



# Rosetta SD and Rosetta microSD

## Secure Digital Flash Storage and Hardware Security Modules

Rosetta SD and Rosetta microSD from SPYRUS combine a high-assurance security controller with a flash memory storage subsystem providing up to 32 GB of storage (based on current projections of flash density) using advanced die-on-die packaging concepts. The security controller chip executes the SPYRUS Cryptographic Operating System (SPYCOS®) on a secure hardware security module (HSM) that integrates with most public key infrastructure (PKI) systems.



Rosetta SD and Rosetta microSD are part of a range of cryptographic devices developed by SPYRUS. Rosetta SD and Rosetta microSD 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 and classified information through the TOP SECRET level.



Rosetta SD products are ideally suited for products such as computers, cell phones, and PDAs that require small size, low power, and high security. They can be released and exported under license exception ENC.

### High Assurance by Design

The security controller chip and SPYCOS operating system used in Rosetta SD and Rosetta microSD devices are the same as those embedded in the Rosetta Series II Smart Card and USB security devices and the Hydra Privacy Card® (Hydra PC™) Series II family of USB encryption devices. The embedded SPYCOS hardware platform protects against active and passive attacks, including an active shield and randomized memory layout to prevent physical tampering, as well as countermeasures against side-channel attacks such as timing analysis, simple and differential power analyses, and differential fault analysis. Hardware-based cryptographic support makes Rosetta SD and Rosetta microSD essentially invulnerable to the Branch Prediction Analysis attacks that have compromised all software-based cryptography on PC based platforms.

Rosetta SD and Rosetta microSD support PKI-based digital certificate functionality such as smart card logon, email digital signatures and encryption, and authenticated Web browsing. Rosetta SD and Rosetta microSD are platform agnostic, seamlessly integrating with a wide range of operating systems. They are designed for certification to FIPS 140-2 Level 3 and for use with classified applications as non-CCI devices. Rosetta SD and Rosetta microSD leverage the architecture, validation path, and experience gained from our development of the Hydra PC family of high-assurance security devices, including the Hydra PC Personal Encryption Device, the first and only commercially available personal USB encryption device that is approved to protect tactical data at the SECRET level and below.

Rosetta microSD provides high-assurance storage and authentication mechanisms in the microSD form factor, which is especially important in mobile devices, including smart phones, PDAs, and the emerging market for mobile internet devices.

## Technical Specifications

### Advanced Functions

- ▲ High-assurance protection for keys, digital IDs, and sensitive data.
- ▲ Supports SD/IO interface standard.
- ▲ Unique serial number for each Rosetta SD and Rosetta microSD module.
- ▲ Approximately 32K of EEPROM available for X.509 certificates and data storage.
- ▲ Advanced random-number generation technology.
- ▲ Supports anti-cloning techniques.
- ▲ Compatible with Microsoft CryptoAPI and Cryptographic API: Next Generation, including support for Windows Vista; and with PKCS #11 Security Policy Enforcer

### SPYCOS® Features

- ▲ Security Policy Enforcer
- ▲ Anti-tearing Memory File Manager preserves file integrity if the device is removed during file transfer

### SD Memory Capacities

- ▲ 2 GB to 16 GB

### Electrical

- ▲ Operating voltage: Vcc = 3.3 to 5VDC
- ▲ Power consumption: ~30mA @ 3.3VDC

### Environmental

- ▲ Operating temperature: -15° C to 55° C
- ▲ Storage temperature: -20° C to 65° C

### Packaging

- ▲ Standard SD form factor
- ▲ microSD form factor

## Standards Compliance

- ▲ SDIO Specification Version 1.10
- ▲ SD Physical Layer Specification Version 2.0
- ▲ ANSI X9.31 RSA Key Generation
- ▲ FIPS PUB 46 Data Encryption Standard
- ▲ FIPS PUB 180-2 Secure Hash Algorithm Standard
- ▲ FIPS PUB 186-2 Random Number Generator
- ▲ 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

### Security Certifications

- ▲ Internal Hardware Security Module designed to meet EAL 5+
- ▲ Designed to meet FIPS 140-2 Level 3 certification

## Cryptographic Algorithms

- ▲ Elliptic Curve Cryptography using the NIST curves in GF(p) (P-256, P-384, P-521\*)
- ▲ ECDH and ECMQV Key Establishment per SP 800-56A
- ▲ ECDSA Digital Signature Algorithm
- ▲ Concatenation KDF
- ▲ RSA 1024 and 2048 Digital Signature Algorithm
- ▲ RSA-1024/2048 key exchange
- ▲ DES, two & three-key triple DES with ECB, CBC
- ▲ AES 128/192/256 with ECB, CBC
- ▲ SHA-1 and SHA-224/256/384/512\* Secure Hash Algorithms with HMAC support

\* Exceeds Suite B cryptographic algorithm standard.

Note: Technical specifications are preliminary and may change without notice.

## 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)



©2007–2010 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Rosetta, 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; 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.

Doc number 400-313001-08