

# LYNKS™ Series II Authentication HSM

High-Assurance Hardware Security Module Specifically Designed for Authentication Applications



The LYNKS Series II Authentication HSM delivers a cost-effective solution for digital signature operations.

The largest suite of algorithms supported in a device of its type provides flexibility to meet high-assurance requirements in the commercial sector. The LYNKS Series II Authentication HSM implements digital signature algorithms in high-speed hardware. Digital signature capabilities include ECDSA with P-256, P-384, and P-521 keys, SHA 256/384/512, and the legacy RSA-1024, RSA-2048, and RSA-4096 algorithms.

SHA-1 and MD5 are included for backward compatibility, but their use is deprecated.

LYNKS Series II Authentication HSM can be used only for digital signing and digital signature verification. It cannot be used for data encryption.

Available in a stackable USB case, the LYNKS Series II Authentication HSM provides the strongest, most economical, future-proof protection for applications.

## Features

- Password required to unlock user's private keys.
- NIST SP 800-90 deterministic random bit generator and X9.31 key generation.
- FIPS 140-2 Level 2 validated overall.
- 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.
- Hardware acceleration for 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

Digital signature algorithms using the NIST curves in GF(p) (P-256, P-384, and P-521)

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 180-2 Secure Hash Algorithm Standard

FIPS PUB 186-2 Digital Signature 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

### ECC Key Generation

P256 3.5 sec  
P384 4.17 sec  
P521 8 sec

### ECC Sign

P256 231 msec  
P384 390 msec  
P521 861 msec

### ECC Verify

P256 951 msec  
P384 2.07 sec  
P521 2.45 sec

### RSA Key Generation

1024 30 sec  
2048 6 min  
4096 8.5 hrs

### RSA Sign\*

1024 161 msec  
2048 6 sec  
4096 2.5 min

### RSA Verify

1024 40 msec  
2048 6 sec  
4096 33 sec

\*RSA key generation time is based on an average



Proudly designed, engineered, and manufactured in the USA

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) 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](http://www.spyrus.com.au)