Product Brief

LiquidSecurity® 2 HSM Adapter

A Unified HSM for the Multi-Cloud Era

Overview

The LiquidSecurity 2 (LS2) HSM Adapter is Marvell's most advanced HSM, offering a unified solution for your General Purpose, Payments, and Compliance needs. LS2 utilizes Marvell's next generation cloud-optimized silicon, providing the highest-performing cryptographic processing in the industry. Designed for cloud-scale deployments and economics, it supports the following functions:

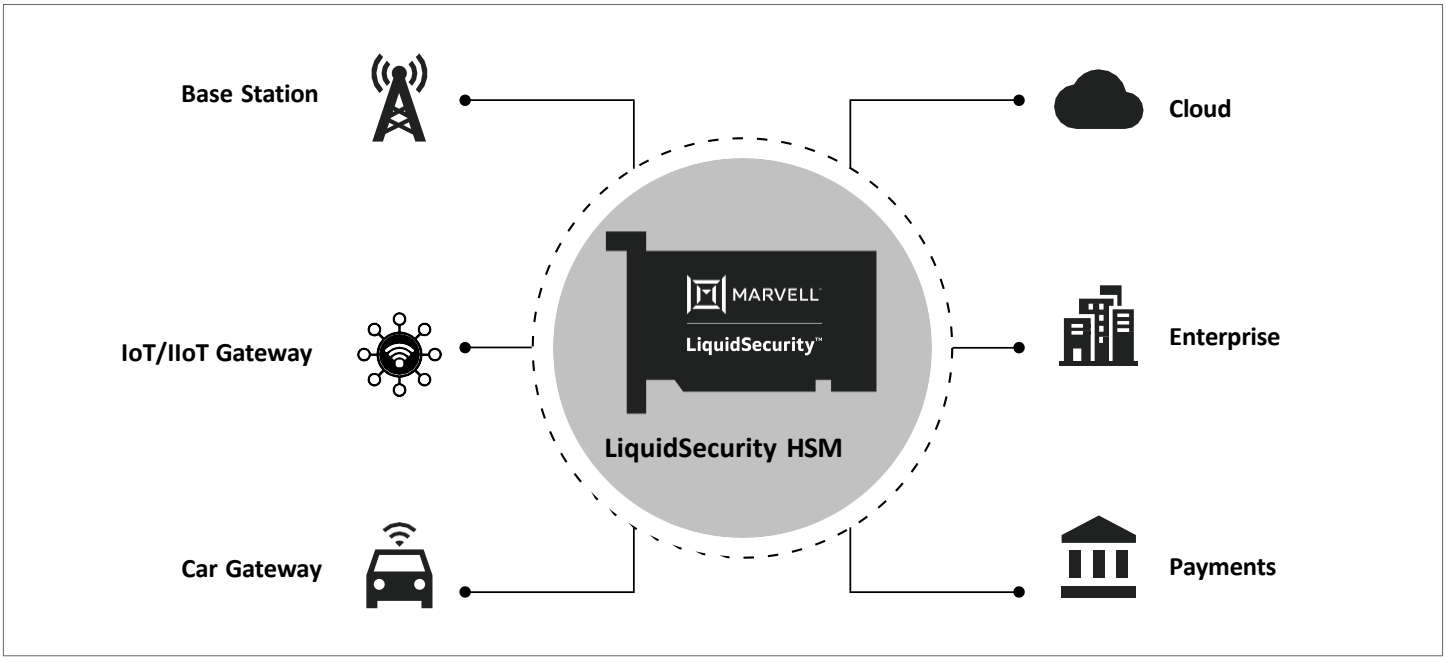
1. Clustering: LS2 adapters can be clustered across different regions for high availability and disaster recovery.
2. Multi-tenancy: Up to 42 cryptographically isolated partitions. Each partition can support an individual customer or application.
3. Multi-Mode: NIST FIPS 140-3 (Level-3) and PCI PTS HSM compliance on the same HSM adapter. Support for non- FIPS mode to run custom applications or algorithms.
4. Platform Software Hosting: Utilizing VMs, the LS2 HSM has a highly flexible architecture that allows for custom applications or algorithms to run within the FIPS boundary of the LS2 HSM.

Quantum computers are here, so it is important to support NIST post-quantum algorithms. LS2 HSM supports the latest post-quantum algorithms in non-FIPS mode. And once ratified by NIST for certification, LS2 will also support these post- quantum algorithms in FIPS mode.

LS2 HSM has a FIPS-compliant security boundary that ensures high integrity of the cryptographic material. Together with a comprehensive software development kit, LS2 enables faster time to market for multi-cloud, hybrid, and OEM deployments with its API-first design. Achieve lowest TCO, reduce your Cap-Ex and Op-Ex with a unified GP and Payments HSM solution on the same LS2 HSM. Develop once and run anywhere with LS2.

LS2 holds millions of cryptographic keys to enable billions of transactions with performance scalability for the most demanding applications.

LS2 Use Cases



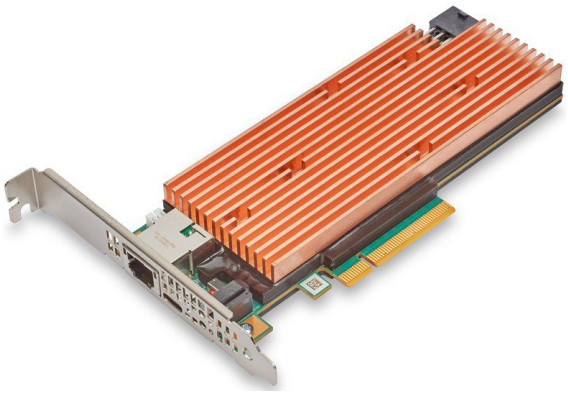
Technical Specifications

HSM Capabilities	Description	
Supported Operating Systems	• RHEL, CentOS, Ubuntu	• Windows Server for Client SDK
APIs	• Java (JCA/JCE) • Microsoft CNG / KSP • OpenSSL Engine	• PKCS#11 • Cfm-API Management Tools
Cryptographic and Secure Operations	• Asymmetric Keys: – RSA: PKCS#1 v1.5 and v2.2 (2K, 3K, 4K key sizes) – ECDH/ECDSA: p-curves, k-curves, Bitcoin curve secp256k1 • Symmetric Keys: – AES (128, 192, 256-bit keys) with CBC, ECB, GCM, CCM, and CMAC – 3DES CBC/ECB modes – Generic secret: <=800 (sign and verify, HMAC multi-call) • Hash/Message digests: SHA1, SHA2 (224, 256, 384, 512) • Key derivation: SP800-108 counter mode, HMAC/ CMAC/HKDF/ECDH	• Key wrap/unwrap/import (SP 800-38F): custom services for deployments • Random number generation (SP 800-90) • MofN quorum control to mitigate single-point failures • Hardware root of trust • Secure boot • Cryptographic agility (crypto-agility): future-proof deployment of new cryptographic primitives and algorithms • Post-quantum cryptography* • Full NSA Suite B algorithms compliant
Payment Functions (LSPay)	• Integrated general purpose and payment HSM • Designed to provide payment HSM services in cloud environment • Secures issuers, payment switches, payment gateways, and acquirers	• LSPay API library • TR-31 key block • TR-34 key transport • PIN translation formats: ISO-0/1/2/3
Safety and Environmental Compliance	• Regulatory certifications: UL, cUL, CB Bundle (2nd/3rd editions) • Immunity: CE EMC (EN55032/EN55035) • Worldwide: China, Korea, South Africa (EMC SABS), Israel SII, UKCA, Taiwan (BSMI/RoHS)	• Emissions: – FCC Doc/ICES-003 – VCCI • AS/NZA CISPR22
Management and Monitoring	• Multiple partitions with flexible resource allocation and role-based access control (RBAC) • Vendor as root of trust, enabling multi-tenancy within HSM adapter and hybrid cloud deployments • HSM adapter and partition-level ownership • TLS-model tunnel from application to HSM for untrusted environments (PFS) • Remote administration • Containerized, isolated partitions • SMBus for diagnostics monitoring, including temperature and boot logs	• Attested audit logs • Tamper-evident and tamper proof: detection and zeroization Security-enhanced Linux • Secure key storage • Certificate storage • SecureMachine (run custom code in HSM boundary) • Mixed-mode (FIPS and non-FIPS) flexible partition • Custom fairshare design to meet cloud SLAs in multi-tenant deployments
Security Certifications	• NIST FIPS 140-3 Level 3* • eIDAS*	• CC EAL4+* • PCI PTS-HSM*
Hardware and Operating Environment	• Low profile (HHHL) PCIe Gen4 x8 • Dimensions: 167mm x 56mm x 19 mm • Ambient temperature: +10°C to +40°C	• Minimum Air Flow: 500 LFM • Relative humidity: 20 – 80% • SMBus, F-RAM support for additional logging, firmware counters

* In Progress

Marvell LS2 Models and Software Packages

Card Size	Height
Standard height (pictured at right)	• 111.28 mm (4.381 inches) maximum
Low profile	• 68.90 mm (2.731 inches) maximum
Package dimensions	• 31 x 23 x 6 cm (12.205 x 9.055 x 2.362 inches)
Weight	• 0.92 kg (2.028 lbs)



Hardware SKUs

LS2 Model	Description	#Partitions	RSA 2K ops/sec	EC P256 ops/sec	AES-GCM ops/par/sec
LS2-A050	• LS2-G-A050-GA-L-B0	21	21,250	50,000	500,000
LS2-A100	• LS2-G-A100-GA-L-B0	32	35,000	50,000	500,000

Software License SKUs

LS2 Model	Description	#Partitions	RSA 2K ops/sec	EC P256 ops/sec	AES-GCM ops/par/sec
LS2-UPGD-GA	• Software License to upgrade performance o LS2-A100	42	42,500	100,000	1,000,000
LS-SW-PQC	• Software License to enable Post-Quantum Cryptography support	NA	NA	NA	NA
LS-SW-PLH	• Software License to enable 3rd Party applications	NA	NA	NA	NA

MARVELL™

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 over 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.

Marvell_2_HSM_PB Revised: 04/24