Token

Résumé du produit

Token Ring

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 AMF

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 Token Ring 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 de sécurité 2FA classiques, une Token Ring n'est utilisable que par son propriétaire, garantissant une vérification biométrique hautement sécurisée à chaque connexion.

Points forts du Token Ring

- 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*

tokenring.com

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

FONCTIONNALITÉS DE TOKEN RING

MFA biométrique d'exception à porter au doigt

Token Ring propose une authentification biométrique multifactorielle conforme FIDO et résistante au hameçonnage, le tout dans un format unique à porter. Le Token Ring offre flexibilité et commodité car il peut être utilisé sur plusieurs plates-formes via des communications NFC et Bluetooth entièrement cryptées. Le facteur de forme portable est toujours accessible à l'utilisateur, favorisant une utilisation continue et une meilleure conformité, améliorant la sécurité de l'ensemble de l'organisation.

Comparaison du risque de méthode d'authentification

Vecteurs d'attaque	Mot de passe	Code OTP	Applications AMF & Auth héritées	Clé d'accès	Token Ring ou 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	√ Aucun cloud utilisé
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.

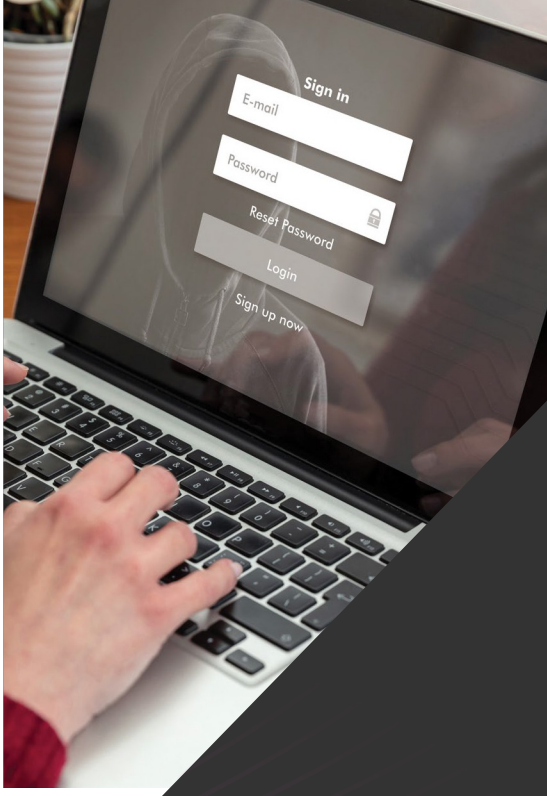
De plus, une gamme croissante de produits et de services d'entreprise prend désormais en charge nativement les clés FIDO clé d'accès pour l'authentification directe entre l'utilisateur final et le service de confiance. Les utilisateurs de produits de sécurité matériels de jeton ont la flexibilité de 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

CARACTÉRISTIQUES TECHNIQUES DE TOKEN RING

Compatibilité avec les appareils et systèmes d'exploitation

- Mobile via NFC
  - iOS
  - Android
- Ordinateur via Bluetooth et NFC
  - Windows
  - MacOS

Capteur d'empreintes digitales

- Tactile capacitif 508 dpi
- 5,45 mm x 6,10 mm
- Résolution en niveaux de gris 8 bits

Voyant LED

- Indicateur d'état multicolore

Bord tactile capacitif

- Détecte les gestes de tapotement des utilisateurs
- Vérification de l'intention et de la présence de l'utilisateur

Élément sécurisé

- Crée et conserve les identifiants FIDO
- Certifié EAL5+. Stockage inviolable
- pour 100 clés

Bluetooth

- BLE 5.4
- Crypté
- Tactile activé

NFC

- Crypté
- Activation par contact

Batterie

- 5 à 7 jours selon l'utilisation
- Recharge complète en 90 minutes
- Charge de secours : 5 minutes

Chargeur

- USB C, 5 volts
- Câble de chargement inclus

Format : bague

- Tailles disponibles : 8 à 12
- Poids : 2 à 5 grammes

Résistance à l'eau

- Certification IP67

Température de fonctionnement

- 0° à 60° C

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

Diminution des besoins en support informatique

Les produits matériels Token sont conçus pour répondre aux exigences IT des entreprises de deux façons distinctes :

1. Token Ring bloque les attaques par ransomware et les fuites de données dues à des méthodes d'authentification insuffisantes, y compris les anciennes solutions MFA.
2. Les authentificateurs Token Ring réduisent considérablement le nombre de réinitialisations de mot de passe, une demande fréquente de support informatique.

Des études menées par Google, Hyper et d'autres ont montré que l'utilisation de clés de sécurité FIDO permet d'éliminer les risques de piratage de comptes, d'accélérer les connexions par quatre, de réduire les appels au support informatique de 92 % et de diminuer les réinitialisations de mots de passe de 95 %.[2]

Conçu pour un déploiement à grande échelle

Les organisations peuvent gérer leurs clés de sécurité Token grâce à la console Token Authenticator. Celle-ci facilite la gestion des clés, les commandes, les expéditions et les retours. Les administrateurs disposent d'un contrôle complet sur l'attribution du matériel, le suivi de l'état, les journaux d'activité et la personnalisation des équipements Token pour des groupes spécifiques, tout en garantissant la sécurité de l'authentification biométrique et des clés privées.

Services professionnels

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

- Configuration IDP
- Intégration dans les écosystèmes existants
- Formation sur les produits Token
- Installation et enregistrement des utilisateurs finaux

Nous savons à quel point il est crucial de protéger les ressources et identités sensibles de votre organisation grâce à une authentification résistante au phishing. Nos ingénieurs spécialisés sont présents pour vous accompagner selon les besoins spécifiques de votre entreprise.

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

À propos de Token

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