



SPYRUS Enterprise Management System (SEMS) Secure Command and Control of Encrypting USB Devices

Introduction

USB storage devices are necessary for data mobility in the modern work environment. With many of them possessing integrated security features such as network authentication, smart card functionality, and password-protected encrypted storage, they have become “must-have” devices for today’s enterprise. However, the advanced functionality within these devices can also pose a major 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 the use of social engineering to obtain not only the device but also the password used to encrypt its contents.

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 requiring you to notify state and local officials along with the affected parties. Even loyal employees sometimes forget about security and carelessly leave their devices or device passwords exposed and unattended.

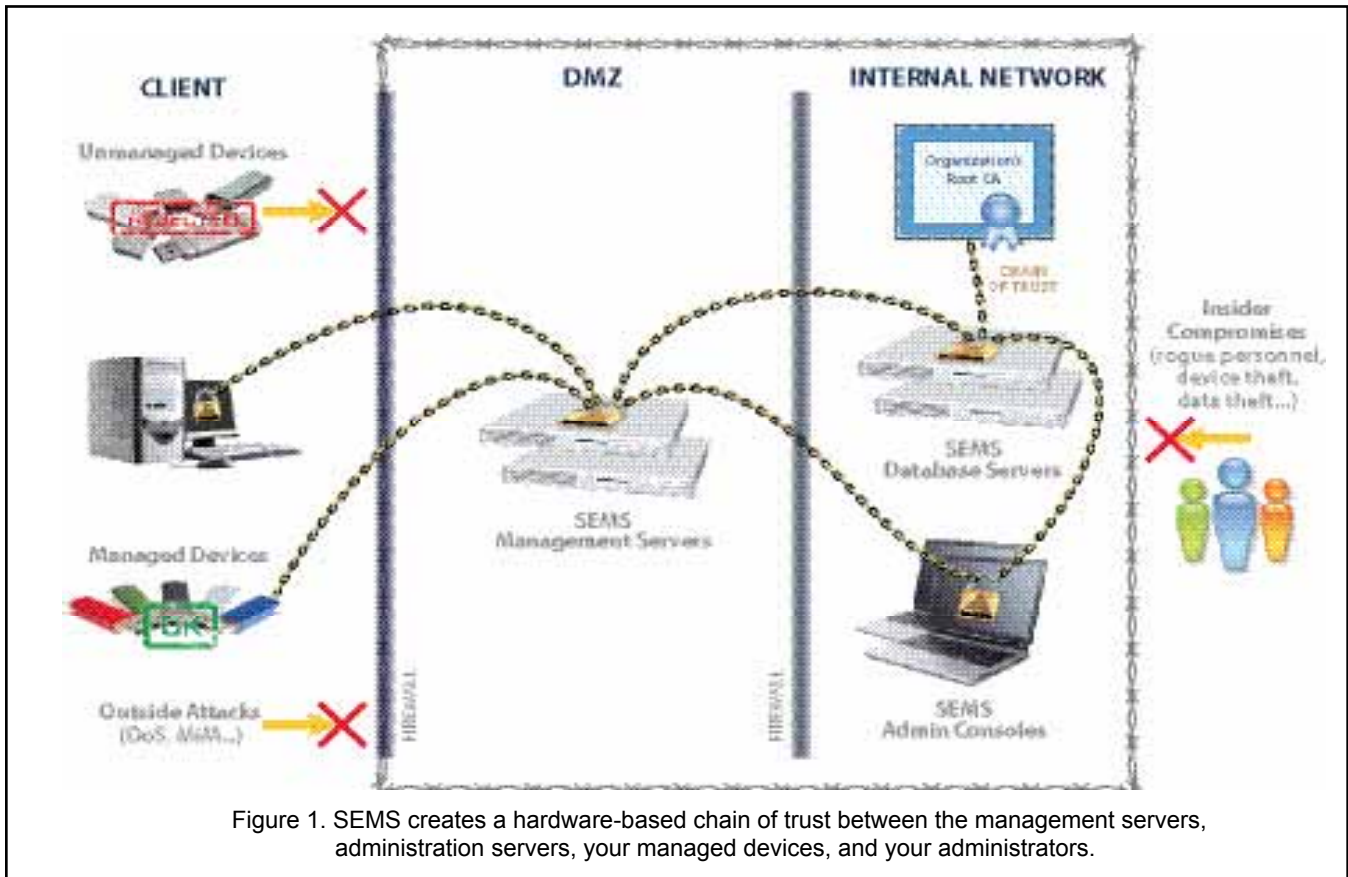


Figure 1. SEMS creates a hardware-based chain of trust between the management servers, administration servers, your managed devices, and your administrators.

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 (see fig. 1). This makes SEMS an invaluable addition to an organization’s security arsenal to help ensure that confidential information cannot leak or be destroyed accidentally or maliciously.

SPYRUS Enterprise Management System

The SEMS device management system, with its open API and available SDK for integration by third party vendors, manages the complete range of SPYRUS USB encryption devices and enables management of third party USB encrypting flash drives. For example, the Kingston DataTraveler 5000 encrypting USB flash drive has already been integrated into SEMS.

SEMS is designed to minimize threats to an organization by providing secure device management and reporting capabilities. The top-level Device screen shows the type of secure USB device, its serial number, to whom it is assigned, and its current status (see fig. 2). Devices can be managed and audited (see fig. 5) no matter where they are located, and the organization's security policies are enforced whether or not a device is connected to a network.

The SEMS system can:

- Deny use of a device
- Disable a device, requiring administrator approval to re-enable it
- Destroy the data and keys on a device, rendering it unusable

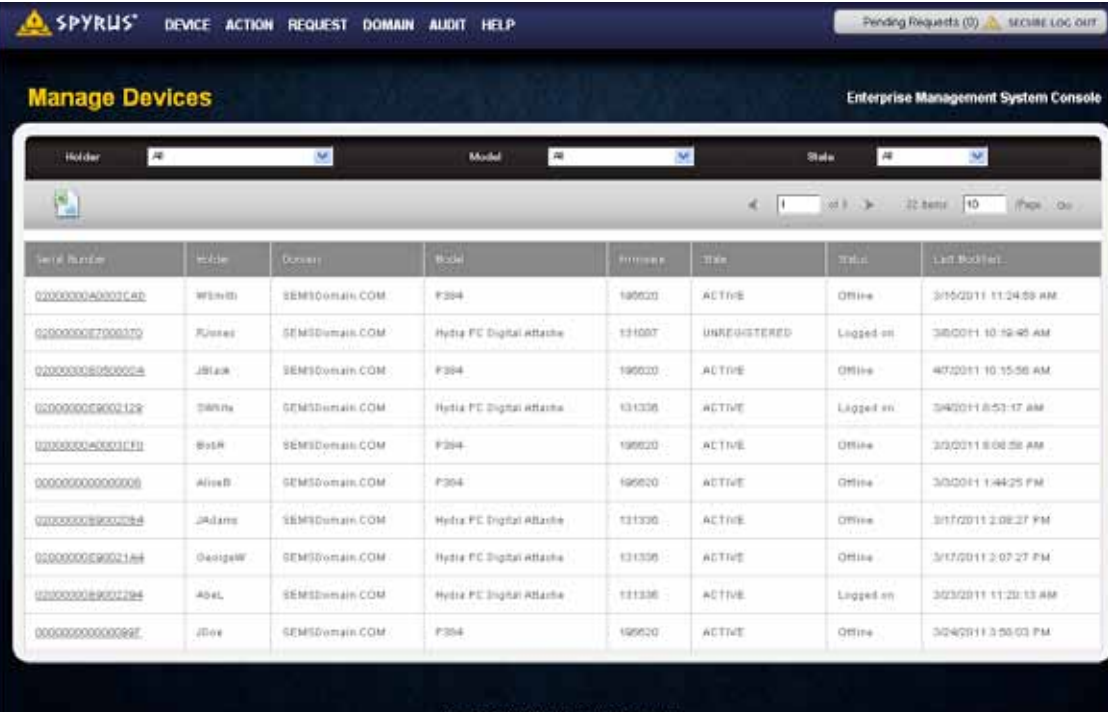
Client / Server Model

The SEMS system uses two cooperating components: the SEMS management server and the SEMS client component running on the endpoint. The SEMS management system allows an administrator to set and enforce security policies 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 creates a secure connection to the SEMS server and determines whether or not the action is permitted. If an administrator has disabled a device, the SEMS client blocks the device's operation, requiring subsequent administrator authorization to re-enable the device.

Offline Mode

SEMS device policies are enforced even when the device cannot connect to the SEMS server. An additional offline policy defines how many times a device can be used before having to re-establish a connection with SEMS. Like online policies, the device can be set to disable or destroy itself if specified offline thresholds are exceeded.



Serial Number	Holder	Domain	Model	Firmware	Title	Status	Last Modified
02000000A000C4b	WInchB	SEMSDomain.COM	F304	190020	ACTIVE	Offline	3/15/2011 11:24:59 AM
02000000E7000370	RJweel	SEMSDomain.COM	Hydra FC Digital ABatch	131007	UNREGISTERED	Logged on	3/8/2011 10:16:46 AM
02000000B0500004	JBlack	SEMSDomain.COM	F304	190020	ACTIVE	Offline	4/7/2011 10:15:56 AM
02000000E900122	DMRhs	SEMSDomain.COM	Hydra FC Digital ABatch	131336	ACTIVE	Logged on	3/4/2011 8:53:17 AM
0200000045001C7F1	BoyaR	SEMSDomain.COM	F304	190020	ACTIVE	Offline	3/2/2011 8:08:26 AM
0000000000000000	AlireB	SEMSDomain.COM	F304	190020	ACTIVE	Offline	3/2/2011 1:44:25 PM
0200000092000054	JAJans	SEMSDomain.COM	Hydra FC Digital ABatch	131336	ACTIVE	Offline	3/17/2011 2:08:27 PM
02000000E9002144	Georgew	SEMSDomain.COM	Hydra FC Digital ABatch	131336	ACTIVE	Offline	3/17/2011 2:07:27 PM
02000000E9002294	AbelL	SEMSDomain.COM	Hydra FC Digital ABatch	131336	ACTIVE	Logged on	3/23/2011 11:20:13 AM
0000000000000082E	JBoe	SEMSDomain.COM	F304	190020	ACTIVE	Offline	3/24/2011 3:50:03 PM

Figure 2. The Device screen shows the device assignee or holder, the type of device, and its current status.

Device	Holder	Action	Authorization Code	Authorized By	Authorization Date	Implementation Date	Status
0000000000000099E	JDvx	UPDATE		benjamin	3/25/2011 11:10:40 AM		PENDING
0000000000002234	AlisL	UPDATE		benjamin	3/25/2011 11:10:40 AM		PENDING
000000000000000A	JRlax	UPDATE		benjamin	3/25/2011 11:10:40 AM	3/25/2011 12:40:53 PM	COMPLETED
0000000000007232	BuR	ENABLE	7245-0401	benjamin	3/25/2011 8:33:34 AM	3/25/2011 8:35:44 AM	COMPLETED
0000000000007232	BuR	DISABLE		benjamin	3/25/2011 1:23:55 AM	3/25/2011 8:30:38 AM	COMPLETED
0000000000000099E	JDvx	ENABLE	4756-0813	benjamin	3/23/2011 1:48:28 PM	3/23/2011 1:50:39 PM	COMPLETED
0000000000000099E	JDvx	ENABLE	7726-7379	benjamin	3/23/2011 11:47:14 AM	3/23/2011 11:50:17 AM	COMPLETED
0000000000000099E	JDvx	DISABLE		benjamin	3/23/2011 4:45:51 AM	3/23/2011 11:48:34 AM	COMPLETED
0000000000000099E	JDvx	ENABLE	8175-0821	benjamin	3/23/2011 11:05:58 AM	3/23/2011 11:09:03 AM	COMPLETED
000000000000000A	JRlax	ENABLE	9902-6818	benjamin	3/18/2011 11:37:03 AM	3/18/2011 11:39:00 AM	COMPLETED

Figure 3. The Actions screen allows the administrator to push commands to devices.

Strong Authentication and Security

With the ability to render a device and its data either temporarily unusable or permanently unrecoverable, it is essential that the management system itself is at least as secure as the devices that it manages. SEMS employs strong cryptographic mechanisms.

Smart card-based authentication is implemented to block unauthorized access to the SEMS administrator console. To prevent a rogue from sending SEMS commands to your organization's devices or connecting a bogus server to your network, the SEMS servers use SPYRUS LYNKS® hardware security modules to generate and store cryptographic keys and to perform cryptographic operations.

Risk-Based Management

SEMS allows for different levels of action dependent upon the level of perceived risk that a device poses to an organization. A SEMS administrator can issue the appropriate command based on whether a device is mislaid, misused, lost, or stolen (see fig. 3).

Mislaid Device

If a device has been temporarily mislaid, but the user is confident that it can be quickly located, an administrator can temporarily "disable" the device, requiring the owner to go through an authorization process to re-enable the device when it becomes available. This "disabling" prevents the device from being used in the interim.

Lost or Stolen Device

In situations where a device is known to be lost or stolen, a SEMS administrator can take more drastic action than simply disabling the device—the device can be destroyed if an attempt is made to logon or use it.

Device destruction means that the cryptographic keys and data are zeroized, rendering the device unusable.

Scales to the Largest Organizations

The PKI-based modular architecture and self-service capabilities (see fig. 4) implemented within SEMS allows continuous expansion as the number of devices under management grows.

Multiple management servers and administrators can be located anywhere within your organization and devices can be migrated from server to server for convenience. You can issue and provision devices at HQ then migrate them to a management server thousands of miles away in the field.

Easily Integrate Third-Party USB Devices

The SEMS system incorporates an open API that allows the management of USB encryption devices from other vendors. The API is provided as part of the SEMS software development kit, which includes sample source code, examples, required resources, and documentation. This API uniquely positions the SPYRUS SEMS system as one of the few products on the market to allow this type of third-party integration.

Vendors can use their own proprietary techniques to implement internal device operations without exposing their proprietary architecture.

SPYRUS provides libraries, header files, and interface

descriptions to enable integration of vendor devices.

The software development kit includes:

- C header files and example source code
- Descriptions of SEMS integration library interfaces and their parameters and result codes
- Sample code
- Libraries initially are supported on Windows with future releases for Linux and Macintosh

Choose Your Devices Wisely

It is important to note that SEMS cannot make a device more secure than it already is. While SEMS enforces administrator authentication and sends commands securely, the way that a vendor implements the actions cannot be controlled by SEMS.

SEMS also cannot increase the native data protection strength of secure USB storage devices.

If overall device security is important, it must be

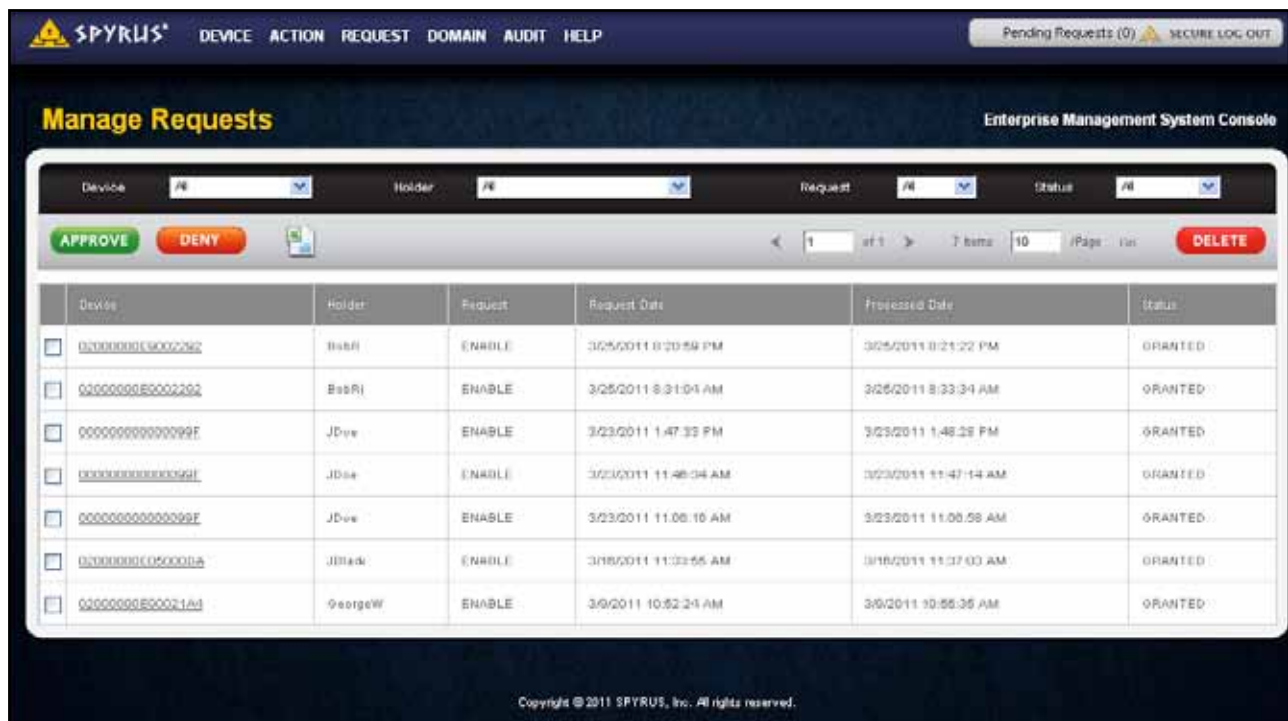


Figure 4. Self-service allows end users to provision and edit their devices under administrator supervision

evaluated independently of the management tool. Of course, SPYRUS encrypting storage devices are recommended, thus ensuring that every link in your secure storage infrastructure is just as strong as the next.

The Strongest Possible 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.

SEMS uses these Suite B algorithms and associated key lengths for digital signature, key agreement, symmetric encryption, and hashing:

- Elliptic curve cryptography (P-256, P-384, P-521)
- Advanced Encryption Standard (including XTS)
- SHA2 (224, 256, 384, 512)
- Elliptic curve Diffie–Hellman (ECDH)



SPYRUS® DEVICE ACTION REQUEST DOMAIN AUDIT HELP Pending Requests (1) SECURE LOG OUT

Device Enterprise Management System Console

02000000A0003DF1 Specifications JAdams **DELETE**
 4/7/2011 6:12:22 PM P384 SEMSDomain.COM
 DISABLED FW: 196620

DISABLE DESTROY

Request Action

1 of 1 2 Items 10 /Page Go

Action	Authorization Code	Authorized By	Authorization Date	Implementation Date	Status
DISABLE		SEMSAdmin	4/7/2011 11:11:57 AM	4/7/2011 6:12:22 PM	COMPLETED
UPDATE		SEMSAdmin	4/5/2011 9:44:03 PM	4/7/2011 6:07:18 PM	COMPLETED

Figure 5. Every device action is logged.

Features and Benefits

- Minimizes 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, enable/disable, 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.
- A SPYRUS LYNKS hardware security module generates and stores keys and performs cryptographic operations to authenticate operations and protect against “man-in-the-middle” attacks.

Specifications

- Plug-in management architecture with open APIs enables vendors to securely integrate their encrypting USB flash drives.
- Includes plug-ins for Hydra Privacy Card® (Hydra PC™) Digital Attaché, Pocket Vault P-384, and Secure Pocket Drive.

Requirements

Management Server

- Dual-core X86 processor, 2 GB RAM, 100 GB hard drive, 2 USB 2.0 ports
- Windows Server 2003 SP2 w/current patches
- .Net Framework 2.0
- SQL Server 2005
- Microsoft Internet Information Services (IIS)
- SPYRUS LYNKS hardware security module
- SPYRUS En-Sign 8.0

Administration Server

- Can be combined with the management server
- Windows Server 2003 SP2 w/current patches
- .Net Framework 2.0
- IIS

Admin Console

- Windows XP SP2 or SP3
- Internet Explorer 7.0, Firefox 3.5.11, or later
- SPYRUS En-Sign 8.0
- Rosetta USB readerless smart card for each administrator

Endpoint

- Windows XP SP3, Vista, or Windows 7
- No special software other than that required for the device itself



Document number 400-420001-05

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) 329-6211 fax

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
info@SPYRUS.com.au



© Copyright 2010 SPYRUS, Inc. All rights reserved. SPYRUS, the SPYRUS logos, Security to the Edge, Hydra Privacy Card, Hydra PC, Hydra PC Digital Attaché, Hydra PC Secure Pocket Drive, Rosetta, LYNKS, En-Sign, and SPYCOS are either registered trademarks or trademarks of SPYRUS in the United States and/or other countries. All other trademarks are the property of their respective owners. Individual SPYRUS products may embody technology protected by one or more of the following patents or patent applications: U.S. Pat. Nos. 7,380,140; 6,088,802; 6,003,135; 6,981,149; U.S. Pat. Appl. Ser. Nos. 12/018,094; 12/126,759.

Specifications subject to change without notice