



nCIPHER HARDWARE SECURITY PLATFORMS

nCIPHER SECURITY PLATFORMS

Hardening applications...

Organizations around the world are creating open, flexible information systems that are linking employees, customers, suppliers and partners, quickly and cheaply. However, 'on-demand' connections to people and machines, anywhere and at any time, challenge the traditional reliance on perimeter security. Security controls must go beyond simply protecting data from outside attack.

nCipher's hardware security platforms are deployed by organizations to underpin their protection of sensitive information. They provide the foundation for strong authentication, secure messaging, data encryption and payment processing.

Security-aware organizations have long recognized that cryptography can underpin trust, providing confidentiality, proof of identity, data integrity and non-repudiation.

Securing sensitive information means defining and enforcing who can access which information under what conditions. Security-aware organizations have long recognized that cryptography can underpin trust, providing confidentiality, proof of identity, data integrity and non-repudiation. This ability to prove identity and protect data not only helps organizations to manage risk more effectively but it also forms the cornerstone of compliance, helping them to meet data security regulations and to satisfy the requirements of increasingly stringent privacy legislation.

Cryptographic security

The appropriate use of cryptography to encrypt information, digitally sign documents and control digital rights is well proven and effectively unbreakable. Hence cryptography is being used to enforce security policy across the extended enterprise. But this powerful technology comes at a price: the keys and certificates that underpin cryptography must be protected from compromise or theft; the performance impact of complex processing must be minimized; and, increasingly, the integrity and accuracy of the time source used to audit these processes must be maintained.

nCipher's security platforms address these challenges:

- Hardware Security Modules (HSMs) that protect cryptographic keys and application logic from compromise in tamper-resistant hardware, validated to the U.S. and Canadian federal standard FIPS 140-2
- SSL Accelerators that offload cryptographic processing to significantly boost server transaction capacity
- Time Stamping Appliances that provide auditable time stamping functionality for core applications requiring non-repudiation



Wherever cryptography is used to protect sensitive data, organizations must deploy 'hard security' controls to manage risk. Central to achieving strong cryptographic security is the protection of keys within a Hardware Security Module (HSM).



nCipher's family of HSMs

Failure to protect and manage cryptographic keys risks shattering a foundation 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 achieving strong cryptographic security is the protection of keys within a HSM.

nCipher's range of HSMs protects 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. 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 a wide range of industry-standard APIs.

nCipher HSMs are built on a common key management framework, nCipher Security World, ensuring that keys can be shared across multiple devices and security policies can be centrally enforced across dispersed groups of HSMs. The key management framework 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.

All nCipher HSMs are designed to ensure that there is no single point of compromise; supporting two-factor authentication, split responsibility and role separation to ensure that there is no single 'super-user' with excessive access rights. Security World technology also 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 a network to provide secure failover.

netHSM™

The netHSM is a network-attached, sharable HSM. It allows multiple servers and applications to access shared hardware-based encryption, decryption and signing functions via secure connections over IP networks. 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 that provides cryptographic resource and acceleration to a particular host server. Directly-attached HSMs are well suited for servers that are handling mission-critical functions, such as PKI root key protection, or for servers that need to handle large volumes of cryptographic processes. Selected nShield HSMs also support nCipher's SEE technology.

payShield™

A 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 the ability to handle the high volumes of symmetric and asymmetric cryptographic functions required by the latest payment systems for the authentication and verification of cardholders.



nCipher's SSL accelerators provide cryptographic acceleration to prevent SSL bottlenecks, increasing customer and user satisfaction

nCipher's family of SSL accelerators

As the demand for privacy and online security grows, organizations are increasingly turning to the industry-standard security protocol Secure Sockets Layer (SSL) to protect critical information. Recently the use of SSL has expanded beyond Web transactions to secure corporate communications in the form of SSL VPNs and server-to-server connections between front-office and back-office applications.

Unfortunately, SSL operations put an extremely heavy load on server resources, potentially slowing server performance to a crawl, even under moderate traffic conditions. nCipher's SSL accelerators provide cryptographic acceleration to prevent SSL bottlenecks, increasing customer and user satisfaction by dramatically improving SSL processing capacity and server throughput for a fraction of the cost of adding additional servers.

nFast™

The nFast SSL accelerator effectively removes the asymmetric cryptographic processing burden associated with SSL security. The nFast 800 is a PCI card for Windows, Linux and Solaris that processes up to 800 SSL transactions per second. The nFast 300 provides support for an extended range of operating systems and specialized APIs.

nFast Ultra™

The nFast Ultra is a hardware SSL proxy that offloads 100% of the SSL protocol processing, including both asymmetric and symmetric cryptography. Designed as a drop-in solution for virtually any server environment, a single nFast Ultra PCI card allows servers to achieve a sustained throughput of up to 10,000 SSL connections per second, and to process a SSL stream of up to 300 megabits per second full duplex.

nForce™

The nForce range of SSL accelerators speeds SSL throughput and secures the cryptographic keys that underpin SSL. A secure Web site's identity is defined by the use of a digital certificate associated with a unique private key. Protecting the private key is critical to maintaining the confidentiality created for each SSL session and the integrity of the Web site's identity. nForce is a tamper-resistant security module that has been independently validated to the FIPS 140 standard.

The nCipher time stamping platform

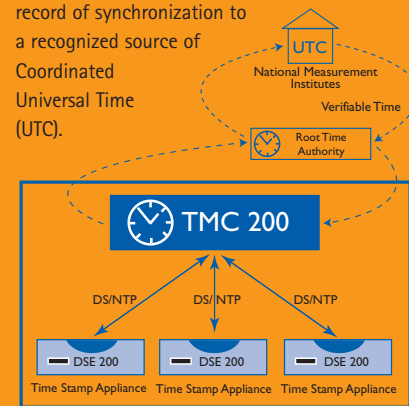
The validity of today's business systems and processes depends on their use of trustworthy and standardized time. Increasingly, legislation and compliance requirements mean that electronic data and documents must embody authoritative proof of time in order to establish when an event occurred. Time-stamping has emerged as one of the key components of a robust PKI, delivering non-repudiation and ensuring the integrity of data is verifiable at a future point in time. Given that local computer time is easy to change and standard Network Time Protocol (NTP) is vulnerable to network attacks, a secure and verifiable pathway to a trusted source of time is a core requirement for business processes. nCipher's time stamping products enable an organization to build digital time stamp signatures into new or existing applications.

DSE 200™

The DSE 200 is an easily deployed network appliance. Securely calibrated via an authenticated network connection, the DSE 200 can provide time stamps to any PKIX compliant time stamp request; avoiding reliance on the unreliable system clock of host servers.

TMC 200™

The TMC 200 is a network appliance incorporating a Rubidium atomic clock for the secure distribution of accurate time. Deploying DS/NTP, an authenticated and encrypted version of NTP, ensures the secure delivery of auditable time to multiple DSE 200 time stamp appliances from a single source. The TMC 200 can also use this secure transport protocol to provide a certified record of synchronization to a recognized source of Coordinated Universal Time (UTC).



Enterprise Time Infrastructure



Nowhere is the need for secure key management greater than in the financial transactions industry

...across the enterprise

nCipher provides simple and cost-effective solutions for organizations to deploy digital signature and time stamping technologies for secure archive, document exchange and certificate validation.

nCipher's security platforms are used to keep critical keys safe, enterprise-wide. They help customers build best-practice cryptographic solutions validated to the FIPS 140-2 standard, locking down sensitive information at every point of risk across the enterprise:

- **Public Key Infrastructure (PKI):**

Failing to properly protect the root private keys that lie at the heart of your PKI puts an entire infrastructure at risk. nCipher's netHSM and nShield are tightly integrated with all leading PKI software to help protect certificate issuance, enhance key management policies and accelerate signing operations across the PKI

- **Content Security & Digital Rights Management:**

nCipher provides simple and cost-effective solutions for organizations to deploy digital signature and time stamping technologies for secure archive, document exchange and certificate validation. Hardware-based cryptography is also being deployed as a best practice control for digital rights management systems, protecting the keys that are used to enforce user rights to ensure that only approved users can unlock documents that would otherwise be safely encrypted

- **SSL Web server & SSL VPN Security:**

Minimizing the processing burden and protecting SSL keys from compromise are vital elements of security for external Web servers, SSL VPNs and internal application servers. nCipher's nFast SSL accelerators deliver best-of-breed performance, while nForce adds security management, enabling customers to move private SSL keys from vulnerable software to tamper-resistant hardware security modules

- **Web Services Security:**

nCipher provides HSMs which integrate into many commercial XML appliances, firewalls, servers and development platforms to protect XML Encryption keys that provide message confidentiality and XML Signature keys that prove identity and deliver data integrity

- **Databases:**

Safeguarding sensitive database information to meet privacy legislation and industry mandates, utilizing tamper-resistant hardware integrated with database security software

- **Authentication:**

HSMs play a central role in the security of strong authentication and access control systems; protecting keys and providing a tamper-resistant environment for the calculations used to check the validity of identity credentials that are presented

- **Payment Processing:**

The need for secure key management is greatest in the financial transactions industry. nCipher's payShield products have been designed to meet the security needs of both traditional payment networks and the latest generation of online payments systems to authenticate users and protect PINs and other confidential information

- **Custom Applications:**

nCipher's family of developer toolkits, including CipherTools™ and CodeSafe™, enable the easy integration of nCipher's hardware security platforms with custom built or commercial applications to enhance security

CORPORATE HEADQUARTERS

Europe & International

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

North America

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



Redefining cryptographic security

nCipher is a leading provider of hardware and software that enable organisations to implement best practice security by addressing the challenges of data confidentiality, authentication and compliance. The foundation of these applications is proven platform technology that meets the challenges of cryptographic key management and performance. Many of the world's leading organizations - from Microsoft and Barclays Bank to PricewaterhouseCoopers and the U.S. Navy - rely on nCipher to deliver a sound e-security infrastructure. Our platform products are particularly well-suited to organizations with high volumes of security-sensitive transactions, such as banking and financial institutions, government departments, e-retailers and online service providers.

nCipher is listed on the London Stock Exchange (LSE:NCH) and is a member of the FTSE TechMARK and FTSE4Good indices, with headquarters in Cambridge, UK.

For more information on nCipher, visit
www.ncipher.com

Every effort has been made to ensure the information included in this brochure 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. ©2005 nCipher Corporation Ltd. nCipher, nFast, nForce, nShield, netHSM, payShield, Security World, CodeSafe, CipherTools, SEE, DSE 200 and TMC 200 are trademarks or registered trademarks of nCipher Corporation Ltd. All other trademarks contained herein are the property of their respective owners.