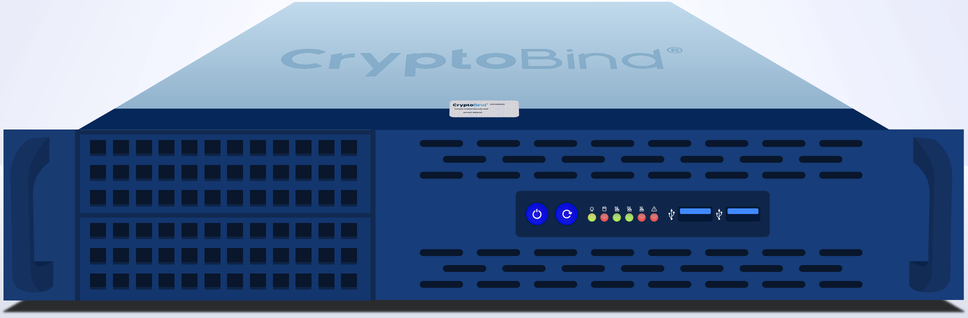
JISA®
Creating Secured Ecosystem

CryptoBind®

LAUNCHING

India’s First Made In India “Payment HSM”



PIN & Card Transaction Verification

Encyption & Key Management

Supporting POS ATM Network Management Protocol

Supporting Key/Data Exchange API standards

Generating PVV and CVV Data, Card Keyset

3-D SecureTM Issuance & Authorization

www.jisasofttech.com

CRYPTOBIND PAYMENT HSM

UNCOMPROMISED PAYMENT SECURITY

Overview

The CryptoBind Payment HSM is an advanced Hardware Security Module designed to meet the demands of General Purpose, Payments, and Compliance applications. Engineered for exceptional performance and scalable cloud deployment, it provides a comprehensive solution for securing cryptographic processes across various environments.

This advanced HSM offers robust cryptographic support tailored for payment applications, safeguarding the entire lifecycle of cryptographic keys. As secure and tamper-resistant devices, CryptoBind Payment HSMs ensure the confidentiality, integrity, and availability of sensitive data. They play a crucial role in the retail and banking industries, protecting cryptographic keys and customer PINs used in transactions at POS systems and ATMs, as well as in the issuance and processing of magnetic stripe and EMV chip cards.

Key Features

Clustering

High Availability & Disaster Recovery: CryptoBind Payment HSM supports clustering across multiple regions, ensuring uninterrupted service and robust disaster recovery capabilities.

Multi-Tenancy

Cryptographic Isolation: With up to 42 isolated partitions, each CryptoBind HSM can securely support multiple customers or applications simultaneously.

Multi-Mode Operation

Compliance Flexibility: Supports NIST FIPS 140-3 (Level-3) and PCI PTS HSM compliance on the same device. Additionally, non-FIPS mode allows for custom applications and algorithms.

Platform Software Hosting

Flexible Architecture: Through virtual machines, the CryptoBind Payment HSM enables the hosting of custom applications or algorithms within its secure FIPS boundary.

Post-Quantum Readiness

Future-Proof Security: Equipped to support emerging post-quantum algorithms in non-FIPS mode, with plans to incorporate these algorithms into FIPS mode upon NIST ratification.

API-First Design

Rapid Deployment: Accelerate time to market with a comprehensive software development kit and an API-first approach that simplifies integration across multi-cloud, hybrid, and OEM environments.

Cost Efficiency

Unified Solution: Achieve the lowest total cost of ownership (TCO) by reducing capital expenditure (Cap-Ex) and operational expenditure (Op-Ex) with a single HSM solution for both General Purpose and Payments needs.

Performance & Scalability

High Capacity & Speed: Manages millions of cryptographic keys and supports billions of transactions with superior performance and scalability.

Techical Specifications

Comprehensive Cryptographic Algorithms:

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

Secure Operations:

- Random number generation (SP 800-90).
- M of N quorum control for fault tolerance.
- Hardware root of trust
- Secure boot
- Cryptographic agility for future-proof security, including post-quantum cryptography

APIs

- Java (JCA/JCE)
- PKCS#11
- OpenSSL Engine
- Secure boot
- Customer API's

Physical Characteristics

- 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% non-condensing
- RoHS Compliant
- Complies with FCC standard for Electromagnetic compatibility (EMC)
- Compliant to UL, CE, WEEE *
- Dimensions (W x H x D): 17.2" (437 mm) x 3.5" (89 mm) x 25.5" (647 mm)
- Gross Weight: 52 lbs (23.59 kg)
- Packaging (W x H x L): 26.7" (678 mm) x 11.4" (290 mm) x 34.5" (876 mm)

Security Certifications

- FIPS 140-3 Level 3 certified Cryptographic Boundary
- PCI PTS-HSM 4.0 certified Cryptographic Boundary

Payment Functions

- Integrated HSM: Combines general-purpose and payment HSM functionalities.
- Cloud-Ready: Tailored for secure cloud environments, safeguarding issuers, payment switches, gateways, and acquirers.
- LSPay API Library
- TR-31 key block
- TR-34 key transport
- PIN translation formats (ISO-0/1/2/3)

Management & Monitoring

- Advanced Partitioning: Multiple partitions with flexible resource allocation and role-based access control (RBAC)
- Multi-Tenancy: Vendor as root of trust, supporting hybrid cloud deployments.
- Secure Channels: TLS-model tunnel with Perfect Forward Secrecy (PFS) for untrusted environments.
- Remote Administration: Manage securely with attested audit logs, tamper-evident protections, and zeroization features.
- 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

About JISA Softech

JISA Softech is a leading provider for comprehensive cybersecurity solutions specializing in Hardware Security Modules (HSM), Public Key Infrastructure (PKI), Cryptography, Tokenisation, Data Encryption (at rest, in transit, and in use), as well as Data Privacy and Protection solution. With a commitment to safeguarding sensitive information and ensuring regulatory compliance, JISA Softech empowers businesses to secure their digital assets and maintain the confidentiality, integrity, and availability of their critical data. Our innovative solutions have been adopted by businesses across India and Middle East to handle mission-critical data security and data protection needs.

- Hardware Security Module
- Enterprise Key Management
- Quantum Cryptography
- PII Data Vault
- Vaultbased & Vaultless Tokenisation
- Data Privacy Module
- Aadhaar Stack (Aadhaar Vault & eKYC)
- Data Masking
- Data Encryption (At Rest, In motion , In Use)
- Application level Encryption
- Column Level Encryption
- Transparent Data Encryption
- Certificate Lifecycle Management
- Confidential Computing
- Homomorphic Encryption
- Data Discovery & Classification
- Authentication (MFA, SSO, FIDO)
- IoT Security Platform

Scan to Save Contact

Questions?

Feel free to contact us

+91 9619-222-553

connect@jisasoftech.com | sales@jisasoftech.com

www.jisasoftech.com

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

Download Brochure