Governments and enterprises across the globe use nCipher hardware security modules (HSMs) for secure cryptographic processing. As a Gold Certified Microsoft Partner, nCipher enhances a range of Microsoft products by reducing cost and complexity associated with the use of cryptography across applications. nCipher HSMs strengthen the root of trust of business applications, providing a certified environment for management and safekeeping of sensitive key material.

nCipher, a leading global provider of data protection and cyber security solutions to government, financial services, high technology and manufacturing.

THE GOAL: MAINTAINING DATA CONFIDENTIALITY AND COMPLYING WITH EVOLVING REGULATIONS
The emergence of advanced persistent threats (APTs) targeting enterprise systems has created a pressing need to improve the protection of sensitive data and to safeguard the integrity of software. Cryptography, namely encryption and digital signature technology, is ideally suited to provide this protection. Cryptography also helps organizations demonstrate compliance with government and industry regulations, and plays a strong role in maintaining high availability for applications and data.

Microsoft and nCipher extend security for critical business applications

Microsoft applications and nCipher hardware security modules enhance data protection with a high assurance solution
- Provide enhanced security of PKI and other enterprise software
- Reduce cost and complexity associated with cryptography
- Embrace best practices for auditing and security compliance
- Deliver high assurance with FIPS and Common Criteria certification

Microsoft and nCipher extend security for critical business applications

nCipher nShield HSMs integrate with Microsoft applications to safeguard and manage cryptographic keys within a high assurance framework.
Microsoft and nCipher extend security for critical business applications

nCipher and Microsoft help organizations strengthen and extend the security of data to facilitate auditing and compliance with government and industry regulations.

THE CHALLENGE: MANAGING CRYPTOGRAPHIC KEYS WITHIN A HIGH ASSURANCE ENVIRONMENT

Cryptography provides a means of verifying identities, controlling access, and protecting critical data. As its usage continues to increase and span multiple applications, growing numbers of keys become difficult to manage. These keys may also be vulnerable to targeted threats. Auditors recommend best-in-class hardware security, such as nCipher nShield HSMs, to safeguard and manage their long term confidentiality and availability for high performance and business continuity.

THE PARTNERSHIP: MICROSOFT AND NCIPHER EMBRACE BEST-IN-CLASS SECURITY AND PERFORMANCE

Microsoft applications maximize business productivity and incorporate cryptography to control user access and to protect the confidentiality and integrity of data. nCipher enhances security by providing HSMs that feature a hardened, tamper-resistant environment for secure cryptographic processing on behalf of multiple Microsoft applications. The trustworthiness of cryptographic operations also depends on a strong supporting key management process. nCipher nShield HSMs provide a comprehensive solution that is certified to demanding global government and industry standards.

nCipher specializes in data protection, delivering technologies that enhance the security of critical business systems. Through an ongoing close collaboration, Microsoft customers have benefited from nCipher high assurance security for more than a decade.

WHY USE HSMs WITH MICROSOFT ENTERPRISE APPLICATIONS?

While it is possible to perform cryptographic processes strictly in software, keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to APTs and other threats which could lead to compromised identities or disclosure of confidential data. HSMs deliver a proven and auditable way to secure valuable cryptographic material. HSMs enable organizations to:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms so keys are only used for their authorized purpose
- Ensure availability by using sophisticated key management, storage and redundancy features to guarantee keys are always accessible when needed
- Deliver high performance to support demanding cryptographic processing and growing key volumes

NCIPHER

nCipher nShield HSMs are high-performance cryptographic devices designed to generate, safeguard, and manage sensitive key material. Certified to stringent security standards, nShield HSMs:

- Protect keys in a secure, tamper-resistant environment
- Enforce security policies, separating security functions from administrative tasks
- Comply with regulatory requirements for public sector, financial services, and enterprises
- Support high-performance elliptic curve cryptography (ECC)

nCipher nShield HSMs are available to match specific performance and budgetary needs:

- nShield Edge: Portable USB-attached for low-volume offline root certificate authority (CA) and developer environments
- nShield Solo/Solo +/Solo XC: Embedded PCI or PCIe for issuing CA/OCSP SSL servers and security appliances
- nShield Connect/Connect +/Connect XC: Network-attached for high-performance issuing CA/OCSP/SSL environments

MICROSOFT

Microsoft has transformed the way businesses create and share content, process transactions, and build collaborative processes. Systems based on Microsoft enterprise applications maximize productivity. To protect data, Microsoft pioneering technologies use cryptography to establish trusted business environments that:

- Manage identities across organizations
- Establish trusted PKI environments
- Control user access
- Protect data confidentiality and integrity

For additional information, please visit www.ncipher.com or www.microsoft.com