SPYRUS®

Rosetta® NcryptNshare™ (RES Pro)

with Rosetta® FIPS 140-2 Level 3 Security

Secure File Encryption and Encrypted File Sharing for Windows on PCs, Tablets and Windows ToGo Drives

Your Files Stay Secure in the Cloud, the Encryption Keys Stay with You

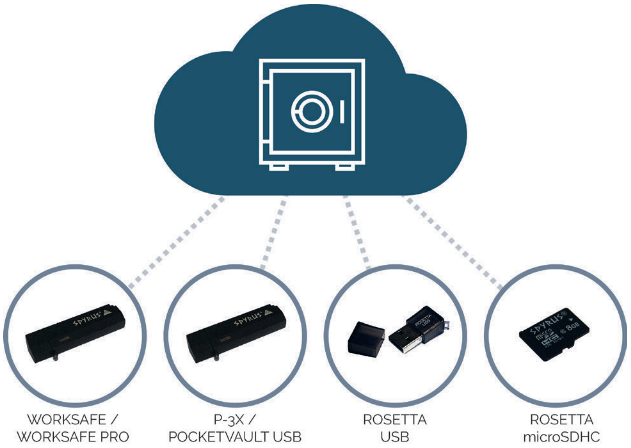
Rosetta NcryptNshare Pro (RES Pro) is a software application that encrypts both individual files and folders of files and allows you to securely share decryption capabilities with other trusted individuals.

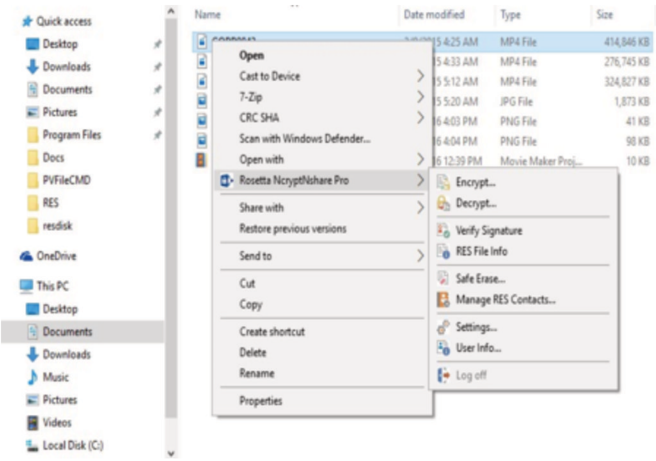
Encrypted files and folders can be safely and securely transported as email attachments or stored on an external disk, server—even in the cloud.

Files are encrypted with keys generated and stored in a SPYRUS hardware encryption device such as a Rosetta smart card/ readerless USB, PocketVault P-3X, WorkSafe/ WorkSafe Pro, or Rosetta MicroSDHC.

You can share encrypted files with other RES Pro users by using any RES application to create and exchange digital certificates to create a list of RES Contacts and create contact groups. You can include any of your RES contacts on a sharing list when you encrypt a file or folder with RES, and those contacts can decrypt that file or folder on their own computer running RES Pro. You can also decrypt encrypted files that are shared with you by your RES Contacts.

RES Pro is compatible with many versions of the Windows operating system, including Windows 7, 8.1, and 10 running on a desktop, laptop, tablet or SPYRUS WorkSafe/ WorkSafe Pro Windows To Go drive.





Date modified	Type	Size
5 4:25 AM	MP4 File	414,846 KB
5 4:33 AM	MP4 File	276,745 KB
5 5:12 AM	MP4 File	324,827 KB
5 5:20 AM	JPG File	1,873 KB
6 4:03 PM	PNG File	41 KB
6 4:04 PM	PNG File	98 KB
6 12:39 PM	Movie Maker Proj...	10 KB

Features and Benefits

- Recovery Agent supports continuity for decryption with a second Rosetta device in case the primary Rosetta key is lost or stolen.

- All key management and critical security functions are implemented in the Rosetta SPYCOS FIPS 140-2 Level 3 certified hardware security module (HSM).

- Encrypt and share all file types.

- Rosetta PKI HSM functionality generates key pairs, store digital certificates, digitally sign and encrypt email, and enables strong authentication.

- RES Pro protect files can be stored in popular cloud collaboration systems to provide an additional layer of data protection while keeping the keys in the hands of the data owners.

SPYRUS®

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

Technical Specifications

Functionality

RSA and Elliptic Curve Cryptography PKI-based digital certificate functionality such as email digital signatures and encryption and authenticated Web browsing.

Works with Rosetta USB, Rosetta microSDHC, P-3X, PocketVault Smart USB 3.0, WorkSafe, and WorkSafe Pro High-assurance FIPS 140-2 Level 3 protection for keys, digital IDs, and sensitive data security devices for secure hardware authentication

Storage Capacities

Up to 1 TB capacity on SPYRUS devices (P-3X Encrypted Storage, Windows To Go USB 3.0). Up to xxx TB on external storage media or system memory.

Electrical

See Technical Specification for the SPYRUS Security Device Used

Environmental

See Technical Specification for the SPYRUS Security Device Used

Packaging

See Technical Specification for the SPYRUS Security Device Used

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

Standards Compliance

FIPS PUB 46-3 Data Encryption Standard; FIPS PUB 180-3 Secure Hash Algorithm; SP 800-90A Random Bit Generator; FIPS PUB 186-4 Digital Signature Standard; FIPS PUB 197 Advanced Encryption Standard; SP 800-38A Block Modes of Operation; SP 800-56A Key Establishment Schemes; FIPS PUB 198 Keyed Hash Message Authentication Code

Security Certifications

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

Cryptographic Algorithms

Elliptic Curve Cryptography is part of a set of cryptographic algorithms published by the U.S. Federal Government 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 Key Establishment

ECDSA Digital Signature Algorithm

Concatenation KDF

RSA 2048 digital signature algorithm

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

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

XTS-AES 256 FDE, AES-CBC file encryption

SHA-1 and SHA-224/ 256/ 384/ 512 secure hash algorithms

Also including:

HMAC (min 112 bit key) keyed hash MAC

SP800-90A HASH_DRBG (RNG)

TDES-3key with ECB, CBC

SUITE B
ON BOARD

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) 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.