



Rosetta™ Micro

Cryptographic Integrated Circuit



Your device needs cryptographic functionality. You can try to design and build it yourself, buy it from an unknown supplier, or source it from SPYRUS, A US- owned and based company that has implemented Suite B cryptography across our entire product line using only vetted personnel.

High Assurance Security Module

Rosetta Micro Series II is the world's smallest and most secure hardware security module (HSM). Designed for embedded cryptographic applications, the 6 mm x 5 mm Rosetta Micro integrated circuit 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 though 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.



Secure By Design

SPYRUS has specialized in high-assurance, cost-effective security processors for almost two decades, and all of this experience is packaged in a ready-to-use form factor for integrators and OEMs.

Rosetta Micro is based on the Infineon SLE66CX642P 16-bit processor running the SPYRUS Cryptographic Operating System (SPYCOS®). To ensure the highest level of security, the chip's native cryptographic functionality has been disabled and re-implemented within SPYCOS.

SPYRUS can customize Rosetta Micro to meet specific customer requirements for capabilities or implementation. One optional feature is a patented K of N split-knowledge technique that enables multiparty access control for cryptographic keys in decryption, key recovery, and similar applications. Another option supports anti-cloning techniques to prove that the chip is unique and authentic.

Implemented in our Hydra Privacy Card® devices, K of N implements mathematically provable security

providing data containment to authorized hosts and devices, by preventing the use of devices on unauthorized computers.

Rosetta Micro is designed and developed at secure facilities in the United States by vetted employees. Firmware updates are installed and tested in-house before shipment directly to the customer.

Enhanced Encryption Support

While the high-strength algorithms comprising Suite B ensure data security for decades, Rosetta Micro also supports legacy algorithms such as RSA, triple-DES, and SHA-1 for backwards compatibility with existing applications.

<i>Feature</i>	<i>SPYRUS Rosetta</i>	<i>Competition</i>
<i>Next-gen Elliptic Curve Cryptography encrypt / decrypt / signing</i>	✓	
<i>Fastest Precise Biometrics Minex match-on-card algorithm (Selected versions)</i>	✓	
<i>OATH one time password (Selected versions)</i>	✓	

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.
- ▲ Validated at FIPS 140-2 Level 3. Designed to support validation 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 by special order.
- ▲ Manufacturing facilities ISO 9000 certified.

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
- 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 & ECC GF(2n) 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 compliant

Electrical

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

Environmental

- Operating temperature: -15° C to 55° C
- Storage temperature: -20° C to 65° C
- Humidity: 90%, noncondensing

MIL & JEDEC Standards

- 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

Cryptographic Standards

- 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
- SP 800-90 Deterministic Random Bit Generators

Security Certifications

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

Cryptographic Algorithms

- Suite B cryptography, a set of cryptographic algorithms promoted 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:

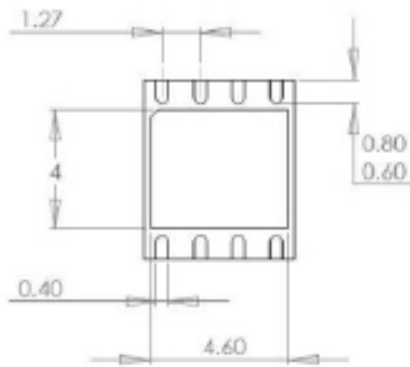
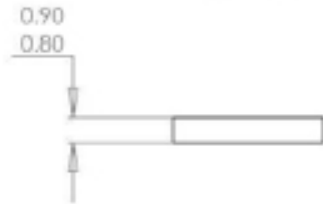
- Elliptic Curve Cryptography (P-256, P-384, P-521)
- ECDH and ECMQV Key Establishment per SP 800-56A
- ECDSA Digital Signature Algorithm
- Concatenation KDF
- RSA 1024 and 2048 digital signature algorithm
- RSA-1024/2048 key exchange
- DES, two & three-key triple DES with ECB, CBC
- AES 128/192/256 with ECB, CBC
- SHA-1 and SHA-224/256/384/512 secure hash algorithms with HMAC support



SPYRUS Rosetta Micro V2.4



Top View



Bottom View

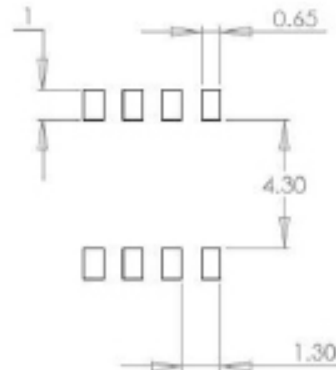
Rev 3 12/17/2009



Land Pattern Viewed From Top

Device Pin Out

- Pin 1 = N/C
- Pin 2 = CLK
- Pin 3 = RST
- Pin 4 = Vdd
- Pin 5 = VSS
- Pin 6 = N/C
- Pin 7 = I/O
- Pin 8 = N/C



ALL DIMENSIONS ARE IN MM.



Microsoft Partner
Gold OEM Hardware
Silver Independent Software Vendor (ISV)

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