SPYRUS®

(613) 282-3691
CRYPTO SOLUTIONS
info@cryptosolutions.ca

Rosetta® microSDHC™ Card

Secure PKI Smart Card and TrustedFlash™storage in a Micro-Sized Device

The Rosetta microSDHC card is an industry-standard secure digital high capacity (microSDHC) form factor available in two security configurations: 1) The Rosetta microSDHC PKI configuration is a public key infrastructure (PKI) device with clear flash. 2) The TrustedFlash™configuration enables hardware AES-256 encryption to provide the strongest commercially available data protection and PKI capabilities to use with public key enabled applications.

Rosetta microSDHC PKI HSM

While PKI smart cards or similar NFC enabled tokens can increase the security of customer applications through the use of multi-factor authentication, encryption, and message signing, using them always requires a special reader or USB port. The Rosetta microSDHC PKI is a smart card contained in a microSDHC package.

The FIPS 140-2 Level 3 certified SPYRUS Cryptographic Operating System (SPYCOS®) used in the Rosetta microSDHC is the same as that used in Rosetta Smart Card, Rosetta USB, the PocketVault P-3X USB 3.0 encrypting storage drives, and the family of Microsoft certified Windows To Go live drives. SPYCOS executes within an EAL5+tamper resistant security controller contained within the body of the Rosetta microSDHC.

The Rosetta microSDHC is a hardware security module designed for use with public key enabled applications like encrypted email, digital signatures, VPN authentication, and Web authentication.

SPYRUS TrustedFlash™microSDHC

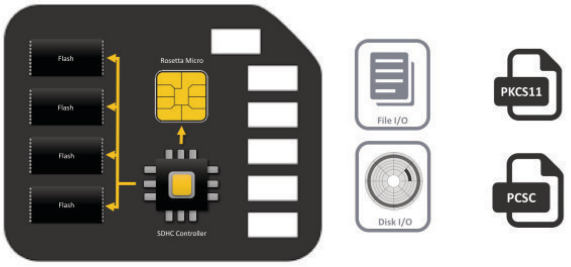
The TrustedFlash microSDHC adds AES-256 hardware encrypted flash memory to the Rosetta microSDHC PKI capabilities. It is designed from the ground up to bring high-assurance information protection to mobile devices through the use of advanced cryptography.

The Rosetta SPYCOS crypto core protects against active and passive attacks by using an active shield and randomized memory layout to prevent physical tampering. It also includes countermeasures against side-channel attacks.

Hardware-based cryptographic support makes the TrustedFlash in the Rosetta microSDHC invulnerable to many attacks that have compromised software-based cryptography on PCs, tablets and mobile devices.

The TrustedFlash provides on-the-fly encryption of the flash memory designed to protect sensitive personal or corporate data and Personally Identifiable Information (PII) in a hardware protected vault. Access to the Trusted Flash can be obtained by inserting the Rosetta micro SDHC card into the microSD or SD port available in most laptops and tablets. The microSDHC form factor is an extremely convenient way to protect data at rest without using the limited USB ports. Access to the encrypted TrustedFlash hardware vault is only made available after a user has successfully logged into the Rosetta microSDHC. The device key is zeroized if the maximum number of bad logon attempts is exceeded. The number of bad attempts can be set by policy. Zeroizing the device key is much more secure and rapid than zeroizing the entire flash memory content.

The Rosetta microSDHC PKI and TrustedFlash configurations will also work with the optional NcryptNshare applications that provide data protection on a file-by-file basis. The combination of NcryptNshare with the SPYRUS
TrustedFlash card provides the ultimate defense in depth data security solution for Windows environments.



The PKI mode configures the file system as a standard non-encrypting flash file systems. The TrustedFlash™ mode configures the file system as a hardware-encrypting file system using Rosetta for all key management features

(613) 282-3691
CRYPTO SOLUTIONS
info@cryptosolutions.ca

Technical Specifications

Functionality

PKI-based key and digital certificate functionality such as encrypted/ signed email, digital signatures, authenticated VPN & Web browsing

TrustedFlash™AES 256-bit hardware self-encrypting configuration option providing flash memory protection with PKI services

Key zeroization when bad Password attempts has been exceeded

FIPS 140-2 Level 3 high-assurance protection for keys, digital IDs, and sensitive data

Unique serial number for each device

Approximately 32K of EEPROM available within security controller for X.509 certificates

Compatible with support for Windows 7, 8, 8.1, 10 and Linux and more on request

Operates with optional NcryptNshare applications

SPYCOS® Features

FIPS 140-2 Level 3 Certified & Algorithm Agility

Memory Capacities

4,8,16 GB

Higher capacities will be supported in Q2 2016

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

Packaging

micro SDHC form factor

Standards and Security

SDIO Specification Version 1.10

SD Physical Layer Specification Version 2.0

FIPS PUB 46-3 Data Encryption Standard

FIPS PUB 180-2 Secure Hash Algorithm Standard

FIPS PUB 186-4 Digital Signature Standard

FIPS PUB 197 Advanced Encryption Standard

FIPS PUB 198-1 Keyed Hash Message Authentication Code (HMAC)

SP 800-38A Block Modes of Operation

SP 800-56A Key Establishment Schemes

SP800-90A. Rev.1 Deterministic Random Bit Generator

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

Military grade cryptography (a set of cryptographic algorithms published by the U.S. Government as part of its cryptographic modernization program to serve as a interoperable cryptographic based for both unclassified information and most classified information)

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

ECDSA Digital Signature Algorithm

Key Agreement / Establishment: CVL (ECC CDH), KAS, KTS

RSA 2048 digital signature algorithm

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

SHA-1, SHA-224/ 256/ 384/ 512 Secure Hash Algorithms

Other FIPS- approved algorithms:

HMAC (min 112 bit key) keyed hash MAC

SP800-90A HASH_DRBG (RNG)

TDES-3, ECB, CBC

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

SUITE B ON BOARD

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

Document number 400-314001-02