SPYRUS®

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. Separate LYNKS models serve as CA HSM or RA HSM.

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. 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 include 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, and legacy RSA 1024, RSA 2048, and RSA 4096 keys.

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

Features

- Password required to unlock user's private keys.
- LYNKS CA HSM can generate new CA key or import an existing CA key.
- NIST SP 800-90 deterministic random bit generator and X9.31 key generation.
- FIPS 140-2 Level 2 validated overall.
- Optional HSM Copy utility can clone a LYNKS CA HSM to create locked-down LYNKS CA HSM replica as backup.
- Tamper-resistant, tamper-evident design and construction.
- Future-proof configuration allows signed firmware updates for new cryptographic algorithms or features.
- Supports applications using Microsoft® Windows® Cryptographic API (MSCAPI), Microsoft Card Module and PKCS #11 interfaces.
- 50 key and certificate slots on device.
- Cryptographic hardware acceleration for AES and SHA-2.
- Microsoft WHQL certified drivers available for Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2008.

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

Proudly designed, engineered, and manufactured in the USA

SPYRUS®

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- and 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, USB 2.0/USB 3.0 compatible

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 3 all categories except physical Level 2 Overall; FIPS rating Level 2 Certificate number 679

Electrical

Operating voltage: Vcc = 5VDC ± 5%

Power consumption: <1 W average

Lithium battery with seven or more years expected storage life

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

RSA/ECC Performance to the Card Edge

AES cypher rate: 165 KBps

3DES cypher rate: 700 KBps

ECC Key Generation		ECC Sign		ECC Verify	
P256	3.5 sec	P256	231 msec	P256	951 msec
P384	4.17 sec	P384	390 msec	P384	2.07 sec
P521	8 sec	P521	861 msec	P521	2.45 sec

RSA Key Generation		RSA Sign*		RSA Verify	
1024	30 sec	1024	161 msec	1024	40 msec
2048	6 min	2048	6 sec	2048	6 sec
4096	8.5 hrs	4096	2.5 min	4096	33 sec

*RSA key generation time is based on an average

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) 832-0123 fax

UK Office
+44 (0) 113 8800494

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

Document number 400-160002-15