
# Drive flash USB con crittografia hardware Kingston IronKey D500S

## Certificazione FIPS 140-3 di Livello 3 (in fase di approvazione), crittografia hardware XTS-AES a 256-bit. Guscio esterno in zinco rinforzato

---

Il drive flash USB migliore della categoria Kingston IronKey™ D500S/SM offre funzionalità di sicurezza di grado militare leader di mercato, che rendono la gamma IronKey il marchio più affidabile per la salvaguardia dei dati sensibili. Il drive include la certificazione FIPS 140-3 di Livello 3 (in fase di approvazione), con ulteriori miglioramenti di NIST, che richiedono upgrade dei microprocessori, per una maggiore sicurezza e protezione contro gli attacchi, con applicazioni governative e militari. I dati sono crittografati e decrittografati sul drive D500S, senza lasciare alcuna traccia sul sistema host. Unitamente alla crittografia hardware XTS-AES 256-bit, il drive include anche un guscio esterno in zinco rinforzato che è impermeabile[1], resistente alla polvere[1], a prova di vibrazioni e urti secondo standard di livello militare[2], resistente agli schiacciamenti e riempito con speciale resina epossidica, per proteggere i componenti interni contro i tentativi di penetrazione.

IronKey D500S rappresenta un elemento essenziale per garantire la conformità alle best practice DLP (Data Loss Protection), offrendo un elevato gradi di resistenza di grado militare, per garantire la conformità con leggi e regolamenti come CMMC, SOC2, NIS2, FISMA, GDPR, PIPEDA, HIPAA, HITECH, GLBA, SOX e CCPA oltre che TAA. Il drive D500S offre un maggior numero di funzionalità rispetto a qualunque altro drive della sua categoria. Ciò ne fa una soluzione di sicurezza all'avanguardia nel settore, per la protezione di dati riservati ad elevato valore.

Il drive D500S effettua un test automatico all'avvio, rilevando problemi associati a temperature o voltaggi eccessivi, che portano allo spegnimento automatico del dispositivo. Per raggiungere livelli di sicurezza ancora più elevati, il drive D500S integra un firmware con firma digitale che lo rende immune agli attacchi malware BadUSB. La protezione contro gli attacchi Brute Force è sempre attiva, per proteggere contro i tentativi di indovinare le password e, in caso di tentativi multipli di accesso con password errate, il drive effettua la cancellazione completa dei dati crittografati.

Il drive offre anche funzionalità multi-password per l'accesso ai dati, con supporto fino a tre password: Amministratore, utente, e password di ripristino monouso. L'amministratore può reimpostare una password Utente, ed è anche possibile generare una password di ripristino monouso per ripristinare l'accesso quando la password Utente va persa.

Il D500S supporta la tradizionale password complessa o la modalità passphrase[3]. Le frasi password possono avere una lunghezza compresa tra 10 e 128 caratteri. L'FBI raccomanda l'uso di password con parole multiple composte da 15 o più caratteri, in quando tale configurazione è più resistente e semplice da ricordare rispetto alle password complesse.[4]

Il drive D500S integra anche una doppia partizione nascosta, una prima assoluta del settore. La funzione consente all'Admin di creare due partizioni sicure personalizzate per account Admin e Utente, che consentono la creazione di un Archivio file nascosto disponibile per l'Utente secondo necessità. Quando si utilizzano sistemi considerati non sicuri, o quando si condivide il drive, l'Archivio file nascosto garantisce la sicurezza e l'invisibilità dei dati, a meno che non venga effettuato l'accesso secondo la corretta procedura.

Grazie a una speciale sequenza di tasti, l'Amministratore può inserire una password che attiva l'eliminazione crittografica dei dati contenuti nel drive, distruggendo i dati per sempre ed effettuando il reset del drive per evitare eventuali accessi non autorizzati in condizioni di sicurezza compromesse.

Per assistere gli utenti con problemi di tastiere, tutte le schermate di accesso password includono il simbolo di un occhio, che consente di visualizzare le password inserite, per evitare il rischio di inserimenti password errati. É anche disponibile una tastiera virtuale in lingua inglese[5], per proteggere l'inserimento della password da keylogger e screenlogger.

Il drive D500S supporta anche due livelli di modalità in sola lettura (protezione contro scrittura). Sia l'amministratore che l'utente possono impostare una sessione che utilizza la funzionalità di sola lettura, al fine di proteggere il drive contro malware o l'accesso su sistemi inaffidabili. L'amministratore può anche impostare una modalità di sola lettura globale, che imposta il drive in modalità di sola lettura fino a quando non viene effettuato un reset.

Il drive offre anche le elevate prestazioni del dual channel, senza alcun compromesso in termini di sicurezza. Il drive include un esclusivo numero seriale composto da 8 cifre che sono le stesse incise sul guscio esterno, con un codice a barre scansionabile, a fini di implementazione o di auditing del drive.

Il drive D500S offre numerose opzioni di personalizzazione, è conforme agli standard TAA/CMMC, ed è assemblato negli Stati Uniti.

### Versioni Managed

Ciò consente ai drive Kingston IronKey D500SM (M = Managed[6]) di effettuare la gestione e l'utilizzo del drive da postazione centralizzata, con la possibilità di gestire anche migliaia di drive parte di flotte governative o aziendali.

---

- Certificazione FIPS 140-3 di Livello 3 (in fase di approvazione), per un livello di sicurezza di livello militare ai vertici
- Opzione multipassword con modalità complessa/frase password

- Doppia partizione nascosta opzionale. Una prima assoluta nella sua categoria
- Password di attivazione cancellazione crittografica, in caso di sicurezza compromessa
- Guscio esterno in zinco rinforzato, per la massima protezione contro attacchi e tentativi di penetrazione, resistenza ad urti e vibrazione secondo standard di livello militare e resistente a polvere e acqua secondo lo standard IP67[7]
- Interfaccia utente intuitiva
- Funzionalità interamente personalizzabili
- Disponibile in versione Managed

# Caratteristiche Principali

- ## Drive USB con crittografia hardware di grado militare

  Crittografia XTS-AES a 256 bit con certificazione FIPS 140-3 di Livello 3 (in fase di approvazione) e upgrade con microprocessore sicuro, per una maggiore sicurezza. Protezioni integrate contro attacchi BadUSB e Brute Force. Nuovo test di autodiagnosi del drive in fase di avvio, che spegne automaticamente il drive quando raggiungono determinate soglie di temperatura o voltaggio.

- ## Opzione multipassword per il recupero dei dati

  Abilitare le password di amministratore, utente e di ripristino monouso. L'amministratore può reimpostare una password Utente e abilitare una password di ripristino monouso per ripristinare l'accesso Utente in caso di perdita della password Utente.

- ## Modalità complessa e frase password

  Scegliere tra modalità password complessa o frase password. Le frasi password possono essere composte da frasi intere o parole multiple, con una lunghezza compresa tra 10 e 128 caratteri che solo l'utente può ricordare. La funzione di visualizzazione password, rappresentata dall'icona a forma di occhio, consente di ridurre il rischio di inserimento password errate.

- ## Una prima assoluta. Doppia partizione nascosta opzionale

  L'amministratore può creare due doppie partizioni nascoste di dimensioni personalizzate. Una per l'amministratore e una per l'utente, generando un archivio file nascosto che consente di tenere i dati sicuri e invisibili, a meno che non venga effettuato l'accesso alla partizione. Le doppie partizioni nascoste offrono un livello aggiuntivo di sicurezza su sistemi non sicuri, oppure quando è necessaria la condivisione dei file.

- ## Password di cancellazione crittografica in caso di necessità

  La password di attivazione della funzione di cancellazione crittografica causa la cancellazione delle chiavi crittografiche, cancellando i dati per sempre ed effettuando il reset del drive.

- ## Modalità sola lettura (scrittura inibita) Global e Session

  Sia l'amministratore che l'utente possono impostare una sessione che utilizza la funzionalità di sola lettura, al fine di proteggere il drive contro malware o l'accesso su sistemi inaffidabili. L'amministratore può anche impostare una modalità di sola lettura globale, che imposta il drive in modalità di sola lettura fino a quando non viene effettuato un reset.

- ## Resistente guscio di protezione secondo lo standard IronKey

  Il guscio in zinco è resistente agli schiacciamenti e integra un riempimento in materiale epossidico che garantisce la massima resistenza ai tentativi di manomissione fisica. Certificato MIL-STD-810F per urti meccanici, vibrazioni e cadute. Certificazione IP67 di resistenza all'acqua[1] e alla polvere[1].

- ## Codice univoco di 8 cifre e codice a barre scansionabile

  Grande risparmio di tempo. È sufficiente leggere o effettuare la scansione del codice a barre durante l'uso, quando il drive viene restituito, nonché in occasione di eventuali audit dei dispositivi fisici.

- ## Interamente personalizzabile

  Abilitazione, disabilitazione, modifica di funzionalità e profilo del drive. Co-logo.

# Specifiche Tecniche

| | |
|---|---|
| Certificazioni chiave | FIPS 140-3 di Livello 3 (in corso di approvazione)<br>MIL-STD-810F<br>Certificazione di conformità TAA/CMMC. Assemblato negli Stati Uniti |
| Interfaccia | USB 3.2 Gen 1 |
| Capacità* | 8 GB, 16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB |
| Connettore | Type-A |
| Classe di velocità[8] | USB 3.2 Gen 1<br>8 GB - 128 GB: 260MB/s in lettura, 190MB/s in scrittura<br>256 GB: 240MB/s in lettura, 170MB/s in scrittura<br>512 GB: 310MB/s in lettura, 250MB/s in scrittura<br><br>USB 2.0<br>8 GB - 512 GB: 30 MB/s in lettura, 20 MB/s in scrittura |
| Dimensioni | 77,9 mm x 21,9 mm x 12,0 mm |
| Impermeabile/Resistente alla polvere[9] | Certificazione IP67 |
| Temperatura di esercizio | da 0°C a 50°C |
| Temperature di stoccaggio | da -20°C a 85°C |
| Compatibilità | USB 3.0/USB 3.1/USB 3.2 Gen 1 |
| Opzioni di personalizzazione | D500S: Abilitazione, disabilitazione, modifica di funzionalità e profilo del drive. Co-logo.<br>D500SM: Modifica del profilo del drive. Co-logo. |

| | |
|---|---|
| Garanzia/supporto | D500S: 5 anni di garanzia con servizio di supporto tecnico gratuito<br>D500SM: 2 anni di garanzia con servizio di supporto tecnico gratuito |
| Compatibile con | Windows® 11, 10, macOS® 11.x – 14.x, Linux[10] Kernel 4.4+ |

# Numeri Di Parte

## Drive Serialized

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

## Drive Serialized Managed

| |
|---|
| IKD500SM/8GB |
| IKD500SM/16GB |

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

# Immagine Del Prodotto


* Parte della capacità totale indicata per i dispositivi di storage Flash viene in realtà utilizzata per le funzioni di formattazione e altre funzioni. Tale spazio non è disponibile per la memorizzazione dei dati. La capacità reale di memorizzazione dati dell'unità è quindi inferiore a quella riportata sul prodotto. Per ulteriori informazioni, consultate la Guida alle Memorie Flash di Kingston, all'indirizzo web Flash Memory Guide.

1. Fare riferimento alle specifiche della scheda tecnica. Il prodotto deve essere pulito e asciutto prima dell'uso.
2. Certificato MIL-STD-810F per urti meccanici, vibrazioni e cadute.
3. La modalità "Passphrase" non è supportata sui sistemi Linux.
4. Da fbi.gov: Oregon FBI Tech Tuesday: Building a Digital Defence with Passwords, 18 febbraio 2020
5. Tastiera virtuale: Supporta esclusivamente la lingua inglese statunitense su piattaforme Microsoft Windows e MacOS.
6. Il servizio di gestione SafeConsole deve essere acquistato separatamente
7. Il prodotto deve essere pulito e asciutto prima dell'uso.
8. La velocità può variare in base all'hardware, al software e alla tipologia di utilizzo dell'host.
9. Certificazione di impermeabilità IEC 60529 IPX8 ottenuta con il coperchio chiuso. Il prodotto deve essere pulito e asciutto prima dell'uso.
10. La funzione ha un supporto limitato su piattaforme Linux. Fare riferimento alla guida utente per ulteriori informazioni. Su alcune distribuzioni di Linux l'esecuzione dei comandi di IronKey dalla finestra terminale dell'applicazione, richiede l'accesso con privilegi di super-user (root).