



SPYRUS®

TRUSTED MOBILITY SOLUTIONS

Rosetta SD

Smart Card and Storage in a Micro-Sized Device



Rosetta SD is a smart-card-based public key infrastructure (PKI) device available in the industry-standard secure digital (SD) form factor. Along with flash memory storage, the Rosetta SD implements the strongest commercially available cryptographic algorithms for unparalleled protection.

Smart Card Capability For Every Device

While smart cards can increase the security of your application through the use of multi-factor authentication, encryption, and message signing, using them always required a special reader or available USB port. Rosetta SD is the first smart card plus secure storage device in the SD card form factor, perfect for tablets and netbooks.

Rosetta SD was designed from the ground up to bring high-assurance information protection to mobile devices through the use of advanced cryptography.

Rosetta SD is designed for use with classified applications as a non-CCI (Controlled Cryptographic Item) device.

Rosetta SD leverages the architecture, validation path, and experience gained from development of the Hydra PC family of portable USB encryption devices, which are approved by USCYBERCOM for use within the US Department of Defense.

The FIPS 140-2 Level 3 validated security controller

and SPYRUS Cryptographic Operating System (SPYCOS®) used in Rosetta SD devices are the same as those used in Rosetta Smart Card, Rosetta USB, and the Hydra Privacy Card® (Hydra PC™) family of USB encryption devices.

This cryptographic core protects against active and passive attacks by using an active shield and randomized memory layout to prevent physical tampering. It also includes countermeasures against side-channel attacks.

Hardware-based cryptographic support makes Rosetta SD invulnerable to many attacks that have compromised software-based cryptography on PC or mobile devices.

Encrypt Data With the PocketVault SD

If you need data protection in addition to PKI functionality, the SPYRUS PocketVault SD protects the SD card with full disk encryption (FDE) and can encrypt files individually using a unique key. Encrypted files can safely be stored anywhere, not just on the SD card, allowing for an almost infinite amount of secured information.

Technical Specifications

Functionality

- PKI-based digital certificate functionality such as smart card logon, email digital signatures and encryption, and authenticated Web browsing
- High-assurance protection for keys, digital IDs, and sensitive data
- Supports SD/IO interface standard
- Unique serial number for each device
- Approximately 32K of EEPROM available for X.509 certificates and data storage
- Advanced random-number generation technology
- Anti-cloning
- Compatible with Microsoft CryptoAPI and Cryptographic API: Next Generation, including support for Windows Vista, Windows 7, and PKCS #11 Security Policy Enforcer
- Optional full disk and file encryption

SPYCOS® Features

- Security Policy Enforcer
- Anti-tearing memory file manager preserves file integrity if the device is removed during file transfer

Memory Capacities

- SD: 2GB to 8GB, SLC or MLC
- microSD: TBD

Electrical

- Operating voltage: $V_{cc} = 3.3$ to 5VDC
- Power consumption: $\sim 30\text{mA}$ @ 3.3VDC

Environmental

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

Packaging

- SD 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
- 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

- FIPS 140-2 Level 3 / EAL 5+ validated crypto core

Cryptographic Algorithms

- Suite B Cryptography, a set of cryptographic algorithms published by the National Security Agency as part of its cryptographic modernization program to serve as an interoperable cryptographic base for both unclassified information and most classified information, including:
 - Elliptic Curve Cryptography (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
 - XTS-AES 256 FDE, XTS-CBC file encryption



For more information about SPYRUS products, visit www.SPYRUS.com or contact us by email or phone.

Corporate Headquarters
1860 Hartog Drive
San Jose, CA 95131-2203
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@SPYRUS.com

East Coast Office
+1 (732) 329-6006 phone
+1 (732) 329-6211 fax

Australia Office
Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phone
+61 7 3220-2233 fax
www.spyrus.com.au
info@SPYRUS.com.au

Microsoft
GOLD CERTIFIED
Partner