Managed KMS

Secure Your Enterprise Keys the Smart Way

Simplify encryption, manage key lifecycles, and meet compliance with ease - powered by JioCloud KMS.

The Challenge

- **Scattered keys, growing risk**
  As systems grow across cloud and on-premise, keeping track of cryptographic keys becomes harder. Without central control,

- **Key management shouldn't be so complicated**
  Too many teams still manage keys in silos - across tools, clouds, and environments. The result? More friction, less speed, and slower app delivery.

- **Compliance pressure is rising**
  From NIST to GDPR, proving control over cryptographic keys is no longer optional. You need clear audit trails and lifecycle visibility - all the time.

The JioCloud Solution

JioCloud's Managed KMS (Key Management Service) offers a modern, cloud-native approach to key management. With on-demand provisioning, scalable architecture, and intuitive self-service inter aces, our solution helps businesses to manage cryptographic keys seamlessly across applications, databases, and workloads. JioCloud KMS removes the complexity of manual key handling, ensuring compliance, agility, and cost efficiency.

Key Features

- **Secure key account management**
  Enables rapid account provisioning and creation, storage and management of keys with seamless automation.

- **API-driven integration**
  REST APIs enable smooth integration with cloud-native and enterprise applications.

- **FIPS certified**
  Enterprise Key Management as a Service provides compliance with FIPS 140-2 Level 1.

- **Role-based access controls (RBAC)**
  Provides fine-grained access control for account admins and users.

- **Tenant-aware design**
  Logical isolation of key associated with respective user accounts ensures secure multi-tenancy.

- **Observability**
  Built-in dashboards monitors historical key activity patterns.

- **High availability deployment**
  Clustering ensures continuous availability and minimal downtime.

JioCloud

What You Gain

- **Agility**
  Simplified integration with applications via APIs, reduces developer friction.

- **Security**
  Keys never leave the secure environment,censuring trust and compliance.

- **Compliance**
  Meets industry regulations such as NIST, HIPAA, GDPR.

- **Efficiency**
  Centralized control prevents key sprawl and reduces operational overhead.

- **Scalability**
  Expands seamlessly across various enterprise workloads.

Use Cases in Action

Application layer encryption

Secure storage of sensitive data by integrating KMS in applications and databases.

Audit-ready compliance

Security teams rely on built-in logs and monitoring tools to prepare for audits, flag anomalies, and maintain governance policies.
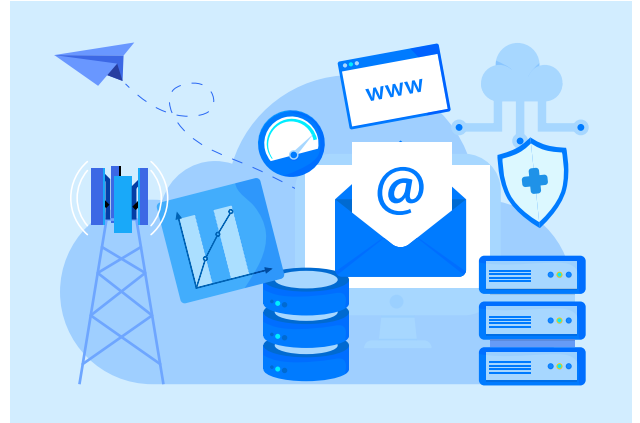
High availability by default

Clustered deployment within a zone ensures your keys remain accessible and secure even during system updates or node-level infrastructure issues.

Top Applications

Ideal for sectors where data security and access control are non-negotiable:

- Financial Institutions
- Government and Public Sector
- Healthcare and Regulated Industries
- Digital Commerce and Identity Platforms
- Cloud-Native Enterprises

Who It's For

- CISOs and Security Architects
- DevSecOps Teams
- Platform Engineers
- System Administrators
- Governance and Compliance Teams

Why JioCloud

- **You own the keys**
Cryptographic keys stay fully under your control — not a third party's. That means stronger assurance for audits, compliance, and governance.

- **Unified security platform**
One-stop platform with unified lifecycle control over the provisioned assets.
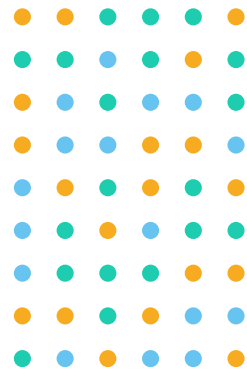
- **Always available**
Clustered deployment and secure backup mean your keys are ready when needed — and protected when not.

- **Built for business**
From day one, you get RBAC, policy enforcement, observability, and zero tolerance for downtime.

- **Made for India**
Compliant with MeitY and CERT-In, supported locally, and ready for hybrid deployments.

JioCloud

Ready to Simplify Key Management?

Take control of your encryption lifecycle—with less complexity.
Reach us out at **jpl.cloudsales@ril.com** or visit **(website)**.