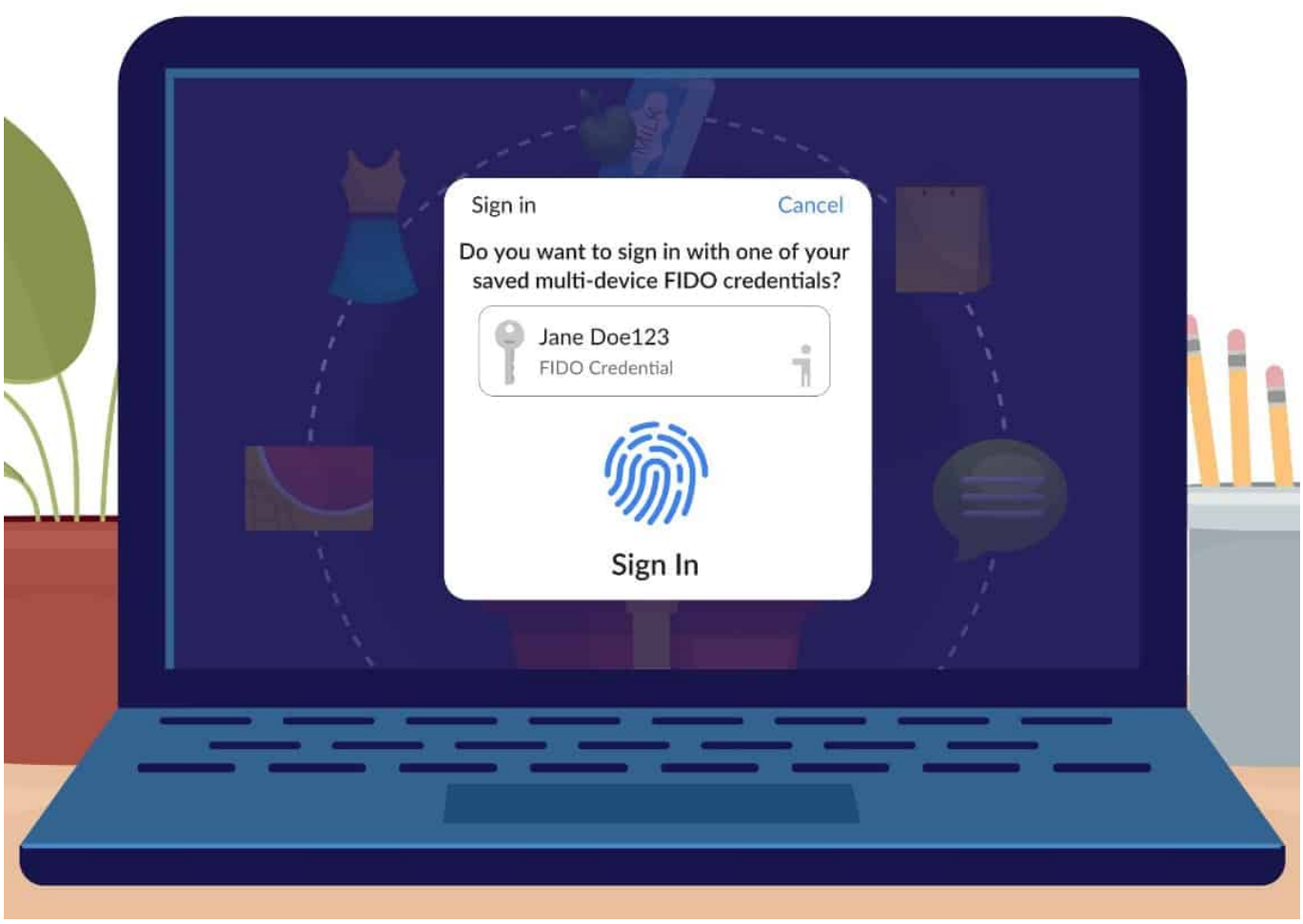
Les « clés de passe », remède universel aux mots de passe ?

Ne dites plus « mot de passe », mais « clé de passe » ? Ainsi Apple, Google et Microsoft ont-ils pris l'habitude d'appeler les identifiants FIDO multi-appareils. Ils ont réaffirmé, à l'occasion de la Journée mondiale du mot de passe, leur intention de les implémenter. Objectif : en faire une réalité à l'horizon 2023.

Les principaux systèmes d'exploitation et navigateurs web ont aujourd'hui implémenté la spécification WebAuthn. Avec elle, les terminaux informatiques peuvent devenir des dispositifs d'authentification forte sur les services compatibles. Les clés qu'ils hébergent leur sont toutefois liées : pour se connecter auxdits services avec d'autres terminaux, il faut refaire une procédure d'enregistrement ; plus contraignante et abaissant le niveau de sécurité.

Les spécifications FIDO et WebAuthn n'ont jamais interdit de synchroniser les clés. Mais dans la pratique, le mécanisme ne s'est pas mis en place. C'est précisément là-dessus que travaillent Apple, Google et Microsoft. Avec un appui précieux : une nouvelle version (« niveau 3 ») de WebAuthn. Actuellement en chantier, elle n'impose pas la synchronisation des clés, mais l'encourage. D'une part, en ouvrant la voie à d'éventuelles *guidelines* sur l'expérience utilisateur – qui se rapprocherait de celle d'un gestionnaire de mots de passe. De l'autre, en introduisant une forme d'alternative.

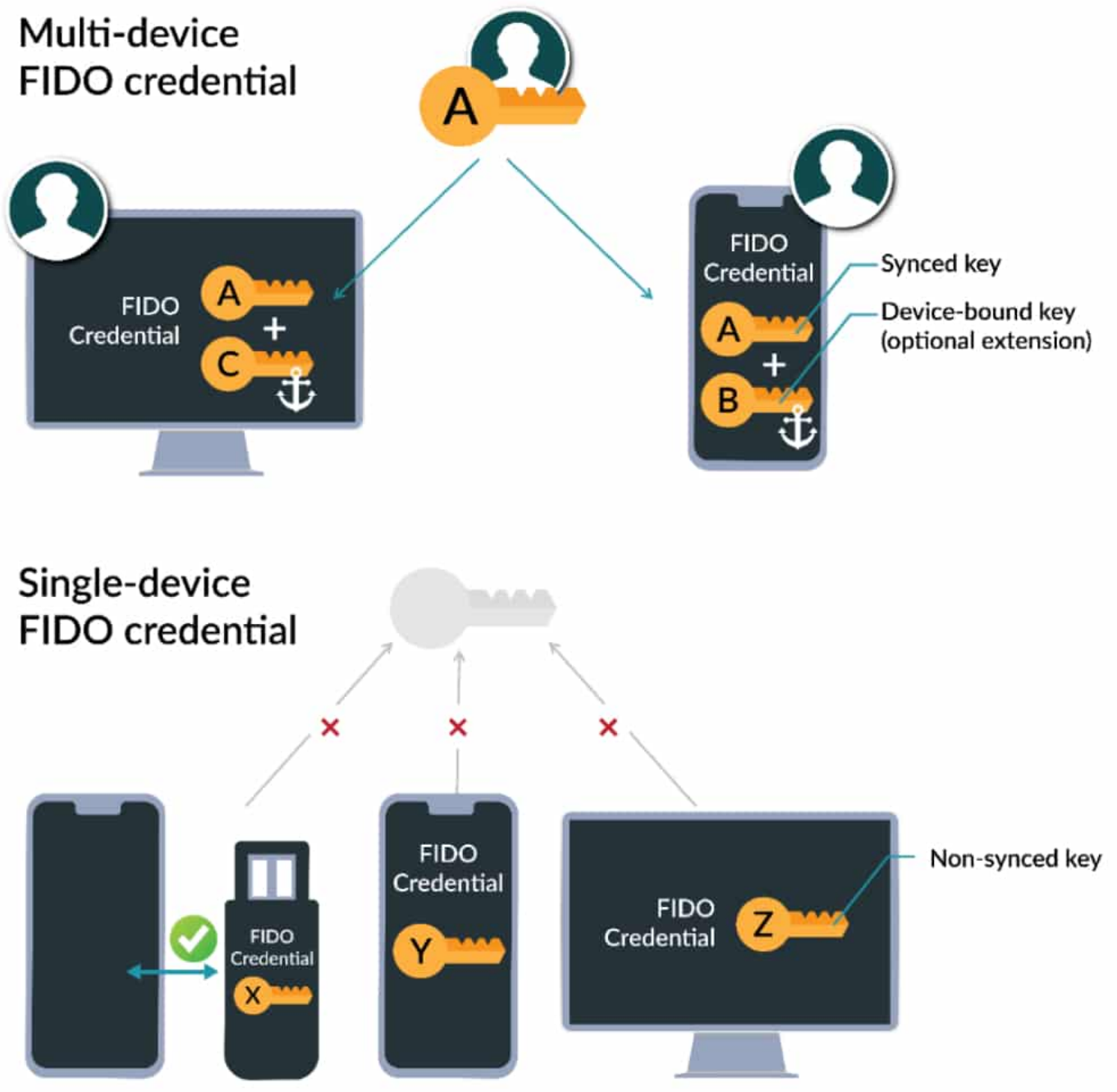


Cette alternative consisterait en une mise à jour du protocole CATP (Client to Authenticator Protocol). Que permettrait-elle ? Dans les grandes lignes, un appareil pourrait récupérer une clé de passe sur un autre, par Bluetooth. Avec une sécurité au niveau de la couche applicative. Une technique que pourraient aussi implémenter les fournisseurs de clés physiques.

Vers une option à double clé

La synchronisation des clés se fera par l'intermédiaire d'un compte (Apple, Google ou Microsoft) connecté au dispositif d'authentification. Le niveau de sécurité reposera donc sur la plate-forme.

Il est aussi question de proposer une extension pour les dispositifs d'authentification ne prenant pas en charge la synchronisation. Les sites et applications pourraient créer, sur les appareils qui s'y connectent pour la première fois, une clé qui faciliterait la réauthentification (B et C sur le schéma ci-dessous).



Le concept est actuellement expérimenté dans l'écosystème Apple, à l'appui du trousseau iCloud, à partir d'iOS 15, de macOS 15 et de Xcode 13. Côté Microsoft, on rappelle que Windows Hello peut déjà servir à s'authentifier sur les sites qui ont implémenté les clés de passe.

Illustration principale © Tiko Adobe Stock