

MARVELL LiquidSecurity and NITROX HSM Adapters

Product Brief

LiquidSecurity and NITROX HSM Client Features	
<p>Supported Crypto Stacks</p> <ul style="list-style-type: none"> • PKCS11, JCE, and OpenSSL <p>C-API-based Management Tools</p> <p>Unlimited usage source code license</p> <p>Supported Operating Systems</p> <ul style="list-style-type: none"> • RHEL7.x, CentOS 7.x, Ubuntu • Xen and KVM 	<p>Algorithms</p> <ul style="list-style-type: none"> • RSA Sign/Verify – Support for PKCS1, PSS (2K, 3K, 4K key sizes) • RSA enc/dec – PKCS1, OAEP (2K, 3K, 4K key sizes) • DSA Sign/Verify • ECDH/ECDSA – p-curves, b-curves, k-curves, Bitcoin curve secp256k1, Curve25519 • 3DES/AES and SHA (1, 2), HMAC-SHA (1, 2) • Key Derivation: SP800-108 Counter Mode/HMAC-KDF
LiquidSecurity and NITROX HSM Features	
<p>Industry-Leading Performance</p> <ul style="list-style-type: none"> • 35K 2K RSA Sign Ops/sec • 300K Symmetric Ops/sec <p>Enhanced On-Card Storage</p> <ul style="list-style-type: none"> • Up to 1 million concurrent SSL contexts • Up to 100,000 concurrent key storage (symmetric and asymmetric) <p>Dynamic Partition Support</p> <ul style="list-style-type: none"> • FIPS 140-2 Level 3 partitions • Individual adapter can be partitioned into 1 to 32 partitions at run time • Partition defined based on key store, symmetric/asymmetric performance, and maximum concurrent sessions 	<p>Role-Based Access</p> <ul style="list-style-type: none"> • Adapter Administrator – No access to key material on partitions, role limited to creating partitions and health checks • Partition Administrator – Cluster management, user management role • Partition User – Key management operations and crypto operations <p>User/Clients Per Partition</p> <ul style="list-style-type: none"> • Support for up to 1000 users per partition • Each user can run multiple applications <p>Support for Single- and Two-factor Authentication</p> <p>Cloning</p> <ul style="list-style-type: none"> • Ephemeral handshake-based cloning to ensure the key rotation for the masking key
Hardware Specifications	
<ul style="list-style-type: none"> • PCIe Gen2 x8 interface • Dimensions: 2.1" x 6.6" • Operating Temperature: 0 to 50°C • Regulatory Certifications: Safety, cTUVus UL, EMC, FCC/ICES, Class B 	<ul style="list-style-type: none"> • SMBus, FRAM support for additional logging, firmware counters • MTBF 1,511,929 hrs (Telcordia SR-332)

Feature Comparison	NITROX HSM Adapter	LiquidSecurity HSM Adapter
Backup/Restore	No	2-key, 3-key Smart card based
Audit Logs	No	Yes
Temperature Monitoring and Boot Logs available over SMBus	No	Yes
Park / Unpark Key Management API	No	Yes

NITROX HSM Adapter Product Comparison Table

Device	System Interface	Isolated Partitions	Performance	
			Max RSA Ops/sec	SSL Record Throughput
CNN3560-NFBE-2.0-G	PCIe Gen 2.0 x8	32	35K (2048b)	10 Gb/s
CNN3530-NFBE-2.0-G	PCIe Gen 2.0 x8	32	18K (2048b)	7 Gb/s
CNN3510-NFBE-2.0-G	PCIe Gen 2.0 x8	24	13K (2048b)	4 Gb/s
CNN3510LP-NFBE-2.0-G	PCIe Gen 2.0 x8	24	10K (2048b)	3 Gb/s
CNN3505LP-NFBE-2.0-G	PCIe Gen 2.0 x8	8	4K (2048b)	1 Gb/s

LiquidSecurity HSM Adapter Product Comparison Table

Device	System Interface	Isolated Partitions	Performance	
			Max RSA Ops/sec	SSL Record Throughput
CNL3560-NFBE-2.0-G	PCIe Gen 2.0 x8	32	35K (2048b)	10 Gb/s
CNL3530-NFBE-2.0-G	PCIe Gen 2.0 x8	32	18K (2048b)	7 Gb/s



ABOUT MARVELL: Marvell first revolutionized the digital storage industry by moving information at speeds never thought possible. Today, that same breakthrough innovation remains at the heart of the company's storage, networking and connectivity solutions. With leading intellectual property and deep system-level knowledge, Marvell semiconductor solutions continue to transform the enterprise, cloud, automotive, industrial, and consumer markets. For more information, visit www.marvell.com.