



SPYRUS®

ENSURING TRUST IN CYBERSPACE



Rosetta™

Smart Card Functionality in convenient form factors



Smart cards can increase the security of your application because the user's private key is encrypted and stored on the security device instead of on the computer. Traditional smart cards require a special reader, but with everyday computing moving toward smaller and more powerful mobile devices, the availability of a smart card reader, or even a USB interface, cannot be guaranteed.

Smart Card Capability For Every Device

Rosetta smart card devices are available in traditional, USB, memory card, and integrated circuit (chip) form factors. The packaging is different but the functionality is identical—smart card-based public key infrastructure (PKI) capability using the strongest commercially available algorithms.

The password required to unlock the Rosetta module is not stored anywhere. When the user enters his password, it is used to reconstruct a master “key encryption key” which is then used to

unwrap a unique key per application that is used to protect private keys.

In addition to using a smart card for multi-factor authentication, it also can be used for encryption and message signing.

Rosetta devices were designed from the ground up to bring high-assurance information protection to almost any computing device through the use of advanced cryptography.

The FIPS 140-2 Level 3 validated security controller chip and SPYRUS Cryptographic Operating System (SPYCOS®) used in the Rosetta SD devices are the same as those used in the Rosetta Smart Card, Rosetta USB, and the Hydra Privacy Card® (Hydra PC™) 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, and authenticated Web browsing.

Rosetta devices leverage the architecture, validation path, and experience gained from development of the Hydra PC family of portable USB encryption devices that are approved by USCYBERCOM for use within the US Department of Defense.

<i>Feature</i>	<i>SPYRUS Rosetta</i>	<i>Competition</i>
<i>Next-gen Elliptic Curve Cryptography encrypt / decrypt / signing</i>	✓	
<i>Smart Card, USB, SD, and IC (chip) form factors</i>	✓	
<i>Fastest Precise Biometrics Minex match-on-card algorithm (Selected versions)</i>	✓	
<i>OATH one time password (Selected versions)</i>	✓	

Technical Specifications

Functionality

- High-assurance protection for keys, digital IDs, and sensitive data
- Available Form Factors / Interfaces
 - SD/IO (secure digital card)
 - ISO 7816 interface (smart card)
 - USB 2.0, backwards compatible with USB 1.1
- 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, Server 2003, and Server 2008.
- Compatible with Microsoft CryptoAPI and Cryptographic API: Next Generation, including support for Windows Vista, Windows 7, and PKCS #11
- Minidriver support for Microsoft Identity Lifecycle Manager (ILM) 2007 or later.

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

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 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 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

Security Certifications

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

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



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