Token

Série BioStick

Prévenir le hameçonnage et le rançongiciel avec le meilleur biométrique AMF

Protection proactive contre le hameçonnage

Conforme FIDO et résistante au hameçonnage AMF, éliminant les failles humaines et les secrets partagés pouvant être exploités.

Vérification biométrique de l'identité

Même en cas de perte ou de vol, la vérification biométrique garantit que seul l'utilisateur enregistré peut accéder et utiliser les identifiants numériques.

Sécurité par proximité

L'authentification n'est possible que lorsqu'on se trouve physiquement près de l'appareil. La AMF locale supprime le risque d'attaques à distance sur l'identité.

Liaison au domaine

La liaison cryptographique au domaine garantit l'authentification uniquement sur des services légitimes. Les sites de phishing ne peuvent plus voler vos accès.

L'avenir de l'authentification d'entreprise est sans mot de passe

Toutes les organisations ont besoin d'une connexion sécurisée et sans mot de passe, garantissant à la fois un haut niveau de sécurité et une expérience utilisateur optimale. L'élimination des mots de passe est le moyen le plus efficace de prévenir le vol d'identité, le hameçonnage et l'ingénierie sociale; qui restent les principaux vecteurs d'attaque dans les attaques réussies de rançongiciel et les violations de données. Token fournit le meilleur, le plus sûr et le plus pratique biométrique AMF.

Allez au-delà des méthodes obsolètes de MFA

Les solutions MFA de nouvelle génération corrigent les faiblesses des méthodes d'authentification traditionnelles : notamment la vulnérabilité face au hameçonnage, des attaques de l'homme au milieu, l'usurpation de carte SIM, et s'appuyant sur les utilisateurs pour reconnaître les menaces sophistiquées.

L'ancien MFA est un problème pour les utilisateurs, mais le BioStick offre un simple et expérience de connexion sans mot de passe en supprimant plusieurs étapes interactives avec un balayage rapide des empreintes digitales. Token offre une solution biométrique sécurisée, évolutive et résistante au hameçonnage, alliant tous les avantages des clés de sécurité matérielles à la souplesse de la gestion logicielle.

Contrairement aux clés matérielles 2FA classiques, le BioStick ne peut être utilisé que par son propriétaire, garantissant une vérification biométrique de l'identité à chaque connexion.

Points forts du BioStick

- Vérification biométrique de l'identité de l'utilisateur
- FIDO2/WebAuthn et FIDO U2F conformes
- Pratique FIDO authentification via Bluetooth, NFC et USB
- Micrologiciel évolutif
- Élément sécurisé résistant à l'altération pour un stockage fiable des identifiants numériques
- Compatible avec Windows, MacOS, Android et iOS*

* La disponibilité de la connectivité hors USB dépend de la compatibilité de la plateforme.

FONCTIONNALITÉS DU TOKEN BIOSTICK

Le plus haut niveau de sécurité et de facilité d'utilisation

Token BioSticks offre non seulement biométrique, conforme FIDO, résistant au phishing AMF, mais aussi une grande expérience utilisateur. La sécurité et la commodité sont rarement combinées, mais le Token BioStick Plus offre flexibilité et commodité car il peut être utilisé sur plusieurs plates-formes via Bluetooth entièrement crypté communications. Les utilisateurs n'ont plus besoin de brancher leur clé de sécurité matérielle et de voler un port USB pour l'authentification : un simple balayage par empreinte digitale permet à FIDO d'accéder en moins de cinq secondes. Sa facilité d'utilisation encourage l'adoption par les utilisateurs, renforçant ainsi la sécurité globale de l'entreprise.

Comparaison du risque de méthode d'authentification

Vecteurs d'attaque	Mot de passe	Code OTP	Applications AMF et Auth héritées	Clé d'accès	Token Ring or Token BioStick
Hameçonnage	X Facile	X Facile	X Facile	√ Non	√ Non
Compromission à distance	X Facile	X Facile	X Facile	! Possible	√ Non
Falsification de site web	X Facile	X Facile	X Facile	√ Non	√ Non
Dispositif volé	! Peut-être	! Peut-être	X Oui	! Possible	√ Non compatible
Piratage de compte cloud	N/A	N/A	X Oui	X Oui	√ Aucune utilisation du cloud
Tamperation possible	X Facile	X Oui	X Oui	X Oui	√ Peu probable (grâce à l'élément sécurisé)
Coercion de l'utilisateur	X Facile	X Oui	X Oui	X Oui	! Physique en personne uniquement (par exemple avec une arme à feu)

Cas d'usage en authentification : SSO et clés d'accès

Une façon courante de mettre en œuvre l'authentification FIDO sans mot de passe et les clés de sécurité matérielle est de protéger les instances existantes d'authentification unique (SSO) ou d'authentification basée sur le fournisseur d'identité.

La centralisation des systèmes SSO et IDP a nettement amélioré l'expérience utilisateur, tout en rendant essentiel pour les organisations de sécuriser l'accès à ces plateformes contre toute intrusion non autorisée. Gérer les accès et les autorisations, en particulier les accès privilégiés, ainsi que le cycle de vie des identités, tout en garantissant à la fois la sécurité et la simplicité d'utilisation, demeure un défi bien connu des équipes de sécurité. L'adoption de la norme FIDO et de clés de sécurité matérielles représente une solution idéale, longtemps recherchée par les experts. Elle offre le niveau de sécurité le plus élevé, une authentification résistante au hameçonnage et sans mot de passe, tout en garantissant une expérience fluide et intuitive pour les utilisateurs.

De plus, une gamme croissante de produits et de services d'entreprise prend désormais en charge nativement les clés FIDO clé d'accès pour l'authentification directe entre l'utilisateur final et le service de confiance. Les utilisateurs de produits de sécurité matériels de jeton ont la flexibilité de choisir la méthode la plus appropriée, ou de combiner les deux, pour s'aligner avec les besoins de leur organisation.

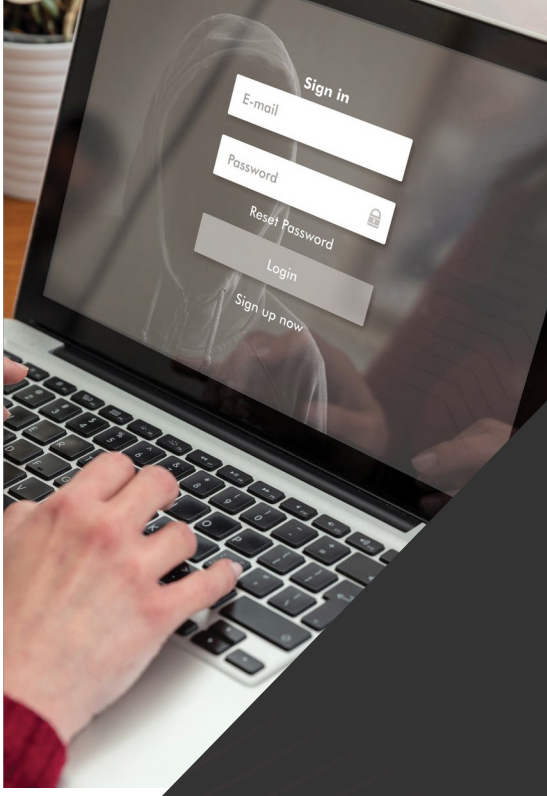
Sécurité proactive

Ces dernières années, il y a eu un changement important parmi les chercheurs et les professionnels de la sécurité. Les organisations ne doivent plus se fier à une approche de sécurité réactive; elles doivent se concentrer sur des contrôles de sécurité préventifs et à l'épreuve de l'avenir.

La prévention des menaces d'identité a été particulièrement critique et primordiale, le souci étant clairement validé dans les rapports et tendances de 2025. Abus de titres de compétences a vu une augmentation constante d'année en année comme le vecteur d'attaque le plus commun, encourageant le sentiment "Les hackers ne s'infiltrent pas, ils se connectent".

Les méthodes utilisées pour voler des informations d'identification ne sont pas sophistiquées, pourtant, elles restent efficaces en raison des vulnérabilités humaines inévitables liées à l'accès et à l'authentification. Grâce à l'IA générative, les attaquants créent désormais facilement des emails d'hameçonnage sophistiqués et des sites frauduleux impeccables pour inciter les utilisateurs à divulguer leurs mots de passe et codes MFA traditionnels. Combinez cela avec l'ingénierie sociale, Attaque de l'intercepteur, l'usurpation de carte SIM, Attaque par fatigue d'AMF, et l'augmentation de 84% des logiciels malveillants Infostealer, et ce n'est pas une surprise la prévention des menaces liées à l'identité fait les gros titres.

Les produits Token peuvent améliorer la sécurité proactive des organisations et de leurs utilisateurs. Fournir une authentification sécurisée, biométrique, certifiée FIDO, requise en 2025 et au-delà.



Le coût moyen d'une violation de données a atteint un niveau record de

$4,88 millions

en 2024[1]. IBM

SPÉCIFICATIONS TECHNIQUES ET OPTIONS DU TOKEN BIOSTICK

	 **Token BioStick**	 **Token BioStick Plus**
USB-C	✓	✓
Bluetooth		✓
NFC		✓
Identification biométrique de l'utilisateur	✓	✓
Conforme à la norme FIDO2	✓	✓
FIDOU2F	✓	✓
Micrologiciel évolutif	✓	✓

Deux modèles. Un sans couture Expérience utilisateur.

Les deux modèles de la gamme Token BioStick sont entièrement évolutifs sur site, fonctionnent sans accroc avec les mêmes applications et la plateforme logicielle Token, et offrent une expérience utilisateur homogène. Ainsi, quel que soit le modèle Token BioStick choisi, les utilisateurs et les entreprises profitent des mêmes fonctionnalités innovantes et d'une grande simplicité d'utilisation.

La distinction principale entre les modèles réside dans leurs options de connectivité. La version standard du Token BioStick propose uniquement une connexion USB, tandis que le Token BioStick Plus intègre le Bluetooth et la technologie NFC. De plus, le modèle Plus est équipé d'une batterie interne rechargeable, offrant une utilisation complète même sans branchement sur un port USB.

Caractéristiques techniques

- Recharge via connexion USB-C 5V
- Température de fonctionnement : de 0°C à 60°C (32°F à 140°F)
- Temps de charge : environ 2 heures
- Élément sécurisé résistant aux altérations, compatible jusqu'à 100 clés ou identifiants uniques
- Capteur d'empreintes digitales capacitif 508 DPI
- BLE 5.4
- Autonomie de la batterie : jusqu'à une semaine entre deux charges
- Prêt à l'emploi : fonctionne dès qu'il est branché, quel que soit le niveau de batterie

La mise en place des clés de sécurité FIDO a permis d'obtenir **zéro compromission de compte, des connexions quatre fois plus rapides**, une **réduction de 92 % des appels au support informatique**, et une **réduction de 95 % des réinitialisations de mot de passe.** [2]

Diminution des besoins en support informatique

Les solutions matérielles Token répondent aux besoins IT des entreprises de deux façons distinctes :

1. Les Token BioSticks bloquent les ransomwares et les fuites de données dues à des méthodes d'authentification insuffisantes, y compris les anciens systèmes de MFA.
2. Les clés Token BioStick réduisent considérablement le nombre de réinitialisations de mots de passe, une demande fréquente auprès du support IT.

Des études menées par Google, Hyper et d'autres ont prouvé que l'adoption des clés de sécurité FIDO a permis d'éliminer les compromissions de comptes, d'accélérer les connexions par quatre, de réduire de 92 % les appels au support informatique et de diminuer de 95 % les réinitialisations de mots de passe.[2]

Conçue pour un déploiement à grande échelle

Les organisations peuvent gérer leurs clés de sécurité matérielles Token via la Console Token Authenticator. Cette plateforme facilite la gestion des clés, la commande, l'expédition et la gestion des retours. Les administrateurs bénéficient d'une visibilité complète sur l'attribution des équipements, le suivi des statuts, la consultation des journaux et la personnalisation du matériel Token pour des groupes spécifiques, tout en maintenant la sécurité des authentifications biométriques et des clés privées.

Services professionnels

Token propose une gamme complète de services professionnels pour accompagner les entreprises dans l'intégration des clés de sécurité FIDO Token, notamment :

- Configuration de l'IDP
- Intégration dans les écosystèmes existants
- Formation sur les produits Token
- Assistance à la configuration et à l'enregistrement des utilisateurs finaux

Nous savons qu'il est essentiel de protéger les ressources et identités sensibles de votre organisation grâce à une authentification résistante au phishing. Nos ingénieurs spécialisés sont prêts à vous accompagner, quelle que soit la solution dont votre organisation a b

1.
2. https://fidoalliance.org/ https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index

À propos de Token

Dans un monde où les identités sont usurpées et les accès compromis, Token révolutionne la sécurité des organisations en proposant une authentification biométrique multifactorielle, sans mot de passe et conforme à FIDO2. Pour en savoir plus, rendez-vous sur **www.tokenring.com**.