

## Secured by SPYRUS™ USB Encryption Devices

Secured by SPYRUS™ USB encryption devices—the Hydra PC™ Personal Encryption Device, the Hydra PC Digital Attaché, and the Kingston DataTraveler 5000—include features to meet a wide range of requirements. See for yourself:



Hydra PC Standard Case with miniSD or microSD Card



Hydra PC Compact Case with microSD Card



Kingston Data Traveler 5000 Secured by SPYRUS™

Feature	Personal Encryption Device	Digital Attaché	Kingston DataTraveler 5000
On-board, hardware-based encryption using a Federal Information Standards Publication (FIPS PUB) 140-2 compliant cryptographic module.	FIPS 140-2 Level 3 on-board, hardware-based file encryption is compliant (certificate #1179).  NSA approved for protecting tactical data at the SECRET level.	FIPS 140-2 Level 3 on-board, hardware-based file encryption & sector-encryption is compliant (certificate #1179, 1215 & 1255).	DT5000 FIPS 140-2 Level 2 on-board, hardware-based sector encryption is compliant (certificate #1215). Level 3 pending.  Kingston DT5000 Secured by SPYRUS: FIPS 140-2 Level 2 (certificate #1227 & 1255). Level 3 pending
Random Number Generator follows NIST SP 800-90 and FIPS 140-2 standards and supports the key size used for Advanced Encryption standard (AES).	RNG meets NIST SP 800-90 (FIPS certificate #3) and FIPS 140-2 standards, and uses FIPS 140-2 key sizes for AES-128/192/256.	RNG meets NIST SP 800-90 (FIPS certificate #3) and FIPS 140-2 standards, and uses FIPS 140-2 key sizes for AES-128/192/256.	RNG meets NIST SP 800-90 (FIPS certificate #10) and FIPS 140-2 standards, and uses FIPS 140-2 key sizes for AES-128/192/256.
AES data encryption algorithm supports 128, 192, or 256-bit key sizes.	Implemented per NIST algorithm certificates 846, 850, & 858. Supports AES-128/192/256 in ECB, CBC, and CTR modes. CBC mode used for all file encryption operations.	Implemented per NIST algorithm certificates 846, 850, & 858. Supports AES-128/192/256 in ECB, CBC, and CTR modes. CBC mode used for all file encryption operations. SP 800-38E XTS-AES mode used for sector-based media encryption.	Implemented per NIST algorithm certificates 1015 & 1016. Supports SP 800-38E XTS-AES-256 mode for sector-based media encryption.

Meets FIPS 140-2 and FIPS PUB 197 and NIST SP 800-38A or E.	Meets Suite B, FIPS 140-2/FIPS PUB 197, and NIST SP 800-38A.	Meets Suite B, FIPS 140-2/FIPS PUB 197, NIST SP 800-38A and SP 800-38E.	Meets Suite B, FIPS 140-2/FIPS PUB 197, and NIST SP 800-38E.
Strong password policy includes ability to require a combination of uppercase letters, lowercase letters, and special characters, including at least one of each, and minimum password character length.	Supports ability to set password complexity policy to require 3 of 4 character options (uppercase, lowercase, numeric, and special) and minimum password length.	Supports ability to set password complexity policy to require 3 of 4 character options (uppercase, lowercase, numeric, and special) and minimum password length.	Supports ability to set password complexity policy to require 3 of 4 character options (uppercase, lowercase, numeric, and special) and minimum password length.
Firmware updates are digitally signed and verified.	Supports digitally signed firmware updates using Suite B SHA-384 (algorithm certificates #837 & 852) and ECDSA P-384 (algorithm certificates #96 & 97).	Supports digitally signed firmware updates using Suite B SHA-384 (algorithm certificates #837 & 852) and ECDSA P-384.	Supports digitally signed firmware updates using Suite B SHA-384 (algorithm certificates #972 & 973) and ECDSA P-384 (algorithm certificate #122).
On-board antivirus scanning	Available	Available	Call for availability



## SPYRUS, Inc.

For additional details about SPYRUS products, visit [www.spyrus.com](http://www.spyrus.com) or contact us at:

▲ USA +1 408 392-9131 [info@spyrus.com](mailto:info@spyrus.com)

▲ Australia +61 7 3220-1133 [info@spyrus.com.au](mailto:info@spyrus.com.au)

