# nShield™

## HARDWARE SECURITY MODULE

PRODUCT | DATA SHEET

*The nShield™ range of hardware security modules (HSMs) provides physical protection for cryptographic keys and sensitive application code. nShield provides a highly secure, tamper-resistant hardware environment enabling sensitive material to be effectively managed and safely stored. nShield has received a FIPS 140-2 security validation at level 2 and level 3, complying with regulatory requirements and industry and government best practice.*

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, organizations can protect applications from internal or external security threats. The nShield product offers a range of performance options and security validations to best fit the individual business requirements.

As an organization grows, the processing demands on the infrastructure can threaten the overall performance of applications-and the response time experienced by customers. nShield's dedicated co-processors accelerate cryptographic operations by offloading processing intensive tasks from the individual host server, and in turn, dramatically increasing the host server's capacity and optimizing the performance of PKI and other cryptographic applications. The nShield range covers a broad spectrum of performance options; from HSMs that can handle up to 4000 transactions per second for critical operational infrastructure to lower acceleration hardware designed for branch office security applications.

All nShield products utilize nCipher's Security World key management system and offer a range of industry cryptographic APIs to integrate into any application or infrastructure. Providing a flexible approach to key management security, nShield uses smart cards to authenticate administrators, grant access rights and share administrative responsibilities-eliminating the need to rely on "super users" who can represent a single point of compromise.

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.

### DEVELOPER SOLUTIONS

For customized application security, nCipher's Developer Solutions can be used in conjunction with nShield to deliver robust hardware-based solutions. Cipher Tools suite of APIs allow quick integration of standard cryptographic functionality; CodeSafe provide a secure, hardware environment for the execution of critical code; payShield provides a range of standardized financial interfaces; Time Stamping Server offers a mechanism for providing validated time to digital signatures. Other Developer solutions offer tools to solve specialized security problems.

nCIPHER™

| 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 |
| DEVELOPER SOLUTIONS | A set of comprehensive development tools and samples to enable quick development of secure applications. |
| ROHS COMPLIANT | As of July 1, 2006 this product complies with the Restriction of Hazardous Substances (RoHS) directive (2002/95/EC) of the European Parliament |

## PRODUCT SPECIFICATIONS

| PRODUCT | CONNECTIVITY | NUMBER OF 1024 BIT RSA SIGNATURES PER SECOND* | FIPS 140-2 VALIDATION | SEE READINESS | ECC SUPPORT |
|---|---|---|---|---|---|
| nShield F2 500 | PCI | 500 | Level 2 | No | Yes |
| nShield F2 2000 | PCI | 2000 | Level 2 | No | Yes |
| nShield F2 4000 | PCI | 4000 | Level 2 | No | Yes |
| nShield F3 500 | PCI | 500 | Level 3 | Yes | Yes |
| nShield F3 2000 | PCI | 2000 | Level 3 | Yes | Yes |
| nShield F3 4000 | PCI | 4000 | Level 3 | Yes | Yes |

*The performance figures quoted have been measured on real systems by nCipher. However, actual system performance depends on application software version, server platform type and other factors.

Full product specifications can be viewed at
www.ncipher.com/cryptographic_hardware/hardware_security_modules/8/nshield

## ABOUT NCIPHER

nCipher protects critical enterprise data for many of the world's most security-conscious organizations. Delivering solutions in the fields of identity management, data protection, enterprise key management and cryptographic hardware, nCipher enables businesses to identify who can access data, to protect data in transit and at rest, and to comply with the growing number of privacy-driven regulations. nCipher is listed on the London Stock Exchange (LSE:NCH).

NCDS/NSHIELD/MARCH2006



**nCipher Inc.**
92 Montvale Avenue, Suite 4500
Stoneham, MA 02180 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!

Identify. Protect. Comply.

nCIPHER™