de données centralisée, mais demeure attaché à l'individu. Ce type de procédé comporte de nombreuses applications telles que l'inclusion de l'empreinte digitale dans la puce d'une carte bancaire permettant de s'assurer que l'utilisateur de la carte est le porteur autorisé par comparaison d'un doigt que l'on présente dans le lecteur associé au guichet automatique et de l'empreinte figurant dans la puce.

6.3 Le droit applicable

Le projet de loi relatif à la protection des données physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative, à l'informatique, aux fichiers et aux libertés, adopté par le Sénat le 01 Avril 2003, dispose en son article 25, 8^{ièment} que sont **mis en œuvres après autorisation de la CNIL**, les traitements automatisés comportant **des données biométriques** nécessaires au contrôle de l'identité des personnes.

La directive communautaire ne traite pas de ces aspects. La directive tout en reconnaissant dans son considérant 52 que le contrôle *a posteriori* par les autorités compétentes doit en général être considéré comme une mesure suffisante, indique dans un considérant 53 que les Etats membres peuvent prévoir un contrôle préalable, s'agissant de traitements susceptibles de présenter des "*risques particuliers au regard des droits et libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités …*".
Autrement dit, la directive laisse clairement une large marge de manœuvre aux Etats membres pour déterminer selon quelle procédure et par quelle institution les autorisations seront accordées.
La France a décidé de se retrancher derrière cette liberté qui lui est offerte par la directive de recourir au régime de l'autorisation préalable de la CNIL et non du contrôle *à posteriori*.

6.4 Pratiques

Comme habituellement, tout fichier contenant des informations privées doit faire l'objet d'une déclaration à la CNIL dans le secteur privé. L'administration est tenue quant à elle de recueillir l'avis préalable de la CNIL.
D'autre part, l'information des personnels et des instances compétentes (Comité d'Entreprise ou, dans le public, Comité Technique Paritaire) est une obligation (cf. art. L432-2 du Code du Travail, pour le privé, dont le non-respect peut constituer un délit d'entrave). De plus, il doit y avoir proportionnalité entre les modalités du contrôle et l'objectif poursuivi (cf art. L120-2 du Code du Travail).

La CNIL et plus généralement les différents organismes internationaux considèrent que la biométrie, hors cadre « criminalité » ne peut servir qu'à authentifier et non à identifier. La CNIL ajoute que l'empreinte digitale est une caractéristique personnelle et ne peut être mise à disposition de quiconque dans une base de données. Elle ne peut être qu'en unique exemplaire sur ou dans le document concerné.

La CNIL parle de base de données centralisée.

Elle considère que : « le risque social est bien moindre lorsque l'échantillon d'une caractéristique biométrique n'est pas stocké dans une base de données centralisée, mais demeure sur soi. ».

Par exemple : inclusion du gabarit de l'empreinte digitale dans la puce d'une carte permettant, par comparaison d'un doigt présenté dans le lecteur et de l'empreinte figurant dans la puce, de s'assurer que l'utilisateur de la carte est son titulaire.

En effet, la CNIL a résumé comme suit sa doctrine concernant la biométrie dans le rapport au titre de 2001, page 171:

- «1 - Les technologies de reconnaissance biométrique ne reposant pas sur le stockage des gabarits dans une base de données ne soulèvent pas de difficulté particulière en termes « informatique et libertés «, dès lors que le gabarit est conservé sur soi (une carte à puce) ou sur un appareil dont on a l'usage exclusif (un téléphone portable, un ordinateur, etc.) et nulle part ailleurs.
- 2 - En revanche, lorsqu'une base de données est constituée dans le cadre d'un dispositif d'identification biométrique, l'élément biométrique retenu peut avoir une incidence sur nos libertés et notre vie privée ; tel est le cas lorsque l'élément biométrique retenu «laisse des traces» dans notre vie quotidienne (ADN, empreinte digitale). Dans un tel cas, le contrôle de finalité et de proportionnalité peut conduire à accepter la mise en œuvre de telles bases de données lorsqu'un impératif particulier de sécurité le justifie.
- 3 - A défaut d'une telle justification particulière, et lorsqu'une base de données de gabarits est constituée, le choix d'un élément biométrique « ne laissant pas de trace » , tel que le contour de la main, la rétine, la reconnaissance vocale, etc. devrait être préféré à la prolifération de fichiers d'ADN ou d'empreintes digitales. Il demeure que loin de tout dogmatisme, la CNIL souhaite poursuivre toute réflexion utile sur le sujet, en liaison avec les professionnels du secteur concerné et ses homologues européens dans le souci de la recherche du meilleur équilibre possible....

7 Lien avec les certificats (PKI/ICP)

Tout comme une donnée biométrique, un certificat de clé publique est un ensemble de données qui permet de vérifier l'identité d'un individu. La donnée biométrique identifie et/ou authentifie une personne à l'aide de ses caractéristiques morphologiques personnelles, alors que le certificat de clé publique permet à une tierce personne de vérifier la relation entre une clé publique (et par extension sa signature) et son propriétaire.
Ces deux éléments sont complémentaires. La donnée biométrique à elle seule ne permet pas de signer un document. Ajouter cette donnée à un document ne crée pas le lien attendu par la loi (Art. 1316-4 de la loi n° 2000-230 du 13 mars 2000) entre un document et l'identité de son signataire. En revanche la signature électronique à l'aide de systèmes cryptographiques à clé publique le permet mais laisse planer un risque sur le processus d'enregistrement du propriétaire des clés. Dans ce processus, l'entité d'enregistrement doit vérifier à l'aide de documents formels papier l'identité de la personne qui se présente. Ensuite ou en même temps cette personne dépose sa clé publique et démontre qu'elle possède la partie privée (clé de signature) correspondante. Si ce processus n'est pas fait avec la plus grande intégrité, un doute peut alors exister concernant l'identifiant (nom, prénom, etc.) qui figure dans le certificat : est-ce bien celui du porteur ?
De même, pour activer la fonction de signature, le porteur devra entrer des données d'activation qui sont le plus souvent un PIN (Personal Identification Number) à quelques chiffres. Là encore, si la clé privée est subtilisée avec le PIN, une autre personne peut signer à la place du propriétaire.

L'association de ces deux technologies peut en revanche renforcer la sécurité sur toute la chaîne de confiance.

Processus d'enregistrement :
Au moment de l'enregistrement, en même temps que la présentation de ses pièces justificatives d'identité, la personne dépose ses données biométriques (le gabarit) qui sont enregistrées à titre de garantie d'identification de la vraie personne physique[4].

Processus de signature :
Dans un système où les clés de signature sont protégées dans une carte à puce (ou équivalent), le gabarit peut alors servir de donnée d'activation de la signature en remplacement du PIN. Lors du processus de signature, le signataire peut activer la fonction de signature en présentant sa caractéristique biométrique à un lecteur associé à la carte ou sur la carte elle-même dans certaines technologies. La fonction de signature est activée s'il y a correspondance entre la caractéristique biométrique et le gabarit de référence enregistré dans la puce.

[4] Sous réserve des protections adéquates de conservation et d'un accord de la CNIL

Signature des données biométriques :
Les données biométriques (gabarit et données additionnelles) peuvent être protégées en intégrité et ou confidentialité. Des techniques de MAC (Message Authentication Code (cryptographie symétrique) ou de signature électronique (cryptographie asymétrique) peuvent être utilisées. Dans la seconde hypothèse, les données signées doivent être accompagnées du certificat correspondant aux clés de signature ou d'un moyen de retrouver ce certificat.
Ces concepts sont décrits en détail dans la norme X9.84 Biometric information management and security.

Données biométriques dans le certificat :
A l'inverse, les données biométriques pourraient être incluses dans un champ privé du certificat. En réalité ceci ne présente aucun intérêt.
Le certificat sert avant tout à valider des signatures électroniques et à définir les conditions de validité de cette signature (clé publique, période de validité, optionnellement limite de garantie, etc.). la présence de la donnée biométrique du signataire n'apporte aucune garantie supplémentaire au vérificateur sur le fait que la signature a été réalisée par la bonne personne mais seulement que le certificat à été délivré à la personne correspondant à cette donnée biométrique.

De plus la donnée biométrique contenue dans le certificat correspond à une donnée statique équivalente au gabarit de référence. Ceci ne correspond pas à la finalité de la biométrie.

8 Glossaire

Origine : Glossaire de l'ENSICAEN <avec l'aimable accord d'ARATEM>, complété par les membres de la commission pour prendre en compte les termes employés dans le présent document.

Attribut biométrique
C'est une caractéristique physique mesurable ou un trait de comportement personnel utilisé pour reconnaître l'identité, ou vérifier une identité déclarée d'une personne enregistrée.

Biclé asymétrique
Ensemble des paramètres utilisés dans un algorithme cryptographique asymétrique. Une biclé asymétrique est composée d'un ensemble de paramètres rendu public, globalement appelé la clé publique, et d'un ensemble de paramètres conservé secret par le propriétaire de la biclé, et appelé la clé privée. Les deux ensembles de clés ont la propriété de rendre impossible par le calcul, la déduction de la clé privée à partir de la clé publique. Il existe plusieurs algorithmes asymétriques parmi lesquels DH (Diffie Hellman), RSA (Ron Rivest, Adi Shamir et Leonard Adleman), DSS (Digital Signature Standard), GQ (Guillou-Quisquater) .

Biométrie comportementale
Il s'agit d'un type de biométrie caractérisée par un trait d'attitude qui est appris et acquis au fil du temps plutôt que par une caractéristique physiologique.

Capture
Méthode de collecte d'un échantillon biométrique d'un utilisateur.

Caractéristique biométrique physique / physiologique
Type de biométrie défini par une caractéristique physique plutôt que comportementale.

Certificat
De façon générique le certificat est un objet informatique logique qui permet de lier de façon intangible une identité d'entité à certaines caractéristiques de cette entité. Lorsqu'une des caractéristiques de l'entité est une clé publique, il s'agira de certificat de clé publique. Si ce n'est pas le cas il s'agira de certificat d'attributs.

Le lien est créé grâce à la signature de l'ensemble des données du certificat par la clé privée de l'autorité qui émet le certificat.

Par extension, le certificat est l'ensemble formé par les données et par la signature de l'autorité sur ces données.

La finalité première d'un certificat est de permettre à un utilisateur de vérifier l'authenticité (identité, caractéristique du propriétaire) de la clé publique qu'il va utiliser pour vérifier la signature produite par le signataire, en se basant sur la garantie apportée par l'autorité de certification.

Clé publique
Partie de la biclé qui est communiquée aux utilisateurs pour vérifier ou chiffrer.

Clé privée
Partie de la biclé asymétrique qui est sous le contrôle unique de son propriétaire pour signer ou déchiffrer.

Comparaison
Processus d'évaluation de correspondance d'un échantillon biométrique avec un ou plusieurs modèle(s) de référence précédemment stocké(s).

Correspondance
Processus de comparaison d'un échantillon biométrique avec une référence déjà stockée et évaluation du degré de similarité. Une décision d'acceptation ou de rejet est fondée sur le dépassement ou non du seuil par le score.

Critère de performance
Critère prédéterminé établi pour évaluer la performance d'un système biométrique et testé.

Degrés de liberté
Nombre de caractéristiques statistiquement indépendantes d'une donnée biométrique.

Donnée biométrique
C'est l'information extraite d'un échantillon biométrique et utilisé soit pour construire un modèle de référence ou pour comparer à des modèles existants.

Echantillon biométrique
Donnée représentant une caractéristique biométrique d'un utilisateur, capturée par un système biométrique.

Enrôlement
Processus de collecte de données physiques d'une personne, de traitement et de stockage des gabarits biométriques de référence représentant l'identité de la personne.

Extraction
Processus de conversion d'un échantillon biométrique capturé en donnée biométrique pouvant être comparée au modèle de référence.

FR (False Rejection)
Le Faux Rejet apparaît lorsqu'un système biométrique n'a pas été capable de reconnaître une personne légitimement enregistrée et s'étant convenablement identifiée comme telle. Dans le contexte le plus courant, l'utilisateur d'un système biométrique doit prendre le Faux Rejet comme un inconvénient.

FA (False Acceptance)
La Fausse Acceptation intervient quand un système biométrique vérifie mal une identité en comparant deux caractéristiques biométriques de deux individus différents. Dans les cas les plus courants, la Fausse Acceptation représente un hasard de sécurité.

FAR (False Acceptance Rate)
Le Taux de Fausse Acceptation (TFA) se rapporte à la probabilité d'une Fausse Acceptation ou d'une vérification incorrecte.

Les fournisseurs de systèmes biométriques utilisent souvent le FAR et le FRR ensemble pour décrire les possibilités du système. De toute évidence, le FAR et le FRR sont

dépendants du niveau seuil (threshold level). Augmenter ce dernier réduirait la probabilité de FA et ainsi améliorerait la sécurité, toutefois, la validité du système serait réduite en raison de l'augmentation du FRR.

FRR (False Rejection Rate)
Le Taux de Faux Rejet (TFR) se réfère à la probabilité statistique qu'un système biométrique ne soit pas capable de vérifier l'identité légitimement clamée d'une personne enregistrée, ou échoue dans l'authentification d'une personne enregistrée.

Gabarit
Donnée résultant de la transformation de données physiques personnelles de celui qui s'enregistre par un système biométrique.

Modèle de référence
Donnée représentant une caractéristique biométrique d'un individu, utilisée par un système biométrique pour permettre la comparaison avec des échantillons soumis a posteriori.

Prétendant
Personne soumettant un échantillon biométrique pour vérification d'une identité.

Seuil de décision
L'acceptation ou le rejet d'une donnée biométrique dépend du passage du score de correspondance au-dessus ou au-dessous du seuil. Ce dernier est ajustable pour rendre le système biométrique plus ou moins strict, cela dépend des éléments requis par tout système d'application biométrique.

Système biométrique
Système automatisé capable de :

- Capturer un échantillon biométrique d'un utilisateur.
- Extraire les données biométriques de l'échantillon.
- Comparer les données biométriques avec celles contenues dans un ou plusieurs modèles de référence.
- Décider du degré de correspondance.
- Indiquer si l'authentification a bien été accomplie.

Temps de réponse
Période temporelle requise par un système biométrique pour retourner une décision sur l'authentification d'un échantillon biométrique.

Tentative d'authentification
Soumission d'un élément à un système biométrique pour identification ou vérification. Un système biométrique peut accepter plus d'un essai pour identifier ou authentifier.

Utilisateur
Personne interagissant avec un système biométrique pour enregistrer ou faire vérifier son identité. (différent de l'opérateur)

9 Documentation

9.1 Adresses de sites Internet

ARATEM (Agence Rhône Alpes pour la maîtrise des TEchnologies de Mesures)
http://www.aratem.org

Association américaine sur les permis de conduire
American Association of Motor Vehicle Administrators (AAMVA), ANSI Driver's License and Identification (DL/ID) Standard
http://www.aamva.com

Association For Biometrics (AFB)
http://www.afb.org.uk

AX-S Biometrics Ltd
http://www.ax-sbiometrics.com

BIOAPI Consortium (BIO API)
http://www.bioapi.org

Biométrie et Authentification
Djamila.Mahmoudi@swisscom.com, PhD, collaboratrice au département Corporate Information and Technology de Swisscom AG, 5 septembre 2000
http://sawww.epfl.ch/SIC/SA/publications/FI00/fi-sp-00/sp-00-page25.html

Canadian Biometric Group – (CATA)
http://www.cata.ca/biometrics/

ENSI Caen
http://www.ensicaen.ismra.fr/~duflos/MiniGlossaire.htm

Etude de John Daugmann concernant la biométrie de l'iris
http://biometrie.online.fr/Liens_index.htm

Etude mensuelle sur les activités des pays en matière de PKI émanant du secrétariat au trésor canadien
http://www.cio-dpi.gc.ca/pki-icp/index_f.asp

Forum français de discussion sur la biométrie

http://biometrie.online.fr

International Civil Aviation Organization (ICAO)
http://www.icao.org

Japan Biometric Authentication Association (JBAA)
http://www.biometrics.gr.jp

Korea Biometric Association (KBA)
http://www.biometrics.or.kr/eng/default.htm

Méthodes d'authentification vocale d'utilisateurs dans les systèmes informatiques, mai 2000

http://www.chez.com/gipp/oraux/aal/

Rapport "At face value" émanant de l'autorité de contrôle des Pays Bas
http://www.cbpweb.nl

Tatouage et dissimulation de données pour des communications audiovisuelles sécurisées
http://www.cnrs.fr/Cnrspresse/n399/html/n399rd09.htm

The Biometric Foundation
http://www.biometricfoundation.org/

The Biometrics Institute (Australie)
http://www.biometricsinstitute.org

The International Biometric Industry Association (IBIA)
http://www.ibia.org

The Security Industry Association
http://www.siaonline.org

9.2 Documents de référence

ANSI X9.84-2000, Biometric Information Management and Security
Biométrie - Bilan de la 1ère réunion de l'OWG 2 de l'ISO/CEI JTC 1/SC 17 (2001-04-19/20, Londres)
Biometric evaluation methodology supplement (BEM) August 2002. The common critéria biometric evaluation methodology working group

Biometric system protection profile for medium robustness environments. March 2002. USA

Biometric device protection profile. September 2001. UK

CNIL, 21ème rapport d'activité 2000, pp. 101 à 120
CORDIS Liste des Projets Européens en biométrie
DIN V 66400 Finger Minutiar Encoding Format and Parameters for On-Card Matching, Version 0.6, 5 June 2002
International Biometric Industry Association (IBIA), BioAPI specification
International Civil Aviation Organization (ICAO), Machine readable travel document, TR Selection of a globally interoperable biometric for machine-assisted identity confirmation with MRTDS, First edition, November 2001
ISO/IEC CD2 7816-11:2001 Information technology, Identification cards – Integrated circuit(s) cards with contacts – Part 11: Personal verification through biometric methods
NIST-ITL, Common Biometric Exchange File Format for Biometric Interoperability (CBEFF)

9.3 Associations et groupes

AFNOR, Association française de normalisation
CG CSA / CN FTS / GE1 : Commission Générale Cartes et Systèmes Associés / Commission Nationale Fonctions Transversales et Systèmes / Groupe d'experts «Biométrie »

Association For Biometrics (AFB)
Association européenne de 37 membres. Forum pour les sociétés (européennes et internationales) promouvant les techniques biométriques. Nombreux sous-comités (éducation, techniques, marketing) et sujets de travail (protection de la vie privée, performances, aspects légaux).

BIOAPI Consortium (BIO API)
Le BioAPI Consortium a été formé en 1998 pour développer une interface de programmation (API) largement acceptée et disponible au service des techniques biométriques.
Près d'une centaines de sociétés sont adhérente à ce consortium.

Biometric Consortium (BC)
Fondé par le gouvernement américain, le Biometric Consortium est un centre de recherche, de développement, de test, d'évaluation et d'application de technologies d'identification / vérification personnelle basées sur la biométrie.

Canadian Biometric Group – CATA

Le CATA (Canadian Advanced Technology Alliance) Biometric Group est une organisation commerciale créée en 2002 pour promouvoir les intérêts collectifs des fournisseurs de technologie biométrique canadienne.

International Biometric Industry Association (IBIA)
L'International Biometric Industry Association (IBIA) est une association commerciale fondée en septembre 1998 aux Etats-Unis pour promouvoir les intérêts collectifs de l'industrie biométrique américaine.

ISO Organisation internationale de normalisation
ISO/IEC JCT1 Subcommittee 17, WG11 Biometric
ISO/IEC JCT1 Subcommittee 37, Biometrics
Japan Biometric Authentication Association (JBAA)
Association japonaise pour la promotion des technologies biométriques.

Korea Biometric Association (KBA)
Association coréenne pour la promotion des technologies biométriques.

Security Industry Association
Créé en 1969, le Security Industry Association (SIA) est un syndicat des professionnels de l'industrie de la sécurité. Le sous-groupe biométrie (Biometrics Industry Group (BIG)) du SIA vise à promouvoir les technologies biométriques au travers des canaux de distribution de l'industrie de la sécurité.

Singapore Biometrics Working Group
Sous-groupe du Kent Ridge Digital Labs (KRDL) dédié à la recherché technologique.

The Biometric Foundation
Association américaine.

The Biometrics Institute
Organisation indépendante créée par le gouvernement australien en 2001.