KINGSTON IRONKEY D500S

Protección FIPS 140-3 de Nivel 3 de grado militar (pendiente) para proteger los datos móviles

La unidad Flash USB Kingston IronKey™ D500S/SM incorpora la avanzada protección de grado militar que convierte a IronKey en la marca de máxima confianza para proteger información clasificada. Cuenta con la certificación FIPS 140-3 de Nivel 3 (pendiente), con nuevas mejoras del NIST que requieren actualizaciones seguras del microprocesador para reforzar la seguridad y las protecciones contra ataques para usos gubernamentales y militares. Los datos se cifran y se descifran dentro de la unidad D500S, sin dejar ninguna huella en el sistema anfitrión. Conjuntamente con el cifrado XTS-AES de 256 bits basado en hardware, se caracteriza por una sólida carcasa de zinc estanca al agua[1] y al polvo[1], resistente al aplastamiento y rellena de epóxido para proteger a los componentes internos contra ataques de penetración.

IronKey D500S es un pilar esencial de las buenas prácticas de Protección contra pérdidas de datos (PPD/DLP), con la más estricta seguridad de grado militar, compatible con las leyes y reglamentos de cifrado de datos, como el RGPD, la HIPAA, la SOX y la CCPA. D500S ofrece más funciones que cualquier otra unidad de su categoría, lo cual la convierte en una solución de seguridad integral para la protección de datos de alto valor.

D500S realiza pruebas de autodiagnóstico al arranque, y si detecta situaciones de recalentamiento o problemas de tensión, la unidad se apaga inmediatamente. Para una mayor tranquilidad, la D500S incorpora un firmware de firma digital, lo cual la hace inmune a ataques de malware BadUSB y de fuerza bruta. La protección contra ataques de fuerza bruta para adivinar contraseñas está siempre activada y, si se excede el número de intentos de empleo de contraseñas no válidas, la unidad se criptoborrará.

Además, ofrece una opción de contraseñas múltiples para acceder a los datos, que admite hasta tres contraseñas: Admin, Usuario y Recuperación de un solo uso Con Admin se puede restablecer una contraseña de usuario y también especificar una contraseña de recuperación de un solo uso si se olvida la contraseña de usuario.

D500S admite el modo tradicional de contraseña compleja o el modo de frase de contraseña[3]. El modo Complejo tradicional admite contraseñas de 8 a 16 caracteres, empleando 3 de 4 conjuntos de caracteres. Las frases de contraseña pueden tener entre 10 y 128 caracteres de longitud. Se trata de una frase con caracteres de espacio, listas de palabras o incluso la letra de una canción, con lo que se simplifica recordar contraseñas con sentido, aunque seguras. El FBI recomienda frases de contraseña de varias palabras, de 15 o más caracteres, como método más resistente y más fácil de recordar que las contraseñas complejas.[5]

La unidad D500S incluye la opción Doble partición oculta, novedad en el sector, mediante la cual el administrador puede crear dos particiones seguras, de tamaño personalizado, para el administrador y el usuario, Esto posibilita un almacén oculto de archivos que puede emplearse para provisionar archivos a la partición del usuario según sea necesario. Cuando se utilizan sistemas que no sean de confianza o cuando se comparte la unidad, los Almacenes ocultos de archivos mantienen los datos protegidos e invisibles, salvo que se acceda a la misma de manera adecuada.

Con una secuencia especial de claves, el administrador puede introducir una contraseña de criptoborrado que criptoborrará la unidad, destruyendo los datos para siempre y restableciéndola para impedir el acceso no autorizado.

Para ayudar a los usuarios con los problemas de teclado, todas las pantallas de introducción de contraseñas incluyen un símbolo de ojo, que mostrará la contraseña introducida para reducir los errores tipográficos. Se proporciona también un teclado virtual, disponible en inglés[4] para ocultar la contraseña introducida de grabadores de pulsaciones de teclado y de pantalla.

Por otra parte, la unidad D500S también admite dos niveles de modos de Solo lectura (protección contra escritura). Tanto el administrador como el usuario pueden configurar el modo de Solo lectura en cada sesión para proteger a la unidad contra el malware de sistemas desconocidos. Además, el administrador puede establecer el modo de Solo lectura global, que configura la unidad en modo de Solo lectura hasta que es reconfigurada.

Además, se caracteriza por su rápido rendimiento, aunque sin sacrificar la seguridad. La unidad incluye un número de serie exclusivo de 8 dígitos, que es el mismo que va electrónicamente grabado en la carcasa, con un código de barras escaneable, lo que facilita su implementación o para fines de auditoría.

La D500S ofrece numerosas opciones de personalización, es compatible con TAA/CMMC y se ensambla en EE.UU.

Modelo Managed (administrado)
Las unidades Kingston IronKey D500SM (M = Managed/Administrado) requieren SafeConsole[2]. Esto posibilita la administración centralizada del acceso y el uso de la unidad dentro de un conjunto de unidades en grandes empresas o administraciones públicas. También se ofrece una versión de administración como opción de personalización.

- Homologación FIPS 140-3 de Nivel 3 (pendiente), la más avanzada protección de grado militar
- Opción de múltiples contraseñas con modos Compleja y Frase de contraseña
- Opción Doble partición oculta, primicia en el sector
- Contraseña de criptoborrado para casos de emergencia
- Resistente carcasa de zinc para protección contra ataques de penetración
- Interfaz de uso sencillo
- Funciones y atributos plenamente personalizables
- Disponible en modo Administrado que requiere SafeConsole[2]

Más ››

CARACTERÍSTICAS/VENTAJAS

USB cifrada por hardware de grado militar — Homologación FIPS 140-3 de Nivel 3 (pendiente) con cifrado XTS-AES de 256 bits y actualizaciones seguras de microprocesador para una mayor protección. Protecciones integradas contra ataques de BadUSB y de fuerza bruta Nuevas pruebas de autodiagnóstico al arranque y de detección de situaciones de recalentamiento o problemas de tensión, en cuyo caso la unidad se apaga inmediatamente.

Opción de varias contraseñas para la recuperación de datos — Permite habilitar las contraseñas de administración, de usuario y de recuperación de un solo uso. Con Admin se puede restablecer una contraseña de usuario y también especificar una contraseña de recuperación de un solo uso si se olvida la contraseña de usuario.

Modo de contraseña compleja o de frase de contraseña — Se puede seleccionar entre los modos de Contraseña compleja o Frase de contraseña. Las frases de contraseña pueden ser oraciones complejas, varias palabras o incluso letras de canciones que solamente usted pueda recordar, de entre 10 y 128 caracteres de longitud. El símbolo de ojo para la introducción de contraseñas contribuye a reducir errores.

Opción Doble partición oculta, primicia en el sector — El administrador puede crear dos Dobles particiones ocultas de tamaño personalizado para el administrador y para el usuario, para acceder a un Almacén oculto de archivos, lo cual permite mantener los datos protegidos e invisibles. Las dobles particiones ocultas aportan protección adicional en sistemas que no sean de confianza o cada vez que es necesario compartir la unidad.

Contraseña de criptoborrado para casos de emergencia — La contraseña de criptoborrado es para emergencias en las que se prevé una vulneración de los datos. Borrará las claves de cifrado, eliminará todos los datos para siempre y restablecerá la unidad.

Carcasa compatible con los estándares IronKey más estrictos — Carcasa de zinc estanca al agua[1] y al polvo[1], resistente al aplastamiento y rellena de epóxido para impedir las manipulaciones físicas.

100% personalizable — Activación, desactivación y modificación de las funciones y del perfil de la unidad. Logotipo compartido.

Solo lectura global/de sesión (protección contra escritura) — Tanto el administrador como el usuario pueden configurar el modo de Solo lectura en cada sesión para proteger a la unidad contra el malware de sistemas desconocidos. Además, el administrador puede establecer el modo de Solo lectura global, que configura la unidad en modo de Solo lectura hasta que es reconfigurada.

ESPECIFICACIONES

Principales homologaciones
FIPS 140-3 de Nivel 3 (pendiente)
compatible con TAA/CMMC, ensamblada en EE.UU.

Interfaz
USB 3.2 Gen 1

Capacidades[6]
8 GB, 16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB

Conector
Tipo A

Velocidad[7]
USB 3.2 Gen 1
8 GB – 128 GB: 260 MB/s en lectura, 190 MB/s en escritura
256 GB: 240 MB/s en lectura, 170 MB/s en escritura
512 GB: 310 MB/s en lectura, 250 MB/s en escritura

USB 2.0
8 GB – 512 GB: 30 MB/s en lectura, 20 MB/s en escritura

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

Estanca al agua[8]
hasta 1,2 m; conforme a la norma IEC 60529 IPX8

Temperatura de servicio
0 °C a 50 °C

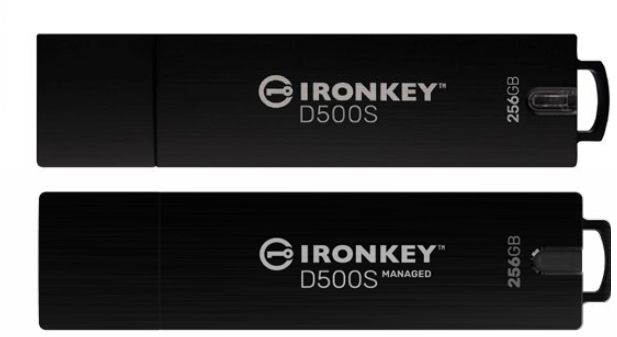
Temperatura de almacenamiento
-20 °C a 85 °C

Compatibilidad
USB 3.0/USB 3.1/USB 3.2 Gen 1

Opciones de personalización
D500S: Activación, desactivación y modificación de las funciones y del perfil de la unidad. Logotipo compartido.
D500SM: Modificación del perfil de la unidad. Logotipo compartido. Versión administrada opcional.

Garantía/asistencia
D500S: 5 años de garantía y asistencia técnica gratuita
D500SM: 2 años de garantía y asistencia técnica gratuita

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



NÚMERO DE PIEZA

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. Consulte las especificaciones de la ficha técnica. El producto debe estar limpio y seco antes de su uso.
2. El servicio SafeConsole Management se contrata por separado.
3. El modo de frase de contraseña no es compatible con Linux.
4. Teclado virtual: solamente admite inglés (EE.UU.) en Microsoft Windows y macOS.
5. De fbi.gov: Oregon FBI Tech Tuesday: Building a Digital Defence with Passwords (Martes tecnológico de FBI Oregón: Construir una defensa digital con contraseñas), 18 de febrero de 2020 (enlace: fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-with-passwords)
6. Una parte de la capacidad total indicada para los dispositivos de almacenamiento Flash se utiliza para el formateo y otras funciones y, por lo tanto, no está disponible para el almacenamiento de datos. Por este motivo, la capacidad real de almacenamiento de datos es inferior a la indicada en los productos. Consulte información más detallada en la Guía de memorias Flash de Kingston.
7. La velocidad puede variar en función de las características del equipo huésped, de los programas y del uso.
8. Homologación IEC 60529 IPX8 para estanqueidad al agua con el tapón colocado. El producto debe estar limpio y seco antes de su uso.
9. La compatibilidad con Linux es limitada. Consulte información detallada en el manual del usuario. Algunas distribuciones de Linux requieren privilegios de superusuario (raíz) para ejecutar correctamente los comandos de IronKey en la ventana de aplicaciones de terminal.