FIDO 2
L'après mot-de-passe se met en place

Insuffisamment complexes, les mots de passe sont à l'origine d'un nombre croissant de fuites de données et, à l'heure du RGPD, l'intérêt d'une authentification forte réapparaît. Le standard Fido 2 pourrait aider à des déploiements massifs de solutions de ce type.

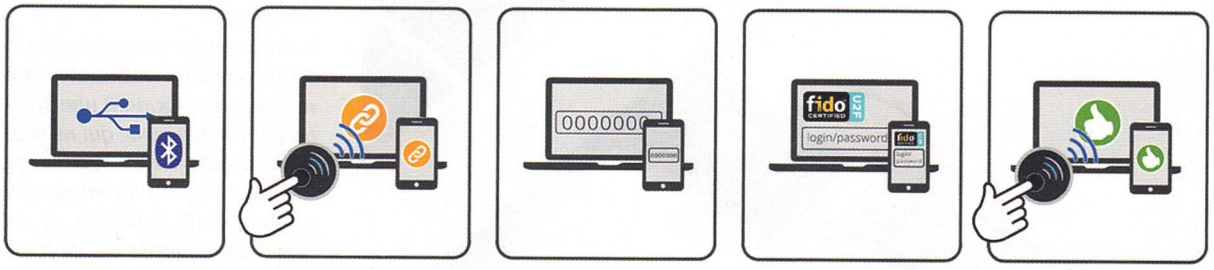
Selon l'édition 2017 du Verizon Data Breach Investigations Report (DBIR), la part des fuites de données provoquées par des vols de mots de passe a grimpé de 50 % à 81 % ces trois dernières années. Alors que les entreprises se mettent massivement au Cloud, des mots de passe trop faibles constituent de moins en moins un rempart efficace contre les hackers. Si le SSO apparaît pour de nombreux RSSI d'entreprise comme un bon moyen d'améliorer la sécurité des mots de passe tout en facilitant l'accès à ces multiples services cloud, nombreux sont ceux qui imaginent l'étape suivante, donc l'après mot de passe.

Cap d'accélérateur lors de la RSA Conference 2018

Lors de la RSA Conference 2018, Google et Microsoft ont simultanément annoncé leur intention de remplacer l'authentification par mot de passe dans leur navigateur en implémentant le standard Fido 2 – pour « Fast IDentity Online ». Jerrod Chong, vice-président en charge des produits chez Yubico, résume ce standard : *« Fido 2 comprend deux éléments : une interface de programmation web (WebAuthn) et un authentifiant (CTAP2). Les deux ont déjà commencé à être mis en place. Mozilla Firefox et Chrome ont récemment inclus la possibilité d'utiliser WebAuthn sur leurs navigateurs. De même que Microsoft, qui a annoncé permettre l'utilisation de WebAuthn sur Edge. »* D'autres éditeurs de navigateurs majeurs se sont engagés à suivre le même chemin dès la fin de l'année.

Créée en 2013, cette alliance regroupe notamment Google, Microsoft, Facebook, eBay, mais aussi Salesforce, Bank of America, Bank of China afin de formaliser les standards d'interopérabilité entre

Le process d'authentification Fido permettant d'activer le device Bluetooth OneSpan DigiPass SecureClick



Activez le Bluetooth sur votre mobile (ou) insérez le terminal SecureClick dans un port USB.

Appuyez sur le bouton du terminal SecureClick pendant 3 secondes pour l'apairer avec votre téléphone mobile.

Une fois le téléphone apairé, entrez le code 000 000. Votre terminal SecureClick est maintenant prêt à sécuriser vos identifiants.

Lorsque vous visitez un site où Fido est activé, enregistrez votre terminal SecureClick en enfoncant le bouton pendant 1 seconde.

Par la suite, pour vous authentifier sur les sites où Fido est activé, il suffit d'un appui court sur le bouton pendant 1 seconde.

« Fido 2 permettra d'abaisser les coûts »

Alain Martin, VP Strategic Partnerships, chez Gemalto, et président du Groupe de travail européen de l'Alliance Fido

« L'arrivée d'un standard permet d'abaisser les coûts et permet aux entreprises de s'affranchir de solutions propriétaires. Avec les nouvelles releases Windows et les nouvelles versions de navigateurs qui vont arriver, Fido sera supporté nativement, si bien que vous n'aurez plus besoin d'implémenter un middleware pour communiquer avec un device d'authentification forte. L'authentification forte va être de plus en plus déployée en entreprise et le monde de l'entreprise est de plus en plus sensibilisé à la protection de ses bases de données. Le middleware Fido sera préinstallé dans les environnements Windows et les navigateurs. Les entreprises n'auront plus qu'à investir dans le device lui-même, qu'il s'agisse d'une clé USB, d'une carte à puce ou le téléphone. »

solutions d'authentification fortes. Quelques jours avant cette annonce, Facebook annonçait son arrivée au board de l'Alliance, preuve de l'intérêt porté au standard par les géants du Net pour muscler la sécurité de leurs accès.

Un mouvement initié dans le B2C qui devrait entrainer les entreprises à sa suite, espère Alain Martin, VP Strategic Partnerships chez Gemalto et président du Groupe de travail européen de l'Alliance Fido : *« L'annonce de Google et Microsoft constitue une étape clé et cela va probablement favoriser l'adoption des standards Fido dans certains segments de marché, notamment dans le domaine de l'entreprise. En effet, les entreprises utilisent l'environnement Windows de Microsoft et de plus en plus le navigateur pour accéder à leurs applications. »*

L'un des avantages de Fido, c'est la démultiplication des facteurs. On trouve Fido sous forme de clés USB, de cartes à puce, intégré dans le PC dans le TPM ou dans les composants TE d'Intel, mais aussi dans les téléphones.

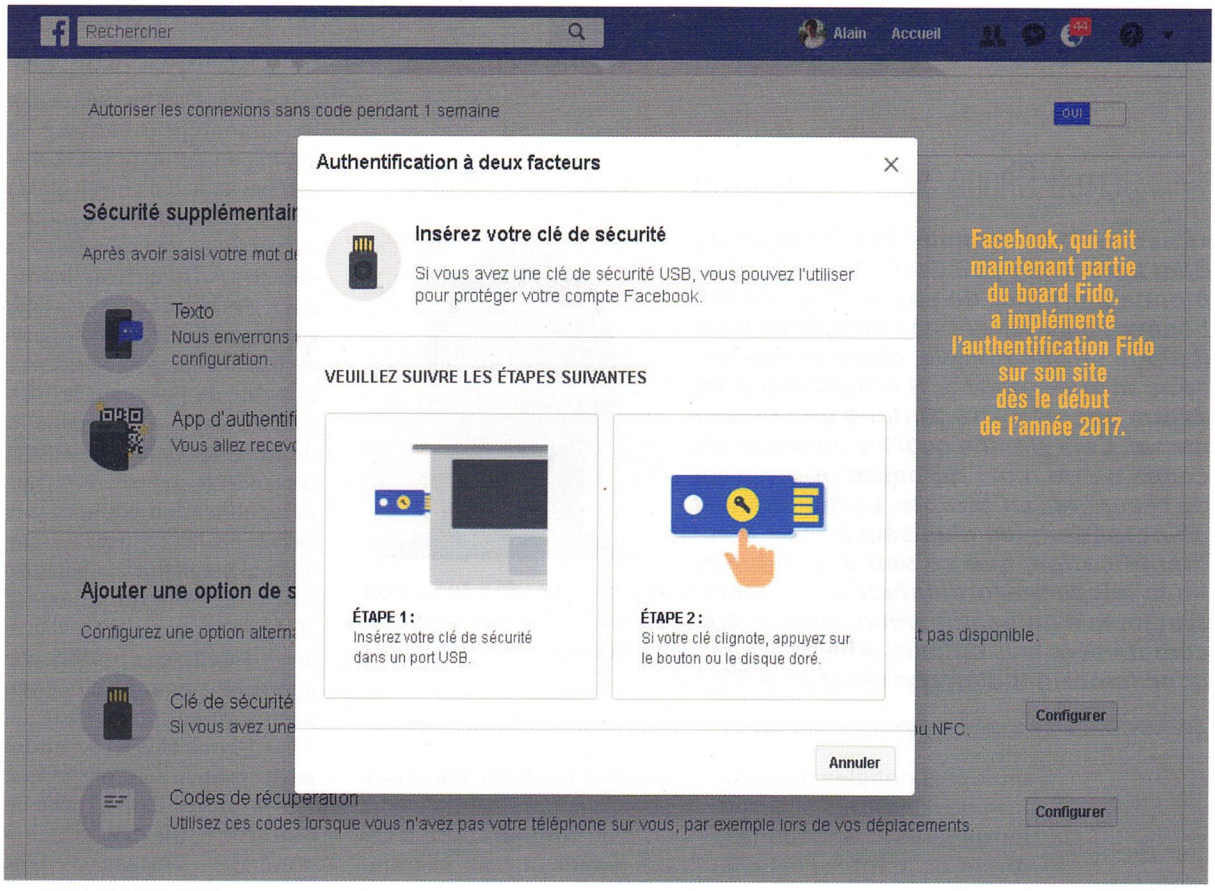
L'heure est à la certification des terminaux

Le standard Fido 2 dévoilé lors de la RSA Conference réunit les travaux de l'Alliance Fido et du W3C, et va permettre de se connecter à une page web, à Microsoft Windows au moyen d'une clé USB, un porte-clés Bluetooth ou RFID, une carte à puce, ou un smartphone.

Désormais, les spécifications et le standard ont été publiés et c'est aux éditeurs et constructeurs de devices de l'implémenter dans leurs solutions comme l'a déjà fait Microsoft dans Windows Hello, sa solution de login.

La technologie étant maintenant en place et standardisée, l'Alliance Fido va maintenant s'attacher à certifier les devices qui voudront bénéficier du sceau Fido 2. L'Alliance a défini six niveaux de sécurité.

Le niveau 1, qui correspond à une sécurité minimale. *« Ce niveau correspond à une solution 100 % logicielle qui ne sera sans doute jugée suffisante pour de nombreux sites web grand public soucieux de ne pas compliquer la vie de leurs utilisateurs »*, explique Alain Martin. *« En remplaçant le mot de passe par Fido niveau 1, elles auront déjà une solution d'accès beaucoup plus sûr qu'un mot de passe. »* L'expert estime qu'il est possible



Facebook, qui fait maintenant partie du board Fido, a implémenté l'authentification Fido sur son site dès le début de l'année 2017.

aujourd'hui de durcir la sécurité d'une solution logicielle, notamment avec la technique de whitebox cryptography. Les éditeurs pourront se targuer du niveau « 1+ » si leur solution parvient à passer des tests de pénétration.

Le niveau 2 correspond à une implémentation dans un environnement sécurisé de l'appareil, un TEE (Trusted Execution Environment), le niveau « 2+ » correspondant à des tests de pénétration plus sévères.

Enfin, les niveaux 3 et « 3+ » qui seront mis en place prochainement, imposeront la présence d'un composant hardware dédié, type carte à puce, qui accroît encore le niveau de sécurité de l'implémentation. Parmi ces modules hardware figurent bien évidemment la carte à puce, le module TPM d'Intel pour les PC et de

« Il faut adapter la sécurité au contexte »

Nicolas Petroussenko, Country Manager France d'Okta

« Il faut renforcer la sécurité par une politique de gestion des identités et des accès qui prennent en compte l'hétérogénéité de solutions et parmi les éléments importants, c'est que l'utilisateur ne doit pas avoir à se relogguer en permanence. Des contextes sont plus sécurisés que d'autres, et certains permettent de s'affranchir du mot de passe. Avec l'adaptive SSO, le système s'adapte au contexte d'utilisation et accorde l'accès en fonction d'un premier challenge, le login/mot de passe, puis un second challenge type MFA (Multi-Factor Authentication) ou rien du tout lorsque l'on est certains de l'identité de la personne qui veut se connecter.

Les start-up « Digital Natives » qui n'ont que pour seule préoccupation de faire du business adopteront vite ce type d'approche. Les très grands comptes qui s'imposent des niveaux de sécurité extrêmement élevés ne seront clairement pas des « early adopters » de ce type d'approche. »

« Beaucoup de RSSI ne savent pas encore ce dont il s'agit ! »

Jerrod Chong, vice-président Produits chez Yubico

« Chaque RSSI souhaite que les usagers dont il s'occupe puissent bénéficier d'un monde sans mot de passe. Cependant, beaucoup ne savent pas encore ce dont il s'agit ! Par exemple, dans un monde sans mot de passe, il n'existera plus aucun secret partagé dans un serveur dorsal. Cela signifie qu'il n'y aura plus de codes ou de mots de passe permettant de récupérer un compte. La solution est de posséder plus d'un seul moyen d'authentification, que ce soit une YubiKey ou le téléphone/ordinateur en lui-même. Si vous perdez tous vos systèmes d'authentification, alors le processus de récupération du compte sera très difficile. Afin de ne pas se retrouver bloqué, il est donc important d'en posséder plus d'un. »

multiples dongles de sécurité commercialisés quelques euros l'unité. Néanmoins, dotés de capteurs d'empreinte, de la reconnaissance faciale, d'une lecture d'iris sur certains modèles, les smartphones apparaissent de plus en plus comme l'outil d'accès numéro 1 pour le grand public, mais probablement aussi pour les entreprises.

Le secteur bancaire en pointe en Europe

Si aux États-Unis les Gafa seront certainement le moteur de Fido 2, en Europe c'est le secteur bancaire qui devrait être le plus actif. En effet, les banques européennes sont soumises à la directive PSD 2 qui leur impose des règles bien plus sévères pour garantir la sécurité des paiements sur Internet. Il ne sera bientôt plus possible de payer sur le Web simplement avec son numéro de carte, les banques devront demander le code secret ou une authentification biométrique. Fido 2 apparaît comme une solution qui permettra aux banques d'aller au-delà du paiement 3D-Secure et de son authentification à deux facteurs par SMS, une approche aujourd'hui décriée par les experts tant il est facile d'envoyer un SMS en se faisant passer pour un autre expéditeur. Pour le moyen terme, l'alliance Fido réfléchit désormais à d'éventuelles extensions dans la blockchain et dans l'IoT.

Alain Clapaud