KINGSTON IRONKEY D500S

Sécurité de niveau militaire FIPS 140-3 niveau 3 (en attente) pour protéger les données mobiles

La clé USB Kingston IronKey™ D500S/SM est dotée des fonctionnalités de sécurité de niveau militaire qui font d'IronKey la marque la plus fiable pour la protection des informations classifiées. Elle est certifiée FIPS 140-3 niveau 3 (en attente) et intègre de nouvelles améliorations du NIST qui exigent des mises à niveau sécurisées des microprocesseurs pour une sécurité et des protections renforcées contre les attaques pour les utilisations gouvernementales et militaires. Les données sont chiffrées et déchiffrées sur la D500S sans qu'aucune trace ne soit laissée sur le système hôte. Outre le chiffrement matériel XTS-AES 256 bits, elle est dotée d'un boîtier en zinc robuste qui est étanche[1], résistant à la poussière[1] et à l'écrasement, et rempli d'époxy spécial pour protéger contre les attaques physiques des composants internes.

La IronKey D500S est un pilier essentiel pour répondre aux meilleures pratiques en matière de protection contre la perte de données (DLP). Elle offre la sécurité de niveau militaire la plus stricte pour assurer la conformité aux lois et réglementations sur le chiffrement des données telles que le RGPD, HIPAA, SOX et CCPA. La D500S offre plus de fonctionnalités que n'importe quelle autre clé de sa catégorie, ce qui en fait une solution de sécurité complète pour la protection des données de grande valeur.

La D500S effectue des autotests au démarrage, et si une surchauffe ou une surtension est détectée, elle s'arrête. Pour davantage de tranquillité d'esprit, la D500S intègre un micrologiciel signé numériquement, ce qui l'immunise contre les logiciels malveillants BadUSB et les attaques par force brute. La protection contre les attaques par force brute étant activée en permanence, elle empêche les tentatives de deviner le mot de passe car si un trop grand nombre de mots de passe erronés est saisi, un effacement chiffré supprime toutes les données de la clé.

Elle propose une option de mots de passe multiples pour accéder aux données, qui prend en charge jusqu'à trois mots de passe : Admin, Utilisateur et de récupération à usage unique. En cas d'oubli du mot de passe Utilisateur, l'administrateur peut réinitialiser le mot de passe Utilisateur et activer un mot de passe de récupération à usage unique pour restaurer l'accès.

La D500S prend en charge le mode de mot de passe Complexe classique et le mode Phrase de passe[3]. Le mode Complexe classique permet des mots de passe de 8 à 16 caractères en utilisant 3 des 4 jeux de caractères. Les phrases de passe peuvent être composées de 10 à 128 caractères. Ce sont des phrases qui peuvent contenir des caractères d'espacement, une liste de mots ou même des paroles de chansons. Cela en simplifie la mémorisation, tout en offrant une très grande sécurité. Le FBI recommande les phrases de passe à plusieurs mots de 15 caractères ou plus, car elles sont plus sécurisées et plus faciles à mémoriser que les mots de passe complexes.[5]

La D500S comprend une option de double partition cachée, ce qui est une première dans le secteur. Cela permet à l'administrateur de créer deux partitions sécurisées de taille personnalisée : une pour l'administrateur et l'autre pour l'utilisateur. On obtient ainsi une réserve de fichiers masqués qui peut être utilisée pour fournir des fichiers à la partition de l'utilisateur, le cas échéant. Lorsque vous utilisez des systèmes non fiables ou que vous partagez la clé, les réserves de fichiers cachés conservent leurs données en toute sécurité et restent invisibles, sauf en cas d'accès légitime.

Grâce à une séquence de touches spéciale, l'administrateur peut saisir un mot de passe d'effacement chiffré qui supprimera définitivement les données de la clé et la réinitialisera pour empêcher tout accès non autorisé.

Pour aider les utilisateurs ayant des problèmes de clavier, tous les écrans de saisie de mot de passe comprennent un symbole d'œil qui affichera le mot de passe saisi afin de réduire les fautes de frappe. Un clavier virtuel est également disponible en anglais[4] pour protéger la saisie du mot de passe contre les enregistreurs de frappe et les enregistreurs d'écran.

La D500S prend également en charge deux niveaux de modes de lecture seule (protection contre l'écriture). L'administrateur et l'utilisateur peuvent définir un mode de lecture seule par session pour protéger la clé contre les logiciels malveillants sur les systèmes non fiables. L'administrateur peut également définir un mode de lecture globale qui place la clé en mode lecture seule jusqu'à sa réinitialisation.

Elle offre également des performances élevées en termes de vitesse, sans compromettre la sécurité. Cette clé comprend un numéro de série unique à 8 chiffres qui est le même en version électronique que celui gravé sur le boîtier, avec un code à barres scannable pour son déploiement ou à des fins d'audit.

La D500S offre de nombreuses options de personnalisation, est conforme à la norme TAA/CMMC, et est assemblé aux États-Unis.

Modèle Managed
Les clés Kingston IronKey D500SM (M = Managed) nécessitent SafeConsole[2]. Cela permet de gérer de manière centralisée l'accès et l'utilisation de tout en parc de clés pour les grandes entreprises ou les gouvernements. Une version Managed en option est également proposée en tant que personnalisation.

- Certifiée FIPS 140-3 niveau 3 (en attente) pour une sécurité de niveau militaire
- Option de mots de passe multiples avec modes Complexe/Phrase de passe
- Première option de double partition cachée du secteur
- Effacement chiffré du mot de passe en cas d'urgence
- Boîtier en zinc robuste pour une protection contre les attaques physiques
- Interface conviviale
- Fonctionnalités et attributs entièrement personnalisables
- Disponible dans un modèle Managed, lequel nécessite SafeConsole[2]

Plus ››

CARACTÉRISTIQUES / AVANTAGES

Clés USB à chiffrement matériel de classe militaire — Chiffrement XTS-AES 256 bits certifié FIPS 140-3 niveau 3 (en attente) avec mises à niveau sécurisées du microprocesseur pour une sécurité renforcée. Protections intégrées contre les attaques BadUSB et par force brute. Nouvel auto-test de la clé au démarrage et détection des conditions de surchauffe ou de surtension entraînant son arrêt.

Mots de passe multiples pour la récupération des données — Activez les mots de passe Admin, Utilisateur et de récupération à usage unique. L'administrateur peut réinitialiser un mot de passe Utilisateur et activer un mot de passe de récupération à usage unique pour rétablir l'accès de l'utilisateur aux données en cas d'oubli de son mot de passe.

Mode Complexe ou Phrase de passe — Choix entre mode Complexe ou Phrase de passe. Les phrases de passe peuvent être des phrases complètes, plusieurs mots ou même des paroles de chanson dont vous êtes le seul à vous souvenir, d'une longueur de 10 à 128 caractères. Un symbole d'œil pour tous les mots de passe saisis permet de réduire les fautes de frappe.

Première option de double partition cachée du secteur — L'administrateur de créer deux partitions sécurisées de taille personnalisée : une pour l'administrateur et l'autre pour l'utilisateur. On obtient ainsi une réserve de fichiers masqués qui assure la protection des données et les rend invisibles à tout utilisateur non légitime. Les deux partitions cachées peuvent fournir une sécurité supplémentaire sur les systèmes non fiables ou lorsque la clé doit être partagée.

Effacement chiffré du mot de passe en cas d'urgence — Le mot de passe d'effacement chiffré est destiné aux situations d'urgence où une violation de données est anticipée. Il efface les clés de chiffrement, supprime définitivement toutes les données et réinitialise la clé.

Boîtier robuste conforme aux normes strictes IronKey — Le boîtier en zinc est imperméable à l'eau[1], à la poussière[1], résistant à l'écrasement et rempli d'époxy pour une sécurité physique inviolable.

Intégralement personnalisable — Activez, désactivez, modifiez les fonctionnalités et le profil de la clé. Co-logo.

Modes lecture seule globale/de session (protection écriture) — L'administrateur et l'utilisateur peuvent définir un mode de lecture seule par session pour protéger la clé contre les logiciels malveillants sur les systèmes non fiables. L'administrateur peut également définir un mode de lecture globale qui place la clé en mode lecture seule jusqu'à sa réinitialisation.

SPÉCIFICATIONS

Principales certifications
FIPS 140-3 Niveau 3 (en attente)
conformité TAA/CMMC, assemblage aux États-Unis

Interface
USB 3.2 Gen 1

Capacités[6]
8 Go, 16 Go, 32 Go, 64 Go, 128 Go, 256 Go, 512 Go

Connecteur
Type-A

Vitesse[7]
USB 3.2 Gen 1
8 Go – 128 Go : 260 Mo/s en lecture, 190 Mo/s en écriture
256 Go : 240 Mo/s en lecture, 170 Mo/s en écriture
512 Go : 310 Mo/s en lecture, 250 Mo/s en écriture

USB 2.0
8 Go – 512 Go : 30 Mo/s en lecture, 20 Mo/s en écriture

Dimensions
77,9 mm x 21,9 mm x 12,0 mm

Étanche[8]
jusqu'à 1,20 mètre ; IEC 60529 IPX8

Température de fonctionnement
0 °C à 50 °C

Température de stockage
-20 °C à 85 °C

Compatibilité
USB 3.0/USB 3.1/USB 3.2 Gen 1

Options de personnalisation
D500S : Activez, désactivez, modifiez les fonctionnalités et le profil de la clé. Co-logo.
D500SM : Modifiez le profil de la clé. Co-logo. Version Managed en option.

Garantie/assistance technique
D500S : Garantie de 5 ans et assistance technique gratuite
D500SM : Garantie de 2 ans et assistance technique gratuite

Compatible avec
Windows® 11, 10, macOS® 10.15.x – 13.x, Linux[9] Kernel 4.4+

RÉFÉRENCES PRODUITS

IronKey D500S	IronKey D500SM
IKD500S/8GB	IKD500SM/8GB
IKD500S/16GB	IKD500SM/16GB
IKD500S/32GB	IKD500SM/32GB
IKD500S/64GB	IKD500SM/64GB
IKD500S/128GB	IKD500SM/128GB
IKD500S/256GB	IKD500SM/256GB
IKD500S/512GB	IKD500SM/512GB

1. Veuillez vous reporter aux spécifications de la fiche technique. Le produit doit être propre et sec avant toute utilisation.
2. Le service de gestion SafeConsole doit être acheté séparément.
3. Le mode Phrase de passe n'est pas pris en charge sous Linux.
4. Clavier virtuel : Prend uniquement en charge l'anglais américain sur Microsoft Windows et macOS.
5. De fbi.gov : Oregon FBI Tech Tuesday : Building a Digital Defence with Passwords (Construire une défense numérique avec des mots de passe), 18 février 2020 (lien fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-with-passwords)
6. Sur une unité de stockage Flash, une partie de la capacité nominale est réservée au formatage et à d'autres fonctions, et n'est donc pas disponible pour le stockage des données. Par conséquent, la capacité réelle disponible pour le stockage de données est inférieure à celle indiquée pour chaque produit. Pour en savoir plus, consultez le Guide des mémoires Flash Kingston.
7. La vitesse est susceptible de varier en fonction de la configuration matérielle et logicielle de l'hôte et de l'utilisation du produit.
8. Certifiée IEC 60529 IPX8 pour l'étanchéité avec le capuchon. Le produit doit être propre et sec avant toute utilisation.
9. La prise en charge des fonctionnalités sous Linux est limitée. Reportez-vous au manuel de l'utilisateur pour plus de détails. Certaines distributions de Linux nécessitent des privilèges de super-utilisateur (racine) pour exécuter les commandes IronKey dans la fenêtre d'application terminale.