KINGSTON IRONKEY

Hardware-Encrypted USB Drives for Government TAA and CMMC Compliance

Strict military-grade data security is an absolute must for compliance with requirements such as TAA and CMMC (Cybersecurity Maturity Model Certification), along with NIST's latest FIPS 140-3 Level 3 certification.

Kingston IronKey is the world's largest manufacturer of hardware-encrypted USB drives.

IronKey Flash drives use the strongest AES 256-bit hardware encryption in XTS mode and select drives comply with the latest FIPS 140 series certifications as well as NIST SP 800-171.

TAA and CMMC Compliant Drives for US Government / Military Procurement

IronKey D500S and S1000 series flagship drives are assembled in the US and are TAA and CMMC compliant – including drive firmware, software, secure microprocessor, printed circuit board (PCB) assembly, and final drive assembly and testing.

Hardware-Encrypted Storage Options for Government Data Protection

IronKey D500S and S1000 series drives safeguard important data with FIPS 140-3 Level 3 (Pending, D500S series) and FIPS 140-2 Level 3 (S1000) certifications with XTS-AES 256-bit always-on hardware encryption. Additionally, they have built-in protections against Brute Force password attacks to crypto-erase the data forever if the drive is under attack, as well as BadUSB protection with digitally-signed firmware.

The drives are filled with NIST lab tested and approved epoxy to dramatically increase tamper resistance and affect an attacker's ability to separately attack the drive's semiconductor encryption and storage components.

Is your data a soft target?

Only best-in-class hardware encryption gives your data the defense it deserves.

Learn more about Kingston IronKey at **kingston.com/IronKey**

more ⟩⟩

Read-Only Settings

Avoid malware attacks with a forced Read-Only mode upon drive login.

Customization Options

IronKey D500S drives can be fully customized to set a custom PID value for endpoint security protection or modify complex password lengths and number of attempts before a crypto-erase happens. Many drive features can also be modified to custom requirements or can be disabled.

IronKey D500S and S1000B drives have the same 8-digit serial number and bar code on the case and internally, making it the easiest in the market for asset tracking.

The following table describes the available drives:

	IronKey D500S (new in 2023)	IronKey S1000B
Drive (Part number)	(IKD500S/xxGB)	(IKS1000B/xxGB)
Description	XTS-AES 256-bit hardware encryption with newest FIPS 140-3 Level 3 (Pending) military-grade certification. Multi-password option (Admin, User, One-Time Reset), Complex or Passphrase mode, Crypto-Erase password, and Dual Hidden Partition options.	XTS-AES 256-bit hardware encryption with FIPS 140-2 Level 3 military-grade certification. Includes a crypto-chip with strong built-in attack protections and fast microSSD storage.
Compliance	• TAA • CMMC compliant from firmware, software, PCB assembly, secure microprocessor, drive assembly and testing • COO USA (Assembled in California) • Data breach mitigation fix in Risk Management Framework • NIST SP 800-171	• TAA • CMMC compliant from firmware, software, PCB assembly, secure microprocessor, drive assembly and testing • COO USA (Assembled in California) • Data breach mitigation fix in Risk Management Framework • NIST SP 800-171
Compatible OS	Windows®, macOS®, Linux	Windows®, macOS®, Linux
Capacities[3]	8GB – 256GB (512GB in 3Q2023)	4GB –128GB
Customizable?	Yes – contact Kingston for options. New features can be disabled or customized for special requirements.	Limited. This drive was built to US government and military standards by IronKey and continues to be built as it was designed: a best-in-class encrypted drive.

#KingstonIsWithYou

KINGSTON IRONKEY™