



TRUSTED MOBILITY SOLUTIONS

SPYRUS Crypto Toolbox

Create Cryptographic Applications for SPYRUS Security Devices

The SPYRUS Crypto Toolbox makes it easy to develop cryptographic applications for LYNKS Hardware Security Module (HSM) Series II, Rosetta Series II, or Hydra Privacy Card® Series II security devices, using Microsoft® Visual Studio® integrated development environments.

SPYRUS CSPs integrate with the Microsoft Cryptographic API (CAPI) providers and Microsoft Foundation Classes for standard cryptographic operations. You can also perform many operations directly on a LYNKS Series II HSM.

SPYRUS CSPs

- ▲ Hardware RSA CSP, an RSA_FULL provider
- ▲ RSA Advanced Encryption Standard (AES) CSP, an RSA_AES provider
- ▲ Digital Signature Algorithm (DSA) CSP, a DSS (signature) provider
- ▲ Elliptic Curve DSA and Diffie-Hellman CSP, an EC_ECDSA_FULL provider

The SPYRUS Crypto Toolbox includes the custom interfaces and libraries needed to interface with SPYRUS LYNKS HSM Series II, Rosetta Series II, and Hydra PC Series II security devices. With the included Rosetta Common Services Interface (CSI) middleware, you have access to all the cryptographic functions for operations performed on security devices, including the latest Suite B cryptographic algorithms.

Sample Source Code Projects

Using the SPYRUS Crypto Toolbox with Visual Studio 6 or Visual Studio 2005, you can create security applications for a variety of uses and environments, including Microsoft .NET Connected Software. To assist your development projects, the Crypto Toolbox includes five complete sample projects (with source code) in C++.

- ▲ **Sample Project 1** Initialize a SPYRUS security device and select the CSP to use.
- ▲ **Sample Project 2** Generate a key pair. Select the key type and algorithm as options.
- ▲ **Sample Project 3** Generate random numbers using the SPYRUS security device.
- ▲ **Sample Project 4** Log on to the SPYRUS security device and perform basic hash/sign/verify operations using various SPYRUS and Microsoft providers.
- ▲ **Sample Project 5** Perform key exchange (RSA) and key agreement (ECDH) between the base provider and the SPYRUS security device, including encrypting and decrypting a file. Allow option to perform key exchange/agreement between a SPYRUS provider and a Microsoft provider.

You can use the sample source code projects as the basis for your own application, use only the code snippets that suit your requirements, or build on an idea and brainstorm something completely new. The following chart details individual operations available in the Crypto Toolbox.

Source Code Projects — Available Operations		
Description	Operation	
Initialize security device. Enumerate CSPs and allow CSP selection.	Initialization	
Generate RSA key pair.	Key Generation	
Generate ECDSA key pair.		
Generate ECDH key pair.		
Generate random number on SPYRUS security device.	Generate Random Number	
Log on, hash, and sign a file with RSA + SHA-1/SHA-2 using SPYRUS security device.	Signature Generation	
Log on, hash, and sign a file with ECDSA + SHA-2 using SPYRUS security device.		
Verify RSA + SHA-1/SHA-2 signature with Microsoft CAPI providers.	Signature Verification	
Verify ECDSA + SHA-2 signature with the SPYRUS CSP.		
Encrypt a message using AES encryption and RSA key wrap	Encryption	RSA Key Wrap
Decrypt a message using AES decryption and RSA key wrap	Decryption	
Encrypt a message using AES encryption and ECDH key exchange	Encryption	ECDH Key Agreement
Decrypt a message using AES encryption and ECDH key exchange	Decryption	

The SPYRUS Crypto Toolbox contains everything you need to develop security-aware applications. The included Rosetta CSI middleware provides device and PKI management utilities in addition to all hardware CSPs.

SPYRUS Crypto Toolbox Components

- ▲ CSP build environment (headers & library files)
- ▲ Rosetta Common Services Interface (CSI) middleware
- ▲ Five sample source code projects
- ▲ Documentation (PDF format)
- ▲ CSP Command/Device Test utility
- ▲ Two Rosetta Series II Smart Cards and one LYNKS Series II HSM (PCMCIA or USB)

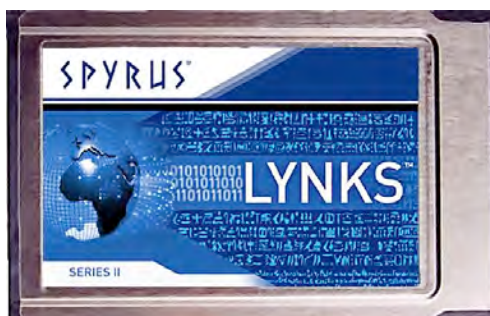
LYNKS and Rosetta Series II Security Devices

SPYRUS Series II security devices provide the strongest support for identity authentication as well as client, server, and embedded security applications. In addition to RSA, DES, 3DES, and SHA-1 legacy algorithms, they implement the new, stronger and faster Suite B cryptographic algorithms, including elliptic curve cryptography with ECDSA, ECDH, ECMQV, AES, and SHA-2.

Rosetta Smart Card Series II is a flexible, cost-effective solution for both large and small organizations. The Rosetta Series II is also available from SPYRUS in a readerless USB format.



The LYNKS Series II HSM is available in either PCMCIA or stackable USB versions.



Specifications

Supported Cryptographic Algorithms

- ▲ RSA 1024, RSA 2048, and DSA 1024 Digital Signature
- ▲ DES, two & three-key triple DES with ECB, CBC
- ▲ Secure Hash Algorithms: SHA-1, MD5, and SHA-224/256/384/512
- ▲ Advanced Encryption Standard (AES) 128/192/256 with ECB, CBC
- ▲ ECDH and ECMQV Key Establishment
- ▲ ECDSA Digital Signature Algorithm

Supported Security Devices

- ▲ LYNKS Series II Hardware Security Module (HSM) PCMCIA
- ▲ LYNKS Series II HSM USB
- ▲ Rosetta Series II Smart Card
- ▲ Rosetta Series II USB
- ▲ Hydra PC Series II

LYNKS and/or Rosetta Series II 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 (including ECDSA)
- ▲ FIPS PUB 197 Advanced Encryption Standard
- ▲ FIPS PUB 198 Keyed Hash Message Authentication Code (HMAC)
- ▲ SP 800-38A Block Modes of Operation
- ▲ SP 800-56A Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
- ▲ Federal Communications Commission Class B certification and CE Mark Certification

Required Software

- ▲ Microsoft Visual Studio 6 or Visual Studio 2005
- ▲ Microsoft .NET Framework Version 2.0
- ▲ Rosetta CSI or Rosetta Basic token management application (Rosetta CSI is included)

Compatible Operating Systems

- ▲ Microsoft Windows® XP Pro SP2
- ▲ Microsoft Windows Server 2003 R2
- ▲ Microsoft Windows Vista



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

