Overview

The Marvell FIPS 140-2 Compliant LiquidSecurity HSM Adapter brings together the high-performance hardware acceleration of the Marvell NITROX III security macro-processors and the trusted strength and security of the FIPS 140-2 standard. The hardware module has a FIPS-compliant security boundary that ensures the integrity of the cryptographic material. Together with a complete software development kit, it significantly reduces the cost, complexity, and time to develop products targeted at high-value, high-security e-commerce and e-business applications.

Design Benefits

- Software and hardware support from Marvell enables a short development cycle and time-to-market process.
- Reduced FIPS boundary size.
- Reduced validation cost and time.
- Instant appliance validation.
- Reduced system complexity.

Target Applications

Secure Web servers
- Web Servers used in e-Commerce
- Signature verification for B2B exchanges

Web Switches and Appliances
- SSL/TLS Termination and Content switching
- Content Aware Server Load Balancing
- SSL Proxy Server

Remote Access Servers using SSL
- SSL VPN appliances
- Servers with SSL secure email
- Other web-enabled applications like CRM and ERP suites
## Technical Specifications

<table>
<thead>
<tr>
<th>HSM Capabilities</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Cryptographic and Secure Operations** | • Asymmetric: RSA, DSA, Elliptical curve (ECDH/ECDSA)  
• Symmetric: AES (CBC, GCM, CCM, and CMAC modes), 3DES, Generic Secret  
• Key Derivation: SP800-108 Counter Mode, HMAC/CMAC/HKDF/ECDH  
• Key wrapping/unwrapping: SP 800-38F  
• Hash/Message Digests: SHA1/SHA2  
• Random Number Generation: SP800-90  
• MofN Quorum Control | |
| **Security Certifications**       | • FIPS 140-2, 140-3*  
• eIDAS* | |
| **Management and Monitoring**     | • Identity-based authentication  
• Multiple Partitions with user/admin levels  
• Remote administration  
• Isolated partitions  
• Audit Logging  
• SMBus for diagnostics monitoring  
• Tamper evident detection and zeroization | |
| **APIs**                          | • Java (JCA/JCE)  
• Microsoft CNG / KSP  
• OpenSSL Engine  
• PKCS#11  
• CfM-API Management Tools | |
| **Safety & Environmental Compliance** | • Safety:  
- UL and CE  
- Emissions:  
  - EN 55024 (1998 W/A1:01 and A2:03) for immunity  
- AS/NZS C1PSR22 Class B  
- WFCC Part 15 Subpart B, sections 15.107 and 15.109 Class B  
- KCC KN32 & KN35, Class B  
- ICES, Class B | |
| **Hardware**                      | • PCIe Gen2 x8 interface  
• Dimensions: 2.1" x 6.6"  
• SMBus, FRAM support for additional logging, firmware counters | |
| **Operating Environment**         | • Ambient temperature range: 0 to 45°C  
• Minimum air flow: 500 LFM | |
| **Reliability**                   | • High Availability and Load Balancing  
• Backup and Restore  
• MTBF 1,511,929 hrs (Telcordia SR-332) | |
| **Supported Operating Systems**   | • RHEL 7.x, CentOS 7.x, Ubuntu  
• Xen and KVM  
• Windows | |
| **Secure Channel**                | • E2E (TLS-based) connectivity from the LiquidSecurity client to FIPS boundary | |

* In Progress
## Part Numbers

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNL3510-NFBE-3.0-G</td>
<td>NITROX III FIPS Adapter with bits enabled to work as Network HSM. LiquidSecurity software access enabled with part.</td>
</tr>
<tr>
<td>CNL3510LP-NFBE-3.0-G</td>
<td>NITROX III FIPS Adapter with bits enabled to work as Network HSM. LiquidSecurity software access enabled with part.</td>
</tr>
<tr>
<td>CNL3530-NFBE-3.0-G</td>
<td>NITROX III FIPS Adapter with bits enabled to work as LiquidSecurity adapter.</td>
</tr>
<tr>
<td>CNL3560-NFBE-3.0-G</td>
<td>NITROX III FIPS Adapter with bits enabled to work as LiquidSecurity adapter.</td>
</tr>
<tr>
<td>CNL3560B-NFBE-3.0-G</td>
<td>NITROX III FIPS Adapter with bits enabled to work as Network HSM. LiquidSecurity Software access enabled with part.</td>
</tr>
</tbody>
</table>