SPYRUS®

Becoming GDPR Compliant

SPYRUS product overview

The GDPR mandate includes substantial penalties (the greater of €10 million or 2% of global annual turnover), if an organization fails to provide a "reasonable" level of protection for personal data, regardless of intent. Global companies, with headquarters outside the EU, remain subject to GDPR penalties for their EU based subsidiaries.

Organizations cannot leave the term "reasonable" up to an evaluator's post event discretion. Legal fees to prove reasonable effort can be as costly as the GDPR penalties themselves. High assurance transparent encryption solutions offered by SPYRUS provide a sound underpinning to meet GDPR, particularly Article 25 covering "data protection by design and by default". The SPYRUS hardware roots of trust, its Rosetta Hardware Security Module (HSM) enabled security products, are the only solutions where reasonability cannot be challenged.

SPYRUS devices, protected by the Rosetta HSMs, are fully encrypted with keys and military grade algorithms, both hardware protected, that have been used for up to classified data protection as a standard commercial product.

Windows To Go

SPYRUS Windows To Go (WTG) live drives turn personal computers, including Surface Pros into compliant enterprise Windows 8, 8.1 or 10 desktops - with or without connectivity. SPYRUS WTG drives boot the OS directly from the hardware encrypted compartment and completely bypass the host computer's hard drive. There is no impact on the host computer and no footprint left behind when the drive is shut down. Features include:

- Built-in PKI smart card
- FIPS 140-2 Level 3 validated
- XTS-AEX 256 hardware encryption
- Read only mode options
- Data vault read/write option (can be used on Surface Prof 4 for secure data management)
- MIL-810 tested hardware providing military ruggedness

SPYRUS can lower your operating costs, adds significant security to your end-points and makes it easier to support BYOD policies for both employees as well as for Contractors and Teleworkers. SPYRUS WTG is even used in Computer Replacement decisions as a way to extend life and performance of computers without the full cost of computer replacement, less than 1/3 the cost.

Rosetta TrustedFlash™

The Rosetta microSDHC card with TrustedFlash™ configuration enables hardware AES-256 encryption to provide the strongest commercially available data protection and PKI capabilities to use with public key enabled applications. It is designed from the ground up to bring high-assurance information protection to mobile devices, laptops and tablets such as Surface Pro 4 for data at rest and in transit. Its convenient form factor enables secure data storage for devices with limited USB ports or devices that only have microSD slots, all without the USB device disadvantage of protruding from the computing platform.

Organizations in the Enterprise, Government, Critical Infrastructure, Healthcare and other verticals will be able to protect sensitive data and privately identifiable information (PII) using SPYRUS's military grade security along with using digital certificates stored in the FIPS 140-2 Level 3 validated onboard HSM to authenticate to networks and to Microsoft cloud services and applications.

Pocket Vault 3-X

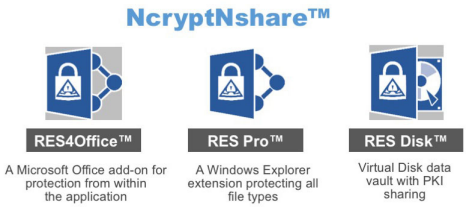
The PocketVault P-3X USB 3.0 encryption device is a high-security, use-anywhere hardware encrypting solid-state disk (SSD) device that protects data like a bank vault. The combination of USB 3.0 and SSD storage adds up to the fastest performance available. The PocketVault P-3X encrypts with a XTS-AES 256-bit key to protect sensitive and confidential data. Why trust today's data with yesterday's security?

The Pocket Vault 3-X adds further security capabilities such as providing authentication and public key enabled (PKE)

SPYRUS®

application services used by enterprise and Government organizations for two factor authentication and secure communications with Microsoft Cloud Services and applications.

The P-3X Courier mode is for use in demanding applications where modifications to data must be restricted to privileged users and Read-Only capabilities are only permitted to limited users. Use cases would have the privileged user putting sensitive data on the P-3X device, such as sales forecasts, sales accounts, financial forecasts, intellectual property, sensitive presentation material or even for data base updates; and limiting the end user to only "reading" the data and not allowing any changes to the data.

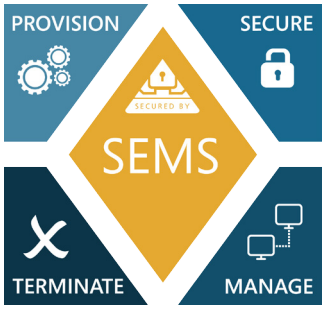


NcryptNshare

NcryptNshare in conjunction with above hardware encrypted and enabled smart card smart card devices supports the multiparty collaboration features of the NcryptNshare applications for end-to-end encryption and sharing between senders and recipients to protect data in transit and at rest. The NcryptNshare™ product line provides encryption, authentication, and collaborative information sharing across Microsoft Office, Office 365 and Microsoft Cloud Services products. The NcryptNshare product family includes:

- RES4Office, a plug in for Office to enable file encryption and secure file sharing;
- RES Disk, which allows creating secure virtual disks for encrypting and secure sharing and;
- RES Pro, a Windows Explorer Extension application that gives the user a right click experience to encrypt any file type and permit secure sharing with any other authenticated RES Pro user.

SPYRUS Enterprise Management System ("SEMS™")



SEMS provides a very strong security and productivity solution for any organization deploying SPYRUS encrypting secure storage drives and/or our Microsoft certified bootable Windows To Go Live Drives. While these drives provide the strongest Data-at-Rest protection when used by the mobile workforce, organizations are faced with another challenge that is the management, audit and policy enforcement of these high capacity, small form factor devices. SEMS solves that problem. SEMS was designed to operate on the Windows server ecosystem on premise or on Microsoft Azure with ability to scale from proof of concept with a small number of devices to deployments with tens of thousands of devices under management.

SEMS extends a true end-to-end security approach to mobile users to protect data at rest; in transit and enabling the enterprise to comply with government regulations. With SEMS device management, enterprise administrators can centrally register, block/unblock, revoke, set policies, audit, and "kill" the SPYRUS hardware encrypted devices.

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