

# 16/06/25 - Unicité et mot de passe

## Unicité

## Mots de passes

Sources :

- <https://www.cnil.fr/fr/securite-chiffrement-hachage-signature>
- [https://cyber.gouv.fr/sites/default/files/2021/10/anssi-guide-authentification\\_multifacteur\\_et\\_mots\\_de\\_passe.pdf](https://cyber.gouv.fr/sites/default/files/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf)
- [https://cheatsheetseries.owasp.org/cheatsheets/Password\\_Storage\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html)
- <https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite>

## CNIL & RGPD

Les manquements les plus souvent constatés lors des contrôles (déjà en 2021) c'était des mots de passes bien trop faibles et stockés en clairs. (Article 5 et 32 du RGPD)

Se protéger derrière le RGPD est donc totalement une raison valide pour accroître notre sécurité et pour bien se couvrir.

## Recommandations pour l'utilisateur

*cf. ANSSI + voir si faire une page dédiée serait utile pour l'utilisateur ?*

1. Utiliser des mots de passe robustes
2. Utiliser un mot de passe différent pour chaque service
3. Utiliser un coffre-fort de mots de passe
4. Protéger ses mots de passe (Pas écrire le mot de passe sur une note sous le clavier, ne pas créer de fichier "mot de passe" sur son poste, ne pas envoyer ses mots de passe par e-mail. (d'autant plus s'ils sont en clair)
5. Utiliser un mot de passe particulièrement robuste pour l'accès à sa messagerie électronique.
6. Choisir un mot de passe sans information personnelle. (pas d'infos publiques connues sur réseau social comme le nom d'un enfant, animal de compagnie...)
7. Modifier les mots de passe par défaut.

## Longueur

Mot de passe au strict minimum de 12 caractères de long, avec minuscules, majuscules, chiffres et caractères spéciaux. (Idéalement longueur de 16 caractères ou plus recommandées)

## Mot de passe oublié

Source : [https://cheatsheetseries.owasp.org/cheatsheets/Forgot\\_Password\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html)

Recouvrement d'accès via une des deux méthodes suivantes :

1. Lien temporaire où on donne un mot de passe généré aléatoirement à l'utilisateur (qui pourra/devra être modifié par l'utilisateur)
2. Lien temporaire de réinitialisation du mot de passe.

Durée recommandée par le NIST (National Institute of Standards and Technology, recommandation du début 2019) -> 24 heures max quand envoyé à une adresse e-mail, mais en 2025 peut-être comparer avec d'autres services existants ? 1 demi-journée ? quelques heures ? **à vérifier**

## Changer mon mot de passe

Depuis l'espace client, s'il est possible de modifier son propre mot de passe, faire en sorte de vérifier :

1. L'utilisateur est authentifié avec une session active.
2. Vérification du mot de passe actuel. C'est pour s'assurer que la personne soit bien légitime. Par exemple, dans un endroit public, un utilisateur peut toujours être connecté sur un navigateur car il a oublié de se déconnecter et de ce fait, si on ne vérifie pas le mot de passe actuel, une autre personne pourrait le modifier.

## Stockage des mots de passe

Pas de stockage en clair, et rappel, un mot de passe doit être haché, pas chiffré (hachage -> fonction dans un sens ; chiffrer -> fonction à double sens).

*Le seul moment où le mot de passe doit être chiffré, c'est uniquement dans un cas extrême où on aurait besoin à un moment du mot de passe original en clair, pour s'authentifier vers un autre système externe qui ne supporterait pas les méthodes modernes d'authentications, donc très rare. (cf. OWASP)*

1. Stocker uniquement les empreintes (résultat d'une fonction de hachage cryptographique comme SHA-2 ou SHA-3) et appliquer une fonction de dérivation comme Argon2id, bcrypt, ou PBKDF2 (cf. cheatsheetseries d'OWASP, ANSSI...)

Algorithmes obsolètes (rappel de la CNIL en Mars 2024) : chiffrements (DES, 3DES), fonctions de hachage (MD5, SHA-1)

Par exemple pour du faire checksum, au lieu d'utiliser MD5 ou SHA-1, aujourd'hui il faudrait utiliser SHA-256. (utilisé entre autres pour les certificats TLS, checksum d'iso Linux...)

2. Doit comporter un sel choisi aléatoirement pour chaque compte et d'une longueur d'au moins 128 bits (cf. ANSSI)

D'après l'article de l'OWASP, les algorithmes de hachage modernes appliquent automatiquement un sel sur le mot de passe généré.

---

Revision #11

Created 16 June 2025 07:45:21 by Quentin

Updated 16 June 2025 09:59:25 by Quentin