

Hydra Privacy card[®] Personal Encryption Device

Designed For Secure Storage and Transfer of Confidential Information

Like A Bank Vault In Your Pocket

The Hydra Privacy Card[®] Personal Encryption Device (PED) is much more than an encrypting USB flash drive. Encrypted files can be stored anywhere, not just on the device.

Think of a vault with individual safe deposit boxes. Even if safecrackers forced open the vault, they would still have to break into each box, one at a time. Like a bank vault, PED provides secure hardware-based protection and encrypts each file using a unique key.

Mandatory file encryption makes PED ideal for organizations with regulatory requirements to protect personally identifiable or mission-critical information, such as financial, healthcare, and government.

Features and Benefits

- Secure USB encryption device.
- Store encrypted data anywhere—on the device, on a server, or in the cloud.
- Infinite storage capacity—uses replaceable microSD card for the lowest cost per GB.
- Data Containment—Even with the correct password, users cannot decrypt files encrypted by the PED unless it is connected to an authorized computer.
- Prohibit writing to rogue devices to prevent data leakage.

- Keys are generated in the device and never exported or escrowed.
- Quorum technology reconstitutes keys as required—they are not stored anywhere.
- Implements Suite B cryptography, an interoperable cryptographic base for both unclassified information and most classified information.
- Files are automatically hashed, compressed, encrypted, sealed, and digitally signed to provide nonrepudiation assurance and protect data integrity by detecting cipher text or plaintext modifications.



Technical Specifications

Capacities*

Entombed 2GB, 4GB, 8GB, 16GB, 32GB

Replaceable standard or SDHC microSD cards for infinite capacity

File Encrypt/Seal/Decrypt/Verify Speed

Up to 1.8MB per second

Dimensions

3.2 x 0.5 x 0.9 inches

Custom design and packaging available, including raw epoxied PC board

Weight

.8 oz (22 grams)

Temperature

Operating: -20°C, +65°C

Storage: -40 °C, +85 °C

Interface

USB 2.0 high speed

Operating System Compatibility*

Windows 2000 SP4

Windows XP SP2+

Windows Vista

Windows 7 32 bit and 64-bit

Security

Multiple individually validated FIPS 140-2 Level 3 security boundaries create a flexible and extensible architecture allowing continuous technology upgrades.

Cryptographic operating system (SPYCOS®)

File encryption

Manageability

Can be managed by the SPYRUS Enterprise Management System (SEMS)

Encryption — Suite B onboard*

File: AES CBC 256 bit

Encryption Keys: 256-bit hardware

Secure Channel: ECDH P-384 and AES 256

PKI Signing: ECDSA P-521 and lower

Hashing: SHA-384

Standards Compliance

FIPS PUB 46 Data Encryption Standard

FIPS PUB 180-2 Secure Hash Algorithm Standard

FIPS PUB 197 Advanced Encryption Standard

SP 800-38A and 800-38E Modes of Operation

SP 800-56A Key Establishment Guidelines

SP 800-90 Random Number Generation

Available from resellers worldwide.

For more information about SPYRUS products, visit www.spyrus.com or contact us by email or phone.



* Dependent on model and case option

Corporate Headquarters

1860 Hartog Drive
San Jose, CA 95131-2203
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@SPYRUS.com

East Coast Office

+1 (732) 329-6006 phone
+1 (732) 832-0123 fax

UK Office

+44 (0) 113 8800494

Australia Office

Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phone
+61 7 3220-2233 fax
www.spyrus.com.au