SPYRUS®

Rosetta® MicroSDHC™ Card

Secure PKI Smart Card and Storage in a Micro-Sized Device

The Rosetta microSDHC card is a smart-card-based public key infrastructure (PKI) device available in the industry-standard secure digital high capacity (SDHC) form factor. The Rosetta microSDHC card implements the strongest commercially available cryptographic algorithms for unparalleled protection.

Smart Card Capability For Every Device

While smart cards can increase the security of your application through the use of multi-factor authentication, encryption, and message signing, using them always required a special reader or available USB port. The Rosetta SDHC card is the first smart card plus secure storage (optional) device in the SDHC card form factor, perfect for tablets and netbooks.

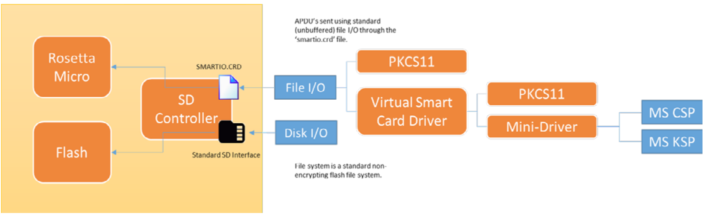
The Rosetta SDHC card was designed from the ground up to bring high-assurance information protection to mobile devices through the use of advanced cryptography.

The FIPS 140-2 Level 3 security controller and SPYRUS Cryptographic Operating System (SPY-COS®) used in the Rosetta SDHC card are the same as those used in Rosetta Smart Card, Rosetta USB, the Hydra Privacy Card® (Hydra PC™), PocketVault USB encrypting storage drives and the family of Microsoft certified Windows To Go drives.

The Rosetta microSDHC card is designed for use with public key enabled applications like encrypted email, digital signatures, VPN authentication, and Web authentication.e.

The 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 Rosetta microSDHC card invulnerable to many attacks that have compromised software-based cryptography on PCs or mobile devices.


Rosetta Micro
SD Controller
Flash
SMARTIO.CRD
Standard SD Interface
APDU's sent using standard (unbuffered) file I/O through the 'smartio.crd' file.
File I/O
Disk I/O
PKCS11
Virtual Smart Card Driver
PKCS11
Mini-Driver
MS CSP
MS KSP
File system is a standard non-encrypting flash file system.

With optional software, the Rosetta SDHC card can be protected by the SPYRUS PocketVault™ Encryptor Pro (PVE Pro) which is a software application that encrypts both individual files and folders of files and allows users securely share decryption capabilities with other trusted individuals. The following table is a summary of the currently available options:

Rosetta microSDHC Part	Available Memory Capacities	Suite B Crypto	Integration with PVE Pro File Encryption
PKI	4, 8, 16 GB	Yes	Yes
PKI, limited size flash	128, 256 MB	Yes	Yes
PKI, Rosetta-based AES 256 volume encryption	4, 8, 16 GB	Yes	Yes
PKI, Rosetta-based AES 256 volume encryption 32 GB	2015	Yes	Yes

SPYRUS®

Technical Specifications

Functionality

PKI-based digital certificate functionality such as smart card logon, email digital signatures and encryption, and authenticated Web browsing

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

Supports SD/IO interface standard

Unique serial number for each device

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

Advanced random-number generation technology

Anti-cloning

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

SPYCOS® Features

Security Policy Enforcer

Anti-tearing memory file manager preserves file integrity if the device is removed during file transfer

Memory Capacities

4,8,16 GB

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

SDHC form factor

Standards and Security

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 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

Suite B 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) and other FIPS- approved algorithms, including:

RNG

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

ECDH

ECDSA Digital Signature Algorithm

RSA 2048 digital signature algorithm

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

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

Specifications subject to change without notice.

Document number 400-313001-14