



Thales nCipher netHSM®

KEY BENEFITS

- > Controls access to critical information
- > Protects your business processes
- > Delivers trusted, FIPS-validated security
- > Provides scalable encryption services

Shared security module for critical business processes

Organizations have more information worth protecting with encryption than ever before. 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. Recent¹ research has reaffirmed the weaknesses of even the most advanced software security measures. Hardware security modules (HSMs) provide the superior protection needed for effective encryption and key management.

¹ <http://citp.princeton.edu/memory/>

>> Thales nCipher netHSM

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 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.

Controls access to critical information

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.

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.
- > **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.

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** – Apply hardware-based security across multiple networked resources.
- > **Failover capability** – Should one nCipher netHSM fail, a second one takes over transparently.



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.thalesgroup.com/InfoSysSecurity.

Thales
Information Systems Security