



# Rosetta SD/miniSD/microSD Series II

## High-Assurance Micro Hardware Security Module and Secure Digital

The unique design of Rosetta SD/miniSD/microSD Series II marries Secure Digital (SD) technology with Public Key Infrastructure (PKI) technology in a standard SD, miniSD, or microSD form factor. Rosetta SD/miniSD/microSD Series II is well suited for both embedded solutions and enterprise solutions. Rosetta SD/miniSD/microSD supports 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/miniSD/microSD Series II is ideally suited for both custom and mass-market products, including computers, cell phones, and PDAs that require small size, low power, and high security. It can be released and exported under license exception ENC.



## High Assurance by Design

The Infineon SLE66CX642P security controller chip in Rosetta SD/miniSD/microSD Series II runs the SPYRUS Card Operating System (SPYCOS®). The chip and SPYCOS operating system are the same as those embedded in the SPYRUS Rosetta Series II Smart Card and USB security devices and the SPYRUS Hydra Privacy Card® Series II.

Rosetta SD/miniSD/microSD Series II provides extensive protection against active and passive attacks. The multi-layer chip design includes an active shield and randomized memory layout to prevent physical tampering. Rosetta SD/miniSD/microSD Series II includes hardware countermeasures against side-channel attacks such as timing analysis, simple and differential power analyses, and differential fault analysis. SPYCOS provides additional algorithmic defenses against side-channel attacks. Rosetta SD/miniSD/microSD Series II is invulnerable to Branch Prediction Analysis attacks that can affect PC-based software cryptography.

When any health or status indicator (such as light, voltage, or glitch sensors) is triggered, Rosetta SD/miniSD/microSD Series II zeroes RAM and requires a hard chip reset. As a safety measure against accidental triggers, keys and variables stored in EEPROM remain intact in these cases.

Private keys and critical security parameters are encrypted and stored on the chip, well protected against exotic chip-peeling and electron microscope attacks. Hardware-enforced delays and key zeroizing prevent PIN-guessing attacks.

Rosetta SD/miniSD/microSD Series II encrypts all elements stored in EEPROM during user logoff and power-down, protecting against the most sophisticated probing-type attacks.

SPYRUS has specialized in high-assurance, cost-effective security processors for over a decade, and all of this experience is packaged in a ready-to-roll form for integrators and OEMs.

## High Assurance in Use

SPYCOS takes full advantage of the native hardware capabilities of the security controller chip to provide a high-assurance architecture and implementation suitable for the most sensitive applications.

The Rosetta SD/miniSD/microSD Series II includes a hardware random number generator, which SPYCOS uses to seed a high-entropy Deterministic Random Bit Generator (DRBG) that is suitable for even the strongest ECC P-521 keys.

## Enhanced Encryption Support

Rosetta SD/miniSD/microSD Series II supports cryptographic algorithms that exceed the U.S. Government's Suite B standard for protecting classified information through the TOP SECRET level. These high-strength algorithms ensure data security for decades. Rosetta SD/miniSD/microSD Series II also supports legacy algorithms for backward compatibility with many existing applications. Rosetta SD/miniSD/microSD Series II enables legacy and advanced PKI-based digital certificate functionality such as smart card logon, e-mail digital signatures and encryption, and authenticated Web browsing. See the technical specifications for a complete list of supported cryptographic algorithms.

## Advanced Features

- ▲ High-assurance protection for keys, digital IDs, and sensitive data.
- ▲ Strongest cryptographic algorithm support commercially available.
- ▲ Uses enhanced 8051 instruction set.
- ▲ Supports SD/IO interface standard.
- ▲ Unique serial number for each Rosetta SD/miniSD/microSD module.
- ▲ Approximately 32K of EEPROM available for X.509 certificates and data storage.
- ▲ Includes a hardware memory management and protection unit.
- ▲ Advanced random-number generation technology.
- ▲ Supports anti-cloning techniques.
- ▲ Supports OATH algorithm for One Time Password (OTP) generation.
- ▲ Tamper-resistant design protects against physical attacks and reverse engineering of on-board applications and data.
- ▲ Designed to support certification at FIPS 140-2 Level 2, Level 3, and even Level 4, depending on application requirements.
- ▲ Compatible with Microsoft CryptoAPI and Cryptographic API: Next Generation, including support for Windows Vista; and with PKCS #11.

## Technical Specifications

### SPYCOS® Features

- ▲ Security Policy Enforcer
- ▲ Anti-tearing Memory File Manager preserves file integrity if the security device is removed during file transfer
- ▲ Kernel-based EEPROM memory manager for dynamic nonvolatile memory allocation
- ▲ Data firewall between applications
- ▲ Hardware accelerator for RSA, ECC, and two-key triple-DES
- ▲ Precise™ Biometrics pattern-matching algorithm

### Integrated Circuit Module

- ▲ Infineon SLE66CX642P 16-bit processor
- ▲ 64K EEPROM, 206K ROM, 5052 RAM
- ▲ 1100 bit Advanced Cryptographic Engine
- ▲ 112-bit/192-bit DDES/EC2 Accelerator
- ▲ Retains data for a minimum of 10 years
- ▲ Minimum 500,000 write/erase cycles at 25° C
- ▲ Security optimized layout and layout scrambling

### SD Memory Capacities

- ▲ 128 MB to 2 GB

### Electrical

- ▲ Operating voltage: Vcc = 3.3 to 5VDC
- ▲ Power consumption: <6 mA @ 3.3VDC <10mA @ 5VDC

### Environmental

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

### Packaging

- ▲ Standard SD form factor
- ▲ miniSD 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 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 Deterministic Random Bit Generators
- ▲ OATH HMAC-based One Time Password (HOTP) Algorithm

### Security Certifications

- ▲ ICC designed to meet EAL 5+
- ▲ Designed to meet FIPS 140-2 Level 2 though Level 4 certification, depending on application requirements.

## 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
- ▲ DSA 1024 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)

**Microsoft**  
**GOLD CERTIFIED**  
Partner