

# Rosetta Micro Series II

## High-Assurance Micro Hardware Security Module for Embedded Applications

Rosetta Micro Series II is the world's smallest and most secure Hardware Security Module. Designed for embedded cryptographic applications, the micro-sized 6 mm x 5 mm Rosetta Micro 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 Micro Series II 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. It is approved for export to most countries under license exception ENC.

### High Assurance by Design and In Use

The Infineon SLE66CX642P security controller chip in Rosetta Micro runs the SPYRUS Cryptographic 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® (Hydra PC™) Series II. The security controller chip is certified under Common Criteria EAL5+ by the German government, and the chip running SPYCOS is currently in evaluation for FIPS 140-2 Level 3. Because the cryptographic boundary completely contains the chip, Rosetta Micro retains FIPS certification when embedded in other devices.

Rosetta Micro provides extensive protection against active and passive attacks, even in cases where the user is also the attacker. The multi-layer chip design includes an active shield and randomized memory layout to prevent physical tampering. Rosetta Micro and SPYCOS provide hardware and algorithmic countermeasures against side-channel attacks such as timing analysis, simple and differential power analyses, and differential fault analysis. Rosetta Micro is invulnerable to Branch Prediction Analysis attacks that can affect PC-based software cryptography.

In response to any attempt to penetrate or probe Rosetta Micro while powered on, SPYCOS zeroizes RAM and all keys, variables, public security parameters, and certificates stored in EEPROM.

When any health or status indicators (such as light, voltage, or glitch sensors) are triggered, Rosetta Micro zeroizes 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.

Decrypted private keys and critical security parameters are stored only in volatile RAM and are zeroized immediately after use. The PIN is never stored on the chip. Hardware-enforced delays and key zeroizing after 10 incorrect PIN entries prevent PIN-guessing attacks.

The Rosetta Micro chip features a true hardware random number generator, which SPYCOS uses to seed a high-entropy Deterministic Random Bit Generator (compliant with NIST SP 800-90) that exceeds requirements for even the strongest ECC P-521 or AES-256 keys.

Rosetta Micro encrypts all elements stored in EEPROM during user logoff and power-down, protecting against the most sophisticated probing-type attacks.

An optional patent-pending K out of N split knowledge technique enables multi-party access control for cryptographic keys in decryption, key recovery, and similar applications, providing mathematically provable security for data containment to authorized hosts and devices, and limiting use of authorized devices to specific computers.

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. SPYRUS can also customize Rosetta Micro to meet specific customer requirements for capabilities or implementation. For example, specific commands can be used to support anti-cloning techniques to prove that the chip is unique and authentic.

Rosetta Micro is designed and developed at secure facilities in the United States by SPYRUS engineers holding U.S. security clearances. Final manufacturing firmware updates are installed and tested in-house before shipment directly to the customer.

## Enhanced Encryption Support

Rosetta Micro 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 Micro also supports legacy algorithms such as RSA, triple-DES, and SHA-1 for backward compatibility with many existing applications. Rosetta Micro 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 hardware protection for keys, digital IDs, and sensitive data.
- ▲ Strongest unclassified cryptographic algorithm support and key strengths commercially available.
- ▲ High performance with low current draw in the smallest package for embedded applications.
- ▲ Uses enhanced 8051 instruction set and supports ISO 7816 interface standard for broad application compatibility.
- ▲ Approximately 32K of EEPROM available for X.509 certificates and data storage.
- ▲ Includes a hardware memory management and protection unit.
- ▲ Advanced high-entropy random-number generation technology ensures secure keys.
- ▲ Supports biometric and other enhanced authentication factors.
- ▲ Supports anti-cloning techniques, such as unique serial number for each Rosetta Micro module and unique digitally signed per-token key pair per module.
- ▲ Tamper-resistant, tamper-reacting design protects against physical attacks and reverse engineering of on-board applications and data, in cases where the attacker possesses a product containing Rosetta Micro.
- ▲ Certification for FIPS 140-2 Level 3 is underway. Designed to support certification at FIPS 140-2 Level 4 and higher, depending on application requirements.
- ▲ APIs are compatible with Microsoft CryptoAPI and Cryptographic API: Next Generation, including support for Windows Vista; and with PKCS #11.
- ▲ Custom libraries and drivers are available for specialized application environments and operating systems.
- ▲ Industrial and/or MIL-SPEC specification qualification available on special order.

## Technical Specifications

### SPYCOS® Features

- ▲ Security Policy Enforcer
- ▲ Cryptographic and Access Control List technologies enforce firewalls between applications.
- ▲ 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
- ▲ Cryptographic firewall between applications
- ▲ Hardware accelerator for RSA, ECC, and two-key triple-DES
- ▲ Precise™ Biometrics pattern-matching algorithm
- ▲ Supports OATH algorithm for One Time Password (OTP) generation

### Integrated Circuit Module

- ▲ Infineon SLE66CX642P 16-bit processor
- ▲ 64K EEPROM, 206K ROM, 5052 RAM
- ▲ 1100-bit Advanced Cryptographic Engine
- ▲ 112-bit/192-bit DDES & ECC GF(2<sup>n</sup>) Accelerator
- ▲ Retains data for a minimum of 10 years
- ▲ Minimum 500,000 write/erase cycles at 25° C
- ▲ Security optimized layout and layout scrambling
- ▲ ROHS complaint

### Electrical

- ▲ Operating voltage: Vcc = 3.3 to 5VDC
- ▲ Humidity: 90%, noncondensing
- ▲ ISO 7816 interface

### Environmental

- ▲ Operating temperature: -15° C to 55° C
- ▲ Storage temperature: -20° C to 65° C
- ▲ Power consumption: <6 mA @ 3.3VDC <10mA @ 5VDC

### MIL & JEDEC Standards Tests Passed

- ▲ High-temperature storage life: MIL-STD-883 Method 1008
- ▲ Temperature cycle report: MIL-STD-883 Method 101 Condition C
- ▲ Temperature humidity exposure: JEDEC JESD22-A101-B
- ▲ HAST JEDEC JESD22-A110-B
- ▲ Preconditioning: JEDEC JESD22 A113-E

## Standards Compliance

- ▲ 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

### Security Certifications

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

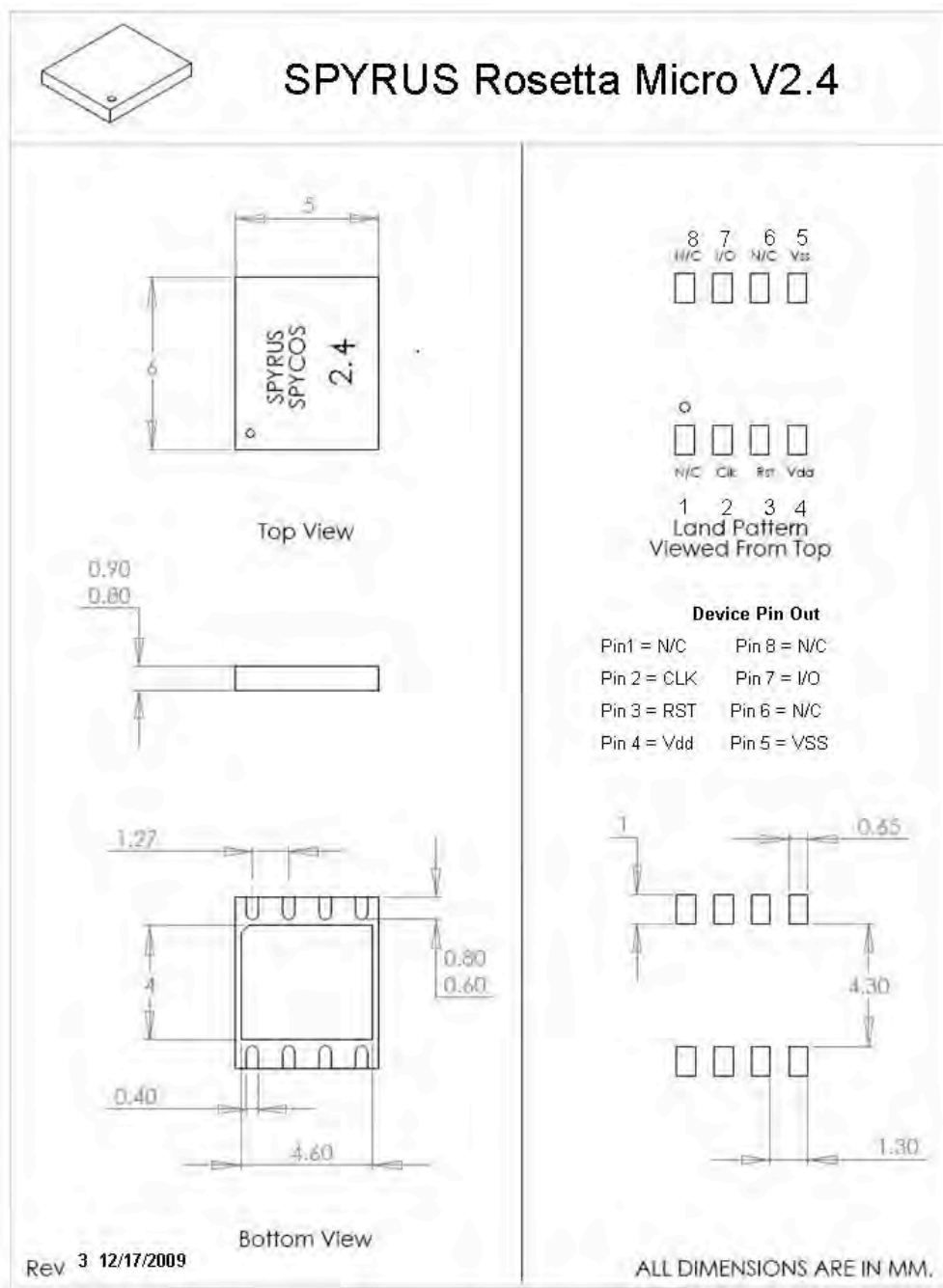
## Cryptographic Algorithms

- ▲ 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 (all seven modes)
- ▲ ECDSA Digital Signature Algorithm
- ▲ Concatenation KDF per SP 800-56A
- ▲ RSA 1024/2048 Digital Signature Algorithm
- ▲ RSA-1024/2048 key exchange
- ▲ 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
- ▲ OATH HMAC-based One Time Password (HOTP) algorithm

\* Exceeds Suite B cryptographic algorithm standard.

Note: Technical specifications may change without notice.

# Dimensions



## 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)

