ORACLE KEY MANAGER 3

SIMPLE, SECURE, SCALABLE ENCRYPTION KEY MANAGEMENT

KEY BENEFITS

- Get up and running quickly—a day or two for most companies—and manage keys easily with user-defined policies.
- Protect encryption keys for full data lifecycle throughout distributed and heterogeneous storage environments.
- Grow without worry since you can manage thousands of storage devices and millions of encryption keys.

Compliance with legal, financial, and regulatory requirements is dependent on data security. If you lose sensitive data and it's not encrypted, your business is exposed to sanctions, penalties and loss of brand equity. Designed to meet stringent enterprise requirements, Oracle Key Manager (OKM) 3 makes it easy to implement and scale storage-based encryption—for operational and archive data—without unnecessary cost and complexity.

Complex Environments – Simple Solution

Distributed and heterogeneous storage infrastructures are a given, so the OKM 3 provides a comprehensive, application and operating system agnostic platform for tape key management from a single pane of glass. OKM 3 is composed of the following elements:

- Key Management Appliance (KMA). Two or more KMAs are connected to form a cluster for high availability of keys and optimized performance. The KMAs create, provision and manage encryption keys based on policies and actions.
- Oracle Key Management GUI and CLI. A graphical user interface (GUI) or two command line interfaces (CLIs) communicate with the Oracle Key Manager cluster from a workstation over an IP network to manage the system.
- Optional Cryptographic Card provides FIPS 140-2 Level 3 compliance to OKM 3.

Simple, Secure, Scalable the Oracle Key Manager 3 is designed with an emphasis on simplicity, security, and scalability so you can realize the following benefits:

- **Security.** Oracle Key Manager 3 is a hardened solution that provides FIPS 140-2 Level 3 compliance and secure key protection throughout key lifecycle, with a dedicated key management and delivery network.
- **Interoperability.** Open standards-based architecture supports diverse storage devices—mainframe to open systems—under a single storage key management system.
- **Availability.** Ensures high availability with active n-node clustering, dynamic load balancing and automated failover.
- **Manageability.** User-defined, policy-based automatic key management with secure client GUI makes it easy to administer the solution in one site or worldwide.
- **Scalability.** On a single clustered Oracle Key Manager appliance pair, you can manage thousands of storage devices and millions of encryption keys. Scale your solution easily and non-disruptively.

Supported Encryption End-points

- Java Applications
- Solaris 11 (ZFS)
- Tape Drives and Libraries

Oracle Key Manager 3 Supported Tape Drives and Libraries					
Drive Types	SL24/48	SL500/ SL150	SL3000	SL8500	9310
HP LTO 4	Yes	Yes/No	Yes	Yes	No
HP LTO 5	Yes	Yes	Yes	Yes	No
IBM LTO 4	No	Yes/No	Yes	Yes	No
IBM LTO 5	No	Yes/No	Yes	Yes	No
HP LTO 6	No	Yes	Yes	Yes	No
IBM LTO 6	No	No	Yes	Yes	No
StorageTek T10000A	No	No	Yes	Yes	Yes
StorageTek T10000B	No	No	Yes	Yes	No
StorageTek T10000C	No	No	Yes	Yes	No
StorageTek T10000D	No	No	Yes	Yes	No
StorageTek T9840D	No	No	Yes	Yes	Yes

Key Features

- **FIPS-certified cryptography.** Uses FIPS 140-2 certified cryptography to provide AES-256 bit encryption keys for stored data.
- **Role-based access control.** Supports NIST SP800-60 operational roles to segregate operational functions.
- **Active clustering and failover.** Provides high availability through active n-node clustering of KMAs with fully automated failover.
- **Near-synchronous replication.** Provides near-synchronous, secure replication of transaction data among KMAs within the cluster.
- **Granular role segregation.** Provides operational segregation through six role definitions—Security Officer, Compliance Officer, Operator, Backup Operator, Auditor, and Quorum Member. Each role is access controlled and functionally restricted, although users can have multiple roles.
- **Quorum**. Quorum required to activate and to perform other sensitive operations such as restoring OKM data backups. Quorum parameters are fully configurable.
- **Centralized policy management.** Data encryption policies are managed centrally through the Compliance Officer role. Policies are automatically replicated for disaster recovery purposes.
- **Audit logging.** Maintains audit logs for all operational and key material events and

transactions.

- **Open standards.** Developed on open standards including X.509v3 certificates, Simple Object Access Protocol (SOAP), and Transport Layer Security (TLS).
- **Secure management client.** Provides a rich cross-platform compatible client for local and remote management via secure client GUI.
- **Multivendor device support.** Capable of providing encryption key management support to Oracle's most popular tape drives including the StorageTek T10000 A/B/C/D, StorageTek T9840D, and LTO4/5/6 tape drives.
- **Enhanced Serviceability.** Offers automated Support Service process by using fault event telemetry from OKM appliance to initiate a service request.

Contact Us

For more information about Oracle Key Manager, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together