JioCloud

Managed HSM

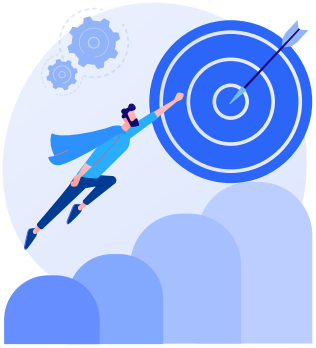
Ensure Compliance, Cut Overhead, Strengthen Security

JioCloud

Deploy cryptographic protection faster with JioCloud HSM — certified, scalable, and built to simplify key management.

The Challenge

- Physical HSMs are complex to deploy, scale, and maintain.
- Strict regulations require certified encryption and full key lifecycle control.
- Applications running across on-premises and cloud need a centralised, secure source of trust.



The JioCloud Solution

JioCloud's Managed HSM (Hardware Security Module) delivers enterprise-grade cryptographic security without the complexity of owning and managing hardware. Built on FIPS 140-2 Level 3 certified HSMs, it ensures secure key generation, storage, and lifecycle management for sensitive workloads. Designed to meet the demand of regulated industries, the service offers high availability, scalability, and compliance — empowering organizations to protect data, digital identities, and transactions with confidence.

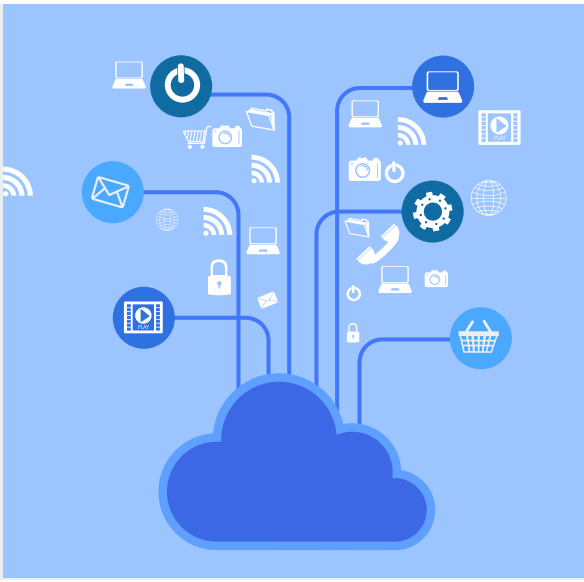
Key Features

- **Certified cryptographic core**
  Protect keys and operations with FIPS 140-2 Level 3 certified HSMs.
- **Seamless API integration**
  Connect easily using PKCS#11, JCE, CSP/CNG for apps, databases, and identity
- **Role-based access control**
  Separate duties with Crypto Officer and Security Officer roles.
- **High availability clusters**
  Maintain uninterrupted service with clustering and automatic failover.
- **Centralized key management**
  Oversee keys from creation to retirement with full audit trails.
- **Tamper-proof security**
  All operations stay within physically secure, tamper-resistant boundaries.
- **Cloud-native scalability**
  Provision capacity elastically to meet workload spikes.
- **Multi-tenant isolation**
  Provide logical separation for teams, apps, or business units.

JioCloud

What You Gain

- **Scalability**
  Scale key operations and clusters on-demand for fluctuating workloads.
- **Security**
  Hardware-backed protection with FIPS-certified assurance against physical and logical threats.
- **Integration**
  Plug into existing commercial applications such as PKI, IAM, IoT, SSL/TLS etc
- **Cost Efficiency**
  Reduce upfront expenditure of owning and managing dedicated HSM appliances.
- **Compliance Ready**
  Align with NIST, GDPR, HIPAA standards effortlessly.



Use Cases

Financial services
Protect customer transactions and meet audit requirements with certified encryption.

Government and public sector
Keep citizen records and national identity systems safe for the long term.

Healthcare
Encrypt and safeguard patient data while staying aligned with HIPAA mandates.

Manufacturing
Ensure IoT devices and supply chain communication are both trusted and secure.

Cloud-native enterprises
Add cryptographic protection into apps and services quickly.

PKI and identity management
Support certificates, digital signatures, and secure identity frameworks.

Who It's For

CISOs who need stronger compliance and centralised control.

PKI and identity architects are building digital trust into their organisations.

Application security managers embedding encryption directly into apps and workflows.

IT compliance leads showing regulators that cryptographic controls are in place.

DevSecOps teams folding automated crypto into CI/CD pipelines.

Platform and cloud security engineers managing keys and policies across hybrid setups.

Why JioCloud

Less complexity - a managed service that removes the pain of hardware setup and maintenance.

Proven assurance - backed by FIPS 140-2 Level 3 certification.

Scales with you - multi-tenant ready, with logical separation for teams or business

Built for the enterprise - integrates smoothly with standard APIs and cloud-native applications.

JioCloud

Take the complexity out of key management.

Connect with us at jpl.cloudsales@ril.com or visit (website) to secure your workloads with JioCloud HSM.