



CryptoBind[®]

Hardware Security Module

www.jisasoftech.com

Hardware Security Module



A High performance hardware based transaction security solution for cloud data centers, Enterprise, government organisation and ecommerce applications



High Security,
Performance &
Reliability

JISA launches Network Security Module (HSM) powered by LiquidSecurity (Marvell) FIPS 140-3 level 3 certified. HSM family provides a solution for elastic and centralized key management and Crypto offload functionality.

In addition to the crypto offloads, this HSM can provide secure key storage with upto 1000 partitions, including master partition. Each partition will have its own users to manage the partition and own configuration policies and hence each partition can be treated as a separate virtual HSM. This HSM also comes with upto 1 lakh key storage capacity in FIPS certified boundary.



KEY FEATURES

- ✔ Upto 1000 partitions available
- ✔ Available for 500 TPS to 35000 TPS @ RSA 2048 bits
- ✔ Upto 1 lakh key storage in FIPS boundary
- ✔ Unlimited client license
- ✔ Up to 10G/sec symmetric / bulk crypto
- ✔ Upto 100 run time scalable and isolated instances per appliance
- ✔ Support for multiple ECC curves
- ✔ PKCS11, JCE, OpenSSL , RestAPI support
- ✔ Division of roles and policies
- ✔ Post Quantum Cryptography Support

Overview

JISA launches Network Security Module powered by LiquidSecurity (Cavium), this family provides a built-in FIPS 140-3 level 3 boundary for elastic and centralized key management and key operation functionality.

JISA's HSM comes with:

- ✔ Upto 1000 partitioned HSMs in a single physical Appliance
- ✔ Upto 100 instances in single physical appliance
- ✔ 100,000 key store independent of key size,
- ✔ 35,000 2048b RSA ops/sec and chaining of up to 20 Appliances,
- ✔ CN35XX family which provides a solution that addresses requirements from few hundred RSA ops/sec or few key stores to 700K RSA ops/sec or 1M key store and everything in-between.

Models and Performance

Model	Performance		Partitions/Instances	Concurrent Usable Keys in FIPS Certified Cryptographic Memory	Key storage in Network Appliance HSM
	Max RSA	Network Connectivity			
	TPS				
J-35000	35000(RSA 2048bits)	1G or/& 10G	100/250/500/1000	1,00,000 Keys	10,00,000 Keys
J-20000	17500(RSA 2048bits)	1G or/& 10G	50/100/250/500	25,000 Keys	1,00,000 Keys
J-10000	10000(RSA 2048bits)	1G or/& 10G	1/10/50/100/250	25,000 Keys	1,00,000 Keys
J-5000	5000(RSA 2048bits)	1G or/& 10G	1/10/50/100/250	10,000 Keys	50,000 Keys
J-2000	2000(RSA 2048bits)	1G or/& 10G	1/10/20/50/100	5,000 Keys	20,000 Keys
J-1000	1000(RSA 2048bits)	1G or/& 10G	1/10/20/50/100	4,000 Keys	15,000 Keys
J-500	500(RSA 2048bits)	1G or/& 10G	1/10/20/50/100	2,000 Keys	10,000 Keys
J-500 Base	500(RSA 2048bits)	1G or/& 10G	1	1,000 Keys	5,000 Keys

Note :

HSM comes with an option of field upgrade to higher TPS with additional license purchase

This product family, available as a Network Security Module, offers a no compromise cost efficient & tamper evident solution that addresses the stringent security requirements of SaaS applications, ecommerce payment systems and Enterprise, Banking and Government security applications especially as they migrate to the Public or Private cloud.

Major applications for this product family include Key Management as-a-Service, Database as-a-Service, Crypto as-a-service, Secure DNS, SaaS Applications and Virtual Private Clouds in the Public Cloud.

Features

Capabilities

- Upto 35K 2048b RSA ops/sec
- Upto 10G Bulk crypto / sec
- Upto 11K ECC ops/sec
- Upto 100K any size key store in crypto memory
- Unlimited protected keys as per FIPS 140-3 Level 3
- FIPS 140-3 level 3 certified Cryptographic boundary
- Onboard key generation, signing and encryption
- Two Factor Authentication
- M of N authentication
- Extensive key and certificate management
- Supports Users and groups from LDAP, local systems, Hadoop and container environments
- Capability to integrate with SIEM solutions
- Single Management UI
- 16 MB Memory within HSM
- MTBF: Minimum 100000 minutes

Supported OS

- Windows, Linux, Solaris, AIX, HP-UX

Operating Environment / Compliance

- Operating temperature: +10°C to +50°C (+50°F to +122°F)
- Storage temperature: -10°C to +55°C (+14°F to +131°F)
- Relative humidity: 10% to 95% noncondensing
- RoHS Compliant
- Complies with FCC standard for Electromagnetic compatibility (EMC)
- Compliant to UL, CE, WEEE *

Physical specifications network appliance

- Available as 1U & 2U appliance
- Device provide isolated components so as to prevent damage within modules and ensure continue operation
- Mechanically rugged and anti-corrosive device including frames and support
- Adequate ventilation and cooling arrangements for heat dissipation
- All components and materials used in the equipment are non-inflammable
- 19 Inch Rack Mount

Network Interface

- Dual network Interface / Four network interface
- Option of 1GbE or/ & 10 GbE
- Copper and Fiber connectivity with port bonding
- IPv4 and IPv6 supported

Out of the Box solution

- Cryptographic APIs such as PKCS11, CAPI, JCE, OpenSSL
- RestAPI for integration and management
- Health checks, Audit logs
- Auto Synchronization of keys between DC-DR
- Auto Backup of keys
- Backup with split key
- Support for NTP for Time Synchronization
- Support for SNMP
- Remote management
- Key Management Facility (Create, Use, Delete, Archive etc.)
- HSM can be hosted in Cloud Network.
- Support CA software like OpenCA and EJBCA
- Keys can be backup in External Drive in encrypted format and restoration would be only in HSM"

Supported Virtual Environment

- VMware, Hyper-V, Xen, KVM, etc.

Division of Roles

- Admin: Create, enable/disable partitions but no access to keys in FIPS boundary
- Partition admin: Create users per partition
- Partition Users: Create, import keys and use them

Power Supply

- 2 x 1U 550W/740W 80+certified Hot Swappable Power Supply
- Power Efficiency : 94%
- Output and Input: 550W/740W with Input 100 - 240Vac
- AC Input Freq. : 50-60Hz
- Power Distributor : O/P: 12V/75A
 - ◇ +5V Max: 30A
 - ◇ +3.3V Max: 24A
 - ◇ -12V Max: 0.6A
- Power supply terminations for different PCBs is uniform.

Cryptographic Algorithms

RSA

- KeyGen: 2048, 3072 and 4096-bit
- PKCS #1.5 SigGen: 1024 and 4096-bit (SHA-224, 256, 384, 512)
- PKCS #1.5 SigVer: 1024, 2048 and 4096-bit (SHA-1, 224, 256, 384, 512)

ECC

- ECC CDH: P-224 and P-256 with SHA-256, P-384 and P-521 with SHA-512
- ECDH compute and SSL suite B key exchange

**Under Approval*

Hash

- SHA: 1, 224, 256, 384, and 512, MD5

ECDSA

- PKG: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K571,
- B-233, B-283, B-409, and B-571
- PKV: All P, K and B curves
- Sig Gen: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, and B-571 (SHA-224, -256, -384, -512)
- SigVer: All P, K and B curves (SHA-1, 224, -256, -384, -512)

RNG

- Hardware Random Number Generator (NDRNG)

Triple-DES

- ECB mode; 3-key;
- TCBC mode; 3-key;
- SP800-38F Triple-DES Key Wrap

Post Quantum Cryptography Support

- ML-KEM as CRYSTALS-Kyber
- ML-DSA as CRYSTALS Dilithium
- SLH-DSA is based on the SPHINCS+

DSA

- PQG Gen: 2048 and 4096-bit (SHA-256)
- PQG Ver: 1024-bit (SHA-1); 2048 and 4096-bit (SHA-256)
- Sig Gen: 2048-bit (SHA-224, -256, -384, -512)
- SigVer: 1024, 2048 and 4096-bit (SHA-1, 224, -256, -384, 512)

DRBG

- SP 800-90A DRBG: AES-CTR 256-bit

AES

- ECB mode: Encrypt/Decrypt; 128, 192 and 256-bit
- CBC mode: Encrypt/Decrypt; 128, 192 and 256-bit
- GCM mode: Encrypt/Decrypt; 128, 192 and 256-bit

Other Supported Algorithms

- PBE, RC2, RC4, RC5, Diffie-Hellman, DES, CAST, ARIA
- KCDSA
- RIPEMD160
- Camellia
- Class II and Class III certificate of all CA



Contact Us:

sales@jisasoftech.com | connect@jisasoftech.com

Phone: +91 9619-222-553

JISA Softech Pvt. Ltd.

A-604, Amar Business Zone, Ganraj Chowk, Veerbhadra Nagar, Baner,
Pune, Maharashtra 411045

www.jisasoftech.com