nCIPHER®

nCipher netHSM

Shared security module for critical business processes

Organizations have more information worth protecting than ever before. Confidential customer data, financial results, and research findings are just a few types of sensitive information at risk. Even the encryption keys that are critical to protecting this data can be vulnerable to attack. Ineffective protection of these keys can lead to financial fraud, loss of intellectual property, and brand damage.

Software protection falls short

Companies face both logical attacks over their networks and physical breaches by staff or intruders. Hackers can use malicious code to capture critical data and the underlying encryption keys. Thieves can quickly copy sensitive data or install backdoors.

As these threats evolve, software-based security cannot keep up. Recent research has reaffirmed the weaknesses of even the most advanced software security measures.

Safeguard data and processes within hardware

nCipher netHSM provides encryption processing, secure code execution, and key protection inside a highly secure, tamper-resistant hardware environment. Critical information is never exposed, so it's much less vulnerable to compromise, whether threats originate within or outside the organization.

Scalable and cost-effective hardware for strategic security initiatives

nCipher netHSM is a shared hardware security module (HSM) that processes and protects encryption keys, critical executable code, and highly confidential data for several network resources.

With nCipher netHSM, sensitive information is safe from logical and physical attacks, enabling you to confidently manage identities, passwords, and critical processes.

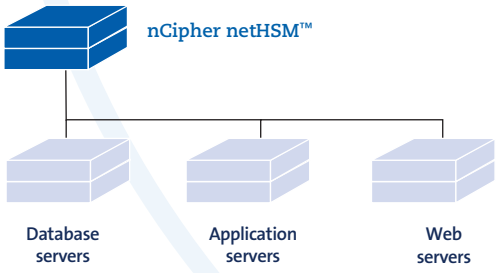
Benefits

Controls access to critical information

Protects your business processes

Delivers trusted, FIPS-validated security

Provides scalable encryption services



The shared nCipher netHSM module provides scalable, cost-effective encryption services to enterprise servers.

Controls access to critical Information

The HSM management system enables you to share keys across several HSMs. Following best practices, it separates the roles of security operators and administrators. nCipher netHSM delivers:

- **Hardware key protection** – Stores keys in a secure, tamper-resistant environment to prevent copying.
- **Tight control of keys** – Smart card authentication firmly controls key access.
- **Secure administration** – Eliminates the need to rely on server administrators who can represent a single point of compromise.

Protects your business processes

nCipher netHSM allows you to execute your mission-critical code within tamper-resistant hardware. Using nCipher CodeSafe, you can run proprietary applications inside nCipher netHSM to take advantage of:

- **Signing of trusted applications** – Ensures trusted applications cannot be manipulated.
- **Intellectual property protection** – Protects proprietary applications against theft.
- **End-to-end security** – Ensures that information is accessible only where it should be.

Delivers trusted, FIPS-validated security

The security features of nCipher netHSM are FIPS-validated and under evaluation for Common Criteria, certifying it for use in high-security environments.

- **Approved for high-security environments** – Appropriate for public sector and security-conscious organizations.
- **Reviewed by the experts** – Accepted by regulatory and compliance organizations.

Technical Specifications

Available performance variants:

- nCipher netHSM 500
- nCipher netHSM 2000

The security features of nCipher netHSM are FIPS 140-2 Level 3 validated and offer encryption services to servers running Microsoft Windows, Sun Solaris, HP-UX, IBM AIX, and Linux.

For more detailed technical specifications, please visit www.ncipher.com.

Provides scalable encryption services

Using standard APIs, nCipher netHSM integrates out of the box with leading enterprise applications, including web and application servers, databases, and public key infrastructures. It can be shared by several servers to provide corporate security services. nCipher netHSM provides:

- **Scalability** – Allows organizations to apply hardware-based security across multiple networked resources.
- **Performance** – Hardware acceleration enables organizations to avoid bottlenecks when signing digital certificates.
- **Fast and cost-effective integration** – Integrates out of the box with leading applications and supports standard APIs to integrate with custom applications.
- **Failover capability** – Should one nCipher netHSM fail, a second one takes over transparently.
- **Support for web services and virtualized servers** – Enables hardware-based key storage for service-oriented architectures (SOAs) or virtualized servers.
- **Cost-effective resource** – Shared use of the module across several servers drastically reduces hardware, licensing and operational costs.

North America
nCipher, Inc.
1655 McCarthy Blvd
Milpitas, CA 95035 USA
92 Montvale Avenue #4500
Stoneham, MA 02180 USA
Tel: +1 800 nCIPHER

EMEA
nCipher Corporation
Jupiter House
Station Road
Cambridge CB1 2JD
UK
Tel: +44 (0) 1223-723600

Asia/Pacific
nCipher K.K.
15th Floor, Cerulean Tower
26-1 Sakuragaoka-cho
Shibuya-ku, Tokyo
Japan 150-8512
Tel: +81-3-5456-5486

www.ncipher.com
info@ncipher.com