



# MySafeID™ Certification Authority

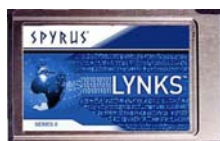
## Self-Contained HW-Based CA for Enterprise Communities

MySafeID™ from SPYRUS combines the proven performance of its LYNKS™ Series II CA Hardware Security Module (HSM) with high-assurance X.509 certification authority software to provide a cost-effective solution for small to medium size enterprises. MySafeID is simple, portable, and flexible. The software CA works on any computer running Microsoft Windows XP—no need for a dedicated server, Active Directory or LDAP, or full Microsoft CA infrastructure—yet MySafeID can generate both the elliptic curve cryptography (ECC) certificates required for high-strength encryption and RSA certificates to support legacy applications.

MySafeID provides a hardware-based chain of trust to ensure the security of encryption, digital signatures, and authentication in closed communities where a defined chain of trust is required but global certificate revocation status validation is not mandatory. MySafeID can also be integrated with an existing full PKI system to ensure global compliance. MySafeID takes security to the edge, wherever the edge may be located.

### LYNKS Series II CA HSM

MySafeID includes a LYNKS Series II CA HSM in a choice of either PCMCIA or stackable USB versions.



The LYNKS CA HSM generates keys and certificates that can be downloaded to a SPYRUS Hydra Privacy Card Series II or Rosetta Series II device. Up to 50 root CA keys and signing certificates of different key strengths and types can be stored on the tamper-resistant FIPS 140-2 LYNKS CA HSM.



With the HSM Copy Utility, the LYNKS CA HSM can be cloned to create a locked-down replica as a backup CA, for auditing preparedness, or for disaster recovery.

### A Bridge to Tomorrow's Cryptographic Support

MySafeID is unique in its ability to generate keys and certificates for every public key cryptographic algorithm currently certified by the National Institute of Standards and Technology (NIST) as Federal Information Processing Standards (FIPS). Supported algorithms exceed the Suite B standards set by the U.S. National Security Agency for protecting certain classified information.

ECC P-256  
ECC P-384  
ECC P-521

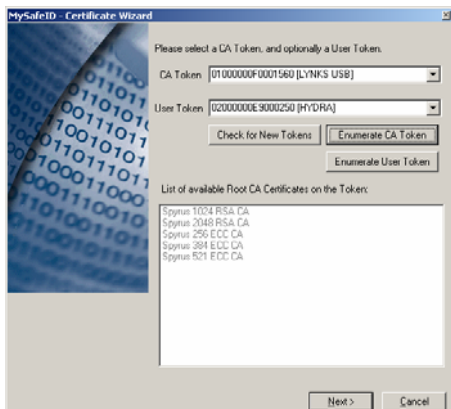
LYNKS CA HSM  
Up to 50 root certificates

RSA-1024  
RSA-2048  
RSA-4096

The self-signed root CA certificate can be explicitly trusted by the defined security community. Software-generated user certificates are signed by the root CA and can be used for security operations such as signing and encrypting email, secure authentication, and Hydra PC encrypted file sharing.

The easy-to-use software interface guides you through the certificate generation process, with no need for special IT staff or training.

The responsibility for data protection starts at the lowest level within an organization, where day-to-day operations requiring open access can pose the greatest vulnerability to security. MySafeID makes it easier to safeguard sensitive information without interrupting your business.



# Technical Specifications

## Supported Algorithms

- ▲ Elliptic Curve Cryptography (ECC) using the NIST curves in  $GF(p)$  (P-256, P-384, and P-521)
- ▲ ECDH and ECMQV Key Establishment per NIST SP 800-56A Key Establishment Guidelines
- ▲ ECDSA Digital Signature Algorithm
- ▲ Advanced Encryption Standard (AES) 128/192/256
- ▲ Secure Hash Algorithms: SHA-1 and SHA-224/256/384/512
- ▲ RSA 1024/2048 Digital Signature and Key Exchange Algorithms.  
(RSA-4096 supported on LYNKS Series II HSM for CA keys only)
- ▲ Two-key and three-key triple DES

## Security Certifications

- ▲ LYNKS Series II: certified for FIPS 140-2 Level 2 Overall, with Level 3 Physical
- ▲ Rosetta Series II and Hydra PC Series II: completing FIPS 140-2 Level 3 validation

## Standards Compliance

- ▲ 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
- ▲ SP 800-56A Key Establishment Guidelines
- ▲ SP 800-90 Random Number Generation

## Software Requirements

- ▲ Microsoft Windows XP SP2 or later

## Components

- ▲ LYNKS HSM dimensions:
  - PCMCIA: 3.37" (85.60mm) x 2.126" (54.00mm) x .196" (4.98mm)
  - USB: 3.64" (92.50mm) x 2.38" (60.50mm) x .385" (9.80mm)
- ▲ Optional HSM Copy Utility comes with software and backup LYNKS Series II HSM

Note: Technical specifications may change without notice.

## SPYRUS, Inc.



For additional details about SPYRUS products, visit [www.spyrus.com](http://www.spyrus.com) or contact us at:

- ▲ USA +1 408 392-9131 [info@spyrus.com](mailto:info@spyrus.com)
- ▲ Australia +61 7 3220-1133 [info@spyrus.com.au](mailto:info@spyrus.com.au)

