

Ogniqualvolta i vostri dipendenti utilizzano i loro drive in viaggio, portandosi a casa i loro dati, espongono la vostra azienda a potenziali rischi. Proteggete i dati sensibili standardizzando su un'unità flash USB IronKey™ Kingston® o su un SSD esterno crittografato hardware. Grazie alla possibilità di poter scegliere tra differenti modelli e capacità, è possibile trovare la soluzione adatta alle esigenze della vostra azienda, indipendentemente dal fatto che si tratti di sicurezza per i dati mobili, o di conformarsi ai regolamenti data at rest o alle direttive data-in-transit, nonché alle leggi, standard o regolamenti globali, come GDPR o CCPA.

Tutti i modelli della famiglia IronKey sono coperti da una garanzia di cinque anni (tre anni nel caso di IronKey Vault Privacy 80 ES e IronKey Keypad 200, due anni nel caso di IronKey D500SM), con servizio di supporto tecnico gratuito, unitamente alla leggendaria affidabilità che caratterizza i prodotti Kingston. Tutti i drive elencati nella sezione seguente sono dotati di crittografia hardware 100%, per rispettare le normative più rigide in materia di sicurezza. Per ulteriori informazioni, visitare kingston.com/ironkey



Descrizione riportata	Serie IronKey Vault Privacy 50	IronKey Vault Privacy 80 ES	Serie IronKey Keypad 200	IronKey D500S	IronKey S1000
Numero di parte	IKVP50/xxGB USB-A IKVP50C/xxGB USB-C ¹	IKVP80ES/xxGB	IKKP200/xxGB	IKD500S/xxGB Serialized IKD500SM/xxGB Managed	IKS1000B/xxGB Basic IKS1000E/xxGB Enterprise
Livello di sicurezza	Aziendale, mainstream	Aziendale, mainstream	Specifiche militari	Specifiche militari/Avanzate	Specifiche militari/ Leader di settore
Capacità ²	8-512GB	480-7.680GB	USB-A 8-256GB USB-C 8-512GB	8-512GB	4-128GB
Crittografia hardware con protocollo AES 256-bit	XTS	XTS	XTS	XTS	On Device Cryptochip + XTS
Certificazione FIPS ³	FIPS 197	FIPS 197	FIPS 140-3 Livello 3 (In sospenso)	FIPS 140-3 di Livello 3 (in corso di approvazione)	FIPS 140-2 Di livello 3
Supporto per password multiple	Ripristino One-Time/ Admin/User	Admin/User	Admin/User	Ripristino One-Time/Admin/ User	
Modalità frasi-password e lunghezza massima	✓ Fino a 64	✓ Fino a 64	✓ Fino a 15	✓ Fino a 128	✓ Fino a 255
Icona dell'occhio per mostrare password immessa	✓	✓			
Firmware firmato digitalmente	✓	✓	✓	✓	✓
Protezione contro Malware BadUSB	✓	✓	✓	✓	✓
"Protezione contro gli	✓	✓	✓	✓	✓
Conforme agli standard TAA	✓	✓		✓	✓
Predisposta per il regolamento GDPR ⁹	✓	✓	✓	✓	✓
Accesso in sola lettura	✓	✓	✓	✓	✓
Protezione antimanomissione		Microprocessore sicuro certificato CC EAL5+	✓ Materiale epossidico	✓ Rivestimento in materiale epossidico	✓ Rivestimento in materiale epossidico
Doppia partizione nascosta				✓	
Password di attivazione cancellazione crittografica	✓			✓	
Impermeabile/Resistente alla polvere ⁴	IPx8		IP68	IP67, MIL-STD-810F	MIL-STD-810F
Opzioni di personalizzazione ⁵	✓		Co-Logo	✓	
Tastiera virtuale	Windows® e macOS®	Touch Screen		Windows® and macOS®	Windows® only
Opzione di gestione Enterprise	Local Management Option for Small/Medium Businesses			✓ D500SM (SafeConsole)	✓ S1000E (SafeConsole)
PID personalizzato - Endpoint / Compatibile DLP	✓			✓	
Materiale del guscio	Alluminio anodizzato	Zinco e plastica	Alluminio anodizzato	Zinco	Alluminio anodizzato
Interfaccia USB	USB 3.2 Gen 1	USB 3.2 Gen 1 External SSD	USB 3.2 Gen 1	USB 3.2 Gen 1	USB 3.1 Gen 1
Sistemi operativi supportati					
Windows® 11, 10	✓	✓ Indipendente dal SO	✓ Indipendente dal SO	✓	✓
macOS® 11.x - 14.x	✓	✓ Indipendente dal SO	✓ Indipendente dal SO	✓	✓
Linux Kernel® v4.4+		✓ Indipendente dal SO	✓ Indipendente dal SO	✓ ⁷	✓ ⁸

1 I nomi USB Type-C® e USB-C® sono marchi commerciali registrati di USB Implementers Forum.

2 Parte della capacità totale indicata per i dispositivi di storage Flash viene in realtà utilizzata per le funzioni di formattazione e per altre funzioni, e quindi tale spazio non è disponibile per la memorizzazione dei dati. Per ulteriori informazioni, consultare la Guida alle Memorie Flash di Kingston, all'indirizzo web: kingston.com/flashguide.

3 Conformità allo standard FIPS (Federal Information Processing Standards) 140-2: "Requisiti di sicurezza per i moduli crittografici". Per ulteriori informazioni, visitare il sito <http://csrc.nist.gov/publications/PubsFIPS.html>.

4 Certificazione di impermeabilità IEC 60529 ottenuta con il coperchio chiuso. Il prodotto deve essere pulito e asciutto

prima dell'uso.

5 Per ulteriori informazioni, visitare la pagina kingston.com/ironkey.

6 I comandi Linux supportano solamente i processori Intel e AMD di tipo i386/x86_64 - Funzionalità limitate.

7 IKD500S e IKD500SM: Supporto per i sistemi operativi Linux a 32-bit e 64-bit. Funzionalità limitate.

8 IKS1000B e IKS1000E: Supporto per il sistema operativo Linux a 32-bit (e 64-bit, se aggiornato al software v6.x.x). Funzionalità limitate.

9 La crittografia può essere parte integrante di un programma GDPR, ma non garantisce la conformità al regolamento GDPR.



IL PRESENTE DOCUMENTO È SOGGETTO A MODIFICHE SENZA PREAVVISO.

©2024 Kingston Technology Europe Co LLP e Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Regno Unito. Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469.

Tutti i diritti riservati. Tutti i marchi e i marchi registrati sono proprietà dei rispettivi titolari. MKF-501.19 IT