



LYNKS™ Series II HSM

High-Assurance Hardware Security Module

The LYNKS Series II Hardware Security Module (HSM) family offers a high-security solution for client, server, and embedded security applications. The LYNKS Series II HSM, with upgraded flash memory and FPGA capabilities, supports the new stronger and faster cryptographic algorithms, including elliptic curve cryptography with EC-DH and ECMQV key establishment, AES, and SHA-2 algorithms, that exceed the U.S. Government's Suite B standard. Available in either PCMCIA or stackable USB versions, the new LYNKS Series II HSM provides the strongest, most economical, future-proof protection for valuable data available anywhere.

Benefits

- ▲ LYNKS Series II HSM delivers a cost-effective solution for Certificate Authority and Registration Authority key operations, digital signatures, and key recovery.
- ▲ Supports RSA 1024, RSA 2056, and RSA 4096 keys. Key generation complies with the stringent X9.31 specification.
- ▲ The cryptographic algorithms meet all requirements for business use and the U.S. Government's Suite B standard for unclassified, releasable algorithms used to protect classified information.
- ▲ Future-proof design allows firmware updates through secure download when new cryptographic algorithms or features become available. Unneeded features can be removed just as easily to fit your requirements.
- ▲ 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.

Features

- ▲ Most secure random number generator and key generation technology
- ▲ FIPS 140-2 Level 2 validated overall
- ▲ PIN required to access user's private keys
- ▲ Optional HSM Copy utility can clone a LYNKS HSM to create a locked-down replica as a backup CA.
- ▲ Tamper-resistant, tamper-evident design and construction
- ▲ Trusted, auditable time stamp (custom option)
- ▲ Supports applications using Microsoft® Windows® Cryptographic API (MSCAPI), Microsoft Card Module and PKCS #11 interfaces
- ▲ Drivers certified by Windows Hardware Quality Labs (WHQL) available for Microsoft Windows 2000, Windows XP, and Windows Server 2003
- ▲ PCMCIA interface and stackable modular design USB interface
- ▲ 50 key and certificate slots on device
- ▲ Cryptographic hardware acceleration for AES and SHA-2



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, OFB, 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

Interfaces

- ▲ PCMCIA 2.1 compliant (PC Card)
- ▲ USB 1.1 compliant and USB 2.0 compatible (USB)

Dimensions

- ▲ PCMCIA: 85.6 mm (3.37") x 54 mm (2.126") x 4.98 mm (.196"), 1.5 oz.
- ▲ USB: 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
- ▲ PCMCIA 2.1 specifications for vibration, shock, bending, torque, & drop

Standards Compliance

- ▲ Microsoft WHQL-certified drivers
- ▲ Microsoft CryptoAPI, Microsoft Card Module 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

SPYRUS, Inc.

For additional details about SPYRUS products, visit www.spyrus.com or contact us at:

- ▲ USA +1 408 392-9131 info@spyrus.com
- ▲ Australia +61 7 3220-1133 info@spyrus.com.au

