CAVIUM

## FIPS 140-2 Accelerator Boards

# NITROX® XL CNN35XX NFBE Hardware Security Module (HSM) Adapter Family

Product Brief

## OVERVIEW

The NITROX® XL CNN35XX NFBE HSM Adapter family is a FIPS 140-2 Level 2 and Level 3 certified Hardware Security Module (HSM) solution with the world's highest performance and key storage capacity. Additionally, CNN35xx NFBE HSM Adapter Family supports multiple partitioned HSMs in a single physical HSM Adapter thereby providing the most flexible solution for multi-tenant/multi-domain cloud infrastructure.

With support for KVM, Xen, Linux, FreeBSD and other Operating Systems, NITROX XL CNN35XX HSM adapter is a perfect embedded HSM solution for servers and appliances such as Web Servers, Application Delivery Controllers, Load Balancers, Networking / Server Appliances, Unified Threat Management Appliances, Remote Access Servers, Public Key Infrastructure and Database Servers. NITROX XL CNN35XX HSM adapter supports crypto APIs such as OpenSSL, PKCS#11, JCA and Microsoft CNG thus enabling multiple applications such as PKI Key generation, DNSSEC, Database and File encryption and SSL & TLS.

## FEATURES

- Up to 32 partitioned FIPS 140-2 level 3 HSMs in single Hardware Security Module (HSM) Adapter
- High SSL / TLS performance
  - Up to 35K 2048-bit key RSA operations / sec
  - Up to 11K ECC operations / sec
  - Up to 10Gbps of bulk crypto throughput
- Enhanced on card storage
  - Up to 500,000 concurrent SSL sessions
  - Up to 50000 concurrent server private keys
- USB port and over the network two-factor authentication
- SP800-90 based Deterministic Random Bit Generator (Random Number Generator) support for FIPS 140-3
- Accelerates and secures cryptographic functions and bulk encryption
- 256-bit AES based key encrypt for key archive and transport
  - Advanced ECC for handshake

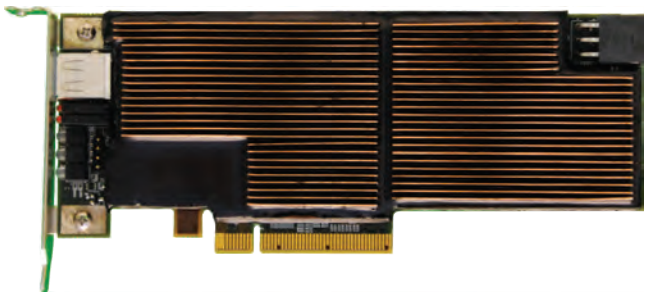
## BENEFITS

- Scalable performance per partition for multi-domain cloud infrastructure
- Support for multiple crypto APIs enables easy integration with Data Center applications
- 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

- Cloud HSM Appliance
- Application Delivery Controllers / Load Balancers
- Networking / Server Appliances
- Database Servers
- Web Servers
- Remote Access Servers
- Unified Threat Management Appliances
- Public Key Infrastructure

NITROX® XL CNN35XX NFBE HSM Adapter Family



CAVIUM

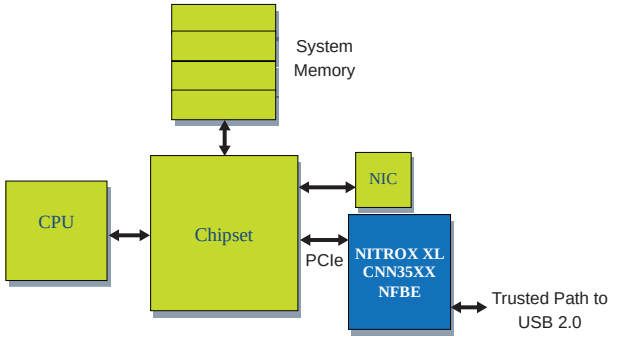
2315 N. First Street
San Jose, CA 95131
**T** 408-943-7100
**F** 408-577-1992
**E** sales@cavium.com
**www.cavium.com**

## FIPS 140-2 Accelerator Boards

# NITROX® XL CNN35XX NFBE HSM Adapter Family

Product Brief

## SYSTEM DIAGRAM




NITROX XL CNN35XX NFBE usage in SSL offload application

## SPECIFICATIONS

- Low profile (2.1" x 6.6") PCIe form factor can easily fit 1U appliance
- PCIe Gen2 x8 interface
- USB 2.0 port for 'Smart Keys' for FIPS 140-2 Level 3
- Support for a wide variety of algorithms
- Modular Exponentiation: RSA / DH Public Key 2048-bit & 4096-bit
- Operating Temperature: 0 to 50° C
- Regulatory Certifications: Safety, cTUVus UL, EMC, FCC/ICES, Class B

## SOFTWARE AND API SUPPORT

- Drivers for Linux and FreeBSD
- Drivers for KVM and Xen
- PKCS#11 Crypto-service provider
- OpenSSL and TurboSSL support
- Java Cryptography Architecture (JCA) support
- API libraries for Card and key management
- API libraries for Cloning
- API libraries for Two factor authentication over Network or USB

## NITROX® CNN35XX NFBE HSM Adapter Family

| Device | System Interface | Partition Support | Performance | | Dimensions |
|---|---|---|---|---|---|
| | | | Max RSA Ops / sec | SSL Record Throughput | |
| CNN3560-NFBE-G | PCIe Gen2.0 x8 | Yes | 35K (2048b) | 10 Gb/s | 2.1" x 6.6" |
| CNN3530-NFBE-G | PCIe Gen2.0 x8 | Yes | 20K (2048b) | 5 Gb/s | 2.1" x 6.6" |
| CNN3510-NFBE-G | PCIe Gen2.0 x8 | Yes | 10K (2048b) | 3 Gb/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**