SPYRUS®

PocketVault™ Encryptor

Secured by SPYRUS with Rosetta® Micro HSM FIPS 140-2 Level 3 Security

Authentication, Encryption, Storage and Secure File Sharing for People on the Go

The SPYRUS PocketVault Encryptor (PVE) introduces the latest version of the SPYRUS secure file encryption and file sharing product line. SPYRUS USB encryption devices were the world's first to implement hardware-based file encryption and file sharing and this innovation is taken to new levels of performance and information assurance in the PVE by the incorporation of hardware-based Elliptic Curve Cryptography in the internal Rosetta Micro Hardware Security Modules. SPYRUS Rosetta technology is designed to work with PVE to securely store and share encrypted files anywhere. The Rosetta Micro ensures interoperability with other members of the SPYRUS family including the Rosetta USB, Rosetta microSDHC, WorkSafe, WorkSafe Pro, PocketVault, andP-3X security devices.

Encrypt Files and Store Them Anywhere

PVE file encryption protects each encrypted file with a unique key, no matter where it is stored, making it an ideal cloud solution. The SPYRUS PVE file encryption provides superior confidentiality through the use of Elliptic Curve Cryptography with key size of P-384 together with AES-256 symmetric encryption.

Secure File Sharing

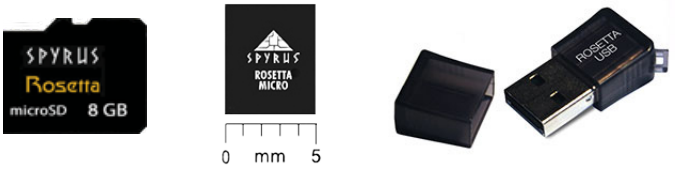
PVE files can be shared with other PVE users whether encrypted files are stored on the SPYRUS WorkSafe Pro, P-3X, SharePoint, or in the Cloud. Each and every file is protected using a unique key that is encrypted (wrapped) with a key encryption key derived from the originators Rosetta Micro HSM along with each recipient's public/private key pair using an EC Diffie-Hellman key agreement. The file originator and receiver keys are conveyed in a PVE Sharing Certificate that is stored in a local PVE Contacts Folder.

Secure Data Recovery

PVE Recovery Agent was designed for organizations concerned about file data recovery if the PVE device is lost or stolen. The PVE secure file sharing architecture can be configured so that the backup PVE device can be defined as a Recovery Agent so that every file that is encrypted will automatically include the Recovery Agent's PVE Sharing Certificate. Depending on policy, the Recovery Agent can optionally be set up to require two-person control and kept securely locked in a safe or a vault offsite.

Rosetta Micro HSM PKI Security Features

In addition to being the security engine for secure file sharing within the PVE, the Rosetta Micro HSM can also function as a PKI security device or smart card for additional functionality. Rosetta Micro HSM security functionality can safeguard a user's Windows logon password and the private keys associated with digital certificates. The Rosetta Micro HSM is compatible with industry-standard protocols for secure S/MIME email systems, Web-based SSL/TLS with mutual authentication, Microsoft Data Access functions, as well as providing RSA and Elliptic Curve Cryptography digital signatures for eForms.



SPYRUS®

Why is SPYRUS Secure File Encryption and Sharing Stronger?

Hardware-based key management security sets SPYRUS apart from the competition. Why is this better?

- SPYRUS uses highly efficient processor with Elliptic Curve Cryptography in the Rosetta Micro HSM
- Keys are generated in the Rosetta Micro HSM and never revealed in the host or to a third party Cloud provider
- Access to Rosetta Micro HSM required two levels of authentication – something you have (the SPYRUS device with Rosetta Micro HSM) and something you know (the password to logon).
- The Rosetta Micro HSM is initially programmed at the factory to destroy the keys and prevent access to encrypted files after 10 incorrect password entries to prevent brute-force attacks. This bad password default value can be changed by the PVE Administrator.
- Rosetta Micro HSM is a tamper-resistant FIPS 140-2 Level 3 hardware module with EAL5+ hardware security, specifically designed to protect keys from reverse engineering attacks

Features and Benefits

- Encrypt and store data anywhere – in the Cloud, on the desktop, or on a SPYRUS WorkSafe Pro bootable Windows 8.1 live drive or P-3X encrypted storage drive.
- Exchange PVE Sharing Certificates to securely share files with other users in a workgroup.
- PVE keys are generated in the Rosetta Micro HSM device and never exported or escrowed after initialization of PVE.
- An organization can provision a Recovery Agent to enable data decryption if a user's PVE Rosetta device is lost or stolen.
- PKI smartcard functionality generates key pairs, store certificates, sign/encrypt email, and enable strong two-factor authentication.
- Implements Elliptic Curve Cryptography and AES 256 CBC mode.
- KeyWitness digital signature operations enable strong non-repudiation and protect files from malware propagation.
- Easy user interface

PVE2Go Easy to Use Interface

Button name	Image	Function
PVE Contacts		Managing your PVE Contacts.
Add Folder		Adding new folders to PocketVault Encryptor.
Delete Folder		Deleting folders from PocketVault Encryptor.
Add Content		Adding new encrypted files to PocketVault Encryptor.
Delete		Deleting encrypted files from PocketVault Encryptor.
Decrypt		Saving an unencrypted copy of files to another location.
Share		Saving an encrypted version of files that can be accessed by people you want to share them with.
Import		Importing encrypted files into PocketVault Encryptor.

SPYRUS®

Technical Specifications

Operating System Compatibility

Windows 10 Preview

Windows 8/8.1

Windows 7

Hardware Security

SPYRUS Cryptographic Operating System (SPYCOS)

File Encryption: AES CBC 256-bit

Key Protection: ECDH P-384 and AES CBC 256

Hashing: SHA-384

Rosetta Micro HSM: Series II and/or Series III for FIPS 140-2 Level 3

FIPS PUB 180-4 Secure hash Algorithm Standard

FIPS PUB 197 Advanced Encryption Standard

SP 800-38A and SP800-38F Modes of Operation

SP800-56A Key Establishment Guidelines

SP800-90A Random Number Generation

SP 800-90A Random Number Generation

Product Models

PVE Pro installs on Windows 7 or Windows 8 platforms (and Windows 10 after Microsoft releases for General Availability) and encrypts and shares files using Rosetta USB, Rosetta microSDHC, PocketVault USB 3.0, P-3X, WorkSafe, or WorkSafe Pro.

PVE2Go is an application that is installed on the WorkSafe Pro Windows live drive or P-3X encrypting USB 3.0 storage drive.

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

Document number 400-240001-02