Fiche Pratique N°65 : Passez aux clés d'accès (passkeys) V1.2

7 nov, 2026 · @Gabriel

Objectif : *remplacer progressivement vos mots de passe par des clés d'accès, presque impossibles à voler par hameçonnage, en les gardant chez vous ou chez un acteur de confiance, et non chez Google, Apple ou Microsoft.*

- ***Public visé :*** *débutant à intermédiaire*
- ***Temps estimé :*** *30 minutes pour l'installation, puis 2 minutes par compte*
- ***Difficulté :*** *★★☆☆☆ (Facile)*
- ***Prérequis :*** *un téléphone ou un ordinateur à jour avec un verrouillage d'écran ; un gestionnaire de mots de passe libre (fiche N°16)*
- ***Fiches associées :*** *N°16 (gestionnaires de mots de passe), N°18 (double authentification), N°29 (Syncthing), N°35 (Vaultwarden), N°47 (arnaques en ligne), N°51 (héritage numérique)*

PARTIE 1 : LES BASES (pour débutants)

1. Le problème : le mot de passe est le maillon faible

Situation	Conséquence
Vous tapez votre mot de passe sur un faux site	L'escroc le récupère et entre dans votre compte
Vous réutilisez le même mot de passe	Une seule fuite ouvre plusieurs comptes
Vous recevez un code par SMS	Un escroc peut vous convaincre de le lui lire au téléphone
Votre téléphone propose d'enregistrer vos clés « dans le cloud »	Vos identifiants se retrouvent chez Google ou Apple, liés à votre compte chez eux

Le risque : un mot de passe peut être deviné, volé dans une fuite ou saisi sur un faux site. Et les clés d'accès, si on accepte les réglages par défaut, renforcent la dépendance aux géants du numérique.

Le bénéfice : une clé d'accès ne se tape pas et ne se vole pas sur un faux site. L'Office fédéral suisse de la cybersécurité la juge plus sûre que le mot de passe. Rangée dans un gestionnaire libre, elle reste sous votre contrôle.

2. Comprendre la clé d'accès

Une clé d'accès (en anglais *passkey*) est un couple de deux clés numériques, créé pour **un site précis** :

Élément	Où il se trouve	Rôle
Clé privée	Dans votre gestionnaire ou votre clé de sécurité, jamais transmise	Signe une preuve à chaque connexion
Clé publique	Chez le site	Vérifie la preuve, sans pouvoir la fabriquer

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°65 : Passez aux clés d'accès (passkeys) V1.2

Élément	Où il se trouve	Rôle
Votre code, empreinte ou visage	Sur votre appareil uniquement	Déverrouille la clé privée ; le site ne les voit jamais

Pourquoi c'est résistant à l'hameçonnage : la clé est liée à l'adresse exacte du site. Sur un faux site, elle ne fonctionne pas : il n'y a rien à voler.

C'est un standard ouvert (FIDO2/WebAuthn) : il n'appartient ni à Google ni à Apple, et des logiciels libres savent le gérer.

3. Où ranger vos clés : notre principe

Par défaut, Android propose de les ranger dans le Gestionnaire de mots de passe de Google, l'iPhone dans le trousseau iCloud, Windows dans Windows Hello. **Refusez :** vos clés seraient liées à votre compte chez ces entreprises américaines, et changer de crèmerie serait plus compliqué.

Solution	Où sont vos clés	Pour qui	Éthique
KeePassXC (ordinateur) + **KeePassDX** (Android)	Dans un fichier chiffré **chez vous**, sans compte ni serveur	Celles et ceux qui veulent zéro cloud	★★★★★ Libre, local
Clé de sécurité Nitrokey (FIDO2)	Dans l'objet, qui ne transmet jamais la clé privée	Clé de secours, comptes très sensibles	★★★★★ Fabricant allemand, matériel et logiciel libres
Bitwarden auto-hébergé (Vaultwarden, fiche N°35)	Sur votre serveur	Familles, personnes déjà auto-hébergées	★★★★☆ Libre, chez vous
Proton Pass	Chez Proton (Suisse), chiffré de bout en bout	Débutants qui veulent la synchronisation sans effort	★★★☆☆ Société suisse, gratuit, clés d'accès sur toutes les formules
Bitwarden en région européenne	Serveurs Bitwarden dans l'Union européenne, chiffré de bout en bout	Qui veut Bitwarden sans auto-héberger	★★★☆☆ Libre, mais société américaine, soumise au Cloud Act
Trousseau iCloud, Gestionnaire Google, Windows Hello	Chez Apple, Google ou Microsoft	—	✗ À éviter

⚠️ **Cloud Act :** Bitwarden est une société américaine. Même si vous choisissez ses serveurs européens, vos données restent soumises au droit américain (Cloud Act), qui permet aux autorités des États-Unis d'en exiger la communication. Votre coffre est chiffré de bout en bout, mais les informations sur votre

gabriel.ananda@mailo.com
CC BY SA

compte ne le sont pas. Pour y échapper, hébergez vous-même Vaultwarden (fiche N°35), ou choisissez Proton Pass (Suisse) ou KeePassXC (local).

Notre conseil : KeePassXC et KeePassDX si vous êtes prêt à gérer un fichier (synchronisé entre vos appareils avec Syncthing, fiche N°29) ; Proton Pass si vous voulez la simplicité. Dans les deux cas, ajoutez une clé Nitrokey comme secours pour vos comptes essentiels.

4. Avant de commencer : liste de contrôle

- ☐ Votre téléphone a un verrouillage d'écran (code, empreinte ou visage)
- ☐ Votre système et votre navigateur sont à jour
- ☐ Votre gestionnaire libre est installé : application, et extension (ou intégration) du navigateur
- ☐ Vous connaissez le mot de passe actuel du compte et vos codes de secours (fiche N°18)
- ☐ L'appareil est **à vous** et n'est pas partagé

⚠️ Toute personne capable de déverrouiller votre appareil peut se connecter avec une clé d'accès qui y est disponible. Ne créez jamais de clé d'accès sur un appareil partagé.

5. Faire de votre gestionnaire libre le fournisseur de clés

Sans ce réglage, votre téléphone enverra vos clés chez Google ou Apple.

1. **Android :** ouvrez les **Paramètres**, cherchez « mots de passe » ou « service de saisie automatique », puis choisissez votre gestionnaire (KeePassDX, Proton Pass ou Bitwarden) comme service préféré. Désactivez le Gestionnaire de mots de passe de Google s'il est proposé à côté.
    - **Vous devez voir :** votre gestionnaire libre seul (ou en premier) dans la liste des fournisseurs.
2. **iPhone :** ouvrez **Réglages**, cherchez « remplissage automatique », activez votre gestionnaire (Proton Pass ou Bitwarden) et désactivez **Mots de passe** (le trousseau iCloud).
    - **Vous devez voir :** votre gestionnaire coché, le trousseau iCloud décoché.
3. **Ordinateur :** installez l'extension de votre gestionnaire (pour KeePassXC, activez l'intégration au navigateur dans ses paramètres).
    - **Vous devez voir :** l'icône du gestionnaire dans la barre du navigateur, connectée à votre coffre.

6. Créer une clé d'accès pour un compte

Commencez par votre **messagerie principale** : c'est elle qui permet de réinitialiser tous vos autres comptes.

1. Connectez-vous au site avec votre mot de passe habituel, **sur l'appareil où se trouve votre gestionnaire**.
2. Allez dans **Paramètres › Sécurité** (ou **Connexion**, **Mot de passe et sécurité**).
3. Cherchez **Clé d'accès**, **Passkey** ou **Se connecter sans mot de passe**, puis **Créer** ou **Ajouter**.
    - **Vous devez voir :** une fenêtre de votre gestionnaire libre qui propose d'enregistrer la clé. Si c'est une fenêtre Google, Apple ou Windows qui s'ouvre, annulez et revoyez la section 5.

gabriel.ananda@mailo.com
CC BY SA

4. Enregistrez la clé et déverrouillez.
    - **Vous devez voir :** la clé listée dans les réglages du site, et une entrée « clé d'accès » dans votre gestionnaire.
5. Déconnectez-vous, puis reconnectez-vous en choisissant la clé d'accès.
    - **Vous devez voir :** la connexion se fait après un simple déverrouillage, sans mot de passe.

Si le site ne propose pas de clé d'accès : gardez un mot de passe unique et long dans votre gestionnaire, avec la double authentification (fiche N°18).

7. À quoi s'attendre

Situation	Comportement normal	À faire
Connexion sur un appareil où le gestionnaire est installé	Le gestionnaire propose la clé ; vous déverrouillez	Rien
Connexion sur un ordinateur sans gestionnaire	Un QR code s'affiche pour utiliser votre téléphone	Voir l'encadré ci-dessous
Le mot de passe existe toujours	Normal : la plupart des sites le gardent en secours	Gardez-le long et unique

⚠️ **Le QR code et la surveillance :** cette méthode (« appareil hybride ») fait transiter la connexion, chiffrée, par un service relais de l'éditeur du système, par exemple Google ou Apple. Le contenu est illisible pour eux, mais la connexion passe par leurs serveurs. Préférez installer votre gestionnaire libre sur l'ordinateur, ou brancher votre clé Nitrokey.

8. Dépannage

Symptôme	Cause possible	Action
Une fenêtre Google, Apple ou Windows s'ouvre au lieu de votre gestionnaire	Le gestionnaire libre n'est pas le fournisseur par défaut	Refaites la section 5
KeePassXC ne propose rien	Intégration au navigateur désactivée, ou base verrouillée	Paramètres › Intégration au navigateur ; déverrouillez la base
« Aucune clé d'accès disponible »	Clé enregistrée dans un autre gestionnaire	Vérifiez dans quel gestionnaire vous l'avez créée
Téléphone perdu ou volé	—	Depuis un autre appareil, retirez la clé dans les réglages de sécurité du compte, puis changez le mot de passe de votre gestionnaire

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°65 : Passez aux clés d'accès (passkeys) V1.2

PARTIE 2 : ALLER PLUS LOIN (pour intermédiaires et avancés)

9. Le choix « zéro cloud » : KeePassXC, KeePassDX et Syncthing

- **KeePassXC** (Windows, macOS, Linux) gère les clés d'accès depuis sa version 2.7.7, via son intégration au navigateur.
- **KeePassDX** (Android, disponible sur F-Droid) les gère depuis sa version 4.2.0.
- Les deux utilisent le même format de fichier chiffré (`.kdbx`). Avant de vous y fier, testez qu'une clé créée sur l'un fonctionne sur l'autre. Synchronisez ce fichier entre vos appareils avec **Syncthing** (fiche N°29), directement d'appareil à appareil, sans serveur tiers.
- ⚠️ Sauvegardez ce fichier régulièrement (fiches N°19a à N°19e) : sans lui, pas de clés.

10. Une clé de sécurité matérielle libre

Une clé **Nitrokey 3** (fabricant allemand, matériel et micrologiciel libres) prend en charge FIDO2. Elle garde vos clés d'accès dans l'objet, sans aucun cloud.

- Utilisez-la comme **second moyen de connexion** pour vos comptes essentiels (messagerie, gestionnaire, banque si elle l'accepte).
- Rangez-la en lieu sûr, séparée de votre trousseau habituel.
- ⚠️ Si elle est votre seul moyen de connexion et que vous la perdez, vous perdez l'accès : ayez toujours une autre clé ou vos codes de secours.

11. Changer de gestionnaire sans tout recréer

Un format d'échange chiffré, défini par la FIDO Alliance, permet de transférer ses clés d'accès d'un gestionnaire à un autre. Apple le propose depuis iOS 26 et macOS 26 ; Google le teste sur Android, sans date annoncée. Si vos clés sont aujourd'hui dans iCloud ou chez Google, c'est l'occasion de les rapatrier dans un gestionnaire libre. Sinon, recréez-les site par site : c'est rapide.

12. Ne jamais perdre l'accès : la règle des deux clés

- **Deux moyens de connexion** pour chaque compte important : votre gestionnaire et une clé Nitrokey (ou un second appareil).
- **Codes de secours** de double authentification sur papier (fiche N°18).
- **Le mot de passe maître de votre gestionnaire :** long, jamais réutilisé, avec son kit de secours imprimé.
- **Vos proches :** prévoyez comment ils accéderont à l'essentiel (fiche N°51).

À savoir avant de se lancer

Crainte fréquente	La réalité
« Les clés d'accès, c'est un truc de Google et d'Apple »	Non : c'est un standard ouvert, géré par des logiciels libres comme KeePassXC
« Le site garde mon empreinte »	Non : elle reste sur votre appareil ; le site ne reçoit qu'une signature

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°65 : Passez aux clés d'accès (passkeys) V1.2

Crainte fréquente	La réalité
« Sans cloud, je perdrai mes clés »	Pas si votre fichier est synchronisé avec Syncthing, sauvegardé, et doublé d'une clé Nitrokey
« Je dois tout changer d'un coup »	Non : ajoutez les clés au fil de l'eau, compte par compte

Challenge 7 jours

- **Jour 1 :** choisissez votre gestionnaire (section 3) et installez-le.
- **Jour 2 :** faites-en le fournisseur de clés par défaut (section 5).
- **Jour 3 :** créez la clé d'accès de votre messagerie principale.
- **Jour 4 :** vérifiez qu'aucune clé ne s'est glissée dans iCloud ou chez Google.
- **Jour 5 :** ajoutez une clé à deux autres comptes.
- **Jour 6 :** configurez une clé de secours (Nitrokey ou second appareil).
- **Jour 7 :** imprimez vos codes de secours et le kit de secours de votre gestionnaire.

Vous allez constater :

- que la connexion est plus rapide qu'avec un mot de passe ;
- que vos identifiants ne dépendent plus d'un géant du numérique.

En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Ranger les clés dans un gestionnaire libre	Vos identifiants restent chez vous	Sections 3 et 5
Créer une clé pour votre messagerie	Le compte le plus important protégé contre l'hameçonnage	Section 6
Éviter le QR code	Moins de passages par les serveurs de Google ou d'Apple	Section 7
Garder deux moyens de connexion	Aucun risque de blocage	Section 12

À retenir absolument

- **Une clé d'accès ne se vole pas** sur un faux site.
- **Refusez iCloud, Google et Windows Hello** comme coffre : choisissez un gestionnaire libre.
- **Jamais sur un appareil partagé.**
- **Toujours deux moyens de connexion** pour chaque compte important.

Test final :

1. Ouvrez votre gestionnaire libre et retrouvez l'entrée « clé d'accès » de votre messagerie.

gabriel.ananda@mailo.com
CC BY SA

2. Déconnectez-vous, puis reconnectez-vous avec la clé.
3. Si c'est votre gestionnaire, et non Google ou Apple, qui vous a ouvert la porte : c'est gagné ✅

Références

- OFCS (Confédération suisse) – Considérations technologiques : clés d'accès (septembre 2025)
- KeePassXC – Version 2.7.7 (prise en charge des clés d'accès)
- Privacy Guides (forum) – KeePassDX prend en charge les clés d'accès (version 4.2.0)
- Wikipédia – Nitrokey (matériel et logiciel libres, FIDO2)
- Proton – Proton Pass prend en charge les clés d'accès sur toutes les formules
- Bitwarden – Gestion des clés d'accès pour tous les utilisateurs, y compris gratuits
- Bitwarden – Régions de serveurs (région Union européenne, choisie à la création du compte)
- Corbado – Connexion par QR code : relais de l'éditeur du système (Google, Apple)
- 9to5Mac – iOS 26 : export et import des clés d'accès
- PhoneArena – Export des clés d'accès sur Android en test

gabriel.ananda@mailo.com
CC BY SA