



Hydra Privacy Card® Digital Attaché

Authentication, Encryption, Storage, and Secure Information Sharing

The Hydra Privacy Card® (Hydra PC™) Series II family of USB encryption devices are the world's first to implement Suite B cryptography, an interoperable cryptographic base for both unclassified information and most classified information.

Unlike encrypting USB flash drives from any other company, Hydra PC devices can store files on removable microSD memory cards, and they can also encrypt and safely store files anywhere.

Because the microSD storage cards are outside of the device's security boundary, any card can be used. If you run out of storage space, buy another card anywhere and use the Hydra PC to erase and format it.

The Hydra PC Digital Attaché can format memory cards with one or two independent partitions. A partition can be either unencrypted or protected with hardware-based XTS-AES 256-bit full disk encryption. Each encrypted partition can be shared with other Digital Attaché users by exchanging Hydra PC Sharing Certificates.

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.

Digital Attaché also supports individual file encryption, protecting each encrypted file with a unique key, no matter where it is stored.

The Hydra PC Digital Attaché allows encrypted files to be stored on the device, the host computer's hard drive, or shared with other authorized recipients via e-mail or by posting on an FTP site anywhere in the world, with complete security.

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 (see the illustration on page 3).

Digital Attaché is uniquely suited to a wide range of applications where the ability to share information securely while preserving integrity and nonrepudiation is vitally important. Such applications include collecting and sharing intelligence and law enforcement information; preserving and authenticating the chain of custody for forensic data, including video surveillance data; protecting electronic health records and personal health information; and maintaining strict confidentiality and integrity of audit data.

Encrypt Files and Store Them Anywhere

The file encryption supported by Digital Attaché provides superior confidentiality for sensitive information through the use of the strongest unclassified private key and symmetric algorithms approved by the US Government, including elliptic curve cryptography (ECC) with key sizes up to P-521 for key wrapping, together with AES-256 symmetric



encryption. These algorithms and key sizes are conservatively estimated to be sufficient to resist cryptanalysis for 170+ years, against all known attacks.

For many applications, assuring the integrity and the nonrepudiation of data origin is even more important than the confidentiality of the data.

For this reason, Digital Attaché hashes the plaintext of the file before compressing and then encrypting the data. At the same time a block of data is being encrypted, a hash of the resulting ciphertext is calculated, even before the data is written out. When the end of the file is reached, both the plaintext and ciphertext hash values are digitally signed, using the user's private ECDSA digital signature key.

When the file is decrypted, the ciphertext hash and digital signature are first verified. Any change detected prevents the file from being decrypted. Likewise, if the plaintext hash does not validate correctly, an error is raised and the decrypted file is not presented to the user.

The fact that the ciphertext is hashed and signed provides another valuable benefit. By rehashing the file and verifying the ciphertext hash against the digital signature, the integrity of the encrypted file can be guaranteed without having to decrypt it. If files are archived at a local site and also at an off-site repository somewhere, no one at either the local or off-site repository could access the file contents without authorization, yet it would be a simple matter to prepare a manifest of all of the files and the digital signatures, and compare the two manifests to ensure that all files are present and that no undetected file corruption has occurred.

Encrypted files can safely be stored anywhere, including public file servers, because they cannot be decrypted without an authorized Digital Attaché. Each encrypted file can be configured with different sharing lists using Hydra PC Sharing Certificates.

Sector-Based Full Disk Encryption

In addition to individual file encryption, the Digital Attaché provides hardware-based, sector-by-sector full disk encryption to data stored on the removable

microSD memory card. This means that all data on the card, including potentially sensitive file names and other metadata, is encrypted at all times.

Each memory 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. 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.

The unencrypted partition can be used just like a conventional USB flash drive and works on almost any computer with a USB port.

Digital Attaché uses the more advanced XTS-AES mode of operation to perform sector-by-sector encryption, using what amounts to double encryption with two keys. An encrypted "tweak" that involves the sector number is computed and then incremented for each block of ciphertext. This mode provides better security than simple ECB mode, and unlike the CBC mode, it protects against attempts to move the contents to a different sector, where a different user might have access.

Secure Data Sharing

Whether stored on the device, on a hard drive, or on the Internet, files to be shared are encrypted using a unique key, and that key is then encrypted (wrapped) with a key encryption key. This wrapping key is derived from the originator's and each recipient's public/private key pair, using an EC Diffie-Hellman key agreement.

As opposed to other USB encryption devices that use a much weaker RSA-2048 key, with an effective key strength of only 112 bits, to wrap an AES-256 key, the ECC keys used within Digital Attaché are well matched to the AES key sizes used.

The user's encryption and digital signature keys are conveyed securely in a Hydra PC Sharing Certificate that includes the Digital Attaché's serial number.

The sharing certificate optionally can include the user's legacy X.509 encryption and signature

certificates, and can be signed with the user's legacy signature key; e.g., RSA. The legacy certificates can come from a government-issued CAC or PIV card.

The authenticity of the user's legacy certificates can be verified back to a trusted root, using conventional PKI path-validation procedures.

Although those legacy keys are not nearly as strong as the ECC keys used within the Digital Attaché, they are strong enough to validate the originating user's identity at the time the file is received, thereby providing nonrepudiation of origin of the file. Only the user who possesses the Digital Attaché and knows the password necessary to log on could have digitally signed the file.

Hydra PC Sharing Certificates also can be embedded within encrypted partitions, allowing Digital Attaché users to securely share the removable memory card with a designated list of known and authenticated Digital Attaché devices. The memory card will not work in an undesignated Digital Attaché, even if the user knows the correct password.

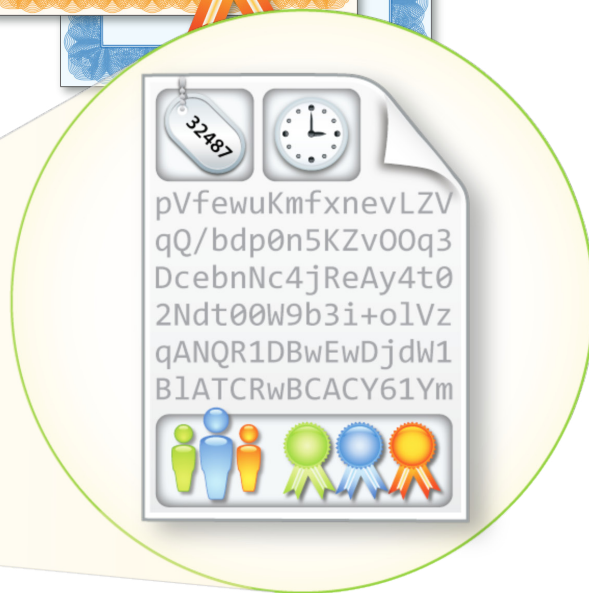
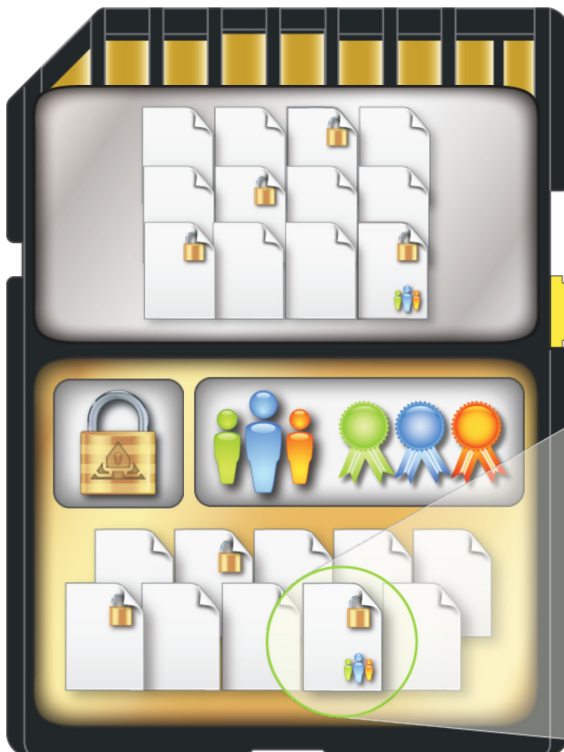
Organizations worried about data recovery if a device is lost or stolen or if the user forgets their password can provision a *Recovery Agent*.

Every time a file or memory card partition is encrypted, the recovery agent's Hydra PC Sharing Certificate is automatically embedded. The Recovery Agent can then decrypt the files or partitions, even if the encrypting Digital Attaché is lost, stolen, or destroyed. The Recovery Agent should be set up to require two-person control and kept securely locked in a safe or vault.

Data Containment



Secure Data Recovery



Recent surveys indicate that the greatest threat of data compromise in an organization comes from insiders with legitimate access to data, who then expose the data without permission. The latest example of this is the WikiLeaks release of thousands of pages of classified information.

Digital Attaché offers numerous options for limiting access to only those users with a specific need for specific data or to specific devices.

An exclusive feature of SPYRUS Hydra PC devices is the Enclave Authentication Value (EAV). The EAV is used to lock a Digital Attaché to an explicitly designated enclave of one or more computers. The Digital Attaché cannot be used in computers that are outside the secure enclave, even if the user knows the logon password.

This provides a further level of protection in a hostile environment. Even if the user is captured and forced to divulge the password, an attacker would still have no access to the Enclave Authentication Value, and without it the device cannot be used outside of the enclave, even with the correct password.

At some point, encrypted data must be decrypted so that it can be used. Once data is decrypted, it could intentionally or unintentionally be compromised by an authorized user.

Hydra PC software protects against this vulnerability by blocking read and write access to removable USB and FireWire storage devices that use a disk file system. This prevents unauthorized file copying to or from the blocked drives.

The Digital Attaché is also available with active antivirus protection. Files are scanned while being encrypted or decrypted, or are being moved on or off of the device.

More Digital Attaché Features

The cryptographic core of every Digital Attaché is the SPYRUS Rosetta micro smart card chip. This allows the Digital Attaché to function as a PKI security device in addition to being an encryption and storage device.

Smart card functionality can safeguard a user's Windows logon password and the private keys associated with digital certificates, as well as providing very strong file and media encryption directly.

The Digital Attaché is compatible with industry-standard smart card logon protocols, S/MIME secure e-mail technology, and Web-based SSL/TLS with mutual authentication. It also can provide two-factor authentication for various full disk encryption programs for the computer's hard drive.

Information stored on the device, such as digital certificates and encrypted files, require a password for access. After 10 incorrect password entries, access is blocked and the keys are zeroized.

At no time is the user's password stored within the Digital Attaché or in the supporting software, not even in encrypted or hashed form. For that reason, even if device was subjected to the most sophisticated national-laboratory chip-peeling attack in an attempt to mount an exhaustive search attack, it would never be successful.

Furthermore, keys or other critical security parameters are never stored in plaintext form within the Digital Attaché. Instead, all keys are encrypted with AES-256, using a Master Key Encryption Key (MKEK).

The MKEK itself is not stored on the chip but is instead reconstituted using a sophisticated K-out-of-N secret-sharing algorithm based on a hash of the user's password, the EAV, and other internal parameters. As a result, once the Digital Attaché user logs off or the token is powered down or removed, the device is completely inert.

Device Management

Every Hydra PC device order includes basic device management software that allows administration operations such as initialization and key management to be restricted to designated personnel for better control in large organizations.

Central management features for enterprise networks include remote software installation,

remote enclave and recovery agent management, and remote administration of policy settings such as event logging and certificate validation.

But sometimes basic device management is not enough. Even loyal employees sometimes forget about security and carelessly leave their devices or device passwords exposed and unattended, and a more advanced management system is required.

The SPYRUS Enterprise Management System (SEMS) was designed using the same next-generation cryptographic algorithms as the Digital Attaché. It minimizes the threat to your organization through secure device management that actively controls devices remotely across an intranet or the Internet. It implements complete device lifecycle management, allowing you to provision, assign, enable/disable, and terminate devices.

Hardware security modules are used to implement PKI, server, and administrator authentication to combat both external and internal threats.

The SEMS system incorporates an open API that allows the management of USB encryption devices from other vendors. The API is provided as part of the SEMS software development kit, which includes sample source code, examples, required resources, and documentation. This API uniquely positions the SPYRUS SEMS system as one of the few products on the market to allow this type of third-party integration.

Vendors can use their own proprietary techniques to implement internal device operations without exposing their proprietary architecture.

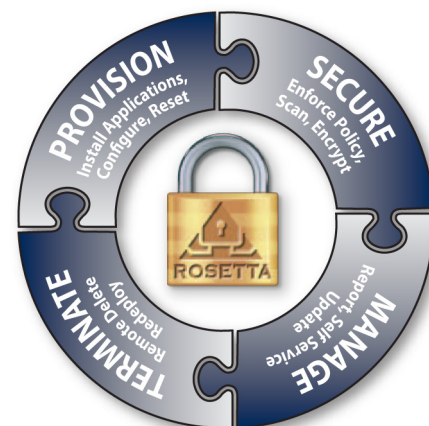
SEMS software is sold separately.

Features and Benefits Summary

- ▲ **Secure** USB encryption device, true smart card PKI security device, 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 Digital Attaché 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 **never 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 email, and enable strong authentication.
- ▲ Compatible with industry-standard smart card logon protocols, S/MIME secure email technology, and Web-based SSL/TLS with mutual authentication.
- ▲ Optional Sentry A-V **active anti-malware** delivers real-time protection to stop malware and worms in their tracks.
- ▲ SPYRUS Enterprise Management System (SEMS) provides complete lifecycle management including provisioning, remote disable/enable, and remote termination.



Why Hardware-Based Encryption is Stronger

Hardware-based encryption sets Hydra PC apart from other encryption solutions that manage encryption operations within software. Why is hardware-based encryption on Hydra PC stronger? Take a look:

- ▲ Hydra PC uses Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES), the strongest available key-generation and encryption algorithms available to the public. These algorithms and key sizes are much stronger than the National Institute of Standards and Technology (NIST) requires for the next 25 years—strong enough to be used for classified information. Even if the computer’s operating system does not yet support advanced algorithms, Hydra PC does.
- ▲ Encryption keys are generated and stored in encrypted form on the Hydra PC and not on the computer. Even if your laptop is lost or stolen,

files encrypted with Hydra PC are completely safe.

- ▲ Access to the Hydra PC requires up to three levels of authentication. Users must have the Hydra PC and know the password. An optional authentication level restricts Hydra PC use to authorized computers. Single factor solutions, which require only a password (and use it as the encryption key) are vulnerable to brute-force attacks.
- ▲ The hardware is programmed to destroy the encryption keys and prevent access to protected files after 10 incorrect password entries. This prevents entry by brute-force attack.
- ▲ The tamper-resistant hardware design protects keys and encrypted files from reverse engineering attacks. A \$10,000 reward offered in early 2010 to anyone who could decode a file encrypted by a Hydra PC device is still unclaimed.

The following table compares important features of various encryption solutions:

	Hydra PC Digital Attaché	USB Flash Drive with SW-Based Encryption	Full Disk Encryption (FDE) on PC
Capacity	Unlimited with replaceable microSD	Limited to flash memory on drive	Available space on computer hard drive
Encrypted File Location	Hydra PC, computer hard drive, external drive, or Internet	Flash drive only	Computer hard drive only
Run-time Processing Integrity Checks?	Yes	No	No in most cases
Encryption Keys Vulnerable?	No—Encrypted on Hydra PC Provable security	Yes—Derived from password and easily broken	Yes—Stored on PC and either weakly encrypted or not encrypted at all
Restrict Use To Authorized PCs?	Yes	No	Product dependent by using TPM module present on some enterprise PCs
Compatible With Smart Card Logon & Digital Certificate Applications?	Yes	No	Product dependent

SPYRUS provides the world’s most secure, portable hardware-based encryption, authentication, and content security/storage products for government and enterprise. Using advanced Suite B cryptographic algorithms, SPYRUS encryption devices protect data against outside threats and limit access to legitimate users with a specific need. SPYRUS cryptographic elements are proudly designed, engineered, and manufactured in the USA to mitigate the risks of untrusted parts entering the supply chain.

Technical Specifications

- Capacity*
 - 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 Embedded Standard
- 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
- Active anti-malware
 - Sentry A-V using McAfee anti-virus engine with auto-update
- 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: 256-bit hardware
 - Secure Channel: ECDH P-384 and AES 256

- 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

How To Buy

- On the USCYBERCOM approved list
- On the DoD IDIQ—call or email sales@spyrus.com
- Federal and civilian agencies can source via DAR ESI/BPA reseller Autonomic Resources (www.autonomicresources.com) #GS-35F-0587R
- Available in the USA from Amazon and 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) 329-6211 fax

Australia Office

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



© Copyright 2010 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Hydra Privacy Card, Hydra PC, Hydra PC Digital Attaché, Hydra PC Secure Pocket Drive, Rosetta, LYNKs, En-Sign, and SPYCOS are either registered trademarks or trademarks of SPYRUS in the United States and/or other countries. All other trademarks are the property of their respective owners. Individual SPYRUS products may embody technology protected by one or more of the following patents or patent applications:
U.S. Pat. Nos. 7,380,140; 6,088,802; 6,003,135; 6,981,149;
U.S. Pat. Appl. Ser. Nos. 12/018,094; 12/126,759.

