

## Accelerator Boards

# NITROX® XL FIPS 140-2 Level 3 Security Accelerator Board Family

### Product Brief

#### OVERVIEW

NITROX PCI and PCIe FIPS 140-2 compliant acceleration boards incorporate both the high performance hardware acceleration of Cavium's Nitrox security macro-processors, and the trusted strength and security of the FIPS 140-2 standard on a single, easy to use hardware security module. The Federal Information Processing Standard (FIPS) is a fundamental component for the rating of cryptographic accelerators. The FIPS 140-2 standard validates and certifies performance of cryptographic modules to insure the trust model can be confidently deployed based on Federal security standards.

NITROX XL NFB and NFBE modules provide NIST certified FIPS 140-2 level 2 and level 3 high performance acceleration modules for vendors of the highest-security SSL e-Commerce, e-Business, and VPN equipment. The NITROX XL FIPS modules come complete with a rich, full-featured set of software drivers, utilities, and reference application software, all delivered in C source code. The hardware module with a FIPS 140-2 compliant security boundary, ensures the integrity of the cryptographic material. Together with a complete software development kit (SDK) NITROX XL FIPS accelerator boards significantly reduce the cost, complexity, and time to develop products targeted at high-value, high-security e-commerce and e-business applications.

#### FEATURES

- SSL/TLS Performance
  - Up to 10,000 1024-bit RSA operations/sec
- Macro-processing for optimal system efficiency
  - Complete SSL handshake or record processing in a single API call
- API's backward compatible with existing, non-FIPS, Nitrox XL SSL/TLS accelerator cards
- On-board storage for up to 100,000 (est.) concurrent SSL sessions & 4096 (est.) concurrent server private keys
  - Maintained and managed on-board by local subsystem
- Separate "Trusted-Path" Administration Interface
  - Serial interface for connection to PIN Entry Device (PED) for FIPS Level 3 configurations
- 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

- Broadest FIPS module performance range for wide application performance and price point solutions
  - Full protocol offload minimizes bus transactions
- Short development time for quick time to market
  - Complete hardware module
  - Same API as non-FIPS SSL API from Cavium Networks
  - Complete C Software Kit including source code
    - Driver & Utilities
    - Reference Application
- Reduced system complexity
  - Entire SSL security implementation on single module
- 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. Mode is set by Security Officer during initialization



CN15XX-NFBE Full Height PCIe FIPS Acceleration Boards



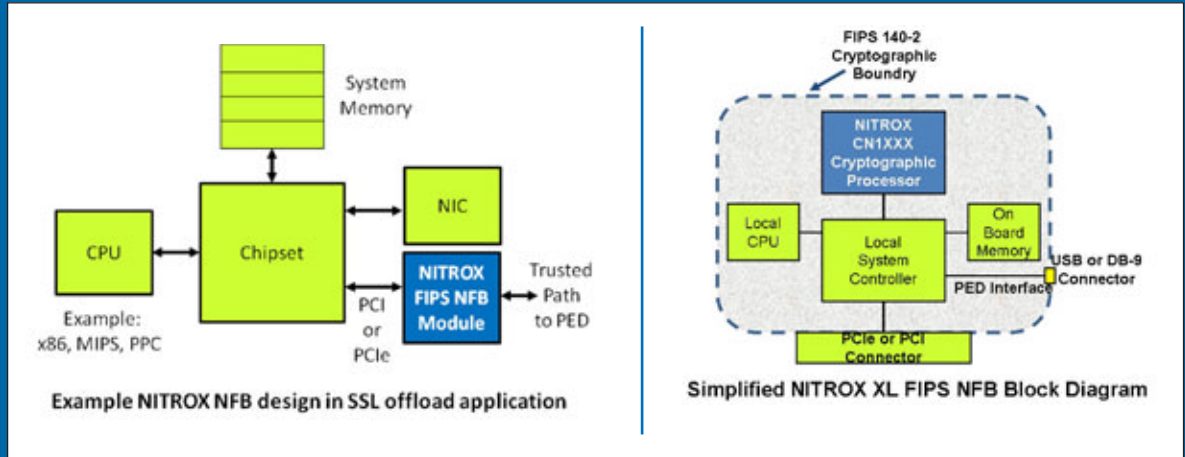
CN11XX-NFB Full Height PCI FIPS Acceleration Boards

## Accelerator Boards

# NITROX® XL FIPS 140-2 Level 3 Security Accelerator Board Family

## Product Brief

### SYSTEM DIAGRAMS



### OPERATING SYSTEMS

- Linux: Fedora Core 6, 2.6.18 kernel for 64-bit architecture or Fedora Core 4, 2.6.11 kernel for 32-bit architecture

### INDUSTRY STANDARD SYSTEM INTERFACES

- PCIe v1.1 x4 lane with CN15XX NFBE processor
- PCI-X 64-bit, 133 MHz with CN1120, CN10XX NFB

### ORDERING INFORMATION

| Device            | System Interface   | Trusted Path Interface for FIPS Level 3<br>*PED sold separately | Performance                       |   | Dimensions for Full Length PCIe Card |
|-------------------|--------------------|---|-----------------------------------|---|--------------------------------------|
|                   |                    |   | MAX RSA1024-bit Exponent with CRT | Full SSL Record Throughput (AES + SHA-1) Mbps |                                      |
| CN1520-350-NFBE-G | PCIe x4 lane       | Mini DB PED (Pin Entry Device)                                  | 10,000                            | 500   | 4.2" x 7.875"                        |
| CN1510-350-NFBE-G | PCIe x4 lane       | Mini DB PED (Pin Entry Device)                                  | 6,000                             | 250   | 4.2" x 7.875"                        |
| CN1120-350-NFB-G  | 64-bit, 66 MHz PCI | Serial PED (Pin Entry Device)                                   | 10,000                            | 500   | 4.2" x 7.1"                          |
| CN1010-350-NFB-G  | 64-bit, 66 MHz PCI | Serial PED (Pin Entry Device)                                   | 6,000                             | 250   | 4.2" x 7.1"                          |
| CN1005-350-NFB-G  | 64-bit, 66 MHz PCI | Serial PED (Pin Entry Device)                                   | 3,000                             | 125   | 4.2" x 7.1"                          |