SPYRUS®

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

SPYRUS NcryptNshare™ for Secure Collaboration

With most employees working from home, public and private enterprises are looking for solutions that support secure collaboration. Employees and managers and even third-party partners need to see who has made what changes and when to presentations, whitepapers, and contracts. Perhaps more importantly, enterprises must ensure that their stakeholders only share data with authorized persons; and, be confident that the data is still protected at its destinations. Most data protection schemes focus on either limiting access or sharing data and hoping for the best. SPYRUS offers an alternative approach.

User-friendly Secure Collaboration

The SPYRUS DevicePatrol™ Platform is comprised of hardened endpoints and endpoint management, in a secure collaboration environment. All DevicePatrol tokens are powered by the SPYRUS Rosetta Microcontroller which can store authentication information, data, digital identity keys, and certificates.

The SPYRUS NcryptNshare application leverages the Rosetta Microcontoller to allow for individual documents, files and folders to include digital signatures, ensuring the source of the shared data. NcryptNshare also creates a personal secure vault on each user's personal computer(s) that cannot be accessed or viewed without the user's DevicePatrol token with the Rosetta Microcontroller that protects the encryption and authentication/ signature keys in FIPS 140-2 Level 3 hardware.

NcryptNshare provides the highest level of object encryption and controlled access so that cloud or other unsecured communication locations/ paths can be used with the highest levels of confidence. For example, a user can share information with only the intended recipient(s) via email, instant message or any sharing medium in any public cloud. A user can create secret file folders only accessable to individuals in groups who have their own token.

The SPYRUS patented "seal" of the encrypted file prohibits any tampering (for instance by malware), ensuring data is protected wherever it is stored. SPYRUS also provides data recovery capability that can be managed by the enterprise should a user's key be lost, disabled or destroyed.

NcryptNshare operates within the SPYRUS Hardware Roots of Trust (aka "Rosetta"). Rosetta is a FIPS 140-2 Level 3 validated security controller chip embedded in all DevicePatrol tokens. In addition to being anti-tamper, Rosetta offers a comprehensive list of cryptographic functions with RSA, elliptic curve and custom algorithms. By leveraging the key protection of Rosetta, NcryptNshare allows users to dynamically assign access to encrypted objects to enforces multi-factor authentication, ensuring that only the right user(s) have access to the information being shared.

NcryptNshare implements next generation elliptic curve cryptography, an interoperable cryptographic base recommended by NIST and global government organizations for both unclassified and classified information.

NcryptNshare supports two use cases that work together for secure collaboration:

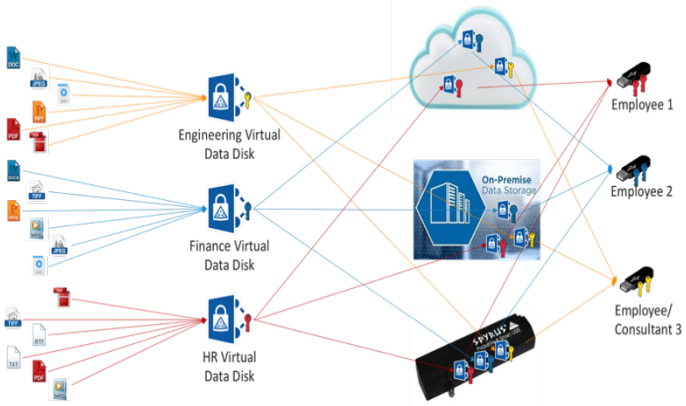
- Desktop: with a simple right click encrypt individual files and folders of files.

SECURED BY SPYRUS

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

- Secure Data Vault: create any number of high-security encrypted virtual vaults on any memory device such as microSD, SD, USB, computer hard drives, or network share drives.

In each case, whether creating an encrypted file or vault, NcryptNshare automatically brings up your personal or enterprise directory for easy point and click assignment of the persons NcryptNshare encryption certificates. With an option for the sender to sign the package.



Powerful Secure Collaboration

By separating access to specific data objects NcryptNshare can encrypt any file format and ensure that only the persons who should have access to an individual's private data has access to that data. The NcryptNshare securely wrap all data, only accessible to the destination device and/or individual, so that the cloud or other unsecured communication paths can be used with the highest levels of confidence.

NcryptNshare enables an enterprise to existing leverage n-premise, cloud and user owned devices to securely share enterprise critical data using secure vitural data disks to create groups and separately encrypt specific files within a vault for specific individuals.

Features and Benefits include:

- Encrypt and share all file types anywhere with the highest level of confidence.
- Decryption keys are in the hands of the data owner and those data is shared with.
- Patented technology reconstitutes keys as required.
- Defense in Depth Data Protection uses a double layer of encryption to protect data at rest.
- Support sharing with individuals or groups.
- Protected data can be stored in popular cloud collaboration systems to provide military grade data protection while keeping the keys in the hands of the data owners and those they choose to share it with.
- Recovery agent supports continuity for decryption in case the primary Rosetta key is lost or stolen.
- Protected data can be made read-only to prevent modification.
- Cryptographic binding permits read-only virtual vaults to be securely accessed without modification for forensic applications.
- Expiration date allows the sender to control the time duration of exposure to sensitive data.
- Digital signature assures data integrity and the originator's identity authenticates that the package was created by the publisher.
- KeyWitness® Notary Mode option enforces the use of hardware-based digital signature keys, providing file level non-repudiation.
- Rosetta PKI HSM functionality generated key pairs, store digital certificates, digitally sign and encrypt email, and enables strong authentication.
- File permissions can be set to disable printing and saving unencrypted versions of the file.
- Optional on-premise or cloud DevicePatrol Server for managing tokens.
- Works with all SPYRUS DevicePatrol tokens.

About SPYRUS

SPYRUS develops and deploys cryptographic solutions in innovative ways, providing the strongest protection for data in motion, data at rest and data in use. For more than 20 years, SPYRUS has delivered encryption, authentication, and digital content security products to government, financial, and healthcare enterprises. SPYRUS solutions enable customers to meet stringent regulatory requirements for data protections across industries.