CipherTools™

DEVELOPER KIT

PRODUCT | DATA SHEET

CipherTools™ is a comprehensive developer kit that allows new or existing applications to be enhanced with nCipher hardware security modules to deliver secure key management for sensitive private keys and increased cryptographic processing performance. In addition to security and performance benefits, integration with nCipher's hardware automatically brings scalability and fail-over resilience to the key management infrastructure. CipherTools may be used to enhance custom solutions and commercial applications.

Widest Range of API's

CipherTools supports a wide range of Industry Standard and nCipher specific APIs, allowing application developers to choose the most appropriate interface. Developers may also take advantage of open standards to migrate existing software-based encryption implementations to use nCipher hardware.

nCipher 'Security World'

nCipher offers a unique framework for key storage and management, 'nCipher's Security World'. For an application developer, the nCipher Security World offers access to a complete security infrastructure for the lifecycle management of key material, with minimal additional programming effort. Additionally nCipher's Security World delivers application transparent scalability, fail-over and disaster recovery mechanisms. The nCipher Security World is automatically integrated with all nCipher-supported APIs. Where required, applications that use nCipher 'nCore' API directly can invoke custom mechanisms for key management.

Platform Independence

As a function of nCipher's Security World, all host-side key data is platform and OS independent and is directly transportable. nCipher's hardware modules interoperate with a wide range of hardware and OS platforms - thus development and deployment platforms can be different, and a range of different deployment platforms can be supported with minimal effort.

		APPLICATION	KEY TYPES	SECURITY POLICY	
INDUSTRY STANDARD APIs	PKCS#11	PKCS#11 Compliant Application	All module supported key types except Rijndael, Arc Four & El Gamal	Subset of Security World features mapped onto Industry Standard API	NCIPHER SECURITY WORLD SUPPORT
	CSP for Microsoft CryptoAPI	Microsoft CryptoAPI Compliant Application	RSA, DSA, DH		
	Java JCA/JCE CSP	JCE 1.2, 1.3 & 1.4 Compliant Application	RSA, DSA, 3DES, Rijndael		
	OpenSSL	Where OpenSSL is currently used without hardware enhancement or where new apps require hardware vendor independence	RSA	Security World features & policies supported	
	BHAPI	BHAPI compliant	RSA		
	'CHIL': Crypto Hardware Interface Library	Where lightweight interface is required to retrofit RSA Key Storage into existing design/application	RSA		
NCIPHER APIs	Key Mgmt. Lib (optional) 'nCore' API 'C' or Java	Custom C or Java Application	All module supported key types (see technical spec.)	Security World features & policies supported Fully custom security policies possible	

nCIPHER™

Hardware options

There is a choice of nCipher hardware security modules (HSMs) that the application will use for security and cryptographic processing. These modules may be chosen from the nCipher nShield™ range, which all support the full range of APIs.

Options include: hardware interface; cryptographic performance levels and independent security validations. It is possible to select a different specification module for application deployment than is used for development. See the separate nShield datasheets for full product details.

Using CipherTools

The Developer Kit includes an nShield HSM and a one-seat licence for one API/OS combination. The kit allows unlimited and licence-free 'nCipher enhanced' applications to be created.

To complement the Developer Kit nCipher provides full support and optional Professional Services' assistance for application integration.

TECHNICAL SPECIFICATIONS

CipherTools™ Developer Kit Contents:

- One nShield F2 SCSI HSM
- 90 days developer support (up to 40 hours), from date of delivery
- Microsoft CryptoAPI:
  - PKCS#11
  - CHIL
  - Microsoft CryptoAPI
  - Java JCA / JCE
  - C Generic Stub (including nCipher Key Management Library)
  - Java Generic Stub (including nCipher Java Key Management Classes)
  - BHAPI

Developer documentation

Further technical details on CipherTools interfaces can be found at: http://www.ncipher.com/documentation

Supported Algorithms

Symmetric Ciphers

- DES
- Triple DES
- CAST
- Rijndael/AES
- Arc Four (compatible with RC4)

Public Key Ciphers

- RSA
- DSA
- El Gamal

Key Exchange Mechanisms

- DH
- DES/3DES XOR

Hash Functions

- SHA-1
- MD5
- MD2
- RIPEMD 160
- HMAC

Supported OS Platforms

- AIX
- HPUX
- Linux
- Solaris
- Windows 2000

Consult on-line documentation for latest details of OS support

CipherTools target hardware: nShield HSM range overview

- PCI and SCSI versions
- Performance to 300 (PCI) / 400 (SCSI) 1024bit RSA signatures per second
- FIPS 140 Level 2 and Level 3 validated
- Scalable Performance by adding multiple HSMs
- Unlimited key storage via Security World mechanism

CipherTools is part of the nCipher SafeBuilder™ family of developer kits, which enable third party developers to build or enhance custom applications based on nCipher's secure hardware platforms.

NCDS/CIPHERTOOLS/FEB2003

nCipher Inc.
500 Unicorn Park Drive
Woburn, MA 01801 USA
Tel: +1 (781) 994 4000
ussales@ncipher.com

nCipher Corporation Ltd.
Jupiter House, Station Rd.
Cambridge, CBI 2JD UK
Tel: +44 (0) 1223 723600
int-sales@ncipher.com

nCipher Corporation Ltd.
15th Floor, Cerulean Tower,
26-1 Sakuragaoka-cho, Shibuya-ku,
Tokyo 150 8512 Japan
Tel: +81 3 5456 5484
int-sales@ncipher.com

Visit our Web site at www.ncipher.com – today!

Redefining cryptographic security

nCIPHER™