Windows 10 : Microsoft va généraliser l'authentification à deux facteurs

C'est un service pour l'instant passé relativement inaperçu dans les premières versions de Windows 10. Tout simplement parce qu'il est, pour l'heure, inactif. Mais **Next Generation Credentials** pourrait bien être à l'origine du principal changement d'usage pour les utilisateurs de Windows. Ce service permettra en effet au possesseur d'un terminal sous Windows 10 d'**enrôler ce terminal dans des mécanismes d'authentification à deux facteurs**, en complément d'un code alphanumérique (PIN) ou d'un facteur biométrique.

La volonté de Microsoft ? « *S'éloigner d'un monde dominé par les authentifications mono-facteur, comme les mots de passe* », écrit l'éditeur dans un billet de blog. Et d'ajouter : « *Nous pensons que cette solution amène la protection d'identité à un niveau supérieur, car elle intègre l'authentification multi-facteur, aujourd'hui limitée à des systèmes comme les smartcard, au cœur du système d'exploitation, éliminant le recours à des périphériques supplémentaires dédiés à la sécurité* ».

Un conteneur dédié et sécurisé

Basé sur un **standard établi par la FIDO Alliance** (où on retrouve Google, PayPal, Visa, Mastercard ou encore RSA), la fonction protège l'utilisateur d'un vol du code (PIN), ou de sa récupération dans une base de données exfiltrée par des pirates, ainsi que d'un vol de terminal. Un seul des deux facteurs d'identification étant, par définition, insuffisant pour accéder à un service protégé par Next Generation Credentials.

Selon Microsoft, les utilisateurs pourront transformer un ou tous leurs terminaux en coffre-fort renfermant leur(s) identité(s). **Un téléphone mobile pourra ainsi centraliser les identités**, et les déployer sur d'autres machines via le WiFi ou le Bluetooth, pour gérer les accès à ces autres terminaux ou à un service distant depuis ces autres appareils. La **paire de clefs cryptographiques** sera fournie soit par **Windows 10, soit par un service de PKI existant**. Les tokens des utilisateurs seront stockés dans un conteneur sécurisé, fonctionnant sur la technologie Hyper-V, afin d'éliminer les risques d'attaques de type Pass The Hash ou Pass the Ticket. « *Cette solution permet d'éviter que les tokens ne soient récupérés même quand le noyau Windows lui-même est compromis* », assure Redmond. Bien entendu, Active Directory (sur site ou sur Azure) ainsi que Microsoft Accounts supporteront cette fonctionnalité, afin de favoriser son adoption.

A lire aussi :
Google sécurise physiquement les comptes, Facebook compare les identifiants piratés
Dix questions pour tout savoir de Windows 10