



SPYRUS®

TRUSTED MOBILITY SOLUTIONS

Hydra Privacy Card® Series II Enterprise Edition

The Hydra Privacy Card (Hydra PC™) Series II is a unique, portable data encryptor and storage drive that implements the strongest hardware-based encryption technology commercially available. The Hydra PC can write encrypted files to the included replaceable miniSD™ memory card, the computer hard drive, a portable drive, and even an Internet-accessible storage drive.

The Hydra PC also serves as a security device to safeguard your Windows logon password and digital certificates. It is compatible with industry-standard smart card logon protocols, S/MIME secure e-mail technology, and Web-based mutual authentication.



Hydra PC is ideal for organizations with regulatory requirements to protect personally identifiable or mission-critical information, such as the financial, healthcare, and government industries.

Leading-Edge Technology

- ▲ **Cryptographic Algorithms and Key Sizes Exceed U.S. Government Suite B Standard for Classified Data** Hydra PC supports the Suite B standard algorithms for AES, ECC, and SHA-2, and adds support for SHA-512 and ECC-521. No other commercially available device offers stronger encryption. Hardware-based encryption ensures the strongest advanced algorithm support, even if the computer's operating system does not yet support these algorithms. Hydra PC also supports 3DES, SHA-1, and RSA legacy algorithms.
- ▲ **Advanced Authentication** A unique Host Authorization Code (HAC) links and restricts a Hydra PC to specific host computers—even with the correct PIN, users cannot decrypt files encrypted by that Hydra PC unless it is connected to a specified host computer.
- ▲ **Secure File Sharing** Share encrypted files and folders anywhere among multiple users.
- ▲ **Control Read/Write Access to Removable Drives** Hydra PC Sentry 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.
- ▲ **Mandatory Recovery Agent** Optional feature automatically includes the encryption keys of a designated Hydra PC each time a file is encrypted. The Recovery Agent can decrypt files even if the encrypting Hydra PC is lost, stolen, or destroyed.

Features

- ▲ Accepts all commercial miniSD™ and miniSDHC™ (high capacity) memory cards.
- ▲ USB 2.0-compliant connection delivers high-speed data encryption and decryption rates. USB 1.1 compatible.
- ▲ Easy-to-use interface integrates with Microsoft Windows file capabilities. Supported on Windows XP and Windows Vista.
- ▲ Designed for FIPS 140-2 Level 3 security validation.
- ▲ Administration operations such as key management and drive blocking can be limited to specific authorized users.
- ▲ Tamper-resistant, tamper-evident processor chip.
- ▲ Also available in new 30% smaller case design.



Technical Specifications

Supported Cryptographic 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

- ▲ Designed to meet FIPS 140-2 Level 3 validation
- ▲ Designed to meet Department of Defense (DoD) requirements for protecting classified data

Electrical/Interfaces

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

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

Note: 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



(c) 2006-2010 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Suite B On Board, Hydra Privacy Card, Hydra PC and Rosetta 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 400-070101-05