Kingston IronKey Hardware-Encrypted Drives - Security Solutions
Manage mobile data threats and reduce risks

Your company is at risk whenever employees use their own drives to travel with data and take work home. Protect sensitive data by standardising on a hardware-encrypted Kingston® IronKey™ USB flash drive or external SSD. With several models and capacities to choose from, there's one that's ideal for your company's needs, whether you're looking for mobile data security or have to comply with data-at-rest or data-in-transit directives, laws, standards or global regulations, such as GDPR or CCPA.

All IronKey drives are covered by a five-year warranty (IronKey Keypad 200 and IronKey Vault Privacy 80 ES have a three-year warranty), free technical support and legendary Kingston reliability. All drives below are 100% encrypted to meet the strictest security policies. For more information, go to **kingston.com/encryptedsecurity**

Featured Description	IronKey Vault Privacy 50	IronKey Vault Privacy 80 ES	IronKey Keypad 200	DataTraveler 4000G2	IronKey D300S	IronKey S1000
Part Number	IKVP50/xxxGB USB-A IKVP50C/xxxGB USB-C®[1]	IKVP80ES/xxGB	IKKP200/xxGB	DT4000G2DM/xxGB Optionally Managed	IKD300S/xxGB Standard IKD300SM/xxGB Managed	IKS1000B/xxGB Basic IKS1000E/xxGB Enterprise
Security Level	Enterprise Mainstream	Small/Medium Business Mainstream	Military Grade	Military Grade	Military Grade/Enhanced	Military Grade/Best-in-Class
Capacities[2]	8-256GB	480-1,920GB	8-128GB	8-128GB	8-128GB	4-128GB
256-bit AES Hardware Encryption Mode	XTS	XTS	XTS	XTS	XTS	On Device Cryptochip + XTS
FIPS Validated[3]	FIPS 197	FIPS 197	FIPS 140-3 Level 3 (Pending)	FIPS 140-2 Level 3	FIPS 140-2 Level 3	FIPS 140-2 Level 3
Multi-Password Support	Admin/User/One-Time Recovery	Admin/User	Admin/User			
Passphrase Mode and Max Length	√ Up to 64	√ Up to 64	√ Up to 15			√ Up to 255
Eye Symbol to See Password Entry	√	√				
Digitally Signed Firmware	√	√	√	√	√	√
BadUSB Malware Protection	√	√	√	√	√	√
Brute-Force Password Attack Protection	√	√	√	√	√	√
TAA-Compliant	√	√		√	√	√
GDPR Ready[9]	√	√	√	√	√	√
Ready Only Access	√	√	√	√	√	√
Tamper Protection		CC EAL5+ certified secure microprocessor	√ Epoxy	√ Epoxy	√ Epoxy Filled	√ Epoxy Filled
Waterproof[4]	up to 4 ft		up to 3 ft	up to 4 ft	up to 4 ft	up to 3 ft
Customizable Options[5]	√			√	√	
Virtual Keyboard	Windows® and macOS®	Touch Screen			Windows® only	Windows® only
Enterprise Management Option	Local Management Option for Small/Medium Businesses			Optional Management (SafeConsole)	√ D300SM (SafeConsole)	√ S1000E (SafeConsole)
Custom PID - Endpoint / DLP Compatible	√			√	√	
Case Material	Anodised Aluminium	Zinc and plastic	Anodised Aluminium	Titanium-Coated Stainless Steel	Zinc	Anodised Aluminium
USB Interface	USB 3.2 Gen 1	USB 3.2 Gen 1 External SSD	USB 3.2 Gen 1	USB 3.1 Gen 1	USB 3.1 Gen 1	USB 3.1 Gen 1
Operating Systems Supported						
Windows® 11, 10	√	√ OS Independent	√ OS Independent	√	√	√
macOS® 10.15x - 13.x	√	√ OS Independent	√ OS Independent	√	√	√[10]
Linux Kernel[6] v4.4+		√ OS Independent	√ OS Independent		√[7,8]	√[8]

1. USB Type-C® and USB-C® are registered trademarks of USB Implementers Forum.
2. Some of the listed capacity on a Flash storage device is used for formatting and other functions and is thus not available for data storage. For more information, visit the Memory Guide at kingston.com/flashguide.
3. Federal Information Processing Standards (FIPS) 140-2: "Security Requirements for Cryptographic Modules". For more information, visit http://csrc.nist.gov/publications/PubsFIPS.html.
4. S1000 conforms to MIL-STD-810F, IKKP200 conforms to IP57, all other drives conform to IEC 60529 IPX8.

Product must be clean and dry before use.
5. For more information, visit kingston.com/usb/encrypted_security.
6. Linux commands support i386/x86_64 Intel and AMD-based processors only – limited features.
7. DTVP30 / IKD300S: Linux 32-bit and 64-bit OS support. Limited features, for more information visit kingston.com/usb/encrypted_security.
8. IKD300SM and IKS1000B Linux 32-bit and 64-bit OS support / IKS1000E: Linux 32-bit OS support. Limited features.
9. Encryption can be part of a GDPR programme but does not ensure GDPR compliance.
10. macOS® 13.x-Unterstützung im 1Q-2023.