

Secure Command and Control of Encrypted USB Flash Drives

The SPYRUS Enterprise Management System (SEMS) was designed from the ground up for secure lifecycle management of USB encryption devices. Its plug-in architecture enables vendors to integrate their devices within the common interface facilities provided by SEMS.

SUPERIOR SECURITY

- Smart card authentication of SEMS administrators
- Hardware-based certificate authority and Public Key Infrastructure (PKI) enforce trust and accountability
- Advanced cryptographic protection provided by AES 256, ECDH P-384, and SHA-256 algorithms

- **Minimize the threat to your organization** through secure device management that actively controls devices remotely across an intranet or the Internet.
- **Complete device lifecycle management**—provision, assign, disable, enable, zeroize, and terminate devices.
- **Protects critical management commands** to prevent an attacker or rogue from taking control of your management system.
- **SPYRUS Rosetta® USB smart cards** are used for multi-factor authentication and certificate-based encryption of management and device communications.
- **SPYRUS LYNKS** hardware security module generates and stores keys and performs cryptographic operations to authenticate operations and protect against “man-in-the-middle” attacks.

SECURED BY SPYRUS®

USB storage devices are necessary for data mobility in the modern work environment. Many USB devices include integrated security features such as network authentication, smart card functionality, and password-protected encrypted storage, making them “must-have” devices for today’s enterprise. However, the advanced functionality within these devices can also pose a threat to an organization and the security of its networks and data. With ever-increasing storage capacities, the consequences of losing a device containing sensitive information, passwords, or cryptographic keys can be extremely damaging. Even if the data is encrypted, a specific device and its owner can be targeted through social engineering to obtain not only the device but also the password that protects its encrypted content.

A rogue employee could store large amounts of valuable data on a device and walk out the door with it and the company’s information. Worse, customer information could leak, possibly triggering notification to state and local governments along with the affected parties. Even loyal employees sometimes forget about security and carelessly leave their devices or device passwords exposed and unattended.

A device management system based on software cryptography cannot be used to protect and control high-assurance hardware security devices because it will become the targeted attack point as the weakest link. For this reason, SEMS was designed using government-approved next-generation cryptographic algorithms. Hardware security modules are used to implement PKI, server, and administrator authentication to combat both external and internal threats.

ACTIVE DEVICE CONTROL

- Deny use of device on managed domain
- Disable device, requiring SEMS approval to enable
- Destroy keys and data on device

The SEMS system uses two cooperating components: the SEMS management server and the SEMS client component running on the endpoint. An administrator can set and enforce security policies on the server for each registered device and define the actions that must be performed by the SEMS client.

Each time the device is used, the SEMS client component automatically attempts to create a secure connection to the SEMS server to determine whether or not the action is permitted. If an administrator has disabled a device, the SEMS client component blocks the device’s operation, requiring subsequent administrator authorization to re-enable the device. If the device cannot contact the server, then offline policies are implemented, including how many times the device can be used before it will block itself from use until reset by an administrator.

STRONG DATA PROTECTION

SPYRUS was the first security manufacturer to implement hardware-based Suite B security across their entire product line. Suite B is a set of cryptographic algorithms



promulgated by the National Security Agency as part of its Cryptographic Modernization Program. Suite B was designed to serve as an interoperable cryptographic base for both unclassified information and most classified information to strengthen the level of information protection within the US Government.

FLEXIBLE DEVICE INTEGRATION

The SEMS system incorporates an open API that allows the management of USB encryption devices from other vendors.

It ships with plug-ins for Hydra Privacy Card® (Hydra PC™) Digital Attaché, PocketVault P-384, and Secure Pocket Drive.



ABOUT SPYRUS

SPYRUS, Inc. provides high-assurance security technology for the U.S. Government, industries required to comply with security regulations, and everyday users who want the best protection for sensitive information. All Secured by SPYRUS® security technology is designed, developed, and manufactured entirely in the USA. SPYRUS hardware and software support the strongest commercially available cryptographic algorithms, including elliptic curve cryptography (ECC) and AES-256, which exceed the U.S. Government Suite B standard. SPYRUS holds patents in the U.S. and abroad that enable peripheral device solutions for data-at-rest storage, secure authentication, secure communication, and full disk encryption, as well as patents relating to data protection and rights management for digital content. SPYRUS is a privately-held U.S.-based company and is a Microsoft managed ISV partner.

Trademark notice: “Protected by U.S. Patents 7,380,140; 6,088,802; 6,981,149; Patents Pending. SPYRUS, the SPYRUS logos, Hydra PC, Trusted Mobility, Secured by SPYRUS, Security to the Edge, Suite B On Board, Rosetta, and LYNKs, are either registered trademarks or trademarks of SPYRUS, Inc. in the U.S. and/or other jurisdictions.

Document number: 415-420002-05