



## LYNKS™ Series II HSM

### High-Assurance Hardware Security Module



The LYNKS Series II Hardware Security Module (HSM) delivers a cost-effective solution for Certificate Authority (CA) and Registration Authority (RA) key operations, digital signatures, and key recovery.

Now you can carry a CA or RA in your pocket that you can securely deploy anywhere without needing a rack full of gear. While perfect for field deployment at a moment's notice, it is equally at home in a data center.

Built on the SPYRUS Cryptographic Operating System (SPYCOS®), the LYNKS Series II implements US Department of Defense Suite B algorithms in high-speed hardware. Part of its Cryptographic Modernization Program, Suite B algorithms are meant to serve as an interoperable cryptographic base for

both unclassified information and most classified information and includes ECDSA-256 and 384, ECDH-256 and 384, AES-128 and 256, SHA-256, and 384. LYNKS also supports ECDSA and SHA with 512 bit prime moduli.

Available in a stackable USB case, the LYNKS Series II HSM provides the strongest, most economical, future-proof protection for valuable data available anywhere.

### Benefits

- Affordable certificate storage solution for TV and video service providers using the Microsoft Mediaroom IPTV software platform
- The largest suite of algorithms supported in a device of its type provides flexibility to meet high-assurance requirements in the commercial sector and for the U.S. Government.
- Future-proof design allows signed firmware updates when new cryptographic algorithms or features become available.
- Unneeded features can be removed to fit your requirements.
- FIPS 140-2 Level 2 validated overall
- Password required to unlock user's private keys
- Optional *HSM Copy* utility can clone a LYNKS HSM to create a locked-down replica as a backup.
- Tamper-resistant, tamper-evident design and construction
- Optional trusted, auditable time stamp
- Supports applications using Microsoft® Windows® Cryptographic API (MSCAPI), Microsoft Card Module and PKCS #11 interfaces

### Features

- In addition to Suite B, LYNKS also supports legacy RSA 1024, RSA 2048, and RSA 4096 keys.
- NIST SP 800-90 deterministic random bit generator and X9.31 key generation.
- Microsoft WHQL certified drivers available for Windows 2000, Windows XP, Windows Vista, Windows 7, and Windows Server 2003
- 50 key and certificate slots on device
- Cryptographic hardware acceleration for AES and SHA-2
- Optional 1U rack-mount physically secures 6 units

# Technical Specifications

## ▲ Supported Cryptographic Algorithms

- RSA 1024, RSA 2048, RSA 4096, and DSA 1024 Digital Signature and Key Exchange Algorithms
- SHA-1, MD5, and SHA-224/256/384/512 Secure Hash Algorithms; HMAC with SHA-1
- DES, two & three-key triple DES with ECB, CBC
- KEA Key Exchange – 1024 exchanges 80-bit SKIPJACK key
- Advanced Encryption Standard (AES) 128/192/256 ECB, CBC, , CTR, and key wrap modes
- Elliptic curve cryptography (ECC) using the NIST curves in GF(p) (P-256, P-384, and P-521)
- ECMQV and ECDH key establishment in accordance with NIST SP 800-56A Key Establishment Guidelines
- ECDSA Digital Signature Algorithm

## ▲ Interface

- USB 1.1 compliant and USB 2.0 compatible (USB)

## ▲ Dimensions

- 92.5 mm (3.64") x 60.5 mm (2.38") x 9.8 mm (.385"), 1.9 oz.



## ▲ Security Certifications

- FIPS 140-2 Level 2 validated with Physical Level 2 and Level 3 options

## ▲ Electrical

- Operating voltage:  $V_{cc} = 5VDC \pm 5\%$
- Power consumption: <1 W average
- Lithium battery with an expected storage life of seven or more years

## ▲ Environmental

- Operating temperature: 0°C to 55°C
- Storage temperature: -20°C to 60°C
- Humidity: 90%, noncondensing

## ▲ Standards Compliance

- Microsoft WHQL-certified drivers
- Microsoft CryptoAPI, and PKCS #11 interoperability
- FIPS PUB 46 Data Encryption Standard
- FIPS PUB 180-2 Secure Hash Algorithm Standard
- FIPS PUB 186-2 Digital Signature Standard
- FIPS PUB 197 Advanced Encryption Standard
- SP 800-38A Block Modes of Operation
- Federal Communications Commission FCC Class B certification and CE Mark Certification-Windows XP Professional SP2

Proudly designed, engineered,



and manufactured in the USA



Document number: 400-160002-11

For more information about SPYRUS products, visit [www.SPYRUS.com](http://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](mailto: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](http://www.spyrus.com.au)  
[info@SPYRUS.com.au](mailto:info@SPYRUS.com.au)

