Rosetta™ Smart Card and USB Series II and Series III

Conventional and Readerless USB Smart Cards

Smart cards increase security by encrypting and storing your private key on the security device instead of on the computer. The SPYRUS Rosetta USB 3.0 is compact and requires no separate card reader, while the Rosetta Series II and Series III Smart Card offers smart card security in a traditional ISO 7816 card format. Smart cards in the enterprise are perfect for multi-factor authentication, encryption, and message signing.

Rosetta Smart Card and Rosetta USB may have different packaging, but the functionality is identical—smart card-based public key infrastructure (PKI) capability using the strongest commercially available algorithms.

The smart card unblock password is never stored anywhere and is used to reconstruct a master "key encryption key," which is then used to unwrap a unique private key protection application.

The smart card unlock password is never stored anywhere. If the password is lost, a special administrator utility and password must be used to unblock the device and reset the password.

Rosetta Smart Card and USB devices were designed from the ground up using advanced cryptography to bring high-assurance information protection to almost any computing device.

Rosetta FIPS 140-2 Level 3 validated security controller chip and SPYRUS Cryptographic Operating System (SPYCOS®) used in the Rosetta Smart Card and USB devices are the same as those used in the award winning Windows to Go WorkSafe Pro and P-3X family of USB encryption devices.

The Rosetta family is platform agnostic, seamlessly integrating with a wide range of desktop and mobile operating systems. It is designed for use with classified applications as a non-CCI (Controlled Cryptographic Item) device.

The crypto core protects against active and passive attacks, using an active shield and randomized memory layout to prevent physical tampering. It also includes countermeasures against side-channel attacks such as timing analysis, simple and differential power analyses, and differential fault analysis.

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

Rosetta devices support PKI-based digital certificate functionality such as smart card logon, email digital signatures and encryption, VPN authentication and authenticated Web browsing.

SPYRUS®

Technical Specifications

Functionality

High-assurance protection for keys, digital IDs, and sensitive data

Available Form Factors / Interfaces

- ISO 7816 interface (smart card)
- USB 2.0

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

WHQL-certified drivers available for Windows XP, Vista, Windows 7, Windows 8, Server 2008 and Server 2012..

CCID and PKCS-11 Drivers

Compatible with Microsoft CryptoAPI and Cryptographic API: Next Generation, including support for Windows Vista, Windows 7, Windows 8 and PKCS #11

Minidriver support for System Center.

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

Integrated Circuit Module

64K EEPROM with 32k for storage

Retains data for a minimum of 10 years

Minimum 500,000 write/erase cycles at 25 C

Electrical

Operating voltage: Vcc = 3.3 to 5VDC

Power consumption: ~30mA @ 3.3VDC

Environmental

Operating temperature: –15˚ C to 55˚ C

Storage temperature: –20˚ C to 65˚ C

Standards and Security

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

SP800-90A Hash_DRBG

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

Cryptographic Algorithms

Suite B cryptography (a set of cryptographic algorithms published by the U.S. Government as part of its cryptographic modernization program to serve as an interoperable cryptographic based for both unclassified information and most classified information) and other FIPS- approved algorithms, including:

Hash_DRBG RNG

Elliptic Curve Cryptography (P-256, P-384, P-521)

ECDH

ECDSA Digital Signature Algorithm

RSA 1024 and 2048 digital signature algorithm (Note: RSA 1024 is deprecated by NIST)

TDES-2 and TDES-3, ECB, CBC

AES 128/192/256 with ECB, CBC, CTR

SHA-1 and SHA-224/256/384/512 secure hash algorithms

HMAC

(Please note security services will vary depending on the version of Rosetta SPYCOS being used in the product.)

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) 832-0123 fax

UK Office
+44 (0) 113 8800494

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

Specifications subject to change without notice.