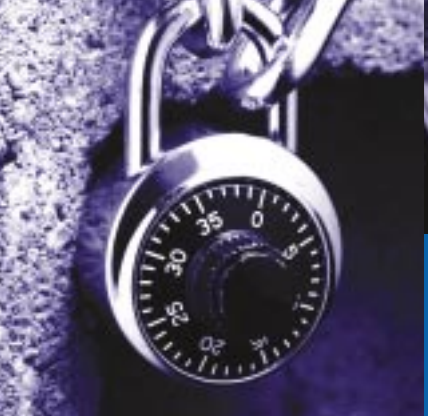

# nShield™

## HARDWARE SECURITY MODULE

PRODUCT | DATA SHEET

*The nShield™ range of hardware security modules (HSMs) delivers secure key management, transaction acceleration, and tamper-resistant physical protection for cryptographic applications.*

nShield is a cryptographic platform for enhancing the security of a variety of applications that use cryptography - from PKI and database encryption to secure authentication and content security. By storing and managing your cryptographic keys in nCipher's highly secure hardware environment, you can truly protect your applications from internal or external security threats. The nShield 800 offers greater private key performance and Elliptic Curve support, plus greatly enhanced capabilities for code protection, key generation and symmetric operations. nShield is ideally suited for use with nCipher's toolkit products, CipherTools and CodeSafe, where the highest cryptographic performance is demanded along with FIPS 140-2 level 3 key protection.

For customized application security, nCipher's developer toolkits can be used in conjunction with nShield to deliver robust hardware-based solutions. The CipherTools™ suite of APIs and software libraries allows the integration of nCipher's flexible key management functionality and cryptographic acceleration capability. To extend the security perimeter further, the FIPS 140 Level 3 versions of the nShield family are 'SEE Ready'. This means that the device can take advantage of nCipher's Secure Execution Engine™ technology to execute C/C++ programs that have been developed with the CodeSafe™ Developer Kit.

### Application integration

Through business alliances with leading providers of software applications, such as PKI and database encryption, nCipher is able to deliver out-of-the-box system interoperability. By providing seamless product compatibility, nCipher and its strategic partners can help reduce deployment risk and expense.

| FEATURE | BENEFIT |
|---|---|
| FIPS 140-2 VALIDATION | Independently certified secure management and storage of private keys |
| OFFLOAD OF CRYPTOGRAPHIC PROCESSING | Removes bottlenecks and frees your server to respond to more requests |
| SECURE EXECUTION ENGINE SUPPORT | Allows developers to protect application code within a secure cryptographic boundary |
| FAILOVER CAPABILITY | Transparently passes all of the processing activities to the next nShield if a device becomes unavailable while in service |
| ON-BOARD REAL-TIME CLOCK | Enables access to a secure time source |
| ADMINISTRATION OF KEYS CONTROLLED THROUGH THE USE OF SMART CARDS | Smart cards authenticate administrators to provide a highly flexible means of sharing responsibilities between individuals within the organization |
| KEYSAFE KEY MANAGEMENT SOFTWARE | Securely create, store, import, back-up, restore or remove application keys |
| nCIPHER SECURITY WORLD FRAMEWORK | A unique and highly secure key management framework, allowing the definition and enforcement of specific security policies |

nCIPHER™

## PRODUCT SPECIFICATIONS

| PRODUCT | FORM FACTOR | FIPS 140-2 VALIDATION | NUMBER OF 1024 BIT RSA SIGNATURES PER SECOND* | SEE READINESS | DEVICE RAM FOR SEE APPLICATIONS | KEY GENERATION PERFORMANCE (1024 BIT RSA) | SYMMETRIC PERFORMANCE | ECC SUPPORT |
|---|---|---|---|---|---|---|---|---|
| nSHIELD F2 | PCI/SCSI | Level 2 | 150 | No | 16 MB | 1 key/sec | Up to 1 MB/sec | No |
| nSHIELD F3 | PCI/SCSI | Level 3 | 150 | Yes | 16 MB | 1 key/sec | Up to 1 MB/sec | No |
| nSHIELD F2 ULTRASIGN | PCI/SCSI | Level 2 | 300/400 | No | 16 MB | 1 key/sec | Up to 1 MB/sec | No |
| nSHIELD F3 ULTRASIGN | PCI/SCSI | Level 3 | 300/400 | Yes | 16 MB | 1 key/sec | Up to 1 MB/sec | No |
| nSHIELD 800 | PCI only | Level 3 | 800 | Yes | 128 MB | 4 keys/sec | Up to 5 MB/sec | Yes |

*The performance figures quoted herein are nominal figures. Actual system performance depends on application software version, server platform type and other factors.

### ELLIPTIC CURVE SUPPORT

ECC support is optional functionality (nShield 800 only)

Via PKCS#11 / nCore APIs:

Support for ECDSA to FIPS 186-2 with the curves listed below.

Support for EC-DH with the curves listed below.

Curves over prime fields (GF(p))
P-192 P-224 P-256 P-384 P-521

Curves over binary fields (GF(2^n))
B-163 B-233 B-283 B-409 B-571
K-163 K-233 K-283 K-409 K-571
(Koblitz curves)

Custom curves can also be supported.

### Operating Systems

- AIX
- Linux
- Solaris
- HP-UX
- Windows 2000
- Windows 2003

### Third Party Applications

For a list of Third Party software that has been integrated with nCipher hardware please visit www.ncipher.com/partners

### APIs

nCipher supports a range of APIs that may be used with the nShield HSM for custom applications

### Cryptographic Algorithms Supported

(Not all algorithms are available in FIPS level 3 mode)

SYMMETRIC CIPHERS

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

PUBLIC KEY CIPHERS

- DSA
- El Gamal
- RSA

KEY EXCHANGE MECHANISMS

- DH
- DES / DES3 XOR

HASH AND HMAC FUNCTIONS

- MD2
- MD5
- RIPEMD 160
- SHA-2
- SHA-1

### Form Factor and Dimensions

- PCI MODULE
  Standard PCI half card
  66 MHz, 64 bits
  PCI 2.3 compliant

- SCSI MODULE
  Fast wide SCSI 2 (also called SCSI 3) with a high density micro-D 68 connector can be mounted in a server's 5.25" drive bay or in a dedicated external enclosure (SCSI products are subject to an End of Life announcement with a Last Time Buy Date of the 1st of May 2006).

### Standards Certification

- FCC:
  CFRA47, Part 15, Subpart B, Class A
- CE:
  EN 55022 Class A
  EN 55024-1
  EN 60950

### Operating Specifications

- Maximum power consumption for PCI: 2.5 amps at 5 volts
- Maximum power consumption for SCSI: 3.0 amps at 5 volts
- Temperature: 10-35 degrees Centigrade
- Relative Humidity: 10-85% non-condensing

NCDS/NSHIELD/MAY2005



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™