Apple, Microsoft et Google entendent déployer ces prochains mois les « passkeys », ou « clés d'accès ». Fonctionnant avec votre smartphone, sans mot de passe à retenir, elles sont présentées comme une méthode d'authentification plus sûre. Explications.

Par Nicolas Six

Publié hier à 11h00, mis à jour hier à 11h00 · Lecture 5 min.

Les « passkeys » sont les dernières nées de l'alliance Fast Identity Online (FIDO), un consortium rassemblant les principales sociétés de la tech. NICOLAS SIX / LE MONDE

Fini, les mots de passe griffonnés sur un bout de papier ? Apple, Microsoft et Google entendent les remplacer par les « passkeys » (que l'on peut traduire par « clés d'accès »), un système en gestation depuis des années.

Les iPhone s'ouvrent aux passkeys lundi 12 septembre, à l'occasion de la sortie de leur nouveau logiciel central iOS 16, et les ordinateurs d'Apple suivront au mois d'octobre, avec l'arrivée du nouveau logiciel central Mac OS Ventura. Windows est pour sa part déjà prêt à échanger des « passkeys » avec iOS, tandis que son éditeur Microsoft affiche son intention d'ajouter prochainement toutes les fonctionnalités supplémentaires des passkeys. Quant à Google, l'entreprise souhaite *« permettre aux développeurs d'utiliser »* cette technologie sur Android d'ici à la fin de l'année 2022. L'enjeu est de taille pour les utilisateurs, les logiciels de ces trois entreprises équipant l'écrasante majorité des ordinateurs et des smartphones en circulation.

Les faiblesses du mot de passe sont désormais connues : beaucoup d'utilisateurs choisissent des mots de passe trop simples que des logiciels spécialisés parviennent à deviner, emploient les mêmes mots-clés pour de nombreux services, ou les donnent par inadvertance aux pirates en se faisant piéger par des campagnes d'hameçonnage (phishing). Les clés d'accès, que chacun va donc se voir proposer de plus en plus souvent à la place du traditionnel mot de passe lors de la création d'un compte sur un site ou une application, sont censées résoudre ces problèmes. Explications.

Lire aussi : Le mot de passe, espèce en voie de disparition

- **Comment fonctionnent les passkeys ?**

Avec les passkeys, pour s'inscrire sur un service, une application ou un site (marchand, par exemple), il vous faudra obligatoirement utiliser un appareil qui vous appartient : un smartphone, un ordinateur ou une tablette. Au moment de l'inscription, le smartphone crée alors deux clés chiffrées, uniques et spécifiques pour chaque service. D'un côté la clé privée, qui reste sur le smartphone, de l'autre, la clé publique, détenue par le site ou l'application en question.

Le service posera une sorte de devinette au smartphone, un « challenge »

Par la suite, à chaque tentative de connexion, le service posera une sorte de devinette au smartphone, un « challenge » que lui seul pourra résoudre grâce à sa clé privée. Une fois ce « challenge » résolu, pour finaliser la connexion, l'utilisateur devra ensuite marquer son approbation et prouver qu'il est bien le propriétaire du smartphone, par exemple en posant son doigt sur le lecteur d'empreintes, en présentant son visage, en tapant un code PIN ou en dessinant un schéma sur l'écran.

Une fois le compte initialisé, la clé privée rejoint un trousseau incluant toutes les passkeys créées pour chaque service utilisé, abrité dans le smartphone et, c'est l'une des grandes nouveautés, dans un espace de stockage en ligne : le Drive de Google, l'iCloud d'Apple, ou le OneDrive de Microsoft, en fonction du logiciel qui équipe l'appareil. Les passkeys seront donc accessibles à tous les appareils partageant le même écosystème, par exemple à l'iPhone, l'iPad et le Macbook d'un usager. Elles seront abritées dans un espace en ligne chiffré que personne, sauf l'usager, ne pourra ouvrir.

- **Les passkeys peuvent-elles être partagées entre Google, Microsoft, et Apple ?**

Oui. Les passkeys peuvent voyager d'un écosystème à l'autre mais, malheureusement, elles ne se synchronisent pas automatiquement entre les clouds d'Apple, Microsoft et Google. Il faut transférer chacun d'eux manuellement.

Prenons le scénario d'une personne qui s'est inscrite à un nouveau service sur son iPhone, lequel stocke désormais la passkey correspondante. Ce particulier ne peut pas se connecter au même service sur son ordinateur Windows, puisque celui-ci n'appartient pas au même écosystème : il ne peut pas réceptionner cette passkey via iCloud. D'ailleurs, il ne peut pas non plus se connecter à ce service depuis le Macbook d'un proche, même si celui-ci appartient au même écosystème, puisque cet ordinateur est

Les plus lus

1 Guerre en Ukraine, en direct : Kiev affirme avoir repris près de 6 000 km² aux forces russes ; Washington reste prudent

2 Emmanuel Macron veut relancer sa réforme des retraites coûte que coûte

3 Guerre en Ukraine, en direct : Volodymyr Zelensky annonce que l'armée ukrainienne a repris près de 6 000 kilomètres carrés aux forces russes

Édition du jour

Daté du mardi 13 septembre

celui-ci appartient au même écosystème, puisque cet ordinateur est connecté à un autre iCloud que le sien.

L'utilisateur peut scanner ce QR code avec son smartphone, dans lequel est stockée la passkey

Cependant, en ouvrant sur un de ces ordinateurs le site Internet du service, l'utilisateur se voit proposer d'afficher un QR code, qui constitue une sorte de demande de connexion. Il peut alors scanner ce QR code avec son smartphone, dans lequel est stockée la passkey. Ce smartphone vérifie automatiquement la présence de l'ordinateur à proximité, via une connexion sans fil Bluetooth, pour s'assurer que la demande ne vient pas d'un pirate opérant à distance. Il ne reste plus au particulier qu'à approuver l'authentification, comme dans la procédure décrite précédemment, par exemple en posant son doigt sur le lecteur d'empreintes.

Le scénario avec QR code sera similaire chaque fois que l'utilisateur aura besoin de se connecter avec deux écosystèmes différents, par exemple à un ordinateur Windows muni d'un téléphone Android, ou à un téléphone Android en étant muni d'un ordinateur Mac.

Par commodité, à la fin de cette procédure, beaucoup de services proposent de créer une nouvelle passkey destinée à l'ordinateur qui n'en avait pas, pour éviter de recommencer cette procédure laborieuse à chaque nouvelle connexion. Contactés par *Le Monde*, Google et Microsoft confirment par ailleurs travailler à ouvrir la gestion des passkeys à des acteurs tiers, tels les éditeurs de gestionnaires de mots de passe, comme LastPass ou Dashlane par exemple. Ceux-ci pourraient stocker les passkeys dans leur propre cloud et les rendre accessibles sous différents écosystèmes.

- **Que se passe-t-il si je perds, casse, ou que l'on me vole mon smartphone ?**

A la différence des mots de passe, les passkeys ne peuvent ni être notées sur un bout de papier, ni mémorisées dans un coin de la tête, ni regroupées dans un gestionnaire de mots de passe. Elles sont enfermées dans la mémoire chiffrée du smartphone, ce qui constitue une incitation supplémentaire à garder cet appareil sur soi en permanence.

Seule solution : réclamer de nouvelles passkeys auprès de dizaines de services client (...). Un parcours du combattant

Cela peut s'avérer gênant, par exemple lorsqu'on souhaite remplacer un smartphone Apple par un modèle Android (ou inversement). Il faut impérativement attendre avant de revendre le vieux smartphone pour pouvoir copier ses passkeys manuellement dans le nouveau

téléphone, une à une, ce qui s'annonce complexe et laborieux. La gêne peut être encore plus grande en cas de vol ou la casse du smartphone : si l'on ne possède aucun autre appareil appartenant au même écosystème que l'engin perdu, on ne pourra pas récupérer les passkeys stockées dans le cloud. Seule solution : réclamer de nouvelles passkeys auprès de dizaines de services client, en prouvant à chaque fois son identité. Un parcours du combattant.

Les choses seraient plus simples si l'on pouvait copier l'intégralité de son trousseau de passkeys d'un écosystème à l'autre. *« C'est une discussion très active en ce moment »,* reconnaît Andrew Shikiar, directeur exécutif de l'Alliance FIDO, qui coordonne cette technologie. Mais pour y parvenir, il faudra trouver une façon sécurisée d'y parvenir, explique Arnaud Jumelet, expert en sécurité chez Microsoft France :

« L'un des mécanismes-clés de la sécurité des passkeys, c'est que l'utilisateur donne son accord pour chaque transfert, clé par clé. On veut éviter qu'un virus puisse aspirer tous les passkeys d'un coup, et il ne sera pas facile de trouver une technologie qui le garantisse, tout en permettant la migration d'un trousseau entier. »

Enfin, certains services continueront malgré tout de collecter nos e-mails et nos numéros de téléphone, notamment pour pouvoir nous identifier au cas où nous perdrions nos passkeys. Selon Srinivasan Sampath, qui pilote chez Google divers projets de sécurité informatique, beaucoup de services continueront même, pendant des années, à employer des mots de passe. *« Mais plus les usagers utiliseront leurs passkeys en priorité pour s'identifier, plus les mots de passe seront réservés à des cas rares, éveillant systématiquement l'attention des gestionnaires de services. »* Ceux-ci pourront consacrer toute leur attention à ces cas particuliers.

Nicolas Six