



## Hydra Privacy Card® Series II Digital Attaché

### Strong Two-Layer Hardware-based Encryption and Microsoft BitLocker Support in a Portable USB Drive

Digital Attaché introduces the first portable hardware-based full disk encryption for removable media, encrypted media sharing capability, and flexible storage options. These new features enhance the functionality of the popular Hydra Privacy Card Series II (Hydra PC™) Enterprise Edition. With Digital Attaché, SPYRUS takes secure data protection to the edge, and beyond.

Digital Attaché adds hardware-based, sector-by-sector full disk encryption to the removable miniSD/microSD or miniSDHC/microSDHC memory card. This means that all data on the card, including file names and other metadata are encrypted at all times. Files can also be encrypted on a file-by-file basis by the Hydra PC and stored on the miniSD/microSD memory card for an extra layer of hardware-based encryption protection.



Removable memory cards can be configured as multiple drives by hardware compartmentalization: one compartment with hardware-based full disk encryption and one clear (unencrypted) compartment. These compartments can then be formatted as actual drive partitions by the host computer. 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 can be protected without decrypting and re-encrypting the entire file each time a single record is accessed. The clear compartment can be used as a conventional USB flash drive, and it makes a convenient place to store Vista BitLocker keys, executable applications, or even Hydra PC encrypted files that require only one layer of encryption protection. Each compartment can be configured with different file access permissions and formatted into additional partitions.

Digital Attaché users can share access to the removable memory card with a designated list of authenticated Digital Attaché devices. The memory card will not work in an undesignated Digital Attaché, even if the user knows the correct PIN.

Current information suggests that the greatest threat of data compromise comes from organization insiders with legitimate access. Digital Attaché provides many flexible options for limiting access to exactly the users with a specific need for the data. This is especially useful for organizations with regulatory requirements to protect personally identifiable or mission-critical information, such as the financial, healthcare, and government industries.

#### All the Proven Features of the Hydra PC Enterprise Edition

Digital Attaché also delivers the same strong encryption and enterprise management features provided by the Hydra PC Enterprise Edition, including the following:

- ▲ 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. Supports AES 128/192/256, ECC P-256/384/521, and SHA-224/256/384/512. 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 3DES, SHA-1, and RSA legacy algorithms for PKI operations.
- ▲ Encrypted files can be shared individually with a secure list of authenticated Hydra PC 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.

- ▲ An exclusive authentication feature can limit the use of a Digital Attaché or Hydra PC 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.
- ▲ A backup Recovery Agent Hydra PC can be designated for encrypted files. Each time a file is encrypted, the Recovery Agent's encryption keys are automatically included. The Recovery Agent can decrypt files even if the encrypting Hydra PC is lost, stolen, or destroyed.
- ▲ 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.
- ▲ Serves as a security device to safeguard your Windows logon password and private keys used with digital certificates. It is compatible with industry-standard smart card logon protocols, S/MIME secure e-mail technology, and Web-based SSL/TLS with mutual authentication.
- ▲ Digital Attaché and Hydra PC Enterprise Edition provide two-factor pre-boot authentication for the SecureDoc software-based full disk encryption application for the computer hard drive. They also support two-factor authentication for other full disk encryption programs.
- ▲ Administrative operations such as key management and drive blocking can be limited to specific authorized users.
- ▲ 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.
- ▲ Keys are generated and stored on the tamper-resistant, tamper-evident security processor chip.
- ▲ Digital Attaché and Hydra PC Enterprise Edition accept all commercial miniSD/microSD™ and miniSD/microSDHC™ (high capacity) memory cards.
- ▲ 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.

### Compare Digital Attaché and Hydra PC Enterprise Edition

Feature	Digital Attaché	Enterprise Edition	Feature	Digital Attaché	Enterprise Edition
Hardware-based full disk encryption of removable media	<b>X</b>		Encrypted and clear compartments on the same miniSD/microSD	<b>X</b>	
Store unencrypted files on miniSD/microSD memory card	<b>X</b>		Securely share miniSD/microSD memory cards	<b>X</b>	
Different access permissions for each compartment on removable media	<b>X</b>		Hardware-based full disk plus single file encryption on miniSD/microSD	<b>X</b>	
Execute applications from clear compartment on removable media	<b>X</b>		Keep executable applications secret and virus free on encrypted compartment of removable media	<b>X</b>	
Strongest commercially available encryption	<b>X</b>	<b>X</b>	Store encrypted files on PC hard disk or external drive	<b>X</b>	<b>X</b>
Single file encryption	<b>X</b>	<b>X</b>	Enclave authentication	<b>X</b>	<b>X</b>
Encrypted file sharing	<b>X</b>	<b>X</b>	Recovery Agent capability	<b>X</b>	<b>X</b>
Dual use as standard security device	<b>X</b>	<b>X</b>	Central enterprise network management features	<b>X</b>	<b>X</b>
Hydra PC Sentry	<b>X</b>	<b>X</b>	Accepts miniSD and miniSDHC memory cards	<b>X</b>	<b>X</b>

# Preliminary 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 coming in Q208: 66.85 mm (2.63") x 24.21 mm (.91" x 8 mm (.31"))

Technical specifications may change without notice.

## 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
- ▲ Digital Attaché's ECC-based file encryption and sealing runs on all Windows platforms.
- ▲ General ECC-based PKI operations require Windows Vista.

Note: Export approval pending.

## 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)



©2008 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. 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. 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

Document number 400-350001-01