



## Clé USB à chiffrement matériel Kingston IronKey D500S

Certifiée FIPS 140-3 niveau 3 (en attente), chiffrement matériel XTS-AES 256 bits, boîtier robuste en zinc

---

La Kingston IronKey™ D500S est une clé USB de pointe 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<sup>1</sup>, résistant à la poussière<sup>1</sup>, résistant aux chocs et aux vibrations conformément aux normes militaires<sup>2</sup> et résistant à l'écrasement, et rempli d'époxy spécial pour protéger les composants internes contre les attaques par pénétration.

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 CMMC, SOC2, NIS2, FISMA, GDPR, PIPEDA, HIPAA, HITECH, GLBA, SOX et CCPA, ainsi qu'à la TAA. La D500S offre plus de fonctionnalités que tout autre appareil de sa catégorie, ce qui en fait une solution de sécurité de pointe pour la protection des données confidentielles 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. 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<sup>3</sup>. Les phrases de passe peuvent être composées de 10 à 128 caractères. 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.<sup>4</sup>

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 dans des situations compromettantes.

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<sup>5</sup> 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 de double canal 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.

- 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 de danger
- Boîtier en zinc robuste pour une protection contre les attaques de pénétration, normes militaires en matière de chocs et de vibrations, étanchéité à l'eau/à la poussière IP67<sup>6</sup>
- Interface conviviale
- Fonctionnalités entièrement personnalisables

## Caractéristiques Principales

- **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. Nouveau test automatique de la clé USB au démarrage, protection thermique et de tension pour arrêter automatiquement les clés lorsqu'elles atteignent certains seuils.
- **Option multi-mots de passe pour la récupération de 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 ou plusieurs mots 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 mdp en cas de situation compromettante**

Le mot de passe d'effacement chiffré efface les clés de chiffrement, supprime définitivement toutes les données et réinitialise la clé.
- **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.
- **Boîtier robuste conforme aux normes strictes IronKey**

Le boîtier en zinc est résistant à l'écrasement et rempli d'époxy pour une sécurité physique inviolable. Certification MIL-STD-810F pour les chocs mécaniques, les vibrations et les chutes. Certification IP67 pour l'étanchéité à l'eau<sup>1</sup> et à la poussière<sup>1</sup>.
- **N° de série unique à 8 chiffres et code-barres scannable**

Gagnez du temps. Il suffit de lire ou de balayer le code-barres lors du déploiement de la clé, à son retour ou lors de n'importe quel audit physique.
- **Intégralement personnalisable**

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

## Caractéristiques

Principales certifications	FIPS 140-3 Niveau 3 (en attente) MIL-STD-810F Conformité TAA/CMMC, assemblage aux États-Unis
Interface	USB 3.2 Gen 1
Capacités*	8 Go, 16 Go, 32 Go, 64 Go, 128 Go, 256 Go, 512 Go
Connecteur	Type-A
Vitesse <sup>7</sup>	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 à l'eau/à la poussière <sup>8</sup>	Certification IP67
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.

Garantie/assistance technique	D500S : Garantie de 5 ans et assistance technique gratuite
Compatible avec	Windows® 11, 10, macOS® 12.x – 15.x, Linux <sup>9</sup> Kernel 4.4+

## Numéros De Pièce

### IKD500S

IKD500S/8GB
IKD500S/16GB
IKD500S/32GB
IKD500S/64GB
IKD500S/128GB
IKD500S/256GB
IKD500S/512GB

## Image Du Produit



\* Une partie de la capacité répertoriée sur cette clé USB est utilisée pour le formatage et d'autres fonctions. Ce périphérique n'est donc pas disponible pour le stockage de données. La capacité réelle disponible pour le stockage de données est alors inférieure à celle indiquée sur les produits. Pour plus d'informations, consultez le [Guide de la mémoire flash de Kingston](#).

1. Veuillez vous reporter aux spécifications de la fiche technique. Le produit doit être propre et sec avant toute utilisation.
2. Certification MIL-STD-810F pour les chocs mécaniques, les vibrations et les chutes.
3. Le mode Phrase de passe n'est pas pris en charge sous Linux.
4. De fbi.gov: [Oregon FBI Tech Tuesday: Building a Digital Defense with Passwords](#), 18 février 2020
5. Clavier virtuel : Prend uniquement en charge l'anglais américain sur Microsoft Windows et macOS
6. Le produit doit être propre et sec avant utilisation.
7. Le débit peut varier en fonction du matériel hôte, du logiciel et de l'utilisation.
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.

CE DOCUMENT PEUT ÊTRE MODIFIÉ SANS PRÉAVIS.

©2024 Kingston Technology Europe Co LLP et Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Angleterre. Tél: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469 Tous droits réservés. Toutes les marques commerciales et les marques déposées sont la propriété de leurs détenteurs respectifs. MKD-08292024

