SPYRUS®

SPYRUS Military Grade Suite B Data Protection Solution...

...for Surface Pro

With ever increasing data mobility and security requirements, government and commercial enterprises are demanding a versatile solution that allows for mobility and productivity without sacrificing data integrity and security. People need a seamless, easy method for secure document transportation, distribution, or for a full secure work space. By using the internal microSD reader in a Surface Pro tablet to interface with a SPYRUS Rosetta microSDHC™ as a hardware "Root of Trust", a user can function as usual, keeping the USB port free for other devices.

The configurable solution consists of the SPYRUS Rosetta® NcryptNshare™ RES Disk™ volume encryption application which allows creation of virtual encrypting vaults on memory devices such as a microSDHC, Secure Digital (SD) card, USB flash drive, hard drive, SSD, or network drive that can be shared with other authenticated RES Disk users. The SPYRUS Rosetta hardware security module (HSM) security devices are used to securely generate and store the user's private keys and used for secure multi-factor authentication and sharing access to the RES Disk virtual encrypting vaults.

When the RES Disk volume encryption application is loaded onto a Microsoft Surface Pro 3 or 4 tablet with the Windows 10 operating system, a Rosetta security device can instantly create a secure work space containing all of a user's required productivity software, VPNs, and layers of hardware and software encryption. Using a Rosetta security device with a VPN client requiring hardware two-factor authentication increases data security without limiting productivity

Rosetta Hardware Security Module (HSM) and Rosetta NcryptNshare RES Disk:

The RES Disk application allows for an encrypted single or multi-user virtual encrypted vault to be created on a Surface Pro or network drive using the FIPS 140-2 Level 3 certified Rosetta HSM microSDHC Suite B security services. With Microsoft Windows 10 group policies and system permissions, the RES Disk virtual encrypted vault can be configured to be the only writable area on the host machine. The Rosetta HSM is used as the "key" for hardware authentication to RES Disk and is available in multiple form factors across the SPYRUS product families to include Rosetta microSDHC, Smart Card or USB token, P-3X USB 3.0 encrypted storage, or the WorkSafe Pro Windows To Go live drive.

Configured on the Surface Pro Tablet with Windows 10:

When RES Disk is configured on a Surface Pro tablet with Windows 10 and BitLocker protection for full drive encryption, the user can have a versatile and secure workstation that has almost no impact on usability, performance or productivity.

The Surface Pro can be configured with Microsoft Windows security group policies to only allow users access to pre-installed applications, VPN clients, and the RES Disk encrypted virtual vault while locking down the rest of the system; including the hard drive on the Surface Pro. An administrator can have enhanced access privileges and use a second Rosetta HSM device for authentication to maintain the operating system and encrypted virtual vault contents. With the Rosetta microSDHC having both a PKI HSM and flash memory, the card can be loaded into the internal microSD reader with a tamper-evident seal with no writeable access to the flash for certain Government use cases. There are no other security tokens for the user to insert or keep track of and no need for additional external authentication devices.

The end user will simply log onto their Windows 10 Surface Pro tablet as normal. The RES Disk login screen will auto load, the user enters their RES Disk password, then authenticate to the RES Disk encrypted virtual vault through the hardware Rosetta HSM and then the RES Disk encrypted virtual vault will be decrypted and accessible for reading and writing.

SPYRUS®

Configured on the WorkSafe Pro Windows To Go Live Drive:

The WorkSafe Pro USB 3.0 SSD live drive can also be configured with Windows 10 and RES Disk with the added benefit of a layer of military strength hardware Suite B encryption. No additional user token will be required in this configuration as the WorkSafe Pro has an integrated Rosetta HSM embedded in the drive. This configuration turns virtually any computer into a secure work space by simply booting the user's work environment from the WorkSafe Pro drive.

Configuration steps:

- Install RES Disk and RES Enterprise Admin Tools in the base system image (Installation only, do not initialize the Rosetta HSM)
- Create Rosetta NcryptNshare Recovery Agent (Admin) security device (if required) which enables access to all RES Disk vaults should the user's Rosetta HSM be lost or stolen
- Create a configuration package (Rosetta configure, RES Disk Virtual Vault creation xml files, RES activation license file, custom shortcuts)
- Load the base Windows image to the workstation or tablet
- Run the RESWiz silent install command, followed by the RES Disk encrypted virtual vault creation silent run path
- Set the RES Disk Virtual Vault to Automount and add to autorun on start list
- Copy the shortcuts
- Enable BitLocker and set System GPOs
- Once the end user authenticates to Windows and sets the RES password, they will only have a single additional password to enter to use the secure Windows tablet

Customized configuration consulting services and use case deployment documents can be created to suit any need.

Specifications:

Windows computer, Rosetta HSM security device, or WorkSafe Pro

RES Disk

Rosetta MicroSDHC

Rosetta USB

WorkSafe Pro™ for WTG

PocketVault™ P-3X

Microsoft Surface™

For more information about SPYRUS products, visit www.spyrus.com or contact us by email or phone.

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

SUITE B ON BOARD

Western Region/Asia/Pacific Region
Tom Dickens
(408) 392-4324 phone
tdickens@SPYRUS.com

Central Region
Steve Tonkovich
(630) 215-9393 phone
stonkovich@spyrus.com

Eastern Region / EMEA
Rich Skibo
(732) 329-6006
rskibo@spyrus.com