



SPYRUS[®]

TRUSTED MOBILITY SOLUTIONS

SPYRUS Security Products

Hydra PC™ Secure Pocket Drive

Insert a preconfigured microSD card and securely boot a Microsoft Windows Embedded Standard environment with all of your applications and data files. When you're done, remove the drive and leave nothing behind. Authenticates and validates device integrity using on-board hardware security at boot time. If the device has been tampered with, it will not boot. Includes full Suite B on Board[®] hardware security (ECDSA P-384, EC-DH, AES-256, SHA-384).



Hydra Privacy Card[®] Series II (Hydra PC™) Digital Attaché

The Hydra PC Digital Attaché combines full disk encryption of all disk headers, temporary files, and hidden files on a sector-by-sector basis with proven file-based encryption. The microSD memory card can be divided into encrypted and clear (unencrypted) partitions, and the card itself can be shared with a designated group of authenticated users. Encrypted partitions can contain both encrypted and clear text files, and all are completely protected by hardware-based full disk encryption even when files are in use. The Hydra PC Digital Attaché integrates easily with BitLocker and SecureDoc encryption systems.



Hydra Privacy Card[®] Series II (Hydra PC™) Personal Encryption Device



The portable Hydra PC Personal Encryption Device implements the strongest hardware-based encryption technology commercially available. Write encrypted files to the included replaceable miniSD memory card, the computer hard drive, a portable drive, and even your Internet-accessible storage drive. The Hydra PC is compatible with industry-standard smart card logon protocols, S/MIME secure e-mail technology, and Web-based

mutual authentication. A unique authentication feature optionally limits the use of a Hydra PC to only an enclave of specifically designated computers.

Hydra PC Personal Encryption Device has received FIPS 140-2 Level 3 validation and is approved to provide confidentiality for tactical data at the SECRET level and below, when operated in accordance with the appropriate operational security doctrine.

Rosetta Micro™ Series II

Rosetta Micro Series II is the world's smallest and most secure Hardware Security Module. Designed for embedded cryptographic applications, the 6 mm x 5 mm Rosetta Micro supports the strongest cryptographic algorithms and key lengths commercially available. It is ideally suited for both custom and mass-market products, including computers, cell phones, PDAs, wired and wireless routers, point-of-sale and gaming terminals, set-top boxes, and industrial control devices that require small size, low power, and high security.



Rosetta SD/microSD Series II



Rosetta SD/microSD Series II devices are engineered for both embedded applications and enterprise solutions. They support the strongest cryptographic algorithms and key lengths commercially available, exceeding the Suite B algorithms and key length recommendations approved by the U.S. Government to protect both unclassified information and classified information through the TOP SECRET level.



Rosetta SD/microSD Series II devices are ideally suited for both custom and mass-market products that require small size, low power, and high security. They can be released and exported under license exception ENC.

Rosetta Series II Smart Card



The Rosetta Series II Smart Card is a flexible, cost-effective solution that incorporates the same chip and SPYCOS[®] operating system as the Rosetta Micro and provides the same strong cryptographic services. The Rosetta Series II Smart Card is an ISO 7816-compliant public key, multi-application smart card. It supports cryptographic algorithms including elliptic curve cryptography (ECC) that exceed standards

mandated by the U.S. government for classified data. The Rosetta Series II Smart Card can also serve as a physical access and ID card.



Rosetta Series II USB



Rosetta Series II USB is a self-contained version of the Rosetta Series II Smart Card that requires no separate card reader. It can store authentication information, data, digital identity keys, certificates, passwords, and biometric templates. Rosetta Series II USB has all of the strong cryptographic capabilities and algorithm support of the Rosetta Series II Smart Card in a tamper-resistant, tamper-evident container. It is USB 1.1 compliant and USB 2.0 compatible.

LYNKS™ Series II USB Hardware Security Module

The LYNKS Series II HSM with upgraded flash memory and FPGA capabilities supports the strongest available cryptographic algorithms, including elliptic curve cryptography with ECMQV and ECDH key establishment, AES, and SHA-2 algorithms. The stackable LYNKS Series II USB HSM delivers a cost-effective solution for Certificate Authority (CA) and Registration Authority key operations, digital signatures, and key recovery functions, and it supports RSA-4096 for CA keys. With the optional HSM Copy Utility, the LYNKS CA HSM can be cloned to create a locked-down replica as a backup CA.



En-Sign Security Device Management Software

En-Sign™ provides capabilities for managing security devices, certificates, and policies; changing token PINs; and configuring sockets. It integrates with certificate-enabled applications such as smart card logon, e-mail digital signature and encryption, Virtual Private Network, and SSL authentication. En-Sign is designed for the enterprise, but it is also perfect for small businesses and individual users. Settings and configurations affect the local machine only. En-Sign can be installed on a single computer or deployed remotely over an enterprise network by using Group Policy. Consoles and utilities are easy to use and require no special IT assistance.

Signal Identity Manager™



Signal Identity Manager provides a policy-based, auditable workflow for managing client hardware security devices (such as Rosetta Smart Card and USB, Hydra PC, and LYNKS HSM), certificates, and biometrics images with seamless integration with Windows Server 2003 Certificate Services, database services, and Active Directory. Role-specific modular consoles control enterprise-wide identity management functions. Business Rules Templates support custom configuration and enforcement of enterprise security policy and rules of operation. The LYNKS RA HSM provides a hardware solution for central key generation and security device key archiving.

MySafeID™ Self-Contained HW-Based Certification Authority (CA)

MySafeID™ combines the LYNKS™ Series II CA Hardware Security Module (HSM) with high-assurance certification authority software to provide a cost-effective solution for small to medium enterprises. MySafeID is simple, portable, and flexible. The software CA works on any computer running Microsoft Windows XP or Vista (no need for a dedicated server, Active Directory or LDAP, or full Microsoft CA infrastructure) yet MySafeID can generate both the elliptic curve cryptography (ECC) certificates required for high-strength encryption and RSA certificates to support legacy applications. MySafeID provides a hardware-based chain of trust to ensure the security of encryption, digital signatures, and authentication in closed communities where a defined chain of trust is required but global certificate revocation status validation is not mandatory. MySafeID can also be integrated with an existing full PKI system to ensure global compliance.

Software Development Kits

SPYRUS software development kits (SDKs) provide development tools for SPYRUS security devices and technology. The SPYRUS Crypto Toolbox makes it easy to develop cryptographic applications for LYNKS Series II HSMs, Rosetta Series II security devices, and Hydra Privacy Card Series II using Microsoft Visual Studio integrated development environments. Other SDKs include LYNKS and Rosetta SDKs and SSL/TLS SDKs.

PAR Smart Card and PIV/CAC Readers



The Personal Access Reader™ (PAR) is available as either a full-featured PAR 2 or a cost-effective PAR MiniUSB version. The PAR 2 features a full-function keypad and two-line alphanumeric LCD display, includes a real-time clock and calculator, and is fully programmable. It runs connected via serial or USB powered interface or standalone on its replaceable battery. The optional PIV DataViewer displays information stored on a PIV/CAC card.



The PAR MiniUSB is a convenient, portable version that uses standard CCID drivers. Its high-speed USB 2.0 interface is USB 1.1 compliant. You can use the PAR MiniUSB reader with standard smart cards or PIV/CAC cards, and there is an optional adapter for SIM/SAM cards.

SPYRUS, Inc.

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

- ▲ Corporate Headquarters California USA +1 408-392-9131 info@spyrus.com
- ▲ East Coast Office New Jersey USA +1 732-329-6006
- ▲ Australia +61 7 3220-1133 info@spyrus.com.au



©2008–2010 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Suite B On Board, 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 400-000003-09