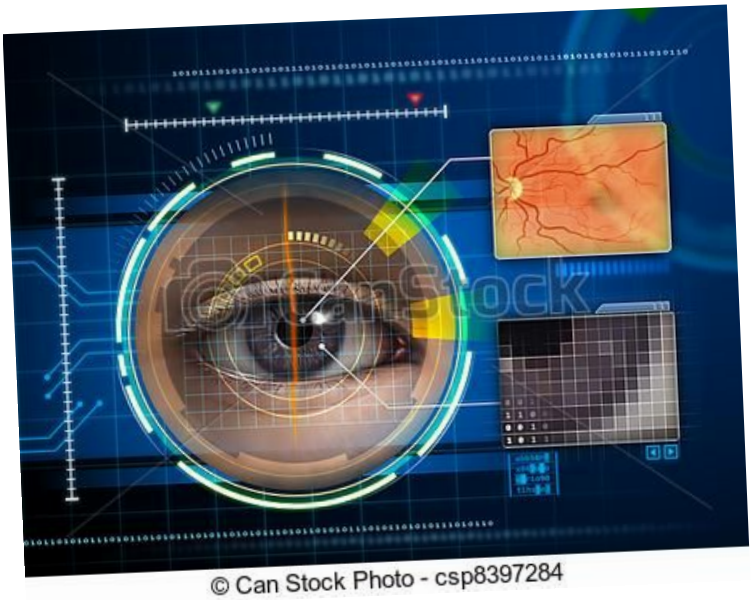
# L'authentification des personnes

Cette notion, d’authentification des personnes, est vaste et propose de nombreuses information subtile et complexe. Pour cela nous allons décrypter ces dernières et mettre en avant les différentes formes d’authentification des personnes.


# Sommaire

# L’authentification “classique”

## Notion:

Lorsqu'un utilisateur veut accéder à un système d'information, il doit dans un premier temps effectuer une procédure d'identification et d'authentification.

L'identification est une phase qui consiste à établir l'identité de l'utilisateur. Elle permet de répondre à la question : "Qui êtes vous ?". L'utilisateur utilise un identifiant ( ou "Compte d'accès", "Nom d'utilisateur" ,"Login") qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.

L'authentification est une phase qui permet à l'utilisateur d'apporter la preuve de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un identifiant ou "code secret" que lui seul connaît.

Le code secret (ou “mot de passe”) d'un utilisateur est une information personnelle qui ne doit en aucun cas être divulgués.

Lorsque deux personnes ou plus connaissent le mot de passe correspondant à une identité d'utilisateur, il s'agit d'une infraction à la sécurité. Sauf en cas de disposition spécifique pour assurer la continuité d'un service (par exemple dans les salles 351,352). Cette disposition est alors clairement définie dans la charte d'usage des personnels.

Majoritairement cela ressemble à ceci :

# Qu’est ce qu’un mot de passe ?

Un mot de passe est un mot ou une série de caractères utilisés comme moyen d'authentification pour prouver son identité lorsque l'on désire accéder à un lieu protégé, à une ressource (notamment informatique) ou à un service dont l'accès est limité et protégé.

# Qu'est-ce qu'un BON mot de passe ?

Un mot de passe doit faire au moins 8 caractères, composé de lettres minuscules et majuscules, de chiffres et de caractères spéciaux. Il faut éviter les mots du dictionnaire, des noms propres (prénom, nom de famille, etc.).


# Plusieurs types d'authentification.

Le mot de passe est il suffisant pour apporter la preuve d’une identité ?

Si une personne annonce mon identité par téléphone et que son interlocuteur lui demande sa date de naissance pour s’authentifier, l'est-il vraiment si c'est la seule information utilisée et qu'elle est aisément récupérable (réseaux sociaux, etc.) ?
L’authentification par simple mot de passe ne remplit pas les conditions de sécurité exigés.
Certains systèmes d’informations de l’Education Nationale imposent un mode d’authentification plus robuste appelé « Authentification forte ».

L'authentification basique

Utilisation de deux vecteurs :

- **Qui je suis** → L'identifiant (login)

  ***et***

- **Ce que je sais** → L'authentifiant (mot de passe)

L'authentification forte

Utilisation d'au moins trois vecteurs :

- **Qui je suis** → L'identifiant (login)
  ***et***
- **Ce que je sais** → L'authentifiant (mot de passe)
  ***et***
- **Ce que je possède** → un certificat, un badge ou une carte à puce
  ***et/ou***
- **Ce que je suis** → une empreinte biométrique

Ces deux techniques d'authentification vont être étudié juste ensuite.

# Les recommandations minimales à respecter:

1. Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
2. Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
3. Ne demandez jamais à un tiers de créer pour vous un mot de passe.
4. Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
5. Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
6. Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
7. Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
8. Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

# L’authentification carte à puce et carte magnétique

## Notion carte à puce:

Une carte à puce est une carte en matière plastique, voire en papier ou en carton, de quelques centimètres de côté et moins d'un millimètre d'épaisseur, portant au moins un circuit intégré capable de contenir de l'information. Le circuit intégré (la *puce*) peut contenir un microprocesseur capable de traiter cette information, ou être limité à des circuits de mémoire non volatile et, éventuellement, un composant de sécurité (*carte mémoire*). Les cartes à puce sont principalement utilisées comme moyens d'identification personnelle (carte d'identité, badge d'accès aux bâtiments, carte d'assurance maladie, carte SIM) ou de paiement (carte bancaire, porte-monnaie électronique) ou preuve d'abonnement à des services prépayés (carte de téléphone, titre de transport).

## Fonctionnement:

Pour être utilisé ,la carte à puce à besoin d’être inséré dans un boîtier. Ce dernier va décoder les informations indiqués sur la puce et permettre ou non l’accès au lieu ou aux ressources protégé par ce système.

Les cartes à puces dans les cartes bancaires ou de la carte vitale sont les exemples les plus explicites.

# Notion carte magnétique:

La carte magnétique utilise un procédé similaire à celui de la carte à puce sauf que les informations ne sont pas stockés sur la carte dans la puce, mais dans une bande magnétique noire appelée piste magnétique.

La piste magnétique est la bande noire ou brune que l'on peut voir sur les cartes bancaires par exemple. Cette bande contient de minuscules particules magnétiques mélangées avec de la résine

# Fonctionnement:

Lors du processus d'encodage, ces particules sont aimantées dans la direction du pôle nord ou du pôle sud. Chaque caractère encodé sur la bande est composé d’un ensemble de bits de valeur 0 ou 1. La polarité des particules magnétiques est changée pour définir chacun de ces bits.

En changeant l'aimantation de ces particules tout au long de la piste, on peut ainsi encoder des informations binaires qui seront transmises au lecteur.

# L’authentification rétinienne

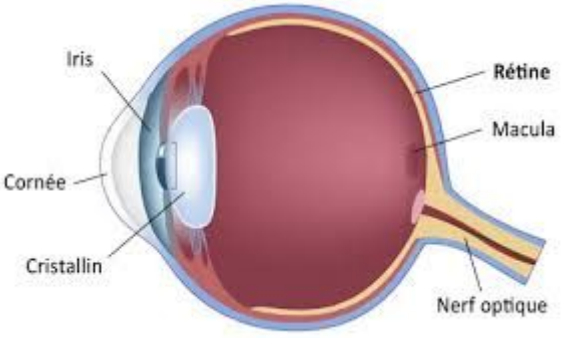
## Notion:

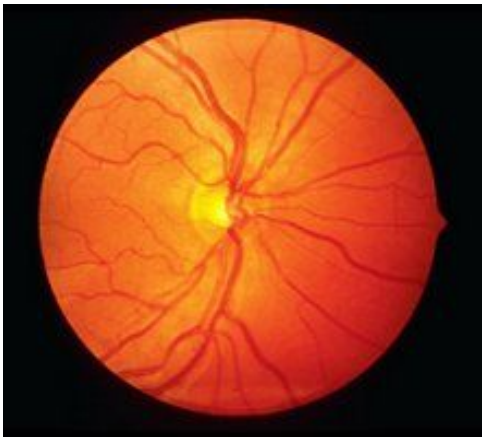
L’authentification rétinienne est le procédé par lequel la rétine de l’oeil va être utilisé comme clef pour l’identification d’une personne.

La rétine est la paroi interne et opposée de l'oeil sur laquelle se projettent les images que nous voyons. Cette paroi est tapissée par un réseau de vaisseaux sanguins, qui forment un motif unique pour chaque individu.

L'identification consiste à éclairer le fond de l'oeil par un faisceau lumineux de faible intensité. (inférieure à celle utilisée pour les examens médicaux). L'utilisateur doit fixer un petit point vert pendant quelques secondes.

Le réseau veineux rétinien est numérisé et cartographié sous forme de lignes et de points. On peut ainsi recenser jusqu'à 400 points caractéristiques (rappelons qu'une empreinte digitale n'en compte que 30 à 40).



La rétine est une mince surface d'environ 0,5 mm d'épaisseur située au fond de chaque il. Elle couvre environ 75 % du globe oculaire.

# Avantages et inconvénients:

Avantages:

La fiabilité est une des plus élevée au monde : le taux d'erreur est de moins de 1 sur 10 millions. Les risques de fraude sont quasi nuls, puisque la partie du corps exploitée n'est pas apparente.

Inconvénients:

Bien que sans danger, l'identification rétinienne nécessite un système intrusif et peu agréable (rayon lumineux envoyé dans l'oeil). La mesure doit s'effectuer à très faible distance du capteur (quelques centimètres), et elle est impossible à travers des lunettes. De plus, une forte alcoolémie ou un diabète modifie le réseau veineux rétinien.

# Applications:

La technique, issue du milieu médical, est connue depuis longtemps : dès les années 70, elle a été utilisée par l'armée américaine. Du fait de son utilisation peu aisée, elle reste aujourd'hui réservée au domaines de haute sécurité. La CIA (Central Intelligence Agency) et le FBI (Federal Bureau of Investigation) ont par exemple adopté l'identification rétinienne, et aussi certaines prisons américaines.

# L’authentification digitale

## Notion:

L’authentification digitale est le principe qui va utiliser les empreintes digitales ( située au bout des doigts) comme clef pour autoriser l’authentification.
Le procédé est simple, l’individu pose son doigt sur une surface spéciale et une photo de l’empreinte est réalisé, suite à cela l’empreinte sera analysé pour accepter ou refuser l’accès.

## Étapes de Traitement:

Plusieurs méthodes sont employées pour reconnaître les empreintes digitales :

-Localisation des minuties:

- cette méthode ne retient que l’emplacement des minuties les plus pertinentes. Elle est peu sensible aux déformations des doigts entre plusieurs vérifications (doigts plus ou moins appuyés sur le capteur).

-Traitement de textures

- des paramètres issus de certaines propriétés de la texture des empreintes (orientation, fréquence, etc.) sont comparés. Cette méthode permet un traitement très rapide, et donc un temps de réponse très court.

Il existe bien d’autres méthodes, mais elle ne sont pas divulguées par les entreprises qui les développent pour un souci de propriétés intellectuelles.

- Le format BITMAP de Windows peut être utilisé comme format d'entrée des images à traiter ainsi que pour échanger des images avec les

applications. L'origine des images n'a pas d'importance (scanner, fichier, caméra, code barre...).

- Filtrage des images (Segmentation).
- Le but de cette étape est de supprimer toute ambiguïté en détectant des zones de bruit et en faisant ressortir la plus grande partie possible d'information utile au système.
- Cette fonction se charge également de détecter l'absence d'empreinte, un niveau élevé de bruit dans l'image (image sale ou lecteur défectueux), un positionnement incorrect du doigt.
- Evaluation de la qualité de l'empreinte capturée.
- Le système calcule un facteur de qualité qui permet d'établir un critère automatique de fiabilité du *"gabarit"* de l'empreinte qui sera ensuite calculée.
- Squelettisation de l'empreinte.
- Dans l'image binarisée (noir et blanc) les lignes se voient clairement mais elles ont des tailles différentes. Pour pouvoir détecter rapidement les minuties (terminaisons, bifurcations), il est nécessaire d'obtenir une image plus schématique de l'empreinte, dans laquelle toutes les lignes ont la même épaisseur (1 pixel).
- Extraction des minuties.
- C'est le processus final qui complète l'obtention de la *"signature"* de l'empreinte.
- A partir d'une image de l'empreinte préalablement traitée, on extrait grâce à différents algorithmes une structure de données (ou signature).

-Le "gabarit" retenu pour caractériser l'empreinte est basée sur un ensemble suffisant et fiable de minuties.

- On entend par suffisant, le nombre minimum de minuties nécessaires pour pouvoir établir des comparaisons fiables entre empreintes. Par expérience, ce minimum se situe à 14 minuties.
- On entend par fiable, les minuties qui ne sont pas influencées par des défauts lors de l'acquisition de l'image ou par l'altération temporaire de l'empreinte digitale (blessure, érosion, etc.).
- Avec un petit nombre de minuties (15 ou 20) correctement localisées, il est possible d'identifier une empreinte parmi plusieurs millions d'exemplaires.

- Généralement, chaque minutie occupe environ un espace de 16 octets sans compactage ni compression. Ceci explique la taille de chaque fichier *"gabarit"*, 240 octets pour 15 minuties et 1600 octets pour 100 minuties.

- Lors du processus d'extraction, on détecte initialement 100 minuties en moyenne, parmi lesquelles environ 60 % correspondent à de fausses minuties qui seront identifiées lors d'un processus ultérieur. Le logiciel extrait donc une quarantaine de minuties réelles de l'empreinte. Cette valeur est nettement supérieure aux minima, ce qui augmente la fiabilité. De plus, ce chiffre est loin du total de minuties détectées, ce qui laisse supposer que n'ayant conservé que les plus fiables, on a éliminé les minuties erronées qui auraient pu détériorer le comportement du système.

## Les principales étapes en images


# L’authentification vocale

## Notion:

L'authentification vocale permet d'authentifier un individu à l'aide de son empreinte vocale, lui évitant ainsi toutes les contraintes liées aux codes confidentiels, mots de passe et autres questions de sécurité. Elle garantit un niveau de sécurité optimal.

## Principe et avantage:


Au cours de l'authentification de la voix, la voix de l'utilisateur est comparée à l'empreinte vocale
stockée pour vérifier l'identité déclinée.

L'utilisation de la biométrie vocale offre de nombreux
avantages, parmi lesquels :
- elle est plus fiable qu'une carte magnétique ou un mot de passe qui peuvent être dérobés,
- elle s'intègre de façon transparente dans une conversation téléphonique
- elle ne nécessite pas de disposer de coûteux dispositifs de lecture ou de scanners, juste d'un
micro ou d'un téléphone. Elle est utilisable à distance et sans contact.

Pour conclure, nous pouvons dire qu'il existe de nombreux moyen d'authentification des personnes, chacun à ses avantages et inconvénients. Chaque utilisateurs devra donc faire le bon choix parmi les moyens d'authentifications et de les utiliser de façon optimale.

## Sources:


https://ssi.ac-strasbourg.fr/bonnes-pratiques/recommandations/lidentification-et-lauthentification/

http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

http://www.linternaute.com/science/biologie/dossiers/06/0607-biometrie/retine.shtml

http://www.biometrie-online.net/technologies/empreintes-digitales

http://www.nuance.fr/landing-pages/products/voicebiometrics/

http://fr.evolis.com/nos-technologies/encodage-pistes-magnetiques