

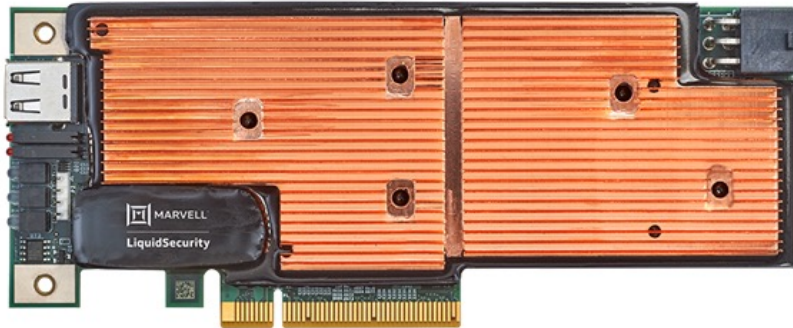
# LiquidSecurity® HSM Adapter

CloudHSM

## 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

HSM Capabilities	Description	
<b>Cryptographic and Secure Operations</b>	<ul style="list-style-type: none"> <li>Asymmetric: RSA, DSA, Elliptical curve (ECDH/ECDSA)</li> <li>Symmetric: AES (CBC, GCM, CCM, and CMAC modes), 3DES, Generic Secret</li> <li>Key Derivation: SP800-108 Counter Mode, HMAC/CMAC/HKDF/ECDH</li> </ul>	<ul style="list-style-type: none"> <li>Key wrapping/unwrapping: SP 800-38F</li> <li>Hash/Message Digests: SHA1/SHA2</li> <li>Random Number Generation: SP800-90</li> <li>MofN Quorum Control</li> </ul>
<b>Security Certifications</b>	<ul style="list-style-type: none"> <li>FIPS 140-2, 140-3*</li> </ul>	<ul style="list-style-type: none"> <li>eIDAS*</li> </ul>
<b>Management and Monitoring</b>	<ul style="list-style-type: none"> <li>Identity-based authentication</li> <li>Multiple Partitions with user/admin levels</li> <li>Remote administration</li> <li>Isolated partitions</li> </ul>	<ul style="list-style-type: none"> <li>Audit Logging</li> <li>SMBus for diagnostics monitoring</li> <li>Tamper evident detection and zeroization</li> </ul>
<b>APIs</b>	<ul style="list-style-type: none"> <li>Java (JCA/JCE)</li> <li>Microsoft CNG / KSP</li> <li>OpenSSL Engine</li> </ul>	<ul style="list-style-type: none"> <li>PKCS#11</li> <li>Cfm-API Management Tools</li> </ul>
<b>Safety &amp; Environmental Compliance</b>	<ul style="list-style-type: none"> <li>Safety: <ul style="list-style-type: none"> <li>UL and CE</li> </ul> </li> <li>Emissions: <ul style="list-style-type: none"> <li>EN 55022 (2015) Class B for digital emissions</li> <li>EN 55024 (1998 W/A1:01 and A2:03) for immunity</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>AS/NZS CIPSR22 Class B</li> <li>WFCC Part 15 Subpart B, sections 15.107 and 15.109 Class B</li> <li>VCCI V-3 (2009.04) Class B for digital emissions.</li> <li>KCC KN32 &amp; KN35, Class B</li> <li>ICES, Class B</li> </ul>
<b>Hardware</b>	<ul style="list-style-type: none"> <li>PCIe Gen2 x8 interface</li> <li>Dimensions: 2.1" x 6.6"</li> </ul>	<ul style="list-style-type: none"> <li>SMBus, FRAM support for additional logging, firmware counters</li> </ul>
<b>Operating Environment</b>	<ul style="list-style-type: none"> <li>Ambient temperature range: 0 to 45°C</li> </ul>	<ul style="list-style-type: none"> <li>Minimum air flow: 500 LFM</li> </ul>
<b>Reliability</b>	<ul style="list-style-type: none"> <li>High Availability and Load Balancing</li> <li>Backup and Restore</li> </ul>	<ul style="list-style-type: none"> <li>MTBF 1,511,929 hrs (Telcordia SR-332)</li> </ul>
<b>Supported Operating Systems</b>	<ul style="list-style-type: none"> <li>RHEL 7.x, CentOS 7.x, Ubuntu</li> <li>Xen and KVM</li> </ul>	<ul style="list-style-type: none"> <li>Windows</li> </ul>
<b>Secure Channel</b>	<ul style="list-style-type: none"> <li>E2E (TLS-based) connectivity from the LiquidSecurity client to FIPS boundary</li> </ul>	

\* In Progress

## Part Numbers

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



To deliver the data infrastructure technology that connects the world, we're building solutions on the most powerful foundation: our partnerships with our customers. Trusted by the world's leading technology companies for 25 years, we move, store, process and secure the world's data with semiconductor solutions designed for our customers' current needs and future ambitions. Through a process of deep collaboration and transparency, we're ultimately changing the way tomorrow's enterprise, cloud, automotive, and carrier architectures transform—for the better.

Copyright © 2022 Marvell. All rights reserved. Marvell and the Marvell logo are trademarks of Marvell or its affiliates. Please visit [www.marvell.com](http://www.marvell.com) for a complete list of Marvell trademarks. Other names and brands may be claimed as the property of others.

**Marvell\_CN35XX\_PB Revised: 08/22**