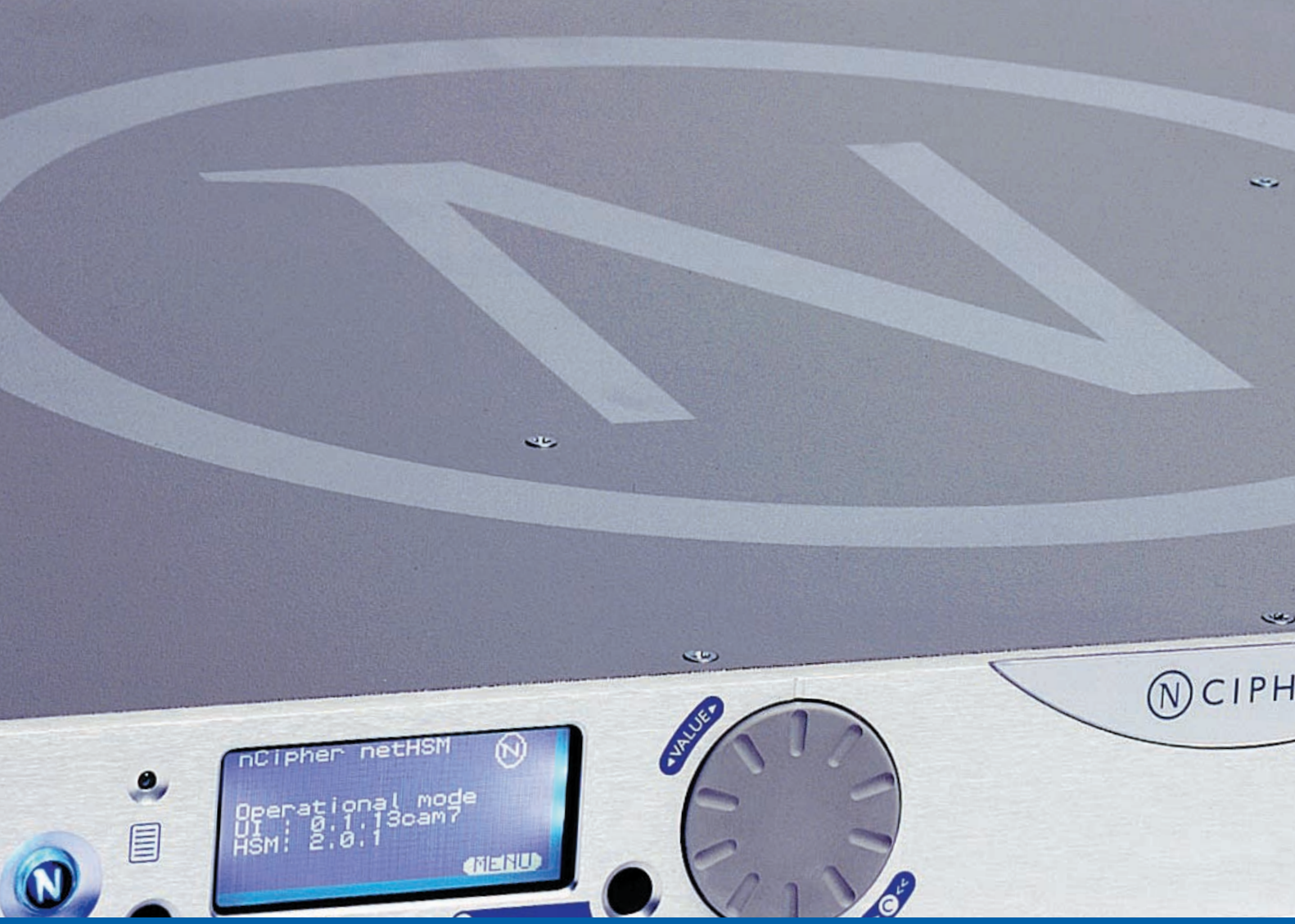


HARDWARE SECURITY MODULES

DEPLOYMENT STRATEGIES FOR ENTERPRISE SECURITY

nCIPHER™

HARDWARE SECURITY MODULES

Deployment strategies for enterprise security

Organizations around the world are creating open, flexible information systems that are linking employees, customers, suppliers and partners, quickly and cheaply using highly interconnected processing, storage and communications resources. However, 'on-demand' connections to people and machines, anywhere and at any time challenges the traditional reliance on perimeter security. Today's security initiatives emphasize strong authentication, protection of intellectual property and customer privacy, protecting information however it moves or wherever it resides.

cryptography relies on the use of keys; failure to protect and manage these cryptographic keys risks shattering an entire layer of security

Cryptography and hard security

To deliver this new level of protection, application developers and system architects are increasingly turning to cryptography to establish identity, provide data confidentiality, prove data integrity and build trust. The appropriate use of cryptography to encrypt information, digitally sign documents and enforce digital rights is well proven and effectively unbreakable. But cryptography relies on the use of keys; failure to protect and manage these cryptographic 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).

nCipher's range of HSMs protect cryptographic keys in a highly secure hardware environment, enabling them to be effectively managed and safely stored. Every nCipher HSM has received an independent FIPS 140-2 security validation, the de facto security benchmark for cryptographic modules.

HSM deployment strategy

HSMs form the basis of best practice cryptographic security, but their role and value go far beyond simply protecting a key against physical attack. Deployed correctly, HSMs provide a basis for cryptographic security that can scale easily, improve system performance and yet be robust and flexible enough to handle the dynamics of real-world situations.

Every organization has a unique set of applications with specific performance and security requirements. These tend to evolve as new opportunities, threats and technologies emerge. To handle the diverse and dynamic needs of today's IT infrastructure, nCipher provides a comprehensive family of flexible, scalable and interoperable HSMs.

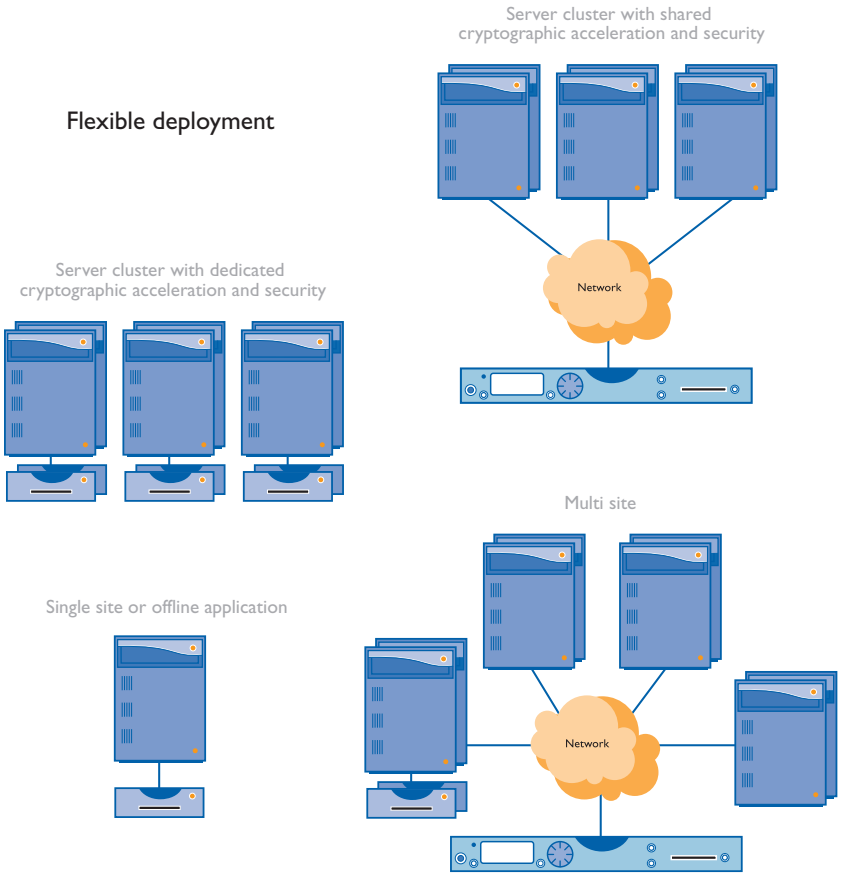
nCipher's family of HSMs

nCipher HSMs use a common key management framework, nCipher's Security World. This means nCipher HSMs are completely compatible with each other, allowing them to be configured in any combination to meet an organization's management, security and budgetary needs. Flexibility in configuration allows an organization to protect an existing investment, reconfigure and reallocate hardware devices as necessary and easily extend the use of 'hard security' to meet new business needs.

nCipher conducts extensive interoperability testing to ensure straightforward HSM integration with leading Web server, application server, PKI and other third-party software packages. In addition nCipher supports industry standard APIs such as PKCS#11 and MS CAPI.

All Security World HSMs feature specialized cryptographic processors to perform CPU-intensive cryptographic operations, therefore offloading them from the host server and, in turn, dramatically increasing server capacity and optimizing the performance of cryptographic applications.

Flexible deployment



The unique capabilities of nCipher's Security World key management framework allows seamless interoperability across all nCipher HSMs, enabling a 'mix-and-match' approach to suit a range of applications

nCipher Security World

Dedicated HSMs and shareable HSMs

nCipher's HSMs are available in two distinct deployment configurations: dedicated, directly-connected cryptographic modules, each attached to individual servers; and network-connected HSMs that can be shared by multiple servers.

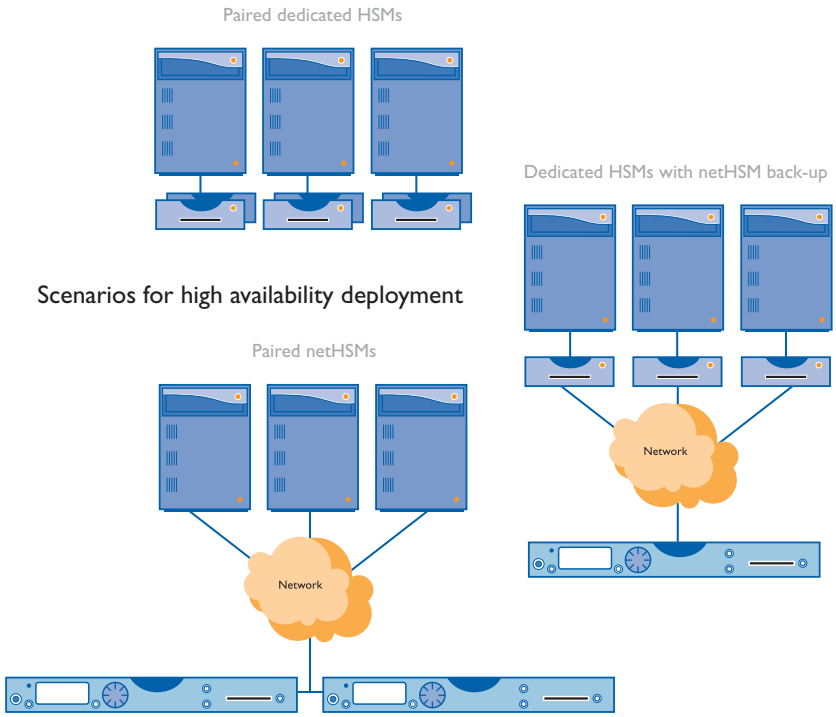
nCipher's dedicated HSMs (nShield, nForce and payShield) provide cryptographic resource to a particular host server, ensuring processing requests are offloaded from the host. In addition the host server benefits from the full cryptographic acceleration capacity of the directly connected HSM. Dedicated HSMs are particularly well suited for servers handling mission critical applications, such as PKI root key protection, or for servers that need to handle large volumes of cryptographic data such as a high traffic SSL web server.

nCipher's shareable netHSM is a highly secure, network-attached HSM that provides a shareable cryptographic resource for multiple servers.

Applications that require access to hardware protected cryptographic keys can access the netHSM over a secured connection. The netHSM provides a cost-effective deployment option, allowing the investment in 'hard security' to be spread across multiple applications or servers. Networked HSMs can provide a lower overall cost of ownership, particularly when there are many servers to be protected or where the use of dedicated HSMs in geographically dispersed systems has the potential to increase administrative costs.

Mix, match and migration

Typically an organization will have a wide variety of applications that employ cryptography, creating a requirement for a range of flexible HSM configurations. As individual applications evolve from a pilot, through localized use, to organization-wide adoption, the use of HSMs will also evolve. For example, isolated pilots of a particular application may utilize a dedicated HSM before transitioning to a centralized, shared HSM as the application is rolled out geographically.



As organizational needs grow, Security World's migration capability allows existing investment in either form of HSMs to be retained. This flexibility in deploying HSMs allows system designers to choose the best configuration based on the needs of the business, rather than the limits of the technology.

The unique capabilities of nCipher's Security World key management framework allows seamless interoperability across all nCipher HSMs, enabling a mix and match approach to suit a range of applications. It also allows the power of different HSMs to be combined in conjunction with a single application. For example, a single netHSM might be used as a back-up/failover unit for group of servers, all equipped with dedicated HSMs.

Security World is best practice

nCipher's Security World framework delivers cryptographic key management features that can scale, are robust and are flexible enough to handle real-world deployments. This powerful solution gives the ability to handle an unlimited number of keys and provides the functions necessary to manage keys throughout the entire key lifecycle from creation to operational use, back-up, recovery, archival and finally destruction.

Security World delivers a common set of features across all nCipher HSMs:

- **Security**
  All HSMs are designed to ensure that there is no single point of compromise within the key management environment. All cryptographic functions take place within a FIPS 140-2 validated HSM. Two-factor authentication, split responsibility and role separation are supported by threshold sets of smartcards. This means 'k' out of a total of 'n' cards must be presented to authorize a specific cryptographic function or administrative activity. This helps to reinforce the specific requirements of a security policy and ensures that there is no single 'super-user' with excessive access rights.

flexible controls help to reinforce the individual requirements of a given security policy, allowing access to individual keys only by authorized users or applications

- **Scalability**
  Storing application keys as encrypted 'key blobs' outside the HSM ensures that there is no restriction on the number of keys that can be stored by any HSM. In addition, the secure storage of keys outside the HSM makes the process of loading application keys into new cryptographic modules, or securely sharing keys across multiple servers, straightforward. In the case of the netHSM, which may be shared by multiple applications, the ability to handle large numbers of keys is critical.

- **Functional separation**
  Every application key has an Access Control List (ACL) that defines the allowable uses of that key. Authorization to use individual application keys can be further controlled through the use of a set of Operator smartcards. This allows different levels of security to be assigned to individual keys in direct relation to their importance. Together these controls ensure that individual keys or groups of keys can be isolated from one another through logical separation. For the netHSM, individual key use can also be restricted to a specific server so that access is granted only to a server that has been strongly authenticated. These flexible controls help to reinforce the individual requirements of a given security policy, allowing access to individual keys only by authorized users or servers, avoiding the need to impose rigid partitioning within an HSM.

- **Resilience**
  Security World technology ensures that there is no single point of failure in any nCipher HSM deployment. Multiple HSMs can be deployed on a single server or across the network to provide secure fail-over. If an HSM is damaged or stolen, keys can be recovered easily by initialising a new module. The Security World key management framework has a range of built-in controls to simplify back-up and recovery.

Protecting custom application software
nShield and the netHSM product ranges feature HSMs that can protect application software in addition to cryptographic keys. Unprotected software used for sensitive application processes can present significant security risks. With more and more applications being automated or hosted in remote locations, ensuring that nobody tampers with the software that executes sensitive applications is as important as protecting cryptographic keys. nCipher's CodeSafe™ developer toolkit works in conjunction with SEE-enabled HSMs to allow the secure execution and maintenance of processes such as authentication, access control, audit logging, time-stamping, metering and digital signatures.

netHSM allows multiple applications to access hardware-based encryption, decryption and signing functions via secure connections over IP networks

Securing applications across the enterprise

nCipher's range of HSMs is used to keep critical keys safe, enterprise-wide. These best-practice cryptographic solutions provide FIPS 140-2 compliance, locking down sensitive information at every point of risk across the enterprise:

- **Web infrastructure:**
  Protecting SSL keys from compromise is a vital element of security for Web servers and intelligent networking devices. nCipher's HSMs combine fast cryptographic processing with best-of-breed security management, moving private SSL keys from vulnerable software to tamper-evident hardware.
- **Applications:**
  Application servers are at the heart of a network, handling both sensitive data and critical security systems such as PKI. nCipher's hardware-based cryptographic solutions can be used to secure sensitive data, signing keys and application code.
- **Web Services security:**
  Web Services are bridging firewalls and penetrating deep into an enterprise's core application environment – increasing the vulnerability to malicious attack. nCipher HSMs are used to protect the keys that underpin XML encryption and signatures as well as transport layer SSL.
- **Payments:**
  HSMs are a mandated component of the Visa and MasterCard specifications such as 3-D Secure and SecureCode for protecting the cryptographic processes associated with cardholder authentication.
- **Databases:**
  Encrypting sensitive database information using a FIPS 140-2 HSM integrated with database security software to meet privacy legislation and industry mandates.

nShield protects cryptographic operations and keys from compromise in tamper-resistant hardware

The nCipher range of HSMs

netHSM™

The netHSM is a FIPS 140-2 Level 3 network-attached, shareable HSM. It allows multiple applications to access hardware-based encryption, decryption and signing functions via secure connections over IP networks. The netHSM supports a wide variety of software applications from leading security vendors including the major Web and application server platforms and commercial PKI software. The netHSM supports nCipher's Secure Execution Engine (SEE) technology allowing the HSM to manage and execute application level software within the protected cryptographic boundary.

nShield™

A dedicated HSM for enhancing the security of all types of applications – from PKI certificate issuance and database encryption to systems employing digital signatures and SSL communications. nShield protects cryptographic operations and keys from compromise in tamper-resistant hardware, federally validated to FIPS 140-2 Level 3, providing nCipher's highest level of cryptographic protection. nShield supports nCipher's SEE technology. nShield is available as a PCI card or SCSI-connected device.

nForce™

A dedicated HSM for securing SSL communications to Web servers and application servers. nForce combines FIPS 140-2 Level 2 validated key security and management with up to 1600 TPS cryptographic acceleration. This protects Web server cryptographic SSL keys from theft or manipulation and provides SSL acceleration to boost server transaction capacity. nForce is available as a PCI card or SCSI-connected device.

payShield™

A FIPS 140-2 Level 3 HSM designed to meet the stringent requirements of the on-line payments industry, including ePayments, EFTPOS and ATMs. payShield combines the highest level of protection with an ability to handle high volumes of symmetric and asymmetric cryptography required by the latest payment systems for the authentication and verification of cardholders. payShield is available as an Ethernet-connected HSM, payShield net, or as a SCSI-connected device.

Developer toolkits

These toolkits enable developers to build customized cryptographic security solutions.

SafeBuilder™ toolkits work in conjunction with netHSM and nShield modules to create a security platform that enables application developers to integrate hardware security into new or existing cryptographic applications to enhance performance and protect keys. This flexible development platform also includes SEE and enables application software to be safely loaded and executed within the confines of a highly secure FIPS 140-2 Level 3 validated HSM.

CORPORATE HEADQUARTERS

Europe & International
nCipher Corporation Ltd.
Jupiter House
Station Road
Cambridge, CB1 2JD
United Kingdom
Tel: +44 (0) 1223 723600
E-mail: int-sales@ncipher.com

North America
nCipher Inc.
500 Unicorn Park Drive
Woburn, MA 01801
United States
Tel: 800 NCIPHER (800 624 7437)
or +1 781 994 4000
E-mail: ussales@ncipher.com

Asia Pacific
nCipher Corporation Ltd.
15th Floor, Cerulean Tower,
26-1 Sakuragaoka-cho, Shibuya-ku
Tokyo 150 8512 Japan
Tel: +81 3 5456 5484
E-mail: int-sales@ncipher.com

nCIPHER™

Redefining cryptographic security

www.ncipher.com

NCBR/HSM/OCT2003