Protecting Critical Enterprise Data

Best practice solutions for encryption, digital signing, and authentication

IDENTIFY, PROTECT, COMPLY

Enterprises are challenged to manage increasingly large and complex security architectures. The importance of cryptographic systems underpinning encryption, digital signing and authentication, requires a flexible management framework that includes secure key management and tamper-resistant cryptographic platforms.

Critical data can take many forms; from user PIN values, credit card details, customer information and healthcare records to corporate secrets and regulatory filings. To manage risk and meet compliance requirements organizations must apply additional security controls and enforce policies that protect data wherever it is stored and whenever it moves or is accessed inside the extended enterprise.

Security-aware organizations have long-recognized that cryptography can provide this level of enforcement, underpinning trust by providing confidentiality, proof of identity, data integrity and non-repudiation. As the use of cryptography becomes pervasive across the enterprise, organizations face the challenges posed by an increasingly large and complex security architecture, where cryptographic keys and management processes are at the heart of trusted encryption, digital signing and authentication processes. Protecting and managing these keys that underpin system security is of paramount importance.

The nCipher Difference – Security World™

nCipher's Security World is a security management architecture that addresses this challenge. It simplifies the management and protection of keys across a large and diverse network of users, applications and endpoints through a flexible hardware-based security infrastructure. This encompasses the established best practice that tamper-resistant hardware based systems are preferred over pure software environments to protect sensitive encryption and signing keys.

nCipher has established a strong reputation through Security World for helping some of the most sophisticated and security-oriented organizations, including 9 of the 10 largest banks in the world, deploy high performance and robust systems to protect their most critical data.

nCipher delivers solutions in two broad categories - an enterprise key management system and a wide range of cryptographic security platforms.

Enterprise Key Management

nCipher's keyAuthority™ solution delivers centralized cryptographic key management and automated key delivery to distributed security applications deployed across large numbers of network-attached endpoints at geographically dispersed locations. Using standard APIs, keyAuthority allows keys to be generated and managed centrally, including critical recovery and escrow functions, before distribution to cryptographic applications - on demand. The central control of keys, security objects and configuration data helps to enforce high-security policies and achieve regulatory compliance.

Cryptographic Security Platforms

nCipher's cryptographic hardware platforms allow organizations to go beyond software based security techniques to protect and manage encryption and signing keys, execute sensitive application code, prove the authenticity of documents and accelerate SSL operations. nCipher provides out-of-the-box integration with numerous commercial security applications through standard's based interfaces in addition to providing a range of developer solutions to support custom applications and embedded deployments.

nCIPHER™

netHSM™

The netHSM is a FIPS 140-2 Level 3 network-attached, shareable Hardware Security Module (HSM) appliance. It allows multiple applications to simultaneously access hardware-based encryption, decryption and signing functions via secure connections over IP networks. In addition to managing and protecting keys 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 tamper-resistant HSM for enhancing the security of virtually any type of server based platform. nShield is commonly used as part of a Public Key Infrastructure (PKI) deployment, to encrypt data at rest or to strengthen any application using digital signatures or SSL communications. nShield is a PCI form factor card that protects and accelerates cryptographic operations and secures keys within a tamper-resistant hardware environment, federally validated to FIPS 140-2 Level 3.

payShield™

A FIPS 140-2 Level 3 validated HSM designed to meet the stringent requirements of the payments industry. payShield implements functionality to support magstripe and EMV-based transaction processing, including 3-D Secure authentication. payShield combines the highest level of protection with an ability to handle high volumes of symmetric and asymmetric cryptography required for the authentication and verification of cardholders.

Classified Document Security Appliance™

The nCipher Classified Document Security Server combines the Adobe LiveCycle Document Security Server, certificate services and FIPS 140-2 validated HSM within a convenient appliance platform to deliver the most streamlined and cost-effective way for organizations to distribute digitally signed and/or encrypted Adobe® Portable Document Format (PDF) files.

nForce™ and nFast®

An ultra high performance PCI card providing a complete SSL sub-system for managing SSL communications on behalf of web servers and application servers. Both product variants provide a convenient drop-in SSL solution that unlike traditional SSL accelerators terminates and originates SSL connections and performs all SSL operations directly on the PC card avoiding the need to reconfigure applications or support complex cryptographic APIs. Both products provide a capacity of up to 10,000 SSL connections per second and in addition the nForce product variant combines nCipher's FIPS validated Security World key management technology.

Time Stamping

nCipher's time-stamping products, Time Stamp Server and Time Source Master Clock, allow organizations to integrate secure digital signatures and auditable time stamping functionality into their critical applications. Time stamping is a core component of a PKI deployment, auditing systems, document archives or code signing processes delivering non-repudiation and ensuring that data integrity is verifiable at any time in the future.

Developer Solutions

nCipher toolkits provide a flexible way for customers to protect their critical information and custom applications. nCipher's developer solutions and cryptographic hardware platforms provide the framework to build products molded to fit the security needs of each business. The CipherTools, CodeSafe, payShield and other toolkits provide standard APIs, reference designs and example code that enables developers to easily leverage the nCipher Security World architecture with almost any application and host system to create a truly secure and scalable security infrastructure.

miniHSM™

For OEMs that need a FIPS validated secure key management sub-system for their own security solutions, nCipher offers a convenient and low risk embedded solution that leverages nCipher's Security World technology to accelerate time to market and avoid internal development costs.

NCF/OVERVIEW/ENGLISH/MAY2007

nCipher Inc.
92 Montvale Avenue, Suite 4500
Stoneham, MA 02180 USA
Tel: +1 (781) 994 4000
ussales@ncipher.com

nCipher Corporation Ltd.
Jupiter House, Station Rd.
Cambridge, CBI 2JD UK
Tel: +44 (0) 1223 723600
int-sales@ncipher.com

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

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

nCIPHER™