MARVELL

Product Brief

LiquidSecurity® 2 Cloud HSM Adapter

The Unified HSM for the Multi-Cloud Era

Overview

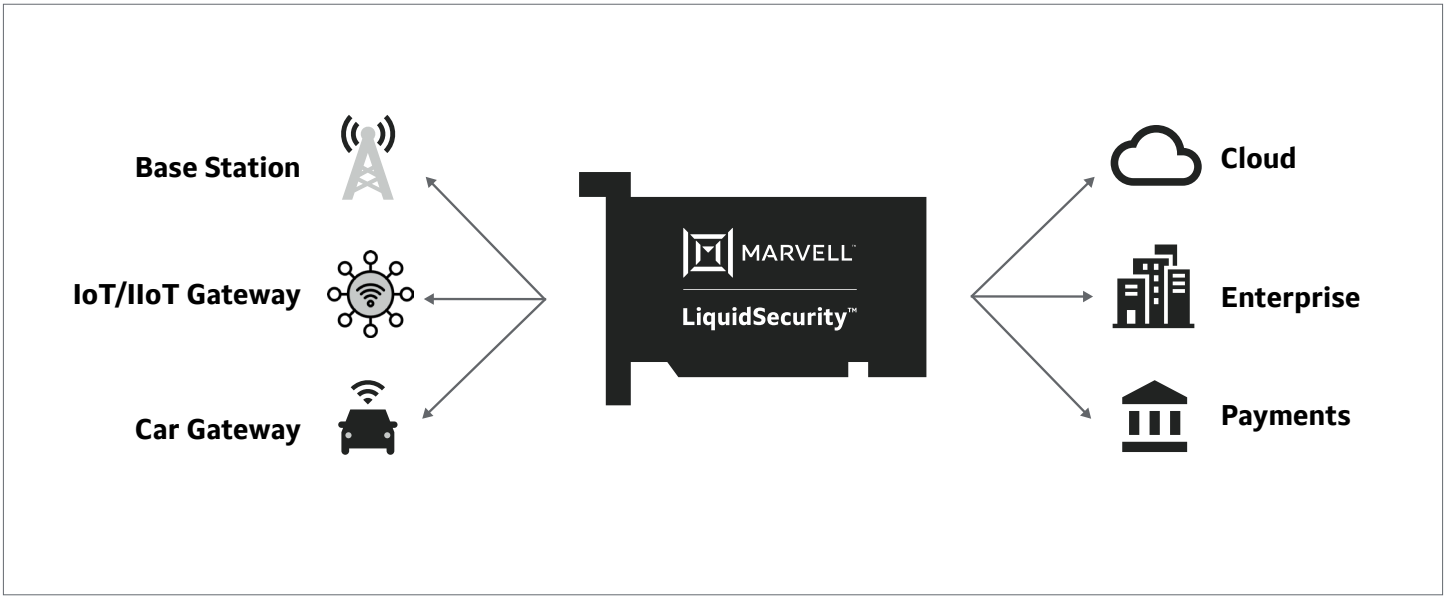
The LiquidSecurity 2 (LS2) Cloud HSM Adapter is Marvell's most advanced HSM, offering a unified solution for your General Purpose, Payments, and compliance needs. LS2 has the highest-performing cryptographic processing, featuring Marvell's next generation cloud-optimized silicon. Designed for cloud-scale deployments and economics, it supports FIPS 140-3 compliance, millions of cryptographic keys to enable billions of transactions, and performance scalability for the most demanding applications in the cloud.

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 on-prem 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 hardware. Develop once and run anywhere with LS2.

The LS2 HSM has a highly flexible architecture that is built for clustering and high availability that predictably scales the cryptographic key services for various applications and tenants that need scalable partitions, key storage, TPS, and low latency. Dedicated resources in the FIPS-certified boundary support the highest density of multi-tenancy in isolated partitions.

LS2 hardware certification can be updated to support new algorithms and variants, such as post-quantum cryptography, providing cryptographic agility, and future-proofing the HSM against vulnerabilities.

LS2 Use Cases



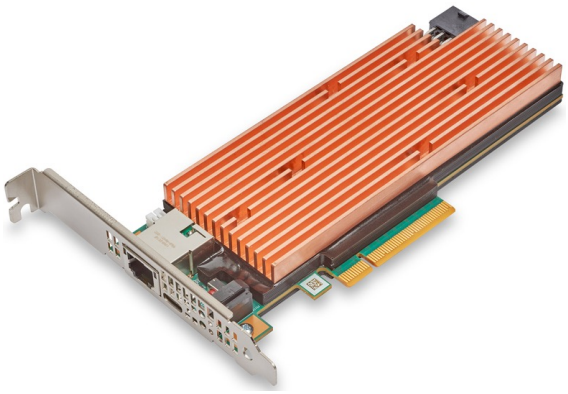
Technical Specifications

HSM Capabilities	Description	
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
Security Certifications	• FIPS 140-2, 140-3* • eIDAS*	• CC EAL4* • PTS-HSM*
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
APIs	• Java (JCA/JCE) • Microsoft CNG / KSP • OpenSSL Engine	• PKCS#11 • Cfm-API Management Tools
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
Hardware and Operating Environment	• Low profile (HHHL) PCIe Gen4 x8 • Dimensions: 167mm x 56mm x 19 mm • Ambient temperature: +10°C to +40°C	• Relative humidity: 20 – 80% • SMBus, F-RAM support for additional logging, firmware counters
Reliability	• High Availability, Load Balancing, Fault Tolerant • Backup and Restore	• MTBF* • Field serviceable
Supported Operating Systems	• RHEL, CentOS, Ubuntu	• Windows Server for Client SDK

* 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



LS2 Model	Description
LS2-G-A300-PR-F-B0	• Base – General Purpose package • LS2-C-A300-SW-X-B0 – Cloud feature package • LS2-O-A300-SW-X-B0 – OEM feature package
LS2-G-A200-PR-F-B0	• Base – General Purpose package • LS2-C-A200-SW-X-B0 – Cloud feature package • LS2-O-A200-SW-X-B0 – OEM feature package
LS2-G-A100-PR-F-B0	• Base – General Purpose package • LS2-C-A100-SW-X-B0 – Cloud feature package • LS2-O-A100-SW-X-B0 – OEM feature package
LS2-G-A050-PR-F-B0	• Base – General Purpose package • LS2-C-A050-SW-X-B0 – Cloud feature package • LS2-O-A050-SW-X-B0 – OEM feature package
LS2-G-A025-PR-F-B0	• Base – General Purpose package • LS2-C-A025-SW-X-B0 – Cloud feature package • LS2-O-A025-SW-X-B0 – OEM feature package

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 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.

Marvell_LS2_HSM_PB Revised: 08/22