L'avenir de l'authentification forte

L'authentification à deux facteurs constitue un impératif de sécurité – mais les solutions traditionnelles sont «compliquées» pour l'utilisateur. Avec Vasco DIGIPASS SecureClick, l'accès sécurisé aux services Web se fait désormais en appuyant sur un seul bouton.

L'accès sécurisé aux applications Web publiques et internes aux entreprises requiert une authentification forte des utilisateurs impliquant au moins deux dispositifs de sécurité sur différents canaux. On connaît par exemple la procédure mTAN dans le domaine de l'e-banking: un code de sécurité supplémentaire est envoyé par SMS sur le téléphone mobile.

Ces solutions d'authentification à deux facteurs sont sûres, mais offrent peu de confort d'utilisation: chaque accès nécessite un mot de passe distinct – et par mesure de précaution, il convient de ne pas utiliser le même partout et de ne pas garder les mots de passe par écrit. Quant au deuxième facteur de sécurité, un code doit être reçu sur un appareil séparé, puis saisi manuellement dans l'application cible. De plus, généralement, il s'agit de solutions propriétaires qui doivent être intégrées individuellement dans les applications.

DIGIPASS SecureClick de VASCO communique sans fil via Bluetooth Low Energy (BLE) avec n'importe quel périphérique compatible BLE et permet une authentification forte en un seul clic.

Un standard pour une authentification à deux facteurs plus confortable

Dans le but de créer un standard pour une authentification à deux facteurs utilisable de façon universelle, Google a développé, avec des partenaires, la spécification U2F (Universal Second Factor). Alliant niveau de sécurité élevé, confort d'utilisation et accessibilité immédiate, U2F sert à attester l'autorisation d'accès pour un nombre infini de services basés sur le Web. Une seconde spécification, intitulée UAF (Universal Authentication Framework), décrit le protocole de réseau pour l'authentification sans mot de passe.

Ensemble, ces deux spécifications constituent le standard FIDO, adopté en décembre 2014 dans sa version 1.0 et développé depuis par l'alliance industrielle FIDO (Fast IDentity Online). Les services Web conformes au standard FIDO évitent aux utilisateurs de devoir mémoriser d'innombrables mots de passe compliqués. Pour l'accès sécurisé et immédiat à un service Web, FIDO utilise une paire de clés générée lors de l'enregistrement, la clé privée étant sauvegardée de manière cryptée sur l'appareil de l'utilisateur et libérée à chaque connexion à l'aide d'un jeton de sécurité (token) ou d'un procédé biométrique.

Actuellement, la plupart des services de Google ainsi que Dropbox, GitHub, OpenSSH et Wordpress sont compatibles avec U2F, et les solutions basées sur FIDO sont faciles à intégrer dans les applications d'entreprises.

Accès en un seul clic

Dans leur première génération, les jetons de sécurité conformes au standard FIDO se présentaient sous la forme de dongles USB, adaptés surtout aux ordinateurs de bureau et ordinateurs portables. Avec DIGIPASS SecureClick, Vasco présente désormais une génération moderne qui communique sans fil et en mode crypté, via Bluetooth Low Energy (BLE), avec un ordinateur, une tablette ou un smartphone. DIGIPASS SecureClick fonctionne instantanément avec n'importe quel périphérique compatible BLE: pour s'authentifier, il suffit de saisir un mot de passe identique pour tous les services, puis de cliquer sur le bouton «Go».

D'un diamètre de 25 mm et d'une épaisseur de 3,9 mm seulement, le jeton circulaire se présente sous la forme d'un porte-clés élégant. A raison de 10 utilisations par jour, la pile CR2012 (remplaçable) a une durée de vie de plus de deux ans. Selon les applications spécifiques aux clients, le jeton peut être personnalisé avec le logo et les couleurs de l'entreprise. Pour les appareils non compatibles BLE, Vasco propose un dongle USB avec fonction SecureClick.

VASCO

Vasco compte parmi les leaders mondiaux de l'authentification, de la signature numérique et de la gestion d'identité et fournit quotidiennement plus de 100 000 jetons de sécurité. Le public connaît surtout les solutions de Vasco utilisées dans l'e-banking, par exemple CrontoSign: un cryptogramme graphique à points colorés est scanné avec la caméra du smartphone afin de générer un mot de passe unique. Le célèbre lecteur de carte PostFinance de couleur jaune a également été créé par Vasco.

Les points forts de Vasco DIGIPASS SecureClick

- Authentification forte en un seul clic
- Accès immédiat
- Un seul mot de passe pour tous les services Web pris en charge
- Dispositif BLE conforme au standard FIDO
- Dongle BLE fourni pour les PC plus anciens
- Durée de vie de la pile (remplaçable): deux ans
- En forme de porte-clés élégant

BOLL
IT Security Distribution

BOLL ENGINEERING SA

En Budron H15,
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60
contact@boll.ch
www.boll.ch