

NETWORK-CONNECTED HARDWARE SECURITY MODULE (HSM)

REDEFINING THE ROI FOR CRYPTOGRAPHIC HARDWARE

As organizations use cryptographic hardware to secure multiple points of risk within their IT infrastructure, it is important that a choice of deployment options is available. The netHSM is a network-attached, shareable, Hardware Security Module (HSM) that enables new and expanded HSM deployment strategies to emerge. Compatible with nCipher's range of directly-connected, dedicated HSMs, the netHSM promotes a cost-effective, enterprise-wide, security solution that is secure, shareable, scalable and interoperable.



SHAREABLE SECURITY RESOURCE

The netHSM is a platform for providing cryptographic services to enhance the security of a variety of applications - from PKI and authentication systems to Web services and SSL protected communications.

The netHSM acts as a network-attached resource for secure cryptographic processing, providing an alternative deployment scenario to the traditional approach of dedicated HSMs on individual servers. By allowing multiple servers to securely access a single HSM to perform cryptographic functions, overall equipment costs can be reduced and system management simplified. Whilst dedicated HSMs are appropriate for security applications and servers that demand guaranteed availability and/or processing power, many deployments encompass multiple servers, either in a single site or across a wide geographic area, where a shareable, network-connected HSM is a perfect solution.

FEATURE	BENEFIT
SHAREABLE CRYPTOGRAPHIC RESOURCE	Provides flexible security for multiple server and multi-site installations, lowering the overall cost of deploying cryptographic hardware
FULLY FIPS 140-2 LEVEL 3 VALIDATED SECURITY BOUNDARY	The netHSM has a proven and fully FIPS-validated security boundary meeting cryptographic best practice for hardware key protection
HIGH CAPACITY	The netHSM allows unlimited key storage and support for up to 20 servers
COMPATIBILITY WITH EXISTING nCIPHER HSM DEPLOYMENT	Seamless integration with existing nCipher deployments allowing retention of initial investments
SECURE USER INTERFACE	The integrated secure user interface requires no external devices or servers for initialization, locking down security
FUNCTIONAL SEPARATION THROUGH FINE-GRAINED CONTROL OF KEYS	Keys can be isolated from one another through logical separation ensuring that access is restricted to authorized users or servers
HIGH PERFORMANCE: 1600 TPS / 1U	Performance for 1024 bit keys extends to 1600 TPS in 1U form factor, minimizing expensive rack space requirements
FULL FAILOVER AND LOAD BALANCING	netHSM can be deployed in high-availability systems. The interoperability of all nCipher HSMs allows failover and load balancing between any combination of netHSMs and dedicated HSMs
FULL RANGE OF APIs / WIDE APPLICATION SUPPORT	Simple integration with applications and proven interoperability with existing nCipher APIs
SECURE EXECUTION ENGINE (SEE)™ SUPPORT	Sensitive application software can be executed within FIPS certified hardware
ELLIPTIC CURVE CRYPTOGRAPHY SUPPORT	Provides developers with hardware key protection for the main ECC curves

netHSM™



Secure by design

Because the security of all cryptographic processing is only as strong as the security of the underpinning cryptographic keys, securing the keys against attack with a FIPS-validated hardware module is essential. nCipher's netHSM has been designed from the ground up to provide;

- FIPS 140-2 Level 3 validated protection for cryptographic key material
- Encrypted network transport
- Strong authentication of servers that use the netHSM for key operations
- Resilience of the device from network attack
- Strongly enforced mechanisms to ensure the integrity of internal system software
- A secure and integrated user interface

Manageability

As networks expand, security teams are typically responsible for the security of multiple servers, often geographically dispersed across a number of distinct sites. While dedicated HSMs provide excellent security, there is often significant management and administration overhead associated with servicing remote locations. By centralizing the hardware security within a single netHSM, a central security team can have complete access to all cryptographic keys and functions while providing the same FIPS-level security to servers worldwide.

To tightly control access to an HSM, nCipher provides a smartcard-based authorization system for use by groups of operators and security administrators. The netHSM also allows many management functions to be accessed remotely. Smartcards can be presented locally at any server with a dedicated HSM and commands are transported over a secure connection. This allows efficient deployment of netHSMs in unattended data-centers or in geographically dispersed locations.

High performance

netHSM performs cryptographic processing on behalf of remotely connected servers. By offloading cryptographic functions from the remote servers, overall server capacity is increased. The netHSM can perform up to 1600 x 1024 bit signing operations per second. The netHSM is a 1U high, 19" wide rack-mounted unit, offering high performance with a low impact on valuable rack space.

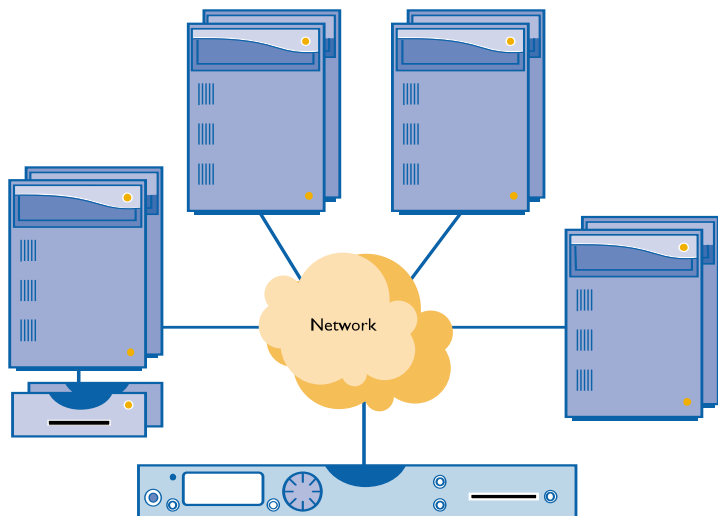
Shareable cryptographic hardware for large or geographically dispersed installations can reduce hardware costs, management costs and footprint costs, increasing the return on your security investment

INTEROPERABLE AND FLEXIBLE

All nCipher HSMs use a common key management framework, nCipher's Security World, making the netHSM completely compatible and interoperable with nCipher's dedicated HSMs. As a result, nCipher HSMs can be configured in any combination to meet an organization's management, security and budgetary needs.

Flexibility in configuration allows an organization to protect existing investment, reconfigure and reallocate hardware as necessary and easily extend security to meet new business needs to maximize return on your security investment

Flexible deployment



Allows multiple servers to securely access a single HSM



NETWORK CONNECTED HARDWARE SECURITY MODULE (HSM)

Uniform integration

For years, nCipher customers have used nCipher toolkits to integrate our dedicated HSMs into either customized or commercial security applications. Because netHSM is compatible with nCipher's complete range of dedicated HSMs, not only are the same integration toolkits used, but the same integration code can be utilized, to quickly and efficiently integrate netHSM into existing security applications.

Rapid integration and deployment allows an organization to efficiently meet regulatory compliance, increasing return on your security investment

SCALABLE CRYPTOGRAPHIC PLATFORM

Future-proof

nCipher's Security World provides the industry-leading model for managing keys by providing fine-grained access control. It avoids the need to isolate applications through inflexible internal partitions which limit the number of keys and servers that can be secured. netHSM allows limitless key storage and allows up to 20 servers to be supported.

netHSM configurations will be defined by business needs and security policy not by technology limitations, increasing the return on your security investment

Building an enterprise-wide cryptographic policy

Many organizations begin using hardware-protected cryptography on a single server, such as on a Web server utilizing SSL. For this application a dedicated HSM attached to a Web server is the most cost-effective solution. However, as the organization's use of cryptography grows to support an expanding on-line presence or the emergence of Web services, a netHSM can be added to secure multiple servers in multiple locations. The netHSM can work in conjunction with existing installations of dedicated HSMs.

The ability to start small and then expand, maintaining the investment in original equipment, increases the return on security investment

INDEPENDENTLY VALIDATED SECURITY

Cryptographic keys are the backbone of all cryptographic operations. However, failure to protect and manage these keys risks shattering an entire layer of security. Many organizations make the mistake of relying on 'soft security', leaving keys unprotected on general purpose servers, vulnerable to attack. Wherever cryptography is used to protect sensitive data, organizations must deploy 'hard security' controls to manage risk. Central to strong cryptographic security is the protection of keys within a Hardware Security Module (HSM).

The netHSM protects cryptographic keys in a highly secure hardware environment, enabling them to be effectively managed and safely stored. The netHSM FIPS security boundary has received an independent FIPS 140-2 Level 3 validation, the de facto security benchmark for cryptographic modules.

In addition to the independent FIPS approval that covers the protection of keys, nCipher has commissioned 3rd party testing of the 'network' properties of the netHSM to validate the resilience of the product from network-based attack.

Hardware protected remote server authentication

To further extend system security, the netHSM optionally supports the ability to strengthen the authentication of remote servers to the netHSM. By supporting hardware tokens at the requesting server, the keys used for authenticating the servers can be secured. This protects against illegitimate key use and promotes end-to-end security.

netHSM and customized security

nCipher's line of toolkits enables custom security applications to take full advantage of the key management, hardware protection and high speed cryptographic processing provided by the netHSM. Utilizing nCipher's CodeSafe™ toolkit, an organization can not only secure cryptographic keys but also sensitive applications and data using nCipher's Secure Execution Engine™ (SEE) technology.

Securing both keys and application software within a FIPS-validated security boundary protects against attacks and can allow secure deployment of new applications, increasing the return on your security investment.

PRODUCT SPECIFICATIONS

PRODUCT	CONNECTIVITY	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)	ECC SUPPORT
netHSM 300	10/100 Ethernet	Level 3	300	Yes	16 MB	1 key/sec	No
netHSM 1600	10/100 Ethernet	Level 3	1600	No	16 MB	1 key/sec	No
netHSM 800	10/100 Ethernet	Level 3	800	Yes	128 MB	4 key/sec	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.

TECHNICAL SPECIFICATIONS

ELLIPTIC CURVE SUPPORT

ECC support is optional functionality (netHSM 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(2ⁿ))
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.

Connectivity

- 2 10/100 Ethernet
- RS232, mini-DIN Serial connection
- PS/2 Keyboard connection

User Interface

- High Resolution Graphic LCD
- 2 x 'Soft' menu keys
- 1 x Scroll / select knob

APIs

- PKCS#11
- CSP for Microsoft CryptoAPI
- Java JCA/JCE CSP
- OpenSSL
- BHAPI
- 'nCore' API 'C' or Java
- CHIL

Algorithms

Symmetric ciphers

- Triple-DES (two and three key)
- AES - Rijndael
- Arc Four (compatible with RC4)
- CAST
- 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

Performance

- RSA 1024: 300 ~ 1600 TPS
- RSA 2048 up to 400 TPS [netHSM 1600]

Mechanical

- Weight 6.4 Kg
- Standard 1U rack mount [19" x 1³/₄ x 17¹/₄], (482mm x 44mm x 440mm)

Electrical

- Input voltage 100-240 AC auto switching 50-60 Hz (nominal)
- Maximum Power Consumption: 460 watts (4 amps at 115 volts AC)

Certification

- FCC: CFR47, Part 15, Subpart B, Class A
- UL: 1950
- CE: EN55022, Class A; EN55024-1; EN60950

Temperature / Humidity (Operational):

+10 to +35 degC; 10 to 85% relative humidity, non condensing

Every effort has been made to ensure the information included in this datasheet is true and correct at the time of going to press. However, the products described herein are subject to continuous development and improvement, and the right is reserved to change their specification at any time. ©2003 nCipher Corporation Ltd. CodeSafe, netHSM, Security World and SEE are trademarks or registered trademarks of nCipher Corporation Ltd. All other trademarks contained herein are the property of their respective owners.

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!