





# Techniques d'authentification

L'authentification est le processus qui permet de vérifier l'identité d'un utilisateur, d'un appareil ou d'un service.

## 1. Authentification par paire de clés (asymétrique)

### Définition :




Utilise un couple de clés : une **clé publique** et une **clé privée**.

-  La **clé privée** est conservée secrètement par l'utilisateur.
-  La **clé publique** peut être partagée librement.
-  Permet l'authentification sans mot de passe.
-  Très utilisée dans les connexions SSH ou pour les certificats SSL/TLS.

## 2. Authentification unique (SSO – Single Sign-On)

### Définition :




L'utilisateur ne s'identifie qu'une seule fois pour accéder à plusieurs services.

-  Simplifie la gestion des accès.
-  Gain de temps : une seule connexion suffit pour toute la session.
-  Courant dans les entreprises (ex : connexion au compte Microsoft ou Google pour plusieurs services internes).

## 3. Authentification par preuve

### Définition :


L'utilisateur fournit une **preuve** de son identité. Elle peut être de trois types :

-  **Ce que je sais** : un mot de passe, un code PIN.
-  **Ce que je possède** : un badge, une carte à puce, un téléphone (code envoyé par SMS, token).
-  **Ce que je suis** : une donnée biométrique (empreinte, reconnaissance faciale, etc.).

## Journaux système (logs)


### Définition :

Fichiers dans lesquels le système enregistre automatiquement les événements et actions effectués.




-  Contiennent :
  - Le **type d'action** réalisée (connexion, modification, suppression...)
  - La **date** et l'**heure**
  - L'**utilisateur** concerné

## Chiffrement : Définition

Le **chiffrement** est un procédé qui transforme un message clair (lisible) en un message chiffré (illisible) à l'aide d'une **clé**.

 Le but : protéger la **confidentialité** des données lors de leur stockage ou transmission.

## Les 3 concepts fondamentaux du chiffrement



1. **Confidentialité**  
 Seul le destinataire autorisé peut lire le message.
2. **Intégrité**  
 Le message ne doit pas être modifié sans être détecté.
3. **Authenticité**  
 Le destinataire peut vérifier l'identité de l'expéditeur.

## Types de chiffrement

### 1. Chiffrement symétrique

- Une **seule clé** pour chiffrer et déchiffrer.
- Rapide et efficace.
- Problème : il faut transmettre la clé de façon sécurisée.

## 2. Chiffrement asymétrique

- Utilise une **paire de clés** :
  -  Clé privée : secrète, gardée par l'utilisateur.
  -  Clé publique : partagée avec tout le monde.
- Plus sécurisé pour l'échange de données sensibles, mais plus lent.



## Chiffrement de César

- Décale chaque lettre de l'alphabet d'un certain nombre de positions (clé).

### Exemple :

Avec un décalage de 3 :

A → D, B → E, C → F, etc.

 Facilement cassable aujourd'hui (par force brute ou analyse fréquentielle).



## Chiffrement pour signer & Hachage



### Signature numérique

- Utilise le **chiffrement asymétrique**.
- Le message est **signé avec la clé privée** → permet de garantir :
  - L'**authenticité** du message.
  - L'**intégrité** : si le message est modifié, la signature devient invalide.



## Hachage

- Transforme un message en une **empreinte unique** (appelée **hash**).
- Impossible de revenir en arrière (fonction **non réversible**).
- Permet de vérifier l'intégrité, sans révéler le contenu.

**Exemples** : SHA-256, MD5 (déconseillé car vulnérable)



## OpenPGP – Définition

- **OpenPGP** est un **standard ouvert** (ou protocole) pour le **chiffrement** et la **signature numérique** des données.



Il permet :

- Le **chiffrement asymétrique** (clé publique/clé privée).
- La **signature numérique**.







## GnuPG (ou GPG) – Définition

- **GnuPG** (GNU Privacy Guard) est un **logiciel libre** qui implémente le **standard OpenPGP**.
- C'est l'outil le plus utilisé pour appliquer OpenPGP dans la pratique.



Il permet :


-  **Chiffrer/Déchiffrer** des fichiers ou des mails.
-  **Signer/Verifier** des documents.
-  **Créer et gérer des paires de clés**.
-  **Échanger des clés** de manière sécurisée.


## IDS – Intrusion Detection System


### Définition :

Un **IDS** est un système de **détection d'intrusion**.

Il **surveille le réseau ou un hôte** pour détecter des comportements suspects ou malveillants.

 Son rôle :

- Analyser le trafic ou les journaux.
- Détecter les symptômes de l'attaques (virus, scans, accès non autorisé...).
- Générer des **alertes** 

 mais ne bloque pas automatiquement/ génération de beaucoup de faux positifs.


## HIDS – Host-based IDS


### Définition :

Un **HIDS** surveille **un seul ordinateur ou serveur** (l'hôte).

 Il vérifie :

- Les **fichiers système**,
- Les **journaux d'événements**,
- Les **activités des utilisateurs**,
- Les **processus et applications**.

 **Avantage** : très précis pour ce qui se passe **à l'intérieur de la machine**.

 **Limite** : pas de détection en temps réel/ utilise des ressources de la machine.

## **NIDS – Network-based IDS**

### **Définition :**


Un **NIDS** surveille le **trafic réseau** en temps réel.

 Il écoute :

- Les paquets entrants et sortants.
- Les connexions réseau.
- Les modèles d'attaque connus.



✓ **Avantage** : permet de voir ce qui circule sur tout le réseau/ détection en temps réel.

✗ **Limite** : faible en cas de trafic intense/ non opérationnel avec flux chiffrer/ difficultés traiter les fragments IP






Bien sûr ! Voici des notes claires, organisées et complètes sur les concepts d'**archivage**, **sauvegarde**, et la **protection des données**, avec quelques références au **Code pénal** .

## **Archivage vs Sauvegarde**

### **Sauvegarde (Backup)**

- **Objectif** : Restaurer les données en cas de perte (panne, erreur humaine, attaque...).
- **Durée** : Courte à moyenne durée.
-  **Fréquence** : régulière, souvent automatique.
-  **Stockage** : interne, externe, cloud, NAS...

## Archivage

- **Objectif** : Conserver des documents ou données à **long terme** pour des raisons :
  - Légales 
  - Historiques 
  - Administratives 
-  Les données archivées ne changent plus.
-  Doit garantir **authenticité, intégrité, lisibilité, et traçabilité**.

## Types d'archivage

1. **Archivage natif**: Les données sont **créées et archivées dès leur production**.
2. **Archivage intermédiaire**: Données **encore utiles** mais pas utilisées quotidiennement.
3. **Archivage définitif**: Données **conservées à vie**, souvent pour des raisons juridiques ou historiques.

## Techniques de protection des données

### Protection physique

- Accès contrôlé aux locaux (badges, caméras, serrures).
- Environnement sécurisé (anti-feu, anti-inondation...).

## Gestion des habilitations

- Attribution des droits d'accès **par rôle**.
- Accès limité au strict nécessaire (principe du **moindre privilège**).



## Traçabilité

- Enregistrement des actions sur les données (logs).
- Suivi des accès, modifications, suppressions.



## Durée de conservation & archivage

Type de document	Durée légale minimale (France)
Factures	10 ans
Bulletins de paie (employeur)	5 ans
Contrats commerciaux	5 ans
Documents comptables/ doc fiscaux	10 ans
Dossier médical (hôpital)	20 ans






# Durcissement des OS (Hardening)

## Définition :

Le **durcissement d'un système d'exploitation** consiste à **réduire sa surface d'attaque** en appliquant des mesures de sécurité :

- Supprimer ce qui est inutile,
- Renforcer les configurations,
- Contrôler les accès.

## Objectif du durcissement

- Protéger l'OS contre :
    - Les intrusions 
    - Les malwares 
    - Les failles d'exploitation 
  - Augmenter la **résilience** globale du système.
- 

## Principales techniques de durcissement

### 1. Suppression des services inutiles

- Désactiver les services non utilisés
- Moins de services actifs

### 2. Renforcement de la configuration

- Modifier les paramètres par défaut (ex : mots de passe, ports...).
- Configurer les pare-feux locaux (iptables, Windows Defender Firewall...).

### 3. **Gestion des utilisateurs et des permissions**

- Supprimer les comptes inutilisés.
- Appliquer le **principe du moindre privilège**.
- Forcer l'utilisation de **mots de passe forts**.

### 4. **Mise à jour et correctifs**

- Appliquer régulièrement les **patches de sécurité**.
- Activer les mises à jour automatiques si possible.

### 5. **Audit et journalisation**

- Activer et surveiller les **logs système** (authentification, accès, erreurs).
- Utiliser des **IDS** pour détecter les intrusions.

### 6. **Chiffrement**

- Chiffrer les disques ou partitions sensibles
- Chiffrer les communications (SSH, HTTPS, VPN...).

### **Exemples d'outils et guides**

- **CIS Benchmarks** : standards de durcissement pour Windows, Linux, etc.
- **Lynis** : audit de sécurité pour systèmes Linux/Unix.
- **Microsoft Security Compliance Toolkit** : outils et recommandations pour Windows.