



Thales nCipher nShield[®]

KEY BENEFITS

- > Controls access to critical information
- > Protects your business processes
- > Delivers trusted, FIPS-validated security
- > Integrates quickly with enterprise applications

Dedicated hardware security module for critical systems

Organizations have more information worth protecting with encryption 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 network attacks and physical breaches by staff or intruders. Hackers can use malicious code to capture data and the underlying encryption keys. Thieves can copy sensitive data or install backdoors.

As these threats evolve, software-based encryption cannot keep up. Recent research¹ reaffirmed the weaknesses of even the most advanced software security measures. Hardware security modules (HSMs) provide the protection needed for effective encryption and key management.

nCipher nShield is a dedicated HSM that is inserted into a single server to protect its encryption keys and trusted applications.

¹ <http://citp.princeton.edu/memory/>

>> Thales nCipher nShield

It offloads and accelerates cryptographic operations, eliminating performance bottlenecks and freeing your infrastructure to handle business processes. Critical information is never exposed, so it's much less vulnerable to compromise.

Controls access to critical information

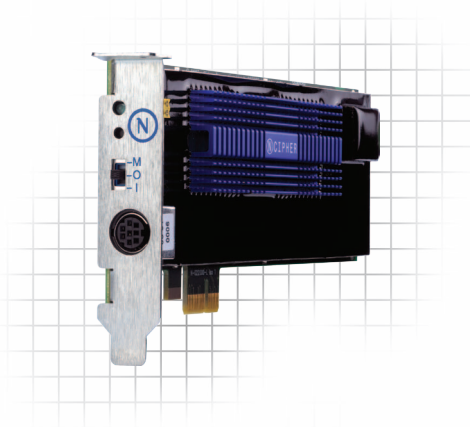
The HSM management system enables you to share keys across several HSMs. It separates the roles of security operators and administrators. nCipher nShield delivers:

- > **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 nShield allows you to execute your code within tamper-resistant hardware. Using nCipher CodeSafe, you can run applications inside nCipher nShield to take advantage of:

- > **Signing of trusted applications** – Protects trusted applications from manipulation.
- > **End-to-end security** – Ensures that information is accessible only where needed.



Delivers trusted, FIPS-validated security

FIPS-validated and under evaluation for Common Criteria, nCipher nShield has been certified for use in high-security environments, making it appropriate for public sector and security-conscious organizations.

Integrates easily with enterprise applications

nCipher nShield seamlessly integrates with existing web and application servers, public key infrastructures, databases, and other enterprise applications. nCipher nShield provides:

- > **Easy deployment** – Can be quickly deployed to critical security applications and servers.
- > **Fast and cost-effective integration** – Integrates out of the box with leading applications and standard APIs.
- > **Failover capability** – Should one nCipher nShield fail, a second one takes over.
- > **Performance** – Hardware acceleration avoids bottlenecks when signing digital certificates.

Technical Specifications

Modules with PCI hardware interface:

- > nCipher nShield 500
- > nCipher nShield 2000
- > nCipher nShield 4000

Modules with PCI Express hardware interface:

- > nCipher nShield 500e
- > nCipher nShield 6000e

nCipher nShield is FIPS 140-2 Level 2 and 3 validated and supports 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