

Hydra Privacy card® Digital Attaché

Designed For Secure Storage, Transfer and Sharing of Information

Like A Bank Vault In Your Pocket

The Hydra Privacy Card Digital Attaché (DA) is much more than an encrypting USB flash drive. Files can be encrypted and stored anywhere, not just on the device.

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

Digital Attaché Features and Benefits

- Secure USB encryption device, true smart card PKI token, key generator, and encryption engine.
- Encrypt and store 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.
- Exchange Hydra PC Sharing Certificates to securely share files or partitions.
- Data Containment—Even with the correct password, users can unlock or decrypt files encrypted by the DA only when it is connected to an authorized computer.
- Prohibit rogue device connection 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.
- A customer-provisioned Recovery Agent enables data decryption if the device or password is lost.
- Implements Suite B cryptography, an interoperable cryptographic base for both unclassified information and most classified information.
- Smart card PKI functionality—generate key pairs, store certificates, sign emails, and enable strong two-factor authentication.
- Compatible with industry-standard smart card log-on protocols, S/MIME secure email technology, and Web-based SSL/TLS with mutual authentication.
- SPYRUS Enterprise Management System (SEMS) provides complete lifecycle management including provisioning, remote disable/enable, and remote kill.



Unlike Any Other Encryption and Storage Device

Encrypted files can be stored anywhere, but the DA also offers local storage on removable microSD memory cards. Each card can be formatted with one or two independent partitions, and a partition can be either unencrypted or protected with hardware-based XTS-AES 256-bit full disk encryption. Each encrypted partition can be configured with different sharing lists with Hydra PC Sharing Certificates, described below.

Files in an encrypted partition can be opened, modified, and saved transparently. Large databases and files stay secure without decrypting and re-encrypting the entire file each time a single record is accessed.

DA also supports individual file encryption, protecting each encrypted file with a unique AES 256 bit encryption key no matter where it is stored. Encrypted files are hashed, compressed, encrypted, timestamped, and digitally signed to provide nonrepudiation assurance and to enforce data integrity by detecting modifications to the plaintext or ciphertext.

Authorized users can export a Hydra PC Sharing Certificate from their own Digital Attachés and optionally sign them with a personal or corporate certificate, government issued CAC, or PIV card.

When an encrypted partition or file is created, the user can embed any number of Hydra PC Sharing Certificates for secure distribution. Only users with embedded certificates can decrypt the file or partition. All other users are denied access.

A security administrator can provision a Recovery Agent for one or more Digital Attaché devices, whose sharing certificate is automatically embedded in every encrypted file or partition. If a device is lost or stolen or if the user forgets their password, the information can be recovered with the Recovery Agent.



Technical Specifications

Capacities

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

Replaceable standard or SDHC microSD cards for infinite capacity

Speed (dependent on microSD card)

Up to 20MB per second read

Up to 10MB per second write

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

Windows 8.0, 8.1



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®)

Sector-based encryption

File encryption

Manageability

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

Encryption—US Department of Defense-approved Suite B cryptography

Sector (FDE): XTS-AES 256 bit

File: AES CBC 256 bit

Encryption Keys: XTS AES 256-bit hardware

Secure Channel: ECDH P-384 and XTS AES 256-bit

PKI Signing: ECDSA P-521 and lower

Hashing: SHA-384

Standards Compliance

Microsoft CryptoAPI, Microsoft Card Module, and PKCS #11 interoperability

FIPS PUB 46 Data Encryption Standard

FIPS PUB 180-2 Secure Hash Algorithm Standard

FIPS PUB 186-2 Digital Signature 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

SP800-38E XTS-AES Media Encryption

Available from resellers worldwide.

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

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