nForce™

HARDWARE SECURITY MODULE FOR SSL

PRODUCT | DATA SHEET

The nForce™ range of Hardware Security Modules (HSMs) delivers unparalleled performance enhancements, scalability and security for a wide range of Internet applications.

A single nForce device can enable Web servers and other Internet applications to achieve sustained throughput of up to 1600 new SSL connections per second — an increase of 10-fold or more. Offloading the cryptographic processing reduces the need for additional servers, reduces administration costs and improves system response time and therefore the user experience. In more demanding situations, multiple nForce devices can be combined for even greater capacity.

A secure Web site's identity is defined by the use of a digital certificate underpinned by a unique cryptographic 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. The only truly secure solution is to store and manage keys in a highly secure hardware environment. nForce is a 'tamper-evident' security module that has been independently validated to the FIPS 140-2 standard. All cryptographic functions, that would otherwise be performed on the insecure server, take place inside the nForce device, ensuring that private keys are always protected from compromise.

All nCipher HSMs share a common key management framework, nCipher's Security World. This delivers security, scalability and resilience for dynamic HSM deployments. All nCipher HSMs can be configured for dual control and split responsibility ensuring that there is no single point of compromise. Scalability is easily achieved by ensuring there is no restriction on the number of HSMs that can work in unison or on the number of keys that can be managed. In addition to boosting capacity, this capability supports high-availability deployments through automatic failover to a second HSM unit. This flexibility allows an organization to add, reconfigure or reallocate hardware to meet new business needs, maximizing the return on investment.

Through business alliances with leading providers of secure Web server software and other applications that rely on SSL, nCipher is able to ensure out-of-the-box system integration. By providing seamless product compatibility, nCipher and its strategic partners can deliver the combined strengths of FIPS validated hardware security with a wide variety of software security applications helping to reduce risk and deployment expense.

FEATURE	BENEFIT
OFFLOADING OF CRYPTOGRAPHIC PROCESSING	Removes bottlenecks and frees your server to respond to more requests
HIGH AVAILABILITY	Dual nForce HSMs can be used for resiliency. The main unit will transparently pass all processing activity to a back-up unit if the device becomes unavailable
FIPS 140 VALIDATION	Independently certified secure management and storage of private keys
ADMINISTRATION OF KEYS CONTROLLED THROUGH THE USE OF SMARTCARDS	Smartcards authenticate administrators to provide a highly flexible means of sharing responsibilities between individuals within the organization
SUPPORT FOR VERISIGN HARDWARE PROTECTED SSL CERTIFICATES	Provides public proof of SSL security and server identity
SNMP SUPPORT	Allows network management consoles to remotely retrieve status information and real-time performance statistics for installed nForce devices

nCIPHER™

PRODUCT SPECIFICATIONS

PRODUCT	FORM FACTOR	FIPS 140-2 VALIDATION	NO. OF NEW 1024 BIT SSL CONNECTIONS PER SECOND*
nFORCE 150 PCI	PCI	Level 2	150
nFORCE 300 PCI	PCI	Level 2	300
nFORCE 150 SCSI	SCSI	Level 2	150
nFORCE 400 SCSI	SCSI	Level 2	400
nFORCE 1600 PCI	PCI	Level 2	1600

*The performance figures quoted herein are nominal figures. Actual system performance depends on application software version, server platform type and other factors.

Application Software

- Apache Web Server
- Sun ONE Web Server
- Microsoft IIS
- Microsoft ISA Sever
- BEA WebLogic Application Server
- IBM HTTP Server
- IBM Tivoli Access Server
- IBM WebSphere Application Server
- Oracle Database & Application Server
- webMethods B2B Server

For the latest list of supported applications please visit www.ncipher.com

APIs and Toolkits

- Microsoft CryptoAPI
- PKCS #11
- OpenSSL
- Java JCE/JCA
- Additional APIs are supported through nCipher's CipherTools Developer's Kit

Cryptographic Algorithms Supported

SYMMETRIC CIPHERS

- AES - Rijndael
- Arc Four (compatible with RC4)
- CAST
- DES
- Triple-DES

PUBLIC KEY CIPHERS

- DSA
- El Gamal
- RSA

KEY EXCHANGE MECHANISMS

- DH
- DES / DES3 XOR

HASH AND HMAC FUNCTIONS

- MD2
- MD5
- RIPEMD 160
- SHA-1

Operating Systems

- AIX
- Linux
- Solaris
- HP-UX
- Windows 2000
- Windows 2003

Form Factor and Dimensions

- SCSI MODULE
  Fast wide SCSI 2 (also called SCSI 3) with a high density micro-D 68 connector. Can be mounted in a server's 5.25" drive bay or in a dedicated external enclosure
- PCI MODULE (nForce 150 and 300)
  Standard PCI half card
  33MHz, 32 bit
  PCI 2.1 compliant
- PCI MODULE (nForce 1600)
  Standard PCI half card
  66MHz, 32 bit
  PCI 2.2 compliant

Standards Certification

- FCC: CFRA47, Part 15, Subpart B, Class A
- CE: EN 55022 Class A
  EN 55024-1
  EN 60950

Operating Specifications

- Maximum power consumption for PCI: 2.5 amps at 5 volts
- Maximum power consumption for SCSI: 3.0 amps at 5 volts
- Temperature: 10-35 degrees Centigrade
- Relative Humidity: 10-85% non-condensing

NCDS/NFORCE/JULY2004

nCipher Inc.
500 Unicorn Park Drive
Woburn, MA 01801 USA
Tel: +1 (781) 994 4000
E-mail: ussales@ncipher.com

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

Visit our Web site at www.ncipher.com – today!

Redefining cryptographic security

nCIPHER™