Kingston IronKey D500S Dispositivo Flash USB encriptado por hardware

Certificación FIPS 140-3 de nivel 3 (pendiente), encriptado por hardware de 256 bits XTS-AES, carcasa de zinc robusta

---

La mejor unidad Flash USB Kingston IronKey™ D500S/SM cuenta con la emblemática seguridad de grado militar que convierte a IronKey en la marca más confiable para proteger información clasificada. Certificación FIPS 140-3 de nivel 3 (pendiente) con nuevas mejoras del NIST que exigen actualizaciones seguras del microprocesador para una mayor seguridad y protección contra ataques en usos gubernamentales y militares. Los datos se encriptan y desencriptan en el D500S sin dejar rastro en el sistema anfitrión. Además del encriptado XTS-AES de 256 bits basado en hardware, cuenta con una robusta carcasa de zinc resistente al agua[1], al polvo[1], a los golpes y a las vibraciones según normas militares[2], a los golpes y con un relleno epoxi especial para proteger los componentes internos de ataques de penetración.

El IronKey D500S es un pilar esencial para cumplir las mejores prácticas de protección contra la pérdida de datos (DLP) con la seguridad de grado militar más exigente para el cumplimiento de las leyes y normativas del encriptado de datos como CMMC, SOC2, NIS2, FISMA, GDPR, PIPEDA, HIPAA, HITECH, GLBA, SOX y CCPA, junto con TAA D500S ofrece más funciones que cualquier otra unidad de su clase, lo que la convierte en una solución de seguridad líder del sector para la protección de datos confidenciales de gran valor.

El D500S se auto comprueba al arrancar y las condiciones de sobre temperatura o tensión provocarán la desconexión de la unidad. Para mayor tranquilidad, el D500S incorpora un firmware firmado digitalmente que lo hace inmune al malware BadUSB. La protección contra ataques de fuerza bruta a la contraseña está siempre activada para evitar que se adivine la contraseña y, en última instancia, el dispositivo se criptoborrará si se superan los reintentos de contraseñas no válidas.

Ofrece una opción de multi-contraseña para acceder a los datos que admite hasta tres contraseñas: Administrador, Usuario y de Recuperación de una sola vez. El Administrador puede restablecer la Contraseña de usuario y también habilitar una Contraseña

de recuperación de una sola vez para restaurar el acceso si se olvida la contraseña de usuario.

El D500S admite el modo Contraseña compleja tradicional o Frase de contraseña[3]. Las frases de contraseña pueden tener entre 10 y 128 caracteres. El FBI recomienda las frases de contraseña de 15 o más caracteres como más seguras y fáciles de recordar que las contraseñas complejas.[4]

El D500S incluye una opción de doble partición oculta, pionera en el sector, con la que el Administrador puede crear dos particiones seguras de tamaño personalizado para el Administrador y el Usuario, lo cual permite un Almacenamiento de archivos oculto que puede utilizarse para suministrar archivos a la partición del Usuario según sea necesario. Cuando se utilizan sistemas no confiables o se comparte el dispositivo, los Almacenamientos de archivos ocultos mantienen sus datos seguros e invisibles a menos que se acceda a ellos correctamente.

Con una secuencia de teclas especial, el Administrador puede introducir una contraseña de criptoborrado que criptoborrará la unidad, destruirá los datos para siempre y restablecerá el dispositivo para impedir el acceso no autorizado en situaciones comprometedoras.

Para ayudar a los usuarios con 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. El Teclado virtual también está disponible en inglés[5] para proteger las contraseñas del registro de teclas (keylogger) y el registro de pantalla (screenlogger).

El D500S también admite dos niveles de Modos de solo lectura (Escritura-Proteger). Tanto el Administrador como el Usuario pueden configurar un modo de sólo lectura basado en la sesión para proteger el dispositivo de malware en sistemas que no sean de confianza. El Administrador también puede configurar un Modo de solo lectura global que configura el dispositivo en Modo de solo lectura hasta el restablecimiento.

También ofrece un rápido rendimiento de doble canal sin comprometer la seguridad. El dispositivo incluye un número de serie único de 8 dígitos que coincide electrónicamente con el grabado en la carcasa, con un código de barras escaneable para el despliegue del dispositivo o con fines de auditoría.

El D500S ofrece muchas opciones de personalización, se ajusta a las normas TAA/CMMC y se ensambla en EE. UU.

Modelo administrado

Las unidades Kingston IronKey D500SM (M = Managed[6]) permiten el manejo centralizado del acceso y uso de las unidades a través de una flota de unidades para grandes empresas o entidades gubernamentales.

- Certificación FIPS 140-3 de nivel 3 (pendiente) para una seguridad de grado militar emblemática
- Opción multi-contraseña con modos Complejo/Frase de contraseña
- Doble opción de partición oculta pionera en la industria
- Contraseña criptoborrable para situaciones comprometedoras

- Carcasa de zinc robusta para protección contra ataques de penetración, estándares militares contra golpes y vibraciones, IP67 a prueba de agua/polvo[7]
- Interfaz fácil de usar
- Características totalmente personalizables
- Disponible en modelo administrado

Características Clave

- ## Unidad USB con encriptación por hardware de grado militar

  Encriptación XTS-AES de 256 bits certificación FIPS 140-3 de nivel 3 (pendiente) con actualizaciones seguras del microprocesador para una mayor seguridad. Protecciones integradas contra los ataques de fuerza bruta y BadUSB. Nueva autocomprobación del dispositivo al arrancar, protección térmica y de voltaje para apagar automáticamente los dispositivos cuando alcanzan ciertos umbrales.

- ## Opción multi-contraseña para la recuperación de datos

  Permite contraseñas de Administrador, Usuario y Recuperación única. El Administrador puede restablecer la Contraseña de usuario y habilitar una Contraseña de recuperación de una sola vez para restaurar el acceso del Usuario a los datos si la Contraseña de usuario es olvidada.

- ## Modo Complejo o de Frase de contraseña

  Seleccione entre el modo Complejo o el de Frase de contraseña. Las frases de contraseña pueden ser oraciones completas o varias palabras que solo usted recuerde, de 10 a 128 caracteres. Un Símbolo de ojo para todas las contraseñas ingresadas ayuda a reducir los errores tipográficos.

- ## Doble opción de partición oculta pionera en la industria

  El Administrador puede crear dos particiones ocultas duales de tamaño personalizado para el Administrador y el Usuario para que un Almacenamiento de archivos oculto pueda mantener los datos seguros e invisibles a menos que se acceda a ellos correctamente. Las dobles particiones ocultas pueden proporcionar seguridad adicional en sistemas no confiables o cuando es necesario compartir dispositivos.

- ## Contraseña criptoborrable para situaciones comprometedoras

  La contraseña criptoborrable borrará las claves de encriptado, borrará todos los datos para siempre y reiniciará el dispositivo.

- ## Modos Global y de Sesión sólo lectura (protec.contra esc.)

  Tanto el administrador como el usuario pueden configurar un modo de Solo lectura por una sesión para proteger el dispositivo contra malware en sistemas que no son de confianza. El administrador también puede configurar un modo de Solo lectura Global que configura la unidad en modo de Solo lectura hasta que se reinicie.

- ## Carcasa robusta creada con los estándares IronKey más altos

  La carcasa de zinc es resistente a los golpes y rellena de epoxi para una seguridad física a prueba de manipulaciones. Con certificación MIL-STD-810F para pruebas mecánicas de choque, vibración y caída. Con certificación IP67 para resistencia al agua[1] y al polvo[1].

- ## Núm. serie único de 8 dígitos y código de barras escaneable

  Ahorro de tiempo, simplemente lea o escanee el código de barras, al iniciar, cuando lo devuelva, así como durante cualquier auditoría física.

- ## Totalmente personalizable

  Habilitar, deshabilitar, modificar las características y el perfil del dispositivo. Logotipo conjunto.

Especificaciones

Certificaciones clave	FIPS 140-3 de nivel 3 (pendiente) MIL-STD-810F Conformidad con TAA/CMMC, ensamblado en EE.UU.
Interfaz	USB 3.2 Gen 1
Capacidades*	8 GB, 16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB
Conector	Tipo-A
Velocidad[8]	USB 3.2 Gen 1 8 GB a 128 GB: 260 MB/s de lectura, 190 MB/s de escritura 256 GB: 240MB/s de lectura, 170MB/s de escritura 512 GB: 310MB/s de lectura, 250MB/s de escritura USB 2.0 8 GB a 512 GB: 30 MB/s de lectura, 20 MB/s de escritura
Dimensiones	77,9 mm x 21,9 mm x 12,0 mm
A prueba de agua/A prueba de polvo[9]	Certificado IP67
Temperatura de funcionamiento	0°C hasta 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: Habilitar, deshabilitar, modificar las características y el perfil del dispositivo. Logotipo conjunto. D500SM: Modificar el perfil del dispositivo. Logotipo conjunto.

Garantía/soporte técnico	D500S: Garantía de 5 años con soporte técnico gratuito D500SM: Garantía de 2 años con soporte técnico gratuito
Compatible con	Windows® 11, 10, macOS® 11.x – 14.x, Linux[10] Kernel 4.4+

Números De Pieza

Dispositivos serializados

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

Dispositivos serializados administrados

IKD500SM/8GB
IKD500SM/16GB

IKD500SM/32GB
IKD500SM/64GB
IKD500SM/128GB
IKD500SM/256GB
IKD500SM/512GB

Imagen Del Producto

* Parte de la capacidad indicada en un dispositivo de almacenamiento flash se emplea para formateo y otras funciones y, por tanto, no se encuentra disponible para el almacenamiento de datos. Por ese motivo, la capacidad de almacenamiento de datos real es inferior a la indicada en los productos. Para más información, consulte la Kingston's Guía de memoria Flash.

1. Consulte la especificación de la hoja de datos. El producto debe estar limpio y seco antes de ser utilizado.
2. Con certificación MIL-STD-810F para pruebas mecánicas de choque, vibración y caída.
3. El modo frase de contraseña no es compatible con Linux.
4. De fbi.gov: Martes técnico del FBI en Oregon (Oregon FBI Tech Tuesday): Construyendo una defensa digital con contraseñas, 18 de febrero de 2020
5. Teclado virtual: Solo es compatible con US English en Microsoft Windows y macOS.
6. Servicio de administración SafeConsole adquirido por separado
7. El producto debe estar limpio y seco antes de ser utilizado.
8. La velocidad puede variar dependiendo del hardware huésped, el software y el uso.
9. Con certificación IEC 60529 IPX8 a prueba de agua con la tapa puesta. El producto debe estar limpio y seco antes de ser utilizado.
10. El soporte a funciones en Linux es limitado. Consulte el manual del usuario para obtener más detalles. Ciertas distribuciones de Linux requerirán privilegios de superusuario (root) para ejecutar los comandos de IronKey correctamente en la ventana de la aplicación de la terminal.