Kensington®

VeriMark™ Empreinte et Clés de Sécurité

Votre partenaire de confiance en authentification multi-facteurs et cybersécurité

Accès Sécurisé Sans Tracas

Les clés d'empreinte et les clés de sécurité NFC transforment la façon dont nous protégeons notre monde numérique. Les clés d'empreinte offrent une authentification rapide, fiable et sans mot de passe en utilisant des données biométriques uniques, rendant l'accès non autorisé presque impossible. Les clés de sécurité NFC ajoutent une couche supplémentaire de commodité et de flexibilité, surtout pour les personnes qui utilisent à la fois des PC et des appareils mobiles. Elles sont simples à utiliser et sont souvent plus économiques que les options biométriques. Ensemble, ces outils offrent une protection multi-facteurs solide, facile à utiliser, hautement sécurisée et conçue pour garder les informations sensibles en sécurité sans vous ralentir.

Questions Principales

- Quel est le **principal objectif** du cas d'utilisation?
- Quels appareils ou **navigateurs** doivent être pris en charge?
- Est-ce que **Windows Hello** ou **Windows Hello pour les Entreprises** ou l'authentification web est utilisée?
- Les utilisateurs accèdent-ils à **un** ou **plusieurs** appareils?
- Plusieurs **utilisateurs** accéderont-ils au **même appareil** à différents moments de la journée?
- Quels **services** sont utilisés?

Tendances de L'Industrie et Perspectives de Recherche

État Actuel de la Sécurité des Appareils

Kensington a sponsorisé une étude, menée par le spécialiste indépendant de la recherche de marché Vanson Bourne, auprès de 1 000 décideurs informatiques seniors responsables de la sécurité matérielle physique de leur organisation. Une des principales conclusions était que l'accès non autorisé aux données de l'entreprise sur les appareils est la principale préoccupation pour 43 % des répondants, suivie de 19 % qui s'inquiètent de la perte de données sensibles en raison de réseaux domestiques non sécurisés. Les organisations se tournent de plus en plus vers l'authentification multi-facteurs (MFA) comme première défense, 30 % des répondants identifiant l'authentification biométrique ou multi-facteurs comme essentielle pour atténuer les menaces à la sécurité.

Adoption de L'Authentification Biométrique

Un nombre croissant d'organisations reconnaissent la valeur des solutions de sécurité biométrique. Selon notre étude de marché, 71 % des organisations interrogées utilisent actuellement des empreintes digitales et/ou des clés de sécurité pour l'authentification à deux facteurs (2FA), tandis qu'un autre 26 % prévoient de mettre en œuvre ces mesures dans un avenir proche. La gamme VeriMark™ de Kensington illustre la sécurité biométrique à la pointe de la technologie, alliant la commodité sans mot de passe à une protection de niveau entreprise. En tant que leader dans la sécurisation du lieu de travail moderne, Kensington propose des solutions conformes à la TAA et au RGPD qui s'intègrent dans les infrastructures existantes, permettant aux organisations de faire face efficacement aux menaces évolutives en matière de cybersécurité.

Source : Vanson Bourne, Recherche sur la sécurité des appareils, octobre-novembre 2024

Sécurité et Commodité Améliorées avec VeriMark™ IT 2.0 et VeriMark™ Desktop 2.0

Les clés biométriques comme VeriMark™ IT 2.0 et VeriMark™ Desktop 2.0 s'intègrent parfaitement à Windows Hello pour offrir une sécurité améliorée et un accès rapide et pratique. Entièrement conformes aux exigences de sécurité de connexion améliorée (ESS) de Microsoft, elles combinent une reconnaissance avancée des empreintes digitales avec les dernières normes d'authentification Windows. VeriMark™ IT 2.0 et Desktop 2.0 garantissent des connexions sécurisées, le chiffrement et la protection en ligne, idéales pour protéger des données sensibles tout en simplifiant l'accès par une simple touche, ce qui en fait un choix parfait pour les professionnels modernes et les environnements informatiques.

Authentification Forte

L'authentification biométrique utilise l'empreinte digitale qui est unique à chaque utilisateur, ce qui en fait une méthode d'authentification très sécurisée.

Faible Risque D'oubli ou de Perte

Contrairement aux mots de passe, les utilisateurs ne peuvent pas oublier ou perdre leurs données biométriques.

Accès Rapide et Pratique

Authentifiez-vous en quelques secondes avec juste une touche—pas de saisie, pas de tracas.

Élever la Sécurité Web avec VeriMark™ Guard 2.1 via MFA

Les empreintes digitales et les clés de sécurité telles que VeriMark™ Guard 2.1 sont idéales pour l'authentification multi-facteurs (MFA) lors de l'accès à des services Web nécessitant une protection renforcée. En tant que solution certifiée FIDO®, elle combine la vérification biométrique ou l'entrée de code PIN avec une authentification basée sur le matériel pour offrir une sécurité forte, résistante à l'hameçonnage. Parfait pour les plateformes financières, les applications d'entreprise ou les comptes cloud sensibles, VeriMark™ Guard 2.1 offre une protection robuste contre le vol d'identifiants tout en maintenant une expérience utilisateur rapide et fluide.

Extrêmement Sécurisé

Les clés de sécurité utilisent une authentification cryptographique forte qui est extrêmement difficile à dupliquer ou à manipuler, les rendant résistantes aux attaques d'hameçonnage et d'ingénierie sociale. En tant que dispositifs certifiés FIDO2, U2F et CTAP2.1, elles soutiennent des normes de sécurité modernes basées sur le matériel qui aident les organisations à respecter des exigences réglementaires strictes telles que HIPAA et PCI DSS.

Facile à Utiliser

Les clés de sécurité sont simples à utiliser et nécessitent un minimum de configuration, ce qui en fait une option pratique pour les utilisateurs.

Accédez à une Sécurité de Niveau Entreprise sans Mots de Passe

La clé de sécurité VeriMark™ NFC+ offre un moyen simple mais puissant de sécuriser l'accès sur plusieurs appareils. Elles combinent la commodité sans fil avec un chiffrement robuste, permettant aux utilisateurs de s'authentifier en tapotant simplement la clé lorsqu'elle est insérée, ou en la tapotant contre un lecteur NFC. Ces clés éliminent le besoin d'enrôlement biométrique, ce qui les rend parfaites pour les postes de travail partagés ou les configurations rapides. Avec une technologie résistante à l'hameçonnage et une certification FIDO®, elles offrent une sécurité de niveau entreprise à un prix abordable, garantissant à la fois l'utilisabilité et la conformité.

Intégration de Windows Hello

VeriMark™ Access permet des connexions Windows rapides et sans mot de passe avec une simple configuration de clé d'empreinte digitale prêt à l'emploi. Lorsque la clé n'est pas disponible, l'application mobile VeriMark™ Companion sert de sauvegarde sécurisée, générant un code à usage unique pour garantir un accès ininterrompu. La solution prend également en charge des environnements multi-utilisateurs nécessitant un changement d'utilisateur rapide et fluide.

Fonctionnalités FIDO2

Certifiées pour le niveau 2 FIDO2 et prenant en charge CTAP2.1, ces clés fonctionnent sur les principales plateformes et navigateurs, y compris Windows, macOS, iOS et Android. Cette clé fournit une solution évolutive et conforme pour les entreprises adoptant la sécurité sans mot de passe.

La Sécurité là Où, Quand et Comment Vous en Avez Besoin

Déploiement en Entreprise

Les produits VeriMark™ sont conçus pour un déploiement d'entreprise évolutif, offrant un moyen simple et rentable de mettre en œuvre une authentification sans mot de passe. Avec une large compatibilité à travers les systèmes d'exploitation, les navigateurs et les plateformes d'identité, les produits VeriMark™ s'intègrent sans effort dans les environnements informatiques existants. Ils prennent en charge la gestion centralisée, respectent les normes de conformité FIDO2 et de l'industrie, et offrent une sécurité résistante à l'hameçonnage sans ajouter de complexité.

Soutient la Conformité au RGPD

Contribue à la mise en œuvre de mesures de cybersécurité conformément notamment aux lois protégeant la vie privée et à des règlements comme le RGPD, la BIPA et la CCPA.

Compatibilité

Les clés de sécurité et d'empreintes digitales VeriMark™ sont conçues pour une large compatibilité, offrant une authentification sécurisée et sans mot de passe sur plusieurs plateformes et services. Cette fonctionnalité multiplateforme fait de VeriMark™ une solution idéale pour les entreprises et les particuliers recherchant une sécurité robuste et résistante à l'hameçonnage sans sacrifier la commodité.

Forces Principal des Clés de Sécurité par Empreinte Digitale

Contrôle D'Accès Biométrique

Le principal avantage est que la possession de la clé seule ne suffit pas, l'empreinte digitale de l'utilisateur doit correspondre. Cela réduit considérablement le risque en cas de perte ou de vol de la clé. Seuls les utilisateurs enregistrés peuvent activer la réponse cryptographique de la clé.

MFA Intégré dans un Seul Appareil

Une clé d'empreinte digitale combine quelque chose que vous êtes (vérification biométrique) avec quelque chose que vous avez (un dispositif de sécurité physique). En pratique, cela permet à la numérisation de l'empreinte digitale de servir d'étape de vérification de l'utilisateur, éliminant ainsi le besoin d'un code PIN ou d'un mot de passe séparé lors de la connexion. Cela crée une expérience de connexion simplifiée où une seule action déverrouille la clé et authentifie tout en imposant plusieurs facteurs d'authentification forts.

Commodité et Rapidité pour L'utilisateur

Pour beaucoup, utiliser une empreinte digitale est plus rapide et plus pratique que de taper des mots de passe ou de prendre un téléphone pour un code OTP. Avec une clé bien conçue, la numérisation de l'empreinte digitale est presque instantanée.

Retour Visuel/Tactile

Les clés biométriques offrent souvent un peu de rétroaction (comme un indicateur LED) lorsqu'une empreinte digitale est acceptée, ce qui peut inspirer confiance. Savoir que la clé vous a activement vérifié ajoute un sentiment de sécurité.

Principaux Avantages des Clés D'Empreintes Digitales VeriMark™

Identification Biométrique: Seuls les utilisateurs enregistrés peuvent accéder.

Connexion Rapide: Toucher et aller—aucune saisie requise.

Résistant à L'Hameçonnage: Authentification basée sur le matériel.

Portable: Utilisation sur plusieurs appareils.

Réglementaire: Soutient le RGPD et est conforme à la norme TAA.

Forces Principales du USB NFC Clés de Sécurité

Compatibilité Entre Appareils

Le grand avantage des clés compatibles NFC est qu'elles fonctionnent sans problème avec les PC et les appareils mobiles. Vous pouvez brancher la clé dans des ports USB standard et la toucher sur des téléphones ou des tablettes via NFC pour vous authentifier sans fil.

Facilité D'Utilisation sur Mobile

Utiliser une clé de sécurité sur un téléphone peut être délicat si le téléphone n'a pas de port USB disponible ou s'il a un étui, mais le NFC résout ce problème. Toucher la clé sur le téléphone est rapide et intuitif et communique sur une très courte distance (dans quelques centimètres), ce qui est pratique et sécurisé (difficile à intercepter).

Idéal pour les Utilisateurs Partagés ou Tournants

Les clés NFC ne stockent pas d'empreintes digitales et ne nécessitent pas de configuration biométrique individuelle, ce qui les rend parfaites pour des environnements où plusieurs personnes ont besoin d'accès, comme les équipes de première ligne, les laboratoires étudiants, ou les ateliers de fabrication.

Sécurité Renforcée

Les clés NFC maintiennent le même niveau élevé de sécurité cryptographique que les autres clés matérielles. Le NFC lui-même est conçu pour la communication à courte portée, ce qui limite considérablement tout risque d'écoute (un attaquant devrait être physiquement à quelques centimètres pendant l'utilisation).

Principaux Avantages des Clés de Sécurité NFC+ VeriMark™

Interface Double: Fonctionne avec USB et NFC pour un accès flexible aux appareils.

Sécurité Résistante à L'Hameçonnage: Protection basée sur le matériel contre l'hameçonnage et le vol d'identifiants.

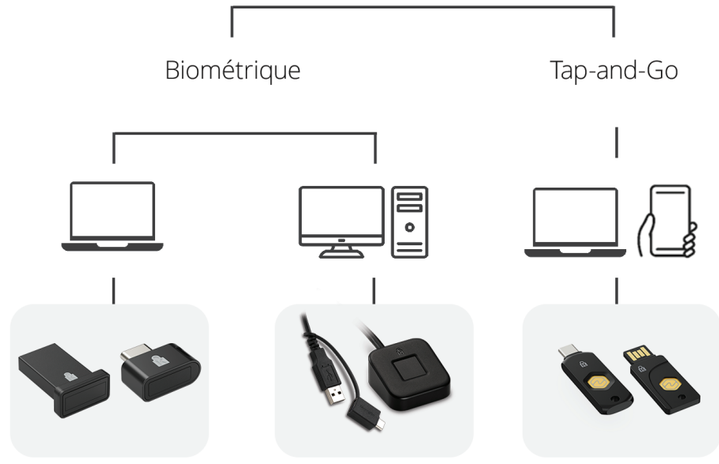
Certifié FIDO2 Niveau 2: Répond aux normes les plus élevées de l'industrie pour l'authentification sans mot de passe et prend en charge CTAP2.1.

Multi-Plateforme: Compatible avec Windows, macOS, Android, iOS et les principaux services et navigateurs.

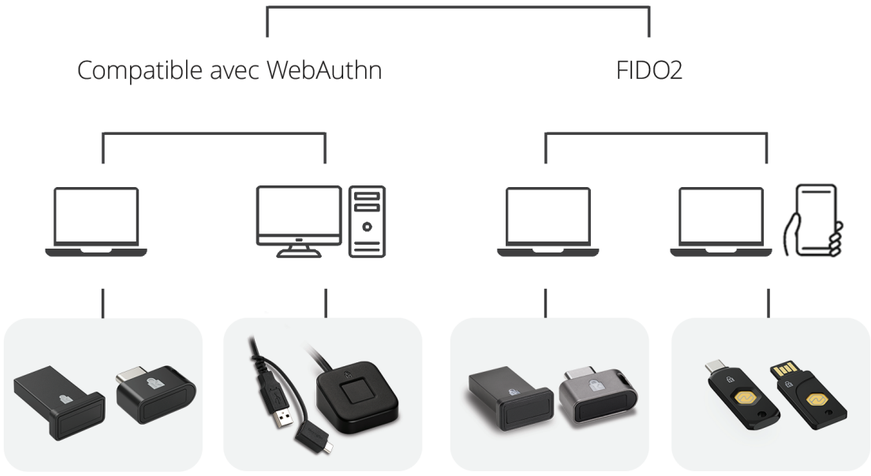
Aucune Configuration Biométrique Requise: Rapide à déployer—aucune inscription d'empreinte digitale requise.

	 **Lecteur TI 2.0 D'Empreintes Digitales**	 **VeriMark™ Clé D'Empreinte Digitale Desktop 2.0**	 **VeriMark™ Guard 2.1 Clé de Sécurité à Empreintes Digitales**	 **Clé de Sécurité VeriMark™ NFC+**
Windows Hello	Windows Hello Windows Hello for Business	Windows Hello Windows Hello for Business	Non pris en charge	Non pris en charge nativement, mais peut accéder via un logiciel (VeriMark™ Access) + Application mobile compagnon
Sécurité de connexion améliorée de Microsoft	Pris en charge par Windows 11	Pris en charge par Windows 11	Non pris en charge	Non pris en charge
FIDO2 et FIDO U2F	Non pris en charge	Non pris en charge	FIDO U2F + FIDO2 Niveau 1 de FIDO2	FIDO U2F + FIDO2 Niveau 2 de FIDO2
CTAP	Non pris en charge	Non pris en charge	Prend en charge CTAP2.1 et rétrocompatible avec CTAP2. 0	Prend en charge CTAP2.1 et rétrocompatible avec CTAP2. 0
Appareil				
Système d'exploitation				
Services de Google, Amazon, Apple et Microsoft				
Services Web				
Gestionnaires de mots de passe				

Connexion sécurisée pour Windows Hello



Connexion sécurisée pour les Services Web



				
	Lecteur TI 20 D'empreintes Digitales	**VeriMark™ Clé D'Empreinte Digitale Desktop 2.0**	**VeriMark™ Guard 2.1 Clé de Sécurité à Empreintes Digitales**	**Clé de Sécurité VeriMark™ NFC+**
No Article	USB-C® : K64705WW USB-A : K64740WW	K64741WW	USB-C® : K65051WW USB-A : K65050WW	USB-C® : K64739WW USB-A : K64738WW
Certifié Pour	Windows Hello Sécurité de connexion améliorée de Microsoft (ESS)	Windows Hello Sécurité de connexion améliorée de Microsoft (ESS)	FIDO CERTIFIED U2F L1 FIDO CERTIFIED FIDO2 L1	FIDO CERTIFIED U2F L2 FIDO CERTIFIED FIDO2 L2
Système D'exploitation				
Type de Clé				
Connection Type	USB-C® ou USB-A	USB-A avec adaptateur USB-C®	USB-C® ou USB-A	USB-C® ou USB-A et NFC
Windows Hello	Pris en charge	Pris en charge	Non pris en charge	Non pris en charge nativement, mais peut accéder via un logiciel (VeriMark™ Accès)
FIDO	Compatible avec WebAuthn	Compatible avec WebAuthn	Certifié FIDO U2F et FIDO2 Niveau 1	Certifié FIDO U2F et FIDO2 Niveau 2
CTAP	S.O	S.O	Prend en charge le protocole CTAP2.1	Prend en charge le protocole CTAP2.1
Clé D'accès	Compatible par biométrie	Compatible par biométrie	Compatible par biométrie	Compatible par NFC ou Tap-and-Go
Type D'authentification par Empreinte Digitale	Match-in-Sensor™	Match-in-Sensor™	Match-in-Sensor™	S.O
Score de Données	Datos de la plantilla de huellas dactilares en la llave	Datos de la plantilla de huellas dactilares en la llave	Datos de la plantilla de huellas dactilares en la llave	S.O
Taux de Rejets Erronés	2 %	2 %	2 %	S.O
Taux D'acceptations Erronées	0,001%	0,001%	0,001%	S.O
Lisibilité	365 degrés	365 degrés	365 degrés	S.O

La clé de sécurité USB-C® NFC+ VeriMark™ est conçue pour renforcer la sécurité numérique sur les services basés sur le web. Cette clé de sécurité USB-C® activée NFC est certifiée pour FIDO2 Niveau 2 et offre une authentification sécurisée, pratique et multiplateforme pour les consommateurs et les utilisateurs d'entreprise. En éliminant les vulnérabilités des mots de passe grâce à une MFA matérielle, cela offre une protection de niveau entreprise contre l'hameçonnage et le vol d'identité.

- Sécurité certifiée FIDO2 de niveau 2
- Support du protocole FIDO CTAP2. 1
- Interface double USB-C® + NFC
- Simplicité et logiciel complémentaire
- Compatibilité multiplateforme
- Compact et portable
- Évalué IP68 et résistant à l'écrasement

Également disponible

En savoir plus en visitant
kensington.com/solutions/product-category/why-biometrics/

Clés D'Empreinte Digitale – Cas D'Utilisation et Objectifs Idéaux

Les clés d'empreinte digitale combinent l'authentification biométrique avec la sécurité matérielle. Elles sont particulièrement adaptées aux environnements où l'assurance de l'identité individuelle est critique.

Soins de Santé

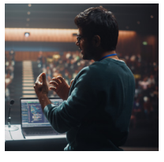
- Accès sécurisé aux dossiers des patients (conformité HIPAA).
- Prévenir l'accès non autorisé aux dispositifs médicaux ou aux terminaux.
- Connexion biométrique pour les cliniciens utilisant des postes de travail partagés.

Finance et Banque

- Accès sécurisé aux plateformes de trading ou aux tableaux de bord financiers.
- Prévenir le vol d'identifiants dans des environnements à haut risque.
- Respecter les exigences réglementaires (par exemple, PCI-DSS, RGPD).

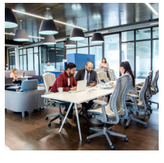
Gouvernement et Secteur Public

- Utilisé dans les institutions fédérales pour l'authentification multifactorielle biométrique.
- Prend en charge FIDO2 et Windows Hello pour les entreprises.



Éducation

- Les enseignants et le personnel utilisent des clés d'empreinte pour une connexion sécurisée.
- Empêche l'accès non autorisé dans les laboratoires informatiques partagés.



TI D'Entreprise

- Utilisé pour la gestion des accès privilégiés.
- Réduit la charge du service d'assistance liée aux réinitialisations de mot de passe.
- Soutient les pistes de vérification et le contrôle d'accès centralisé.

Clés NFC – Cas D'Utilisation et Objectifs Idéaux

Les clés NFC offrent une authentification sans contact et sont idéales pour les environnements mobiles, multi-utilisateurs ou orientés vers le consommateur.

.

Vente au Détail et Point de Vente

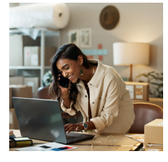
- Authentification sans contact pour les terminaux de point de vente.
- Changement rapide entre les comptes du personnel.
- Prévenir les transactions non autorisées.

Transport et Logistique

- Les conducteurs utilisent des clés NFC pour accéder aux outils de planification des itinéraires.
- Connexion sécurisée aux systèmes de gestion de flotte.
- Idéal pour les environnements difficiles (classe d'étanchéité IP68).

Éducation

- Les étudiants tapent pour se connecter à des appareils partagés.
- Les administrateurs informatiques gèrent l'accès sans avoir besoin d'enrôlement biométrique.



Consommateur et PME

- Connexion sans mot de passe pour les appareils personnels.
- Configuration facile pour les utilisateurs non techniques.
- Compatible avec Apple ID, Google, Microsoft, et plus.

Secteur Public - Travail sur le Terrain

- Connexion simplifiée pour les travailleurs mobiles.
- Aucun besoin d'enregistrement d'empreinte digitale ou de mémorisation de code PIN.
- Fonctionne hors ligne et sur plusieurs plateformes.

POUR DE PLUS AMPLES RENSEIGNEMENTS: 1-855-692-0054 | sales@kensington.com

Kensington
The Professionals' Choice™