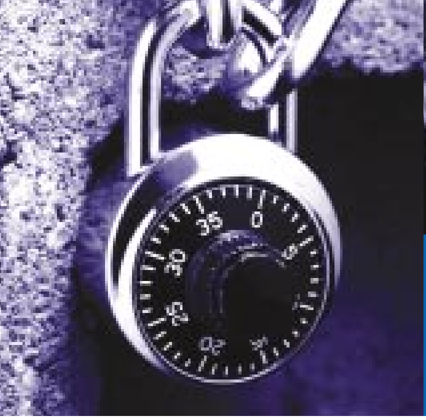

nForce Ultra™

TAMPER-RESISTANT SSL OFFLOAD CARD

PRODUCT | DATA SHEET

The nForce Ultra™ is a tamper-resistant SSL offload card that has been independently validated to the U.S. and Canadian federal standard FIPS 140-2. It removes the processing burden associated with SSL security in virtually any server environment. nForce Ultra combines the benefits of SSL acceleration with best-practice security for the cryptographic keys that underpin SSL security, protecting the confidentiality of each SSL session and the integrity of the server's identity.

The SSL standard and its successor TLS have emerged as the benchmark for secure communications over IP networks. SSL provides both privacy and authentication in any situation where data may be compromised and, as a result, is used almost universally to protect e-commerce transactions and other web-based communications. Recently the use of SSL has expanded to secure corporate communications in the form of VPNs and server-to-server connections between front-office and back-office applications.

The nForce Ultra delivers two significant benefits to your SSL infrastructure: accelerating SSL performance and providing FIPS 140-2 validated key management for enhanced security and compliance with data privacy regulations.

ENHANCING SSL PERFORMANCE

The intensive cryptographic processing and protocol handling required to establish SSL sessions can cripple a server by exhausting CPU horsepower, slowing down critical applications. This can result in acute server bottlenecks, particularly in the case of back-office or application servers where CPU capacity is already under pressure. Consequently, many security architects have faced a stark choice: to deploy SSL very sparingly, for example limiting its use to web-based services, or to deploy large numbers of expensive servers to handle the increased processor load.

The nForce Ultra SSL Offload card provides all the functionality necessary to establish an SSL or TLS secure connection over an IP network. It comes equipped with an Ethernet interface and effectively replaces the existing network interface of the host server. Encrypted SSL traffic arriving over the network is decrypted and passed to the host and traffic passing back to the network is encrypted whenever SSL protection is required. Non-SSL traffic passes through the card transparently. The nForce Ultra card has been optimized to provide market-leading performance, delivering up to 10,000 transactions per second (TPS) and on-going throughput of 300MB full duplex.

ENHANCING SSL SECURITY

A server's SSL private key is the primary means of proving the server's identity and is the cryptographic secret used to create encrypted sessions for each connection. However, if this private key is stored in a software environment and exposed in server memory, it becomes vulnerable to compromise. Key-finding attacks can put the security of the whole system at risk. Armed with your SSL private key, an intruder can destroy the authenticity and privacy of your secure service. They could impersonate a legitimate Web site or hack data as it crosses the wires, eavesdropping on secure traffic, stealing user's passwords, PINs or other valuable information. Increasingly, data privacy regulations mandate the provision of additional protection for cryptographic keys.

nForce Ultra is a tamper-resistant offload card that has been independently validated to the FIPS 140-2 standard. Because all of the SSL operations are terminated directly on the PCI card, there are no complicated integration steps or cryptographic APIs to support. This ensures simple integration into virtually any platform running Windows, Solaris or Linux, delivering a protective subsystem within your server for the management of cryptographic keys.

NCIPHER™

FEATURE	BENEFIT
FIPS 140-2 VALIDATION*	Independently certified secure management and storage of SSL keys
FULL OFFLOAD OF SSL PROCESSING	Transparent addition of SSL security to existing and new applications via a single, comprehensive solution
DEDICATED HARDWARE SOLUTION FOR SSL PROCESSING	By offloading all SSL processing from the host CPU, performance is preserved for the business process in question
HIGH PERFORMANCE CRYPTOGRAPHIC PROCESSING	Capable of supporting up to 10,000 new SSL/TLS connections per second and combined throughput of 300MB per second
PLUG-AND-PLAY INTEROPERABILITY	Runs with any IP-enabled application running on Windows, Solaris or Linux operating systems
INTEGRAL NETWORK INTERFACE (10/100/1000 – RJ45 ETHERNET)	Easy installation requiring no application reconfiguration or support for cryptographic acceleration APIs

*In submission.

PRODUCT SPECIFICATIONS

OS Support

- Windows 2000 and Windows Server 2003
- Linux - Kernels 2.4 and 2.6 and a variety of Linux distributions including Redhat 9.0 and Redhat Enterprise 4
- Solaris - Solaris SPARC 9 and 10

PCI Hardware Specification

- PCI Card 4.2 x 6.6 inches (1/2 length, full Height)
- 10/100/1000 - BaseT Ethernet (RJ45)
- PCI 2.2/2.3; PCI-X 1.0a Bus Connector up to 133 MHz
- Operating voltage: +5 volts and +3.3 volts
- Signalling voltage: +3.3 volts
- Typical power consumption: 17 watts
- Operating Temperature: 10-35 degrees centigrade with airflow (200 LFM recommended)

SSL/TLS Operation

- Fully offloads SSL/TLS processing including handshaking, record handling and all cryptography
- Supports SSL V3.0, TLS V1.0 (RFC 2246)
- Stores up to 256 certificates

Cryptographic Algorithms

- RSA: 1024-bit, 2048-bit and 4096-bit, public and private key processing
- ARC4, DES, 3DES and AES bulk cipher algorithms

Performance

- Up to 10,000 RSA SSL handshakes per second (1024-bit RSA decryptions)
- 300 Megabit Full-duplex throughput
- Up to 100,000 Simultaneous connections

FIPS Validations

- Asymmetric Cryptographic Boundary - FIPS 140-2 Level 3
- Symmetric Cryptographic Boundary - FIPS 140-2 Level 1

Gigabit Ethernet Network Port

- Full-duplex 10/100/1000 RJ-45 Ethernet network interface
- Handles IEEE 802.3 (RFC 1042) or DIX (RFC 894) frames
- Supports IEEE 802.3, 802.3u, 802.3x, 802.3z, and 802.3ac Ethernet specifications
- Supports MTUs up to 1500 bytes
- Pass-through of IEEE 802.1q VLAN tags

IP Layer Processing

- Processes IPv4 (RFC 791) datagrams
- Pass-through of IP header fields such as source/destination addresses and Type of Service (TOS)
- Calculates and verifies header checksums
- Supports limited ICMP messaging (RFC 792)
- Non-SSL traffic can be passed through unaltered to host or blocked

TCP Layer Processing

- Terminates TCP streams from clients and to servers (designated SSL/TLS connections)
- Supports standard TCP functions per RFCs 793, 813, and 1122
- Extracts/inserts SSL/TLS records
- Supports transparent pass-through of non-SSL/TLS traffic
- Segmentation and reassembly (including reordering)
- Performs TCP port translation (source and/or destination)
- Calculates/verifies pseudo-header checksums
- Fast Retransmit/Fast Recovery (RFC 2581)
- Round Trip Time Estimation (Karn's Algorithm)
- Slow Start (RFC 896)
- Window Scaling (RFC 1323)

Standards Certification

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

Every effort has been made to ensure the information included in this datasheet 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, nForce Ultra, are trademarks or registered trademarks of nCipher Corporation Ltd. All other trademarks contained herein are the property of their respective owners.

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

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

Redefining cryptographic security

NCIPHER™