L'authentification sans mot de passe , une réponse moderne aux limites du MFA

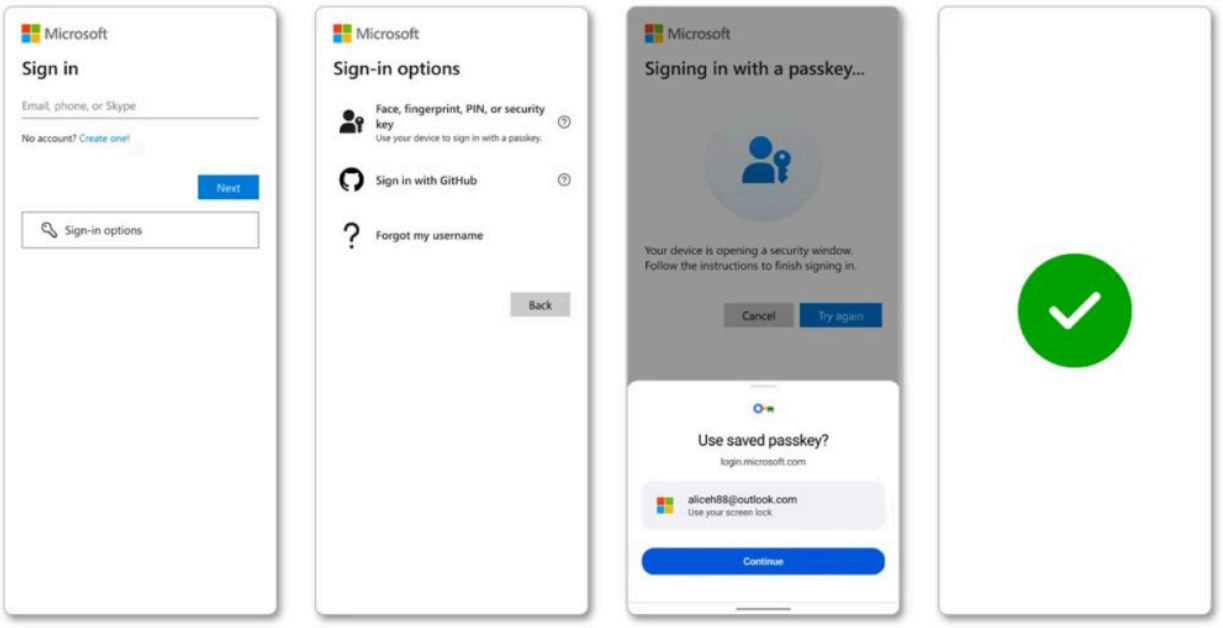
Avec l'intensification des cyberattaques et les limites croissantes du mot de passe traditionnel, les grandes entreprises technologiques (Apple, Google, Microsoft) accélèrent la généralisation de l'**authentification sans mot de passe**, ou **passkeys**. Ces dernières permettent aux utilisateurs de se connecter à leurs comptes à l'aide d'un dispositif biométrique (empreinte, visage) ou d'un token physique, supprimant ainsi le besoin de mémoriser ou de saisir un mot de passe.

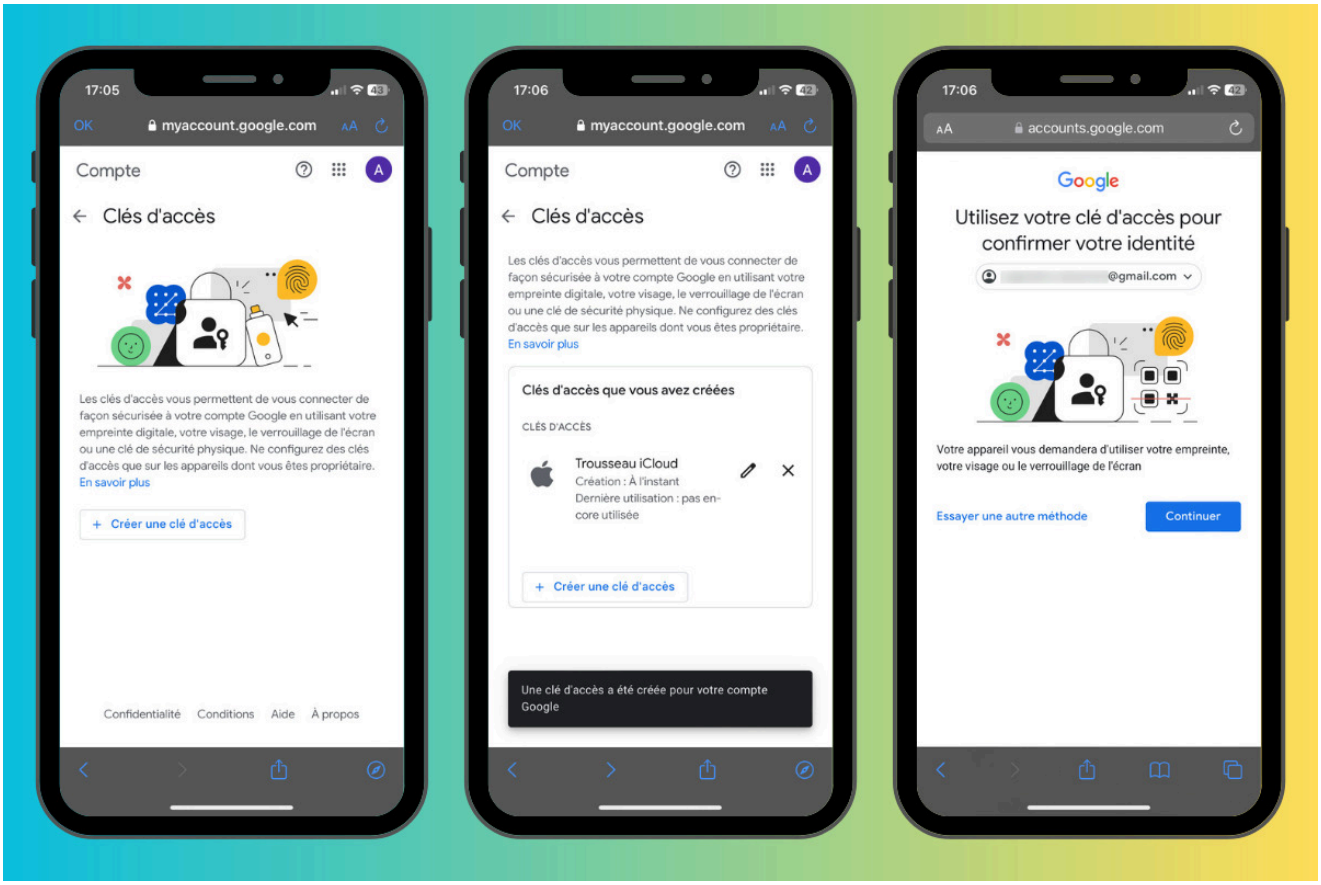
Passwordless Authentication	VS	Multi-Factor Authentication (MFA)
Eliminates the use of passwords		Used in conjunction with passwords
Easier login experience		Adds more friction to the login experience
Can be difficult to deploy		Easy to deploy
Can be costly		Free MFA options available

Ce changement s'impose comme une réponse directe aux faiblesses du **MFA classique (authentification multifacteur)**. Si le MFA reste plus sécurisé qu'un simple mot de passe, il est lui-même la cible de techniques d'attaque récentes : **phishing MFA**, **attaques par rebond**, **harcèlement d'approbation (push fatigue)**, etc. Ces tactiques manipulent les utilisateurs pour qu'ils approuvent par erreur une connexion malveillante.

Face à cette évolution des menaces, des solutions telles que **Microsoft Entra ID** ou **Okta** adaptent leur approche en intégrant des contrôles contextuels intelligents (localisation, comportement inhabituel, etc.), des alertes dynamiques, et surtout, la prise en charge native des passkeys. Le tout vise à **réduire le facteur humain comme maillon faible** dans la chaîne de sécurité.

> Cette transition vers l'authentification sans mot de passe représente un tournant stratégique dans la gestion sécurisée des identités et des accès, simplifiant l'expérience

> utilisateur tout en renforçant la posture de cybersécurité des organisations.
>
> 
>



Sources :

- Microsoft passe au sans mot de passe par défaut pour les nouveaux comptes
- Adoption des passkeys : plus de 15 milliards de comptes en ligne peuvent les utiliser
- L'état des passkeys en 2025 : vers une adoption généralisée
- Attaques de phishing ciblant les outils Microsoft