Oracle Key Manager
Overview and Frequently Asked Questions

Overview

Oracle Key Manager (OKM) 3.0 provides a comprehensive key management platform for tape-based storage in the most diverse environments. Developed on open security standards, the system consists of these integrated parts:

- **Key Management Appliance (KMA):** Multiple KMAs are connected via an IP network to form a Key Manager (KM) cluster. A minimum of two KMAs is required per installation site.
- **Encrypting devices:** Data storage devices that are connected to the KM cluster via dedicated communication network.
- **Oracle Key Manager**: A graphical user interface (GUI) that runs on a workstation. It communicates with the Oracle Key Manager cluster over an IP network to configure and manage the system.

Oracle Key Manager delivers the following functionality for storage networks:

- Registers and authenticates encrypting storage devices
- Automatically creates, provisions, and deletes encryption keys in accordance with system policies

Customer Benefits

Oracle Key Manager 3.0 is designed with an emphasis on simplicity, security, and scalability to realize the following benefits:

- **Secure key retention:** OKM 3.0 securely retains encryption keys for the full data lifecycle, which can exceed a decade.
- **Interoperability:** Open standards architecture supports diverse storage devices—mainframe to open systems—under a single storage key management system.
- **Manageability**: Ensure high availability with active n-node clustering, dynamic load balancing, and automated failover. User-defined, policy-based automatic key management with secure client GUI makes it easy to administer the solution in one room or worldwide.
- **Scalability**: A single clustered OKM appliance pair can manage thousands of storage devices and millions of encryption keys. Allows the user to scale the system easily and non-disruptively.

Oracle Key Manager
Overview and Frequently Asked Questions

Frequently Asked Questions

Does Oracle Key Manager perform any data encryption?

The encrypting devices, such as encrypting tape drives, perform data encryption in the storage system. OKM manages and protects the crypto keys used to encrypt the data.

What is the minimum configuration of Oracle Key Manger?

The OKM system at a minimum requires a pair of key management appliances (KMAs), an encryption-enabled storage device (i.e. T10000 drive), a connectivity kit to connect the encrypting device to the OKM cluster, and an encryption key for each device enrolled in the system.

How large does the system scale?

The OKM system has been tested to manage up to three thousand encrypting devices and up to one million keys.

Can the system support multiple locations?

Widely dispersed physical locations can be a part of the same OKM cluster, as long as necessary Ethernet connectivity between KMAs is maintained.

What are the system management requirements of Oracle Key Manager?

OKM is based on self-contained appliances, requiring no maintenance/management other than for security-related functions (such as enrolling encrypting devices and establishing security policies.)

What standards does Oracle Key Manager meet?

The OKM implementation utilizes concepts and algorithms found in NIST SP800-60 and NIST FIPS140-2 standards, and relies on open standards such as: X.509v3, Simple Object Access Protocol (SOAP), and Transport Layer Security (TLS).

How is the Oracle Key Manager cluster protected from intrusion?

The system is protected using a quorum of members for its most sensitive functions. A specific number of quorum members must supply their passwords in order to perform security-critical functions, such as powering up the system and unlocking the password database.

How are keys protected within Oracle Key Manager?

Keys within OKM are secured by AES 256 encryption, and locked with split-key password derived from quorum members' passwords.

How are communications protected within Oracle Key Manager?

OKM uses TLS certificates created during the device enrollment process to authenticate the communication channel. Additionally, all communications between OKM and the encrypting devices are encrypted using AES256 algorithm.

Are there any licenses required for this solution?

Every drive enrolled in the OKM requires a purchase of encryption license key.

What professional services are available to assist with an Oracle Key Manager implementation?

OKM installations require Oracle Key Manager Integration Services. Additionally, it is recommended that customers utilize the Encryption Architecture, Design and Implementation Planning Service to assist with preparation for their OKM implementation.

FIPS 150-2 Level 3 Card Manufacturer?

OKM untilizes the Thales nSheild F3 500+ card.

What is the certification number for the FIPS 140-2 Level 3 card?

Certificate number is 2644 from NIST.

Oracle Key Manager
Overview and Frequently Asked Questions

What is FIPS 140-2 Level 3?

The module is tamper evident and tamper resistant. The Federal Information Processing Standards (FIPS) 140-2 validation scheme is for cryptographic modules and jointly administered by the US National Institute of Standards and Technology (NIST) and the Canadian Communications Security Establishment (CSE). Testing is performed by certified independent test laboratories with validation ultimately being approved by NIST.

ORACLE®

SUN STORAGE

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

Oracle Corporation

Worldwide Headquarters
500 Oracle Parkway
Redwood Shores, CA
94065
U.S.A.

Worldwide Inquiries
Phone
+1.650.506.7000
+1.800.ORACLE1

Fax
+1.650.506.7200

oracle.com