



Hydra Privacy Card® Series II Digital Attaché

The Hydra Privacy Card Series II (Hydra PC™) Digital Attaché from SPYRUS adds hardware-based encryption for removable media, encrypted media sharing, and flexible storage options to the high-assurance features of the popular Hydra PC Enterprise Edition. With Digital Attaché, SPYRUS takes secure portable data protection to the edge, and beyond.

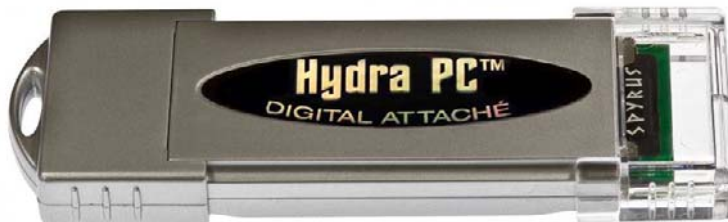
Studies suggest that the greatest data compromise threat comes from organization insiders with legitimate access. Digital Attaché can limit data access to exactly the users with a specific need, especially important for financial, healthcare, and government organizations with regulatory requirements to protect personally identifiable or mission-critical information.

Digital Attaché accepts all commercial miniSD/microSD™ and miniSD/microSDHC™ (high capacity) memory cards.

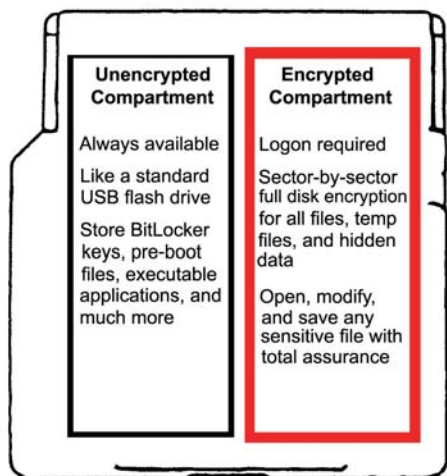
Hardware-Based Full Disk Encryption on Removable Memory

Digital Attaché enables advanced hardware-based, sector-by-sector encryption on the removable miniSD/microSDHC or microSD/microSDHC memory card.

Files can also be encrypted on a file-by-file basis by the Hydra PC and then stored on the memory card for two-level hardware-based encryption protection.



Encrypted and Unencrypted Storage on the Same Memory Card



Memory cards can be configured with one or two hardware compartments. Users can specify a compartment with hardware-based full disk encryption or an unencrypted compartment and can configure the size of each compartment.

Any file in the encrypted compartment can be opened, modified, and saved without becoming vulnerable to interception, because the files are protected by full disk encryption. Large databases and files stay secure without decrypting and re-encrypting the entire file each time a single record is accessed.

Both encrypted and unencrypted compartments can be configured with different file access permissions and formatted into additional partitions.

High-Strength Encryption Security and Key Management

Digital Attaché supports the strongest cryptographic algorithms and key lengths commercially available, exceeding the Suite B algorithms approved by the U.S. Government to protect both unclassified and classified information through the TOP SECRET level. There is no need to upgrade the operating system or other applications to take advantage of this high-strength cryptographic protection. Digital Attaché also supports legacy algorithms for PKI operations.

Each file is encrypted with a unique key and then hashed and signed, greatly increasing security over AES-256 encryption and providing proof against tampering attempts. Keys are generated and stored on the tamper-resistant, tamper-evident security processor chip. The private keys are never exported.

A backup Recovery Agent Hydra PC can be designated to ensure access to encrypted files. Each time a file is encrypted, encryption keys for the Recovery Agent are automatically included. The Recovery Agent can later decrypt the files even if the encrypting Digital Attaché is lost, stolen, or destroyed.



Digital Attaché provides two-factor pre-boot authentication when used with the WinMagic SecureDoc software-based full disk encryption application for the computer hard drive. Digital Attaché also supports two-factor authentication for full disk encryption programs such as Microsoft Vista BitLocker.

Securely Share Encrypted Files with Other Users

Encrypted files can be shared individually with a secure list of authenticated Digital Attaché or Hydra PC Enterprise Edition users. Users create a digital identification record, called a Hydra PC Identity, based on a digital certificate. Any number of Hydra PC Identities can be added to a share list when the file is encrypted. All users on the share list can decrypt the file, but no one else has access.

Total Security for Sensitive Portable Data

An exclusive authentication feature limits the use of a Digital Attaché to a specifically designated enclave of one or more computers. The Digital Attaché or Hydra PC cannot be used in computers that are outside the enclave, even if the user knows the correct PIN.

After a user-configurable number of incorrect PIN entries, the Digital Attaché erases all keys and certificates, making it impossible to decrypt any files encrypted using those keys. Administrators can also configure an increasing delay after each incorrect PIN entry before the next logon can be attempted to discourage brute-force attacks.

The Hydra PC Sentry feature blocks read and write access to removable USB and IEEE 1394 (FireWire) storage devices that use a disk file system. This feature prevents unauthorized file copying to or from blocked drives. Hydra PC Sentry is your best weapon against USB-introduced viruses.

A Digital Attaché can serve as a conventional security device to safeguard your Windows logon password and digital certificate private keys. It is compatible with industry-standard smart card logon protocols, S/MIME secure e-mail technology, and Web-based SSL/TLS with mutual authentication.

Administrative operations such as key management and drive blocking can be limited to specific authorized users.

Designed for the Enterprise

Central management features support large enterprises. Software components can be distributed and installed from a remote location on the enterprise network. Hydra PC enclaves and Recovery Agents can be managed through a central network database. Administrative settings, such as event logging for audits and digital certificate validation, can be configured by using the Microsoft Management Console.

The easy-to-use software interface is integrated with Microsoft Windows Explorer file management capabilities, and runs on Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

Technical Specifications

Supported Algorithms

- ▲ Elliptic Curve Cryptography (ECC) using the NIST curves in $GF(p)$ (P-256, P-384, and P-521)
- ▲ ECDH and ECMQV Key Establishment per NIST SP 800-56A Key Establishment Guidelines
- ▲ ECDSA Digital Signature Algorithm
- ▲ Advanced Encryption Standard (AES) 128/192/256 with ECB, CBC, CTR, and key wrap modes
- ▲ Secure Hash Algorithms: SHA-1 and SHA-224/256/384/512
- ▲ RSA 1024 and 2048 Digital Signature and Key Exchange Algorithms
- ▲ Two-key and three-key triple DES

Security Certifications

- ▲ In validation for FIPS 140-2 Level 3

Electrical/Interfaces

- ▲ Operating voltage: $V_{cc} = 5VDC \pm 5\%$
- ▲ Power consumption: <1 W average
- ▲ USB 2.0 high-speed compliant
- ▲ MiniSD/MiniSDHC memory interface

Device Dimensions

- ▲ 95 mm (3/74") x 31.7 mm (1.24") x 9.53 mm (.375")
- ▲ New option: 66.85 mm (2.63") x 24.21 mm (.91") x 8 mm (.31")

- ▲ Environmental
- ▲ Operating temperature: $-20^{\circ}C$ to $65^{\circ}C$
- ▲ Storage temperature: $-20^{\circ}C$ to $65^{\circ}C$
- ▲ Humidity: 90%, noncondensing

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 Block Modes of Operation
- ▲ SP 800-56A Key Establishment Guidelines
- ▲ SP 800-90 Random Number Generation
- ▲ IEEE P-1619 Disk Encryption Standard

Operating System Support

- ▲ Microsoft Windows 2000, Windows XP, Windows Server 2003, and Windows Vista
- ▲ ECC-based file encryption and sealing operations run on all supported Windows platforms.
- ▲ General ECC-based PKI operations require Windows Vista.

Note: Digital Attaché is authorized for export and reexport under section 742.15 (b) (2) of the Export Administration regulations. It meets requirements for mass-market encryption commodities classified under ECCN 5A992.

Technical specifications may change without notice.

SPYRUS, Inc.



For additional details about SPYRUS products, visit www.spyrus.com or contact us at:

- ▲ USA +1 408 392-9131 info@spyrus.com
- ▲ Australia +61 7 3220-1133 info@spyrus.com.au



©2008–2009 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Hydra Privacy Card, and Hydra PC 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; 5,761,305; 5,889,865; 5,896,455; 5,933,504; 5,999,626; 6,122,736; 6,141,420; 6,336,188; 6,487,661; 6,563,928; 6,618,483, U.S. Pat. Appl. Ser. Nos. 60/886,087; 61/043,118; 12/126,759; 09/434,247; 09/558,256; 09/942,492; 10/185,735; Can. Pat. Appl. Ser. Nos. 2176972; 2176866; 2202566; 2174261; 2155038; 2174260; E.P. Pat. Appl. Ser. No. 96201322.3; 97106114.8; 96105920.1; 95926348.4; 96105921.9; PCT/US08/51729.

Document number 400-350001-04