

Accelerator Boards

NITROX[®] XL CN16XX NFBE Adapter Family

Product Brief

OVERVIEW

The NITROX XL CN16XX NFBE Adapter family delivers the world's fastest FIPS 140-2 level 2 and 3 certified Hardware Security Module (HSM) with PCIe Gen 2.0. This family of adapters offers up to 45,000 RSA operations per second and 5 Gbps of bulk crypto performance and is certified to the stringent US Government security standards. Furthermore, this FIPS family delivers an unmatched solution to the increasing performance, cryptographic and time to market requirements of the financial, government and healthcare vertical markets. The NITROX XL adapters are integrated into a wide range of appliances including Remote Access Servers, Public Key Infrastructure, Database Servers, Web Servers, L4+ Switches, Load Balancers, Networking / Server appliances and Unified Threat Management Appliances.

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 and PKCS#11, key management utilities, test utilities and reference code for easy portability. The Crypto-API's are common between Cavium's FIPS and the non-FIPS products, providing customers with tremendous R&D leverage and re-use.

FEATURES

- Highest Performing FIPS 140-2 Hardware Security Module (HSM) Adapter Family
- SSL / TLS Performance
 - Up to 45,000 RSA operations / sec
 - Latest IO interface, PCI-Express Gen2 x 4
- Macro processing for optimal system efficiency
 - Complete SSL handshake or record processing in a single API call
- On-board storage for up to 200,000 concurrent SSL sessions
- On-board storage for up to 4096 concurrent server private keys
- Separate "Trusted-Path" Administration Interface for FIPS140-2 Level 3
 - USB 2.0 Interface
- Authenticated / Unauthenticated Operator Roles
 - User – normal operational role on the module
 - Security Officer – security administration tasks such as User creation
 - Public User – for access to status information and diagnostics before authentication

BENEFITS

- Scalable performance of 7.5K RSA operations / sec to 45,000 RSA operations / sec
- Scalable bulk crypto throughput performance of 750 Mb/s to 5Gb/s
- Short development time for quick time to market
 - Complete hardware module
 - Common APIs for both FIPS and non-FIPS product providing tremendous R&D leverage and re-use
 - Complete C Software kit including source code
 - Drivers & utilities
 - Reference application
- Physical and logical Cryptographic boundaries
 - Secure, tamper-proof enclosure provides a barrier. All components are encompassed within the Cryptographic boundary. Keys cleared if enclosure is breached
- Configurable security modes for multiple security level product families
 - Operates in FIPS 140-2 modes, either level 2 or level 3

NITROX[®] XL CN16XX NFBE Adapter Family

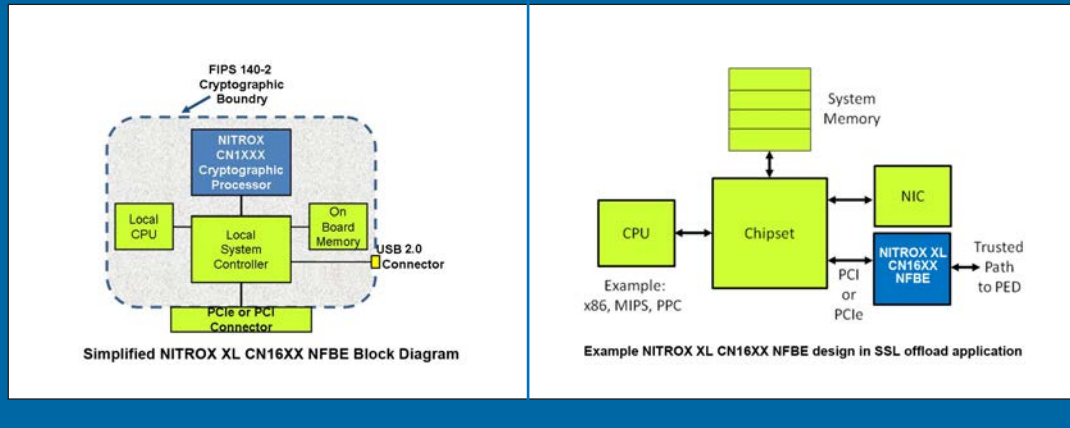


Accelerator Boards

NITROX® XL CN16XX NFBE Adapter Family

Product Brief

SYSTEM DIAGRAMS



SPECIFICATIONS

- Low profile (2.1" x 6.6") PCIe form factor can easily fit 1U appliance
- PCI-Express Gen2 x4 interface, latest connectivity
- Optional RJ45 interface, providing a dual functionality of HSM and Ethernet
- USB 2.0 port for 'Smart Keys'
- Firmware upgradeable to FIPS140-3 support (based on review of current specifications)
- Firmware upgradeable to support ECC
- Power < 25 watts
- Operating Conditions
 - Operating temperature: 0 to 50° C
 - Air flow: 150LFM (minimum)
- Regulatory Certifications
 - Safety – USA / Canada: cTUVus UL
 - EMC – USA / Canada: FCC / ICES, Class A

SOFTWARE SUPPORT

- Drivers for Linux and FreeBSD
 - RHEL 5.3, Fedora core 10.x
 - FreeBSD 6.3 and 7.2
- API libraries for Card and Key management
- Performance optimized SSL macro-APIs
- PKCS#11 Crypto-Service-Provider
- OpenSSH

NITROX® XL CN16XX NFBE Adapter Family

Device	System Interface	USB Port	NIC Interface	Performance		Dimensions
				Max RSA Ops / sec	Full SSL Record Throughput	
CN1620-NFBE3-2.0-G	PCIe Gen2.0 x4	1 x USB 2.0	N/A	45,000	5 Gb/s	2.1" x 6.6"
CN1620-NFBE2-2.0-G	PCIe Gen2.0 x4	1 x USB 2.0	N/A	30,000	3 Gb/s	2.1" x 6.6"
CN1620-NFBE1-2.0-G	PCIe Gen2.0 x4	1 x USB 2.0	N/A	15,000	1.5 Gb/s	2.1" x 6.6"
CN1610-NFBE1-2.0-G	PCIe Gen2.0 x4	1 x USB 2.0	N/A	7,500	750 Mb/s	2.1" x 6.6"
CN1620-NFBE3NIC-2.0-G	PCIe Gen2.0 x4	1 x USB 2.0	2 x 1GbE	45,000	5 Gb/s	2.1" x 6.6"
CN1620-NFBE2NIC-2.0-G	PCIe Gen2.0 x4	1 x USB 2.0	2 x 1GbE	30,000	3 Gb/s	2.1" x 6.6"
CN1620-NFBE1NIC-2.0-G	PCIe Gen2.0 x4	1 x USB 2.0	2 x 1GbE	15,000	1.5 Gb/s	2.1" x 6.6"
CN1610-NFBE1NIC-2.0-G	PCIe Gen2.0 x4	1 x USB 2.0	2 x 1GbE	7,000	750 Mb/s	2.1" x 6.6"