

Meet

PocketVault SD

from SPYRUS®

Encryption Software on a Smartcard Device

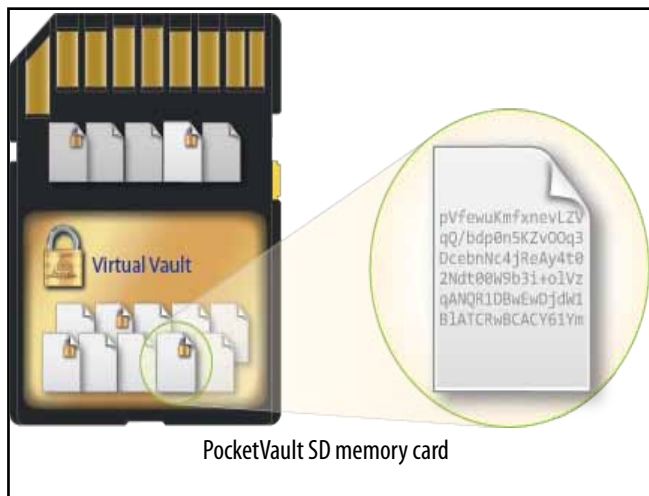
Like A Bank Vault In Your Pocket

PocketVault SD combines PocketVault encryption software with a Rosetta SD smartcard services device. PocketVault SD is perfect for netbooks, tablets, or any computing device where you don't want to use a large USB flash drive.

PocketVault SD provides sector-based encrypted storage on an Encrypted Virtual Vault, an encrypted disk image file that resides on the Rosetta SD and appears in Windows Explorer as a lettered drive.

The cryptographic components in every SPYRUS encryption device are designed, engineered, and manufactured in the United States by carefully vetted personnel.

PocketVault SD implements both AES-XTS 256-bit full disk encryption and granular AES-CBC file encryption.



PocketVault SD memory card

Encrypted files can safely be stored anywhere, not just on the SD card. Why trust today's information with yesterday's security?

Features and Benefits

- ▲ **Encrypt for the Life of Your Data**—PocketVault SD implements next-generation Suite B cryptography, an interoperable cryptographic base promulgated by the US government for both unclassified information and most classified information.
- ▲ **Encrypted files can be stored anywhere**—on the Rosetta SD card, inside the Encrypted Virtual Vault, on your computer, on a file server, or in the cloud.
- ▲ **Key Generation**—Keys are generated in the device using a random number generator compliant with NIST SP 800-90
- ▲ **Key Recovery**—Patent-pending technology reconstitutes keys as required—they are not stored anywhere.
- ▲ **Cross-platform capability**—allows you to securely move encrypted data across heterogeneous systems.
- ▲ **Smart Card Functionality**—This means that you can safely use it for storing certificates and signing credentials for many applications.

Technical Specifications

Functionality

- Independent Encrypted Virtual Vault and file-by-file encryption can be combined for defense in depth. Software is available for Microsoft Windows and other selected operating systems, and an SDK is available for building custom applications
- 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
- Unique serial number for each device
- Approximately 32K of EEPROM available for X.509 certificates and data storage
- Compatible with Microsoft CryptoAPI and Cryptographic API: Next Generation, including support for Windows Vista, Windows 7, and PKCS #11 Security Policy Enforcer

Memory Capacities

- SD: 2GB to 8GB, SLC or MLC

Electrical

- Operating voltage: $V_{cc} = 3.3$ to 5VDC
- Power consumption: $\sim 30\text{mA}$ @ 3.3VDC

Environmental

- Operating temperature: -15°C to 55°C
- Storage temperature: -20°C to 65°C

Packaging

- SD form factor

Standards Compliance

- SDIO Specification Version 1.1; 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; SP 800-90 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 published 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
 - XTS-AES 256 FDE, XTS-CBC file encryption



Proudly designed, engineered,



and manufactured in the USA



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
info@SPYRUS.com.au

