



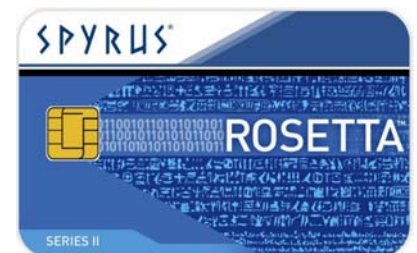
Rosetta® Series II Smart Card & USB

High-Assurance Cryptographic Security Devices

Rosetta Series II security devices draw on a 10-year legacy of proven performance to provide the strongest support for identity authentication. Available as a smart card, a SIM card, or a self-contained USB token that requires no separate reader, the Rosetta Series II is a flexible, cost-effective security solution for both small and large organizations.

Benefits

- ▲ **Secure Protection for Your Identity** The private key, password, and biometric template are encrypted and stored on the security device instead of on the computer. The PIN required for access is never stored on the security device.
- ▲ **Enhanced Cryptographic Algorithms** The Suite B cryptographic algorithms meet all requirements for business use and the U. S. Government's requirements for unclassified, releasable algorithms to be used to protect classified information.



Features

- ▲ Most secure random number generator and key generation technology
- ▲ Designed for FIPS 140-2 Level 2 and Level 3 validation
- ▲ Supports biometrics for two- and three-factor authentication
- ▲ Capacity for 20+ X.509 version 3 certificates
- ▲ Tamper-resistant, tamper-evident design and construction
- ▲ SPYRUS® Cryptographic Operating System (SPYCOS®)
- ▲ Supports applications using Microsoft® Windows® Cryptographic API (MSCAPI), Microsoft Card Module and PKCS #11 interfaces
- ▲ Ideal for Security In A Box® or En-Sign™ applications
- ▲ Supports OATH algorithm for One Time Password (OTP) generation
- ▲ WHQL-certified drivers available for Windows 2000, XP, and Server 2003
- ▲ WHQL-certified Minidivers for Microsoft Smart Card Base CSP for Windows XP, Server 2003, Vista



Supported Cryptographic Algorithms

- ▲ RSA 1024 and 2048 Digital Signature Algorithm and DSA 1024 Digital Signature Algorithm
- ▲ DES, two- and three-key triple DES with CBC
- ▲ Advanced Encryption Standard (AES) 128/192/256 ECB, CBC
- ▲ SHA-1 and SHA-224/256/384/512 Secure Hash Algorithms with HMAC support
- ▲ Elliptic curve cryptography (ECC) using the NIST curves in GF(p) (P-256, P-384, and P-521)
- ▲ ECDH key establishment in accordance with NIST SP 800-56A Key Establishment Guidelines
- ▲ ECDSA Digital Signature Algorithm

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

- ▲ 64K EEPROM
- ▲ Retains data for a minimum of 10 years
- ▲ Minimum 500,000 write/erase cycles at 25 C

Security Certifications

- ▲ ICC designed to meet EAL 5+
- ▲ Designed for FIPS 140-2 Level 2 and Level 3 validation

Electrical

- ▲ Operating voltage: $V_{cc} = 5VDC \pm 5\%$
- ▲ Power consumption: <300 mW
- ▲ ISO 7816 interface (smart card)
- ▲ USB 1.1 compliant and USB 2.0 compatible

Environmental

- ▲ Operating temperature: $-15^{\circ}C$ to $55^{\circ}C$
- ▲ Storage temperature: $-20^{\circ}C$ to $65^{\circ}C$
- ▲ Humidity: 90%, noncondensing

Standards Compliance

- ▲ Microsoft CryptoAPI, Microsoft Card Module and PKCS #11 interoperability
- ▲ Microsoft WHQL-certified drivers and Minidrivers
- ▲ OATH HMAC-based One Time Password (HOTP) algorithm
- ▲ 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
- ▲ Federal Communications Commission Class B certification and CE Mark Certification

SPYRUS, Inc.

For additional details about SPYRUS products, visit www.spyrus.com or contact us at:

- ▲ USA +1 408 392-9131 info@spyrus.com
- ▲ Australia +61 7 3220-1133 info@spyrus.com.au

