

# Windows 10 : avec de la biométrie dedans !

Il y aura bien de la biométrie dans le futur OS de Redmond, Windows 10. Lors du sommet sur la cybersécurité organisé en fin de semaine dernière par la Maison Blanche, Microsoft a annoncé avoir rejoint [l'alliance FIDO](#) (Fast Identity Online), qui vise à changer le mode d'authentification online. Autrement dit, à **renvoyer le couple login / mot de passe aux oubliettes**. Après une première mouture de sa norme éponyme, livrée en décembre dernier, ce consortium travaille aujourd'hui à [sa version 2.0](#). Celle-ci met en œuvre deux protocoles : *l'Universal Authentication Framework* (UAF) et *l'Universal Second Factor* (USF).

Permettant l'authentification biométrique à travers des dispositifs comme le lecteur d'empreinte digitales, la reconnaissance vocale et l'analyse rétinienne, l'UAF se présente comme un substitut au mot de passe. A l'inverse, l'USF constitue un simple complément basé sur un élément physique (clé USB, appareil connecté en NFC), visant à mettre en place une authentification multi-facteur...

## Se connecter à Azure ou Office 365

Windows 10 sera **compatible avec ces différents protocoles** destinés à rendre l'authentification plus sécurisée qu'à l'heure actuelle, en insistant sur la dimension d'interopérabilité. La **préversion de l'OS** (« Technical Preview ») permet déjà de **tester le standard FIDO 2.0** pour l'ouverture de sessions, la connexion à Azure Active Directory et l'accès à des applications SaaS comme Office 365 Exchange Online, Salesforce, Citrix, Box et Concur.

Autre contributeur majeur de l'alliance FIDO, Google avait mis la norme en œuvre début 2013 à travers la clé USB [Yubikey](#), avec l'ambition d'appliquer cette technologie à des objets du quotidien comme les montres, les bracelets et les bagues, [rappellent nos confrères d'ITespresso](#).

Un an plus tard, Google mettait la main sur la start-up israélienne [SlickLogin](#), qui s'était fait connaître pour son système d'authentification basé sur le transfert de clés sécurisées par ultrasons entre un PC et un smartphone. La solution est conçue pour s'intégrer dans toute application – ou dans une page Web – en ajoutant quelques lignes de code.

**A lire aussi :**

[La biométrie vient au renfort de la sécurisation des mobiles](#)

**Crédit photo : ra2studio / Shutterstock**