CAVIUM

FIPS 140-2 Accelerator Boards

NITROX® XL CN16XX NFBE HSM Adapter Family

Product Brief

OVERVIEW

The NITROX XL CN16XX NFBE HSM Adapter family is the world's fastest FIPS 140-2 Level 2 and Level 3 certified Hardware Security Module (HSM) with PCI-Express Gen 2.0 interface. The NITROX XL HSM adapter is designed to offer maximum value by efficiently delivering cost effective FIPS 140-2 validated network security to Linux, FreeBSD and Java environments. This family of HSM adapters efficiently offloads and protects SSL / cryptographic transactions by leveraging the highest performing processor and security processor technology from Cavium, and can deliver performance of up to 45,000 RSA operations per second and up to 5 Gbps of offloaded IPsec or bulk crypto performance. The NITROX XL HSM adapter frees up the processor cycles for application level processing and reduced cost of ownership.

The NITROX XL HSM family of adapters is 140-2 Level 3 certified. The security parameters never leave the card without proper encryption. Cavium provides a comprehensive Software Development Kit that includes C-source code for Linux and FreeBSD drivers. The SDK also includes APIs for OpenSSL, OPenSSH, PKCS#11 and Java Cryptographic Extensions. The NITROX XL FIPS adapter family can be integrated into wide range of equipment including Web Servers, L4+ Switches, Load Balancers, Networking / Server Appliances, Unified Threat Management Appliances, Remote Access Servers, Public Key Infrastructure and Database Servers.

FEATURES

- Highest Performing FIPS 140-2 Hardware Security Module (HSM) Adapter Family
- SSL / TLS performance
  - Up to 45K 1024-bit key RSA operations / sec
  - Up to 8.5K 2048-bit key RSA operations / sec
  - Up to 5Gbps of bulk crypto throughput
- Enhanced on card storage
  - Up to 200,000 concurrent SSL sessions
  - Up to 4096 concurrent server private key
- USB port for two-factor authentication
- Support for FIPS 140-2 Level 3 EAP FAST TLS Extensions
- Accelerates SSL cryptographic functions and bulk encryption including IPSec
- 256-bit AES based key encrypt for key archive and transport
  - Advanced ECC is used for handshake
- SP800-90 based Deterministic Random Bit Generator (Random Number Generator) support for FIPS 140-3
- Supports 32-bit and 64-bit Linux and FreeBSD SDK
- Supports Java Cryptographic Environment (JCE)

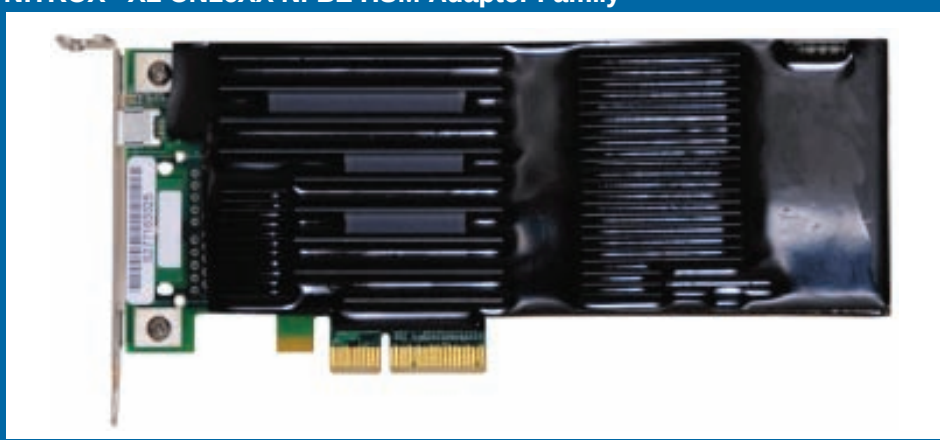
BENEFITS

- Highest and scalable performing FIPS 140-2 HSM adapter
- Firmware upgradable to support FIPS 140-3
- Widest array of OS drivers, API support and block ciphers
- Short development time for quick time to market
  - Complete hardware module
  - Common APIs for both FIPS and non-FIPS product
  - Complete SDK including source code for drivers, utilities and reference application
- Physical and logical Cryptographic boundaries
  - Secure and tamper evident enclosure
  - All keys are secured within cryptographic boundary.

APPLICATIONS

- L4+ Switches
- Load Balancers
- Networking / Server Appliances
- Database Servers
- Web Servers
- Remote Access Servers
- Unified Threat Management Appliances
- Public Key Infrastructure

NITROX® XL CN16XX NFBE HSM Adapter Family



CAVIUM

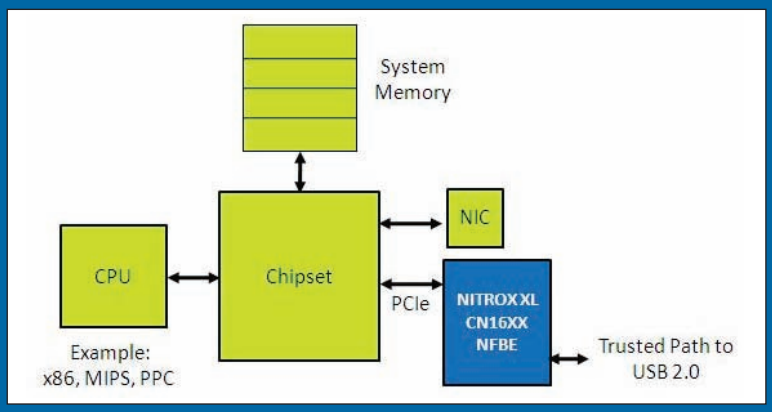
2315 N. First Street
San Jose, CA 95131
T 408-943-7100
F 408-577-1992
E sales@cavium.com
www.cavium.com

FIPS 140-2 Accelerator Boards

NITROX® XL CN16XX NFBE HSM Adapter Family

Product Brief

SYSTEM DIAGRAMS



NITROX XL CN16XX NFBE usage in SSL offload application

SPECIFICATIONS

- Low profile (2.1" x 6.6") PCIe form factor can easily fit 1U appliance
- PCIe Gen2 x4 interface providing latest connectivity
- USB 2.0 port for 'Smart Keys' for FIPS 140-2 Level 3
- Firmware upgradeable to FIPS 140-3 support
- Support for a wide variety of algorithms
- Modular Exponentiation: RSA / DH Public Key 1024-bit, 2048-bit & 4096-bit
- Power: <25 Watts
- Operating Temperature: 0 to 50° C
- Airflow – 150LFM (Minimum)
- Regulatory Certifications: Safety, cTUVus UL, EMC, FCC/ICES, Class A

SOFTWARE AND API SUPPORT

- Drivers for Linux and FreeBSD
  - RHEL 5.3, Fedora Core 10.x, FreeBSD 6.3 and 7.2
- Java Cryptographic Extension support
- OpenSSL and TurboSSL support
- PKCS#11 Crypto-service provider
- OpenSSH
- API libraries for Card and key management
- Performance optimized SSL macro APIs

NITROX® XL CN16XX NFBE HSM Adapter Family

Device	System Interface	USB Port	Performance		Dimensions
			Max RSA Ops / sec	Full SSL Record Throughput	
CN1620-NFBE3-1.0-G	PCIe Gen2.0 x4	1 x USB 2.0	45K (1024b), 9K (2048b)	5 Gb/s	2.1" x 6.6"
CN1620-NFBE1-1.0-G	PCIe Gen2.0 x4	1 x USB 2.0	15K (1024b), 3K (2048b)	1.5 Gb/s	2.1" x 6.6"
CN1610-NFBE3-1.0-G	PCIe Gen2.0 x4	1 x USB 2.0	7.5K (1024b), 1.5K (2048b)	750 Mb/s	2.1" x 6.6"

2315 N. First Street
San Jose, CA 95131
T 408-943-7100
F 408-577-1992
E sales@cavium.com
www.cavium.com

Nitrox-NFBE HSM-PB-1.0 Printed in the USA