Association Loisirs et culture

# *Passkeys : à quoi ça sert, comment ça marche et pourquoi vont-ils remplacer les mots de passe*

**Jean Marie Herbaux**

## Table des matières



Les passkeys vont devenir la nouvelle méthode d'authentification populaire pour accéder à ses comptes sur les sites web et applications. Plus sécurisés et plus pratiques que les mots de passe, ils vont peu à peu devenir la norme pour prouver son identité sur internet. Voici ce que vous devez savoir à leur sujet .

## 1. LE POURQUOI :

Depuis qu'internet s'est démocratisé auprès du grand public, nos comptes des différentes plateformes auxquelles nous nous inscrivons sont protégés par des mots de passe. Nous n'avons jusqu'ici connu que cette forme de défense pour préserver l'accès à nos informations et profils, si bien qu'il est aujourd'hui difficile d'imaginer un monde dans lequel ils n'existeraient plus, ou du moins d'une manière très différente. Et pourtant, les mots de passe ne sont pas forcément la solution la plus sécurisée ou même la plus pratique pour s'assurer que nous seuls sommes en mesure d'accéder à nos comptes.
Les grandes firmes du numérique développent depuis des années des alternatives visant à enfin mettre un terme à la domination des mots de passe et améliorer l'expérience des utilisateurs. C'est ainsi que sont nés les *passkeys*, dont vous devriez beaucoup entendre parler dans les mois et années à venir.

## 2. LES PASSKEYS, C'EST QUOI ?

Un passkey est une clé d'accès (ou clé d'identification) contenant des données chiffrées prouvant que vous êtes bien le propriétaire du compte auquel vous tentez de vous connecter.
Les passkeys reposent sur le principe du chiffrement asymétrique, qui implique l'existence de deux clés de chiffrement, une clé publique (stockée sur les serveurs de la plateforme) et une clé privée (stockée localement sur l'appareil de l'utilisateur), qui se synchronisent entre elles lors d'une tentative de connexion.

## 3. LES PASSKEYS, COMMENT ÇA MARCHE, À QUOI ÇA SERT ?

Comme lorsque vous créez un mot de passe à la création d'un nouveau compte actuellement, vous pouvez choisir d'opter pour un passkey sur les services qui prennent en charge cette technologie. Dans ce cas, la plateforme en question va générer les deux clés (publique et privée), qui fonctionnent ensemble. Seule votre clé privée sera reconnue par la clé publique dans le cadre du protocole de chiffrement et permettra la connexion au compte par l'intermédiaire du passkey.

L'appareil physique n'est pas la seule couche de protection permettant de valider la connexion. Une méthode d'identification prise en charge par le terminal en question, au choix de l'utilisateur, permet de se connecter. Il peut s'agir d'un déverrouillage biométrique (reconnaissance faciale, empreinte digitale), d'un code PIN, d'un schéma…

L'intérêt des passkeys est d'allier :

L'aspect pratique :

- Accéder à ses comptes en utilisant le même procédé que le déverrouillage de son appareil, sans avoir besoin de se remémorer ses mots de passe ou d'utiliser un gestionnaire.
- L'aspect sécurité :
- Une connexion chiffrée qui requiert à la fois l'accès physique à l'appareil et la connaissance de la méthode d'identification.

## 4. EN QUOI LES PASSKEYS SONT-ILS PLUS SÉCURISÉS QUE LES MOTS DE PASSE ?

Si les gestionnaires de mots de passe contribuent à rendre les mots de passe plus sûrs, ces derniers restent faillibles. Malgré la mise en place de systèmes basés sur des mots de passe à usage unique et la double authentification, le constat est sans appel : la sécurité des comptes laisse à désirer et les risques de piratage et de hameçonnage restent très élevés. Les passkeys ne sont pas une solution parfaite, mais octroient tout de même plus de garanties que les mots de passe traditionnels.

- La première couche de sécurité réside dans le stockage de la clé privée sur un appareil dont l'utilisateur est propriétaire. Bien entendu, cette donnée se trouve dans un espace protégé par une technologie de chiffrement. De plus, elle n'est jamais communiquée directement aux plateformes auxquelles nous nous connectons : à chaque tentative de connexion, le site web ou l'application va poser une énigme au terminal de l'utilisateur, qui est le seul à pouvoir la résoudre. Un jeton est alors généré pour valider la transaction et autoriser la connexion.

- La seconde strate est le besoin de s'identifier par une information biométrique (préférablement), ou par un élément d'authentification qui n'est pas connu des plateformes (code PIN, schéma à dessiner sur un écran tactile) pour les appareils ne proposant pas de possibilité d'authentification par reconnaissance faciale ou d'empreintes digitales. Détourner une combinaison entre clé privée et biométrie demande des efforts bien plus importants que de se procurer un mot de passe, et même de tromper la double authentification.

- Le phishing ne fonctionne plus, car il est improbable que l'utilisateur révèle sa clé privée à un tiers. La majorité des utilisateurs ne saura d'ailleurs même pas comment identifier sa clé privée. Les fuites de données sont limitées, car les plateformes ne disposent que de la clé publique, qui ne sert à rien sans la clé privée qui lui est associée. Et comme chaque combinaison est unique, un seul compte peut être compromis à la fois. Les attaques par force brute perdent également de leur intérêt. Et si un pirate parvient finalement à récupérer les deux clés qui composent un passkey, reste l'authentification à passer.

## 5. GOOGLE, MICROSOFT, APPLE… QUI VEUT REMPLACER LES MOTS DE PASSE PAR LES PASSKEYS ?

L'adoption des passkeys est poussée par l'Alliance FIDO (Fast IDentity Online), fondée en 2013, dont la mission est de résoudre le manque d'interopérabilité entre les dispositifs d'authentification forte et de développer ainsi que de promouvoir des normes d'authentification contribuant à réduire la dépendance aux mots de passe. La devise de FIDO est “Simpler, Stronger, Authentication : Solving the World's Password Problem”, que l'on peut traduire par “Authentification plus simple et plus forte : résoudre le problème mondial des mots de passe”.

Google, Microsoft et Apple font partie des plus fervents supporters de la disparition du mot de passe. Ils ont largement contribué à la création de leur alternative et probable futur remplaçant, et ont annoncé leur volonté conjointe de renforcer le support des standards FIDO, les passkeys donc, afin d'accélérer la transition vers cette technologie. Les trois firmes américaines font partie du conseil d'administration de l'Alliance FIDO, qui comprend également Samsung, Amazon, Intel, Lenovo, Meta (Facebook) ou encore Qualcomme. Des acteurs majeurs du paiement numérique comme PayPal, Mastercard, Visa et American Express sont aussi présents au tableau. Paradoxalement, nous y trouvons aussi des sociétés spécialisées dans la gestion de mot de passe, comme LastPass, Dashlane

et 1Password, qui devront s'adapter et évoluer lorsque la norme des passkeys supplantera les mots de passe.

Pour l'instant, peu de plateformes (sites web ou applications) proposent à leurs utilisateurs l'authentification par passkey. Outre Google, Microsoft et Apple, Dropbox, eBay, Facebook, Nvidia, PayPal, Twitter, WordPress ou encore Shopify font figure de pionniers.

## 6. QUE SE PASSE-T-IL LORSQUE L'ON CHANGE D'APPAREIL ?

Les passkeys se veulent plus pratiques que les mots de passe, mais la situation actuelle n'est pas des plus favorable à leur adoption massive et il faudra encore du temps et de nombreux efforts de la part des constructeurs et des éditeurs pour les rendre attractifs. L'un des obstacles qui se dressent devant les utilisateurs aujourd'hui est le changement d'appareil, qu'il s'agisse d'un smartphone, d'une tablette ou d'un PC, puisque la clé privée est enregistrée localement dessus.

Un système de synchronisation des clés d'accès est prévu lorsque l'on reste au sein du même écosystème. Vous pouvez donc transférer simplement vos passkeys enregistrés sur votre smartphone Android vers votre nouveau mobile Android par le biais de votre compte Google. Si vous passez d'un iPhone à un autre compte Android ou inversement, la synchronisation devient bien plus compliquée. De même, il n'existe actuellement pas de solution native efficace pour que les passkeys générés depuis votre PC sous Windows soient rendus disponibles depuis votre smartphone Android par exemple.

Pour l'instant, chaque transfert de passkey d'un environnement logiciel à un autre nécessite une procédure manuelle, particulièrement rébarbative s'il y a de nombreux passkeys à gérer. Un système de QR code à scanner avec son smartphone a été pensé. L'appareil mobile fait alors office de passerelle, validant lui-même la demande de connexion pour l'autre appareil. Pour des questions de sécurité, il est cependant nécessaire que le Bluetooth des deux terminaux soit activé, afin de garantir que le PC qui effectue la requête se trouve bien physiquement aux côtés du propriétaire du compte et qu'il ne s'agit pas d'une tentative d'accès malveillante à distance. Généralement, il est possible après cette manipulation de générer un passkey pour un appareil secondaire fréquemment utilisé, afin d'éviter de devoir utiliser son terminal principal à chaque fois.

À l'avenir, des outils seront mis en place pour permettre le transfert rapide et simplifié de ses clés d'identification d'un écosystème à un autre, à l'instar des options d'importation et d'exportation des gestionnaires de mots de passe. D'ailleurs, ceux-ci semblent être parmi les plus prompts à chercher des solutions à ce problème, ce qui leur permettrait de ne pas perdre l'intérêt des utilisateurs qui abandonnent les mots de passe pour les passkeys. Mais là encore, les écosystèmes doivent évoluer, et c'est pourquoi Android 14 supportera les passkeys dans les gestionnaires de mots de passe tiers.

Chez Google, la solution qui paraît prévaloir pour partager ses passkeys entre ses différents appareils est Chrome. Le navigateur est compatible avec les clés d'accès depuis sa version 108, est disponible sur tous les écosystèmes et est déjà pourvu de son propre gestionnaire de mots de passe intégré, ce qui en fait la plateforme idoine et évidente pour gérer ses passkeys.

## 7. QUAND LES PASSKEYS VONT-ILS REMPLACER LES MOTS DE PASSE ?

Les mots de passe ont encore de beaux jours devant eux. Les utilisateurs ne sont pas prêts à basculer du jour au lendemain vers les passkeys et une longue période de transition va s'opérer, durant

laquelle mots de passe et passkeys vont coexister. Les services web et applications devront aussi s'adapter et passer à cette technologie, ce qui peut prendre du temps. Les normes FIDO nécessitent généralement les dernières versions des systèmes d'exploitation, éliminant d'office les appareils les plus anciens de toute compatibilité. Un renouvellement des équipements est donc nécessaire avant de voir les passkeys prendre définitivement le relais des mots de passe. Une autre problématique liée aux clés d'accès est la dépendance aux grands éditeurs d'OS et de software, ce qui pourrait laisser un certain nombre d'utilisateurs réticents sur le carreau. Il est impossible de prédire quand nous assisterons à la mort des mots de passe, mais ceux-ci devraient survivre à court terme.

## 8. COMMENT CONFIGURER DES PASSKEYS SUR VOTRE COMPTE GOOGLE ?

Les passkeys sont devenus officiellement un moyen de se connecter aux services de Google depuis le début du mois de mai 2023. Voici la procédure à suivre pour commencer à les utiliser au sein de l'écosystème de la filiale d'Alphabet :

Rendez-vous à l'adresse https://myaccount.google.com/ et connectez-vous à votre compte Google.
Dans le menu situé à gauche de l'écran, cliquez sur la section *Sécurité*.
Scrollez vers le bas jusqu'à atteindre la partie *Comment vous connecter à Google*. Cliquez sur la ligne *Clés d'accès*, positionnée entre l'option *Validation en deux étapes* et *Mots de passe*.
Saisissez le mot de passe de votre compte Google s'il vous est redemandé.
Cliquez sur le bouton bleu *Utiliser des clés d'accès pour activer la fonctionnalité*.

Désormais, vos appareils Android créeront automatiquement un passkey pour votre compte Google lors de votre prochaine connexion. Vous pouvez aussi cliquer sur *Créer une clé d'accès* en bas pour générer manuellement un passkey sur un appareil d'un autre écosystème. Authentifiez-vous avec votre *méthode d'identification habituelle* (Windows Hello dans notre cas), et le tour est joué ! Pour vérifier que tout fonctionne bien, ouvrez votre navigateur en navigation privée et tentez de vous connecter à votre compte Google. Normalement, vous n'avez plus besoin de renseigner votre mot de passe, il suffit de vous authentifier avec votre PIN, votre empreinte digitale ou par reconnaissance faciale. **Rappelons qu'il est primordial de ne configurer des clés d'accès que sur les appareils dont vous êtes le propriétaire**.

En attendant, pour une meilleure sécurité face aux cybermenaces :
Un conseil, vérifiez régulièrement que votre adresse de messagerie et vos mots de passe n'ont pas fuité sur internet, à l'aide, par exemple, du site https://haveibeenpwned.com/.
Et si vous ne l'avez pas déjà fait, adoptez sans tarder les clés de sécurité, ces fichiers chiffrés qui commencent à remplacer les mots de passe classiques (Les passkeys ne rendent pas seulement nos identifiants plus difficiles à voler, elles facilitent la création et la gestion des codes d'accès, sans avoir à les mémoriser ou à les noter dans un calepin. Plus d'excuse pour le «123456»…

## 9. Inspiré du site web :

Passkeys : à quoi ça sert, comment ça marche et pourquoi ils vont remplacer les mots de passe (phonandroid.com)