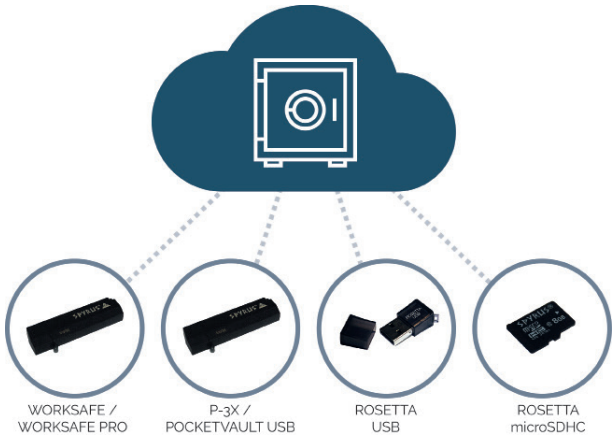
SPYRUS®

NcryptNshare™ RES Disk™ for Windows

Why trust today's information with yesterday's security?

Like A Bank Vault In Your Pocket



RES Disk combines SPYRUS military grade encryption software with a Rosetta PKI HSM in one of multiple form factors to create a high-security vault for strong data protection.

RES Disk is perfect for desktops, laptops, tablets, or any other Windows computing device. It works with local drives, network shares and cloud storage. RES Disk protects Data at Rest and enables secure data sharing with other user designated team members.

Unlike most other data protection solutions, RES Disk uses a FIPS 140-2 Level 3 Rosetta security module as a hardware root of trust to generate and protect digital identities and keys.

Cryptographic components in every SPYRUS security device are designed, engineered, and manufactured in the United States.

Features and Benefits

- Encrypt for the Life of Your Data—RES Disk implements next generation military grade elliptic curve cryptography, an interoperable cryptographic base recommended by NIST and global government organizations for both unclassified and most classified information.
- Encrypted virtual vaults can be stored anywhere—on the SPYRUS storage device, on your PC, on a file server, or in the cloud.
- RES Disk creates multiple encrypted virtual vaults that can be shared with other Rosetta users on Windows 7, 8, 8.1, and 10 platforms.
- With shared RES certificates, an encrypted virtual vault can be shared with individual or group contacts importing and exporting the RES Disk virtual vaults.
- Exported RES Disk virtual vaults can be made Read-Only to prevent any files from being modified or removed by the recipients.
- Cryptographic binding permits Read-Only virtual vaults to be securely accessed without modification for forensic applications.
- Keys are generated in the FIPS 140-2 Level 3 certified Rosetta HSM using a HASHDRBG random number generator compliant with NIST SP 800-90.
- Patented technology reconstitutes keys as required.
- Defense in Depth Data Protection using a double layer of encryption will protect data at rest by using a SPYRUS hardware-encrypting storage drive in combination with RES Disk.

SPYRUS®

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

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

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

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.

Document number; 400-520001-03