

nFast 800™

SSL ACCELERATOR

The nFast 800 SSL Accelerator is a high-performance PCI card that enables your organization to cost-effectively optimize your secure Web server's performance. This "Plug and Play" product sets a new standard for price-performance value, at a price point that allows for unprecedented deployment of Secure Socket Layer (SSL)... and all from nCipher, the leading provider of enhanced security for electronic transactions.

PRODUCT DATA SHEET



Expanding SSL Deployment

SSL has become the standard method for securing Internet communications by encrypting sensitive information. However, the use of SSL often comes at the price of acute server bottlenecks. SSL transactions require multiple, highly-intensive mathematical processes that Web server platforms are ill-equipped to handle. A handful of SSL requests can cripple a server by exhausting CPU horsepower and prevent even normal operations from being performed. The result is that site

architects have used SSL only very sparingly in an attempt to reduce the impact on Website performance.

The nFast 800 enables organizations to expand deployment of SSL encryption on their public Web site or company intranet and therefore, offer essential privacy to more than just select users on only the most critical pages.

Accelerated Performance

A single nFast PCI card allows Web servers to achieve sustained throughput of up to 800 SSL connections per second, delivering a 500 percent performance improvement over typical non-accelerated Web servers. By reducing the load on your Web server's CPU through the use of a dedicated security processor, which forms the heart of the nFast 800, the server is largely unaffected by the use of SSL and is able to process information, perform transactions and serve content as normal.

Multiple nFast PCI cards can be installed to scale linearly, providing both load-balancing and fail-over capability, virtually guaranteeing that your customers never have to wait for a secure connection. With nFast, your organization can add the "equivalent power" of additional servers, at a fraction of the cost.

FEATURE	BENEFIT
OFF-LOAD OF CRYPTOGRAPHIC SSL PROCESSING	Removes bottlenecks and frees your server to respond to more requests
PRESERVE OPTIMAL SERVER PERFORMANCE	By offloading SSL processing, you can preserve performance to efficiently handle other critical server functions
PLUG AND PLAY INTEROPERABILITY	Compatible with Microsoft Windows 2000 & 2003 running IIS, as well as Apache web servers running on Linux and Sun™ ONE on Solaris
FAIL OVER CAPABILITY	Transparently passes all of the processing to the next nFast or back to server software (for single unit installs)
HIGHLY SCALABLE ARCHITECTURE	Multiple nFast cards can be easily added to a single server for even higher processing power and capacity

The nFast 800 works seamlessly with Windows 2000 & 2003 server running Microsoft IIS. It also supports Linux-based servers running Apache Web server with OpenSSL and Sun™ ONE Web Server via PKCS#11. The nFast 800 supports the industry-standard Simple Network Management Protocol (SNMP) for manageability, allowing network management consoles to remotely retrieve real-time performance statistics for installed nFast devices.

nCipher IT Security Solutions

nFast 800 is part of nCipher's family of IT security solutions, giving you the ability to secure points of risk across your enterprise enabling secure communications, data protection, tamper-resistant software applications and enhanced security management.

PRODUCT SPECIFICATIONS

PCI Hardware Specification

- Standard PCI half-card
- PCI version 2.2, 32/64-bit, 33/66-MHz bus interface
- Operating voltage +5 volts
- Maximum power consumption: 2.1 amps at 5 volts
- Operating Temperature: 0-55 degrees centigrade

Cryptographic Algorithms

- RSA: 512-bit, 768-bit, 1024-bit, 1536-bit, and 2048-bit RSA public-key and private-key processing
- DSA: 512-bit, 768-bit, and 1024-bit DSA signing and verification
- Diffie-Hellman: 512-bit, 768-bit, 1024-bit, 1536-bit, and 2048-bit D-H session-key generation

Note that not all APIs support all available algorithms and key lengths.

Performance

- Up to 800 RSA: SSL handshakes per second (1024-bit RSA decryptions)

Software Support

Windows 2000 & 2003 Server Family

- Hardware acceleration for CryptoAPI (CAPI) via the OffloadModExpo function
- SNMP management support for the Windows Server family SNMP Service
- CIM (Common Information Model) management support via Windows Management Instrumentation (WMI)

Linux

- Kernels 2.2 and 2.4 and a variety of Linux distributions including Redhat 7.0, 7.1, 7.2
- Complete OpenSSL engine off-load support for Apache-based web servers
- SNMP management support

Solaris

- Solaris 2.6, 2.7, 2.8
- PKCS#11 API
- SNMP management support
- Sun™ ONE Web Server support

Standards certification

- FCC: CFR47, Part 15, Subpart B, Class B
- CE: EN55022 Class B
EN55024
EN60950