Oracle® Key Manager 3

Security Guide

Release 3.0

E49728-01

January 2014

ORACLE®

Oracle Key Manager 3 Security Guide, Release 3.0

E49728-01

Primary Author: OKM Development Team

Contents

Preface

This document describes the security features of Oracle Key Manager 3 (OKM 3).

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of OKM 3.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Overview

This section gives an overview of the product and explains the general principles of application security.

Product Overview

The Oracle Key Manager (OKM) creates, stores, and manages encryption keys. It consists of the following components:

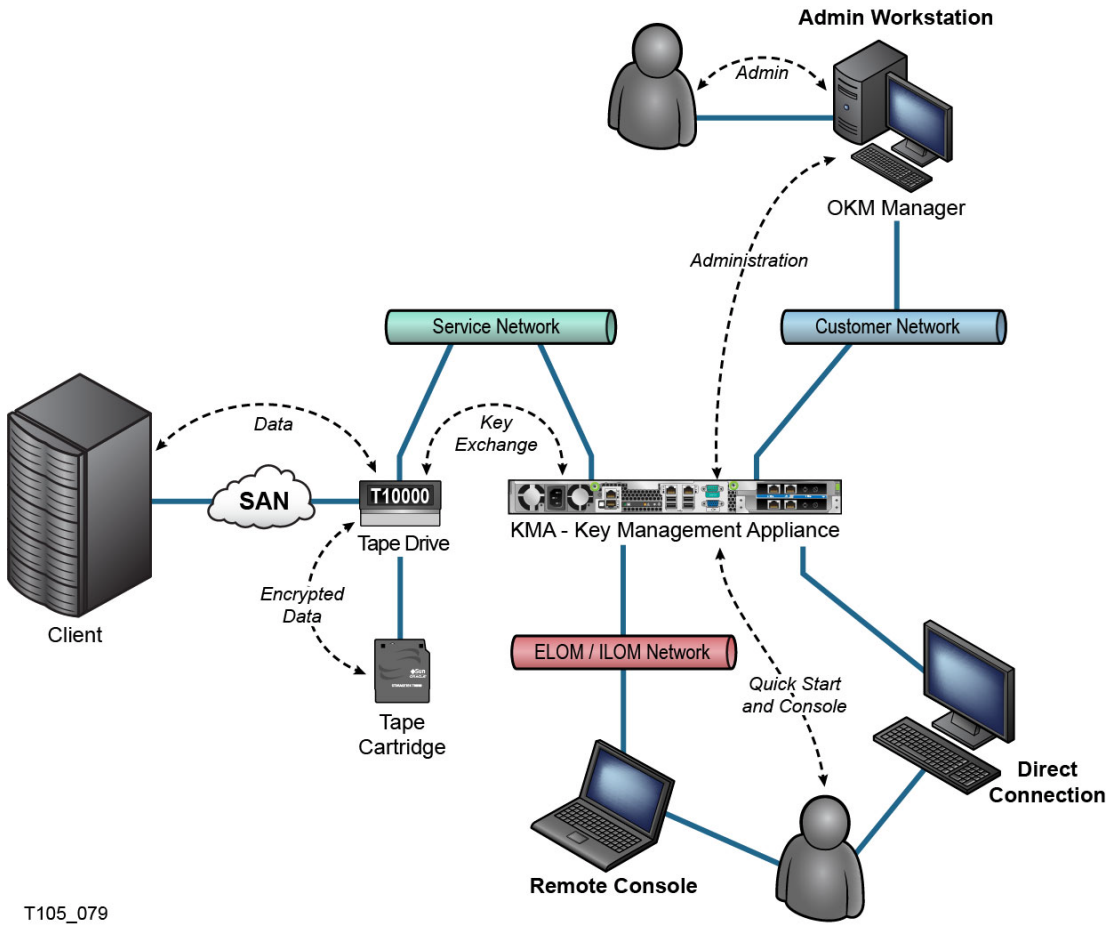
- Key Management Appliance (KMA) – A security-hardened box that delivers policy-based Lifecycle Key Management, authentication, access control, and key provisioning services. As a trusted authority for storage networks, the KMA ensures that all storage devices are registered and authenticated, and that all encryption key creation, provisioning and deletion is in accordance with prescribed policies.
- Oracle Key Manager GUI – A Graphical User Interface that is executed on a workstation and communicates with the KMA over an IP network to configure and manage the OKM. The Oracle Key Manager GUI must be installed on a customer-provided workstation.
- Oracle Key Manager CLIs – Two Command Line Interfaces that are executed on a workstation and communicate with the KMA over an IP network to automate commonly issued administrative operations. The Oracle Key Manager CLIs must be installed on a customer-provided workstation.
- OKM Cluster – The full set of KMAs in the system. All of these KMAs are aware of each other and replicate information to each other.
- Agent – A device or software that performs encryption, using keys managed by the OKM Cluster. A StorageTek encrypting tape drive is an example of an agent. Agents communicate with KMAs using the KMS Agent Protocol. The Agent API is a set of software interfaces that are incorporated into the agent hardware or software.

The OKM uses TCP/IP networking for the connections between KMAs, Agents, and workstations where the Oracle Key Manager GUI and CLIs are running. To provide flexible network connections, three interfaces are provided for network connections on each KMA:

- The management connection – Intended for connection to the customer network
- The service connection – Intended for connection to the agents
- The ILOM/ELOM connection – Intended for connection to the ILOM or ELOM on the KMA

See the example in the following image:

Figure 1–1 Connections to the KMA



General Security Principles

The following principles are fundamental to using any application securely.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. The latest Oracle Key Manager upgrade packages and installers are available on the My Oracle Support web site: http://support.oracle.com.

Restrict Network Access to Critical Services

Keep your business applications behind a firewall. The firewall provides assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over-ambitious granting of responsibilities, roles, grants, and so on especially earlier on in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration, and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check the My Oracle Support web site yearly for revisions.

2

Secure Installation

This section outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems.

Understand Your Environment

To better understand your security needs, ask yourself the following questions:

Which resources am I protecting?

Many resources in the production environment can be protected. Consider the resources you want to protect when deciding the level of security you must provide.

The primary resource to be protected is typically your data. Other resources are outlined here because they are associated with managing and protecting your data.Various concerns with protecting data include data loss (that is, data being unavailable) and data being compromised or disclosed to unauthorized parties.

Cryptographic keys are often used to protect data from unauthorized disclosure. Thus, they are another resource to be protected. Highly reliable key management is essential to maintaining highly available data.

Another layer of resources to be protected includes the assets within the Oracle Key Manager Cluster itself, including the Key Management Appliances.

From whom am I protecting the resources?

These resources must be protected from everyone who does not have authority to access them. These resources should be physically protected. You should consider which of your employees should have access to these resources. Then identify which types of operations each employee should be able to issue in the Oracle Key Manager environment?

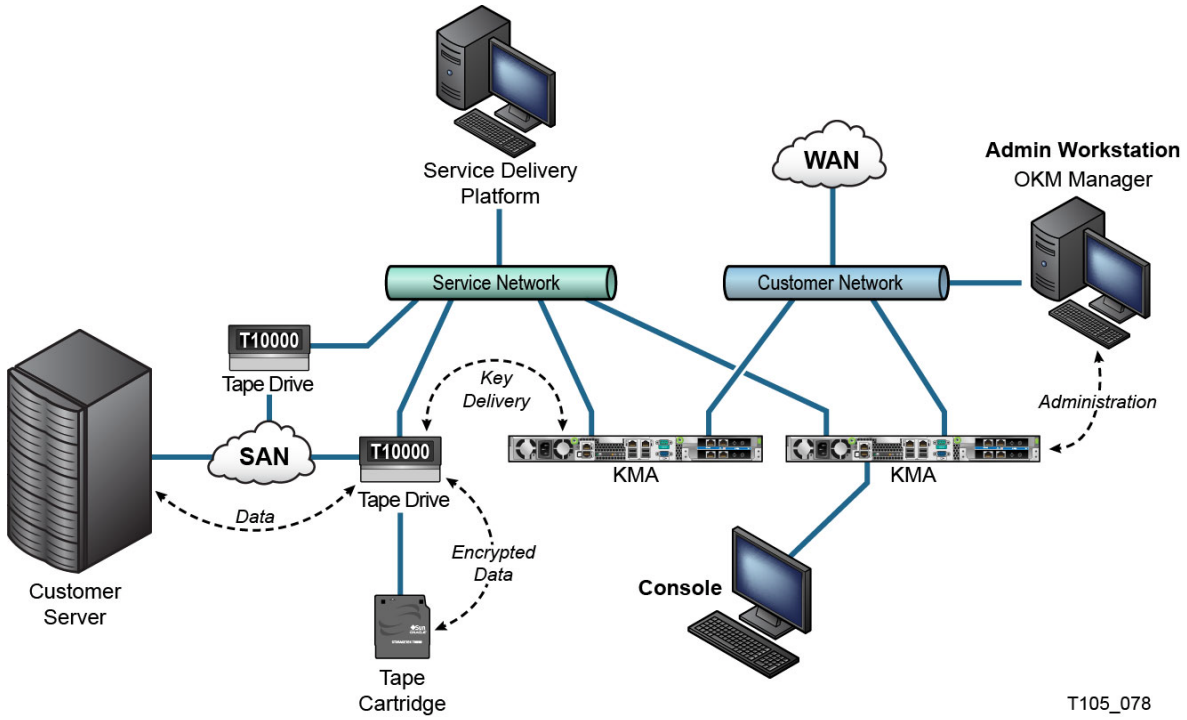
What will happen if the protections on strategic resources fail?

In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use your resources. Understanding the security ramifications of each resource will help you protect it properly.

Recommended Deployment Topologies

The following figure shows a typical deployment of an Oracle Key Manager solution.

Figure 2–1 Typical Deployment of OKM Solution



Installing a Key Management Appliance

This section describes how to install and configure an OKM Key Management Appliance securely.

KMAs are manufactured as hardened appliances with Oracle Key Manager functionality already available on them.

Installing and configuring KMAs in an OKM Cluster include the following steps:

1. For each KMA, install it in a rack.
2. For each KMA, secure its BIOS and its ILOM.
3. Configure the first KMA in the OKM Cluster.
4. Add additional KMAs to the OKM Cluster.

More information about planning the deployment of an OKM Cluster appears in the Oracle Key Manager Systems Assurance Guide included in the Oracle Key Manager documentation libraries located at:

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto

Installing a KMA in a Rack

An Oracle Customer Service Engineer installs a KMA in a rack according to procedures outlined in the Oracle Key Manager Installation and Service Manual. Oracle service personnel may refer to this manual for more detailed information.

Securing the BIOS of a KMA

Oracle Key Manager KMAs are manufactured with recent Embedded Lights Out Manager (ELOM) or Integrated Lights Out Manager (ILOM) and BIOS firmware. The BIOS of a KMA should be secured by either an Oracle Customer Service Engineer or by the customer. The BIOS should also be secured after the ELOM or ILOM firmware is upgraded.

Securing the BIOS consists of setting particular BIOS settings in order to prevent changes to the BIOS that may compromise security.

The following procedure shows an example of accessing the BIOS Setup Utility through the ILOM of a KMA for a Sun Fire X4170 M2 server. Access the BIOS Setup Utility through the ELOM of a KMA for a Sun Fire X2100 or X2200 M2 server. The BIOS settings of relevance in this procedure are the same on all of these server types.

Note: Netra SPARC T4-1 servers do not have a BIOS; there are no BIOS procedures for users to follow for this server.

1. Log into the ILOM web-based interface. Follow (or navigate) to:

   Remote Control > Redirection

   and click Launch Redirection to launch the Remote Console.

2. Follow (or navigate) to

   Remote Control > Remote Power Control

3. In the Remote Console, monitor normal boot messages. When the American Megatrends screen appears, press the F2 key to launch the BIOS Setup Utility.

   See "ILOM Security Hardening" information in the OKM 3.0 Administration Guide if you want to harden the ILOM.

In the BIOS Setup Utility, do the following steps:

1. Go to the Security tab, navigate to the Change Supervisor Password field, press the Enter Key, and specify a password. Retain this password.
2. After specifying the supervisor password, the User Access Level field should appear. Navigate to the User Access Level field and change the setting from “Full Access” to “Limited.”
3. Go to the Boot tab. Navigate to Boot Device Priority and make the following changes:

Tab	Field Name	Value
Boot	1st Boot Device (under Boot Device Priority)	HDD:P0-SEAGATE ST95000NSSUN500G 101
Boot	2nd Boot Device (under Boot Device Priority)	Disabled
Boot	3rd Boot Device (under Boot Device Priority)	Disabled

4. Press the F10 key to save these changes and select OK to confirm.

Let the system boot up. Now that you have defined a supervisor password in the BIOS, the system will prompt for this password when someone accesses the BIOS Setup Utility.

For more information about navigating around the BIOS Setup Utility, refer to the "Configuring BIOS Settings" section of the Sun Fire X4170, X4270, and X4275 Servers Service Manual at:

http://download.oracle.com/docs/cd/E19477-01/820-5830-13/index.html

Securing the ILOM of a KMA

Oracle Key Manager KMAs are manufactured with recent ILOM and BIOS firmware. The ILOM of a KMA should be secured by either an Oracle Customer Service Engineer or by the customer. The ILOM should also be secured after the ILOM firmware is upgraded.

Securing the ILOM consists of setting particular ILOM settings in order to prevent changes to the ILOM that may compromise security.

The following procedure includes accessing the Integrated Lights Out Manager (ILOM) of a KMA that is a Sun Fire X4170 M2 server.

1. Open a web browser. Log into the ILOM using its web-based interface. Refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Daily Management – Web Procedures Guide at below link for more information about using the ILOM web interface: http://docs.oracle.com/cd/E19860-01/E21446/E21446.pdf
2. Newly manufactured KMAs have a default password for the "root" user. This password should be changed and retained.
3. Navigate to Configuration > System Management Access > SNMP. For "Settings", the use of SNMPv3 is recommended (v1 and v2c can be disabled). Disable "Set Requests" to prevent configuration changes from being made through SNMP.
4. Navigate to Configuration > System Management Access > IPMI. If the Auto Service Request (ASR) feature was introduced in OKM 2.4, then enable IPMI. Otherwise, disable IPMI if there are no plans to use it. Leaving this interface open exposes this KMA to reboot.
5. Navigate to Configuration > System Management Access > CLI. Configure the session timeout as the default setting allows CLI sessions to remain open indefinitely.
6. Navigate to Configuration > System Management Access > WS-Man. Disable this service if there are no plans to use WS-Management and CIM. Leaving this interface open exposes the KMA to attackers knowledgeable of the WS-Management protocol.
7. Navigate to Configuration > Clock. The ILOM clock is not synchronized with the host clock on a Sun Fire X4170 M2 server. So that ILOM event can be correlated with server events, the ILOM date and time should be set manually to UTC/GMT time or configured to synchronize with an external NTP server, preferably the same NTP server that is used by the KMAs in this OKM Cluster. See the Oracle Key Manager Administration Guide which is included in Oracle Key Manager documentation libraries at:

   http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto
8. Navigate to Configuration > Timezone. The ILOM timezone should be set to "GMT."

9. Navigate to User Management > User Accounts. Use of user accounts and roles is recommended over using just the default root account. See the "User Account Management" section of the Oracle Integrated Lights Out Manager (ILOM) 3.0 Daily Management - Concepts Guide at:

   http://download.oracle.com/docs/cd/E19860-01/index.html

10. Navigate to Remote Control > Host Control. The "Next Boot Device" value should be set to "Default (User BIOS Settings)."

11. Navigate to Maintenance > Firmware Upgrade. The ILOM firmware should be kept up to date and updated as described in the Oracle Integrated Lights Out Manager (ILOM) 3.0 Daily Management - Web Procedures Guide. As a precaution, the KMA should be shut down from the OKM Console before upgrading ILOM firmware.

If you suspect that ILOM configuration changes are causing problems, you can restore ILOM settings to default values by following the instructions in the "Troubleshooting The Server and Restoring ILOM Defaults" section of the Sun Fire X4170, X4270, and X4275 Servers Service Manual at:

http://download.oracle.com/docs/cd/E19477-01/820-5830-13/index.html

Configuring the First KMA in an OKM Cluster

Before configuring the first KMA, first identify key split credentials and user IDs and passphrases to be defined in this OKM Cluster. Useful worksheets appear in the Oracle Key Manage Systems Assurance Guide included in the Oracle Key Manager documentation libraries. Provide these key split credentials and user IDs and passphrases to the appropriate personnel. Refer to the Quorum Protection section later in this document for more information.

Note: Retain and protect these key split credentials and user IDs and passphrases!

Open a web browser, launch the Remote Console, and launch the OKM QuickStart utility within the Remote Console. To initialize the OKM Cluster on this KMA, follow the Initialize Cluster procedure described in the Oracle Key Manager Administration Guide included in the Oracle Key Manager documentation libraries.

The key split credentials and a user with Security Officer privileges are defined during this procedure. After the QuickStart procedure is completed, the Security Officer must log into the KMA and define additional OKM users.

Considerations When Defining Key Split Credentials

Defining fewer key split user IDs and passphrases and a lower threshold is more convenient but is less secure. Defining more key split user IDs and passphrases and a higher threshold is less convenient but is more secure.

Considerations When Defining Additional OKM Users

Defining fewer OKM users, some of whom have multiple roles assigned to them, is more convenient but is less secure. Defining more OKM users, most of whom have only one role assigned to them, is less convenient but is more secure as it facilitates tracking operations performed by a given OKM user.

Adding Additional KMAs to the OKM Cluster

Open a web browser, launch the Remote Console, and launch the OKM QuickStart utility within the Remote Console. To add this KMA to the OKM Cluster, follow the Join Cluster procedure described in the Oracle Key Manager Administration Guide included in the Oracle Key Manager documentation libraries.

Considerations When Adding Additional KMAs

Oracle Key Manager offers the convenient option of Autonomous Unlock for each KMA. This option is defined during the QuickStart procedure for the first and additional KMAs in a Cluster and can be modified by the Security Officer later.

If Autonomous Unlock is enabled, then the KMA will automatically unlock itself at startup and will be ready to provide keys without requiring quorum approval. If Autonomous Unlock is disabled, then the KMA will remain locked at startup and will not provide keys until the Security Officer issues a request to unlock it and a quorum approves this request.

For maximum security Oracle discourages enabling autonomous unlock. For more information about the Autonomous Unlock option, refer to the Oracle Key Manager Version 3.0 Security and Authentication White Paper at:

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

Characteristics of Hardened KMAs

As stated above, KMAs are manufactured as hardened appliances with Oracle Key Manager functionality already available on them. As hardened appliances, they have the following characteristics:

- Unneeded Solaris packages are not included in the Solaris image. For example, ftp and telnet services and utilities do not appear in the Solaris image.
- KMAs do not produce core files.
- The standard Solaris login(1) utility has been replaced with the OKM Console. Thus, users cannot log into the Solaris console.
- The ssh service is disabled by default. For customer support purposes, the Security Officer can enable the ssh service and define a support account for a limited amount of time. This support account is the only available account and has limited access and permissions. Solaris auditing tracks commands that the support account invokes.
- The root account is disabled.
- Solaris single user mode is disabled.
- KMAs are not equipped with a DVD drive.
- USB ports are effectively disabled.
- Unused network ports are closed.
- The Hardware Security Module is certified to FIPS 140-2 Level 3, therefore providing both tamper-evident and tamper-resistant features in addition to certified cryptographic algorithms.
- The newer KMAs based on Sun Fire X4170 M2 servers are tamper evident (ILOM fault) when the chassis door is accessed while power is applied.

3

Security Features

This section outlines the specific security mechanisms offered by the product.

Potential Threats

Customers having encryption-enabled agents are primarily concerned with:

- Disclosure of information in violation of policy
- Loss or destruction of data
- Unacceptable delay in restoring data in case of catastrophic failure (for example, in a business-continuity site)
- Undetected modification of data

Objectives of the Security Features

The objective of the security features of Oracle Key Manager are to:

- Protect encrypted data from disclosure
- Minimize exposure to attacks
- Provide sufficiently high reliability and availability

The Security Model

This section of the security guide should give a high level overview of the threats that the system is designed to counter and how the individual security features combine to prevent the attacks.

The critical security features that provide these protections are:

- Authentication – Ensuring that only authorized individuals get access to the system and data
- Authorization – Access control to system privileges and data; this access control builds on authentication to ensure that individuals only get appropriate access
- Audit – Allows administrators to detect attempted breaches of the authentication mechanism and attempted or successful breaches of access control

For more information about the security and authentication aspect of the Oracle Key Manager, refer to the Oracle Key Manager Version 3.0 Security and Authentication White Paper at:

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

Authentication

The Oracle Key Manager architecture provides for mutual authentication between all element of the system: KMA to KMA, agent to KMA, and the Oracle Key Manager GUI or CLI to KMA for user operations.

Each element of the system (for example, a new encryption agent) is enrolled in the system by creating an ID and a passphrase in the OKM that is then entered into the element to be added. For example, when a tape drive is added to the system, the agent and KMA automatically run a challenge/response protocol based on the shared passphrase that results in the agent obtaining the Root Certificate Authority (CA) certificate and a new key pair and signed certificate for the agent. With the Root CA certificate, agent certificate, and key pair in place, the agent can run the Transport Layer Security (TLS) protocol for all subsequent communications with the KMAs. All certificates are X.509 certificates.

The OKM behaves as a root certificate authority to generate a root certificate that KMAs use in turn to derive (self-sign) the certificates used by agents, users, and new KMAs.

Access Control

Access control is of following types:

- Users and Role-Based Access Control
- Quorum Protection

Users and Role-Based Access Control

The Oracle Key Manager provides the ability to define multiple users, each with a user ID and passphrase. Each user is given one or more pre-defined roles. These roles determine which operations a user is permitted to perform on an Oracle Key Manager system. These roles are:

- Security Officer – Performs Oracle Key Manager setup and management
- Operator – Performs agent setup and day-to-day operations
- Compliance Officer – Defines Key Groups and controls agent access to Key Groups
- Backup Operator – Performs backup operations
- Auditor – Views system audit trails
- Quorum Member – Views and approves pending quorum operations

A Security Officer is defined during the QuickStart process, which sets up a KMA in an OKM Cluster. Later, a user must log into the Cluster as a Security Officer using the Oracle Key Manager GUI in order to define additional users. The Security Officer can choose to assign multiple roles to a particular user and can also choose to assign a particular role to multiple users.

For more information about the operations that each role allows and how a Security Officer creates users and assigns roles to them, refer to the Oracle Key Manager Administration Guide included in the Oracle Key Manager documentation libraries at:

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto

This role-based access control supports National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 operational roles to segregate operational functions.

Quorum Protection

Some operations are critical enough to require an additional level of security. These operations include adding a KMA to an OKM Cluster, unlocking a KMA, creating users, and adding roles to users. To implement this security, the system uses a set of key split credentials in addition to the role-based access described above.

Key split credentials consists of a set of user ID and passphrase pairs, together with the minimum number of these pairs necessary to the system to enable completion of certain operations. The key split credentials are also referred to as "the quorum" and the minimum number as "the quorum threshold."

Oracle Key Manager allows up to 10 key split user ID / passphrase pairs and a threshold to be defined. They are defined during the QuickStart process when the first KMA in an OKM Cluster is configured. The key split users IDs and passphrases are different from user IDs and passphrases that are used to log into the system. When a user attempts an operation that requires quorum approval, the defined threshold of key split users and passphrases must approve this operation before the system performs this operation.

Audits

Each KMA logs audit events for operations that it performs, including those issued by agents, users, and peer KMAs in the OKM Cluster. KMAs also log audit events whenever an agent, user, or peer KMA fails to authenticate itself. Audit events that indicate a security violation are noted. A failure to authenticate is an example of an audit event that indicates a security violation. If SNMP Agents are identified in the OKM Cluster, then KMAs also send SNMP INFORMs to these SNMP Agents should they encounter a security violation.

A user must properly log into the OKM Cluster and must have a role assigned to it before it is allowed to view audit events.

KMAs manage their audit events. KMAs remove older audit events based on retention terms and limits (counts). The Security Officer can modify these retention terms and limits as needed.

Other Security Features

Oracle Key Manager provides other security features. For more information about these and other OKM features, refer to the Oracle Key Manager Overview at:

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf

Secure Communication

The communication protocol between an agent and a KMA, a user and a KMA, and a KMA and a peer KMA is the same. In each case, the system uses the passphrase for the entity initiating the communication to perform a challenge/response protocol. If successful, the entity is provided with a certificate and its corresponding private key.

This certificate and private key can establish a Transport Layer Security (TLS) 1.0 (secure sockets) channel using 2048-bit RSA. Establishing this session results in the endpoints agreeing on an Advanced Encryption Standard (AES) 256-bit key. The TLS cypher suite is non-negotiable so KMA client endpoints may not negotiate a weaker suite. All subsequent communications are encrypted with this AES 256-bit key. Mutual authentication is performed; each end of any connection authenticates the other party.

Hardware Security Module

KMAs have an available Hardware Security Module, which is ordered separately. This Hardware Security Module -- a Sun Cryptographic Accelerator (SCA) 6000 card – is FIPS 140-2 Level 3 certified and provides Advanced Encryption Standard (AES) 256-bit encryption keys. The SCA 6000 card supports a FIPS 140-2 Level 3 mode of operation and OKM always uses the card in this manner. When the OKM Cluster operates in FIPS compliant mode, encryption keys do not leave the cryptographic boundary of the SCA 6000 card in unwrapped form. The SCA 6000 card uses a FIPS-approved random number generator, as specified in FIPS 186-2 DSA Random Number Generator using SHA -1 for generating encryption keys.

When a KMA is not configured with an SCA 6000 card, cryptography is performed using the Solaris Cryptographic Framework (SCF) PKCS#11 soft token.

AES Key Wrapping

Oracle Key Manager uses AES Key Wrapping (RFC 3994) with 256-bit key encrypting keys to protect symmetric keys as they are created, stored on the KMA, transmitted to agents or within key transfer files.

Key Replication

When the first KMA of an OKM Cluster is initialized, the KMA generates a large pool of keys. When additional KMAs are added to the Cluster, the keys are replicated to the new KMAs and are then ready to be used to encrypt data. Each KMA that is added to the Cluster generates a pool of keys and replicates them to peer KMAs in the Cluster. All KMAs will generate new keys as needed to maintain the key pool size so that ready keys are always available for agents. When an agent requires a new key, the agent contacts a KMA in the Cluster and requests a new key. The KMA draws a ready key from its key pool and assigns this key to the agent's default key group and to the data unit. The KMA then replicates these database updates across the network to the other KMAs in the Cluster. Later, the agent can contact another KMA in the Cluster in order to retrieve the key. At no time is any clear text key material transmitted across the network.

4

Linux PKCS#11 KMS Provider

A new Linux PKCS#11 KMS provider accompanies the Oracle Key Manager release. An administrator can download the Linux PKCS#11 KMS provider from the My Oracle Support web site and install it on an Oracle Enterprise Linux server. The Linux PKCS#11 KMS provider has the same security characteristics and authenticates with Oracle Key Manager appliances as other agents do.

The Linux PKCS#11 KMS provider stores a log file and profile information under a /var/opt/kms/username directory. The user and/or administrator should manage this log file manually or by using a utility such as logrotate.

Access control to the /var/opt/kms/username directory should be restricted through appropriate permissions. Within the profile directory the authentication credentials for the agent are retained within a PKCS#12 file. The PKCS#12 file is secured with a password.

For more information about the Linux PKCS#11 KMS provider, refer to the Oracle Key Manager Administration Guide included in the Oracle Key Manager documentation libraries at:

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto

A

Secure Deployment Checklist

The following security checklist includes guidelines that help secure your key management system:

1. Install each KMA in a physically secure environment.
2. Secure the BIOS on each KMA.
3. Define the key split configuration for this Oracle Key Manager Cluster.
4. Set the autonomous unlock setting for each KMA as appropriate.
5. Define Oracle Key Manager users and their associated roles.
6. Practice the principle of least privilege.
   a. Grant each Oracle Key Manager user only those roles as needed.
7. Monitor activity on the Oracle Key Manager Cluster.
   a. Investigate any errors, especially Security Violations, that are logged in the Oracle Key Manager audit log.
8. Back up the core security when the key split configuration is initially defined and whenever the key split configuration is modified.
9. Perform Oracle Key Manager backups on a regular basis.
10. Store core security backup files and Oracle Key Manager backup files in a secure location.

B

References

Oracle Key Manager documentation libraries at:
http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto

Oracle Key Manager Installation and Service Manual

Oracle Integrated Lights Out Manager (ILOM) 3.0 Daily Management - Web Procedures Guide at:

http://download.oracle.com/docs/cd/E19860-01/index.html

Oracle Integrated Lights Out Manager (ILOM) 3.0 Daily Management - Concepts Guide at:

http://download.oracle.com/docs/cd/E19860-01/index.html

Sun Fire X4170 M2 and X4270 M2 Servers Product Notes at:

http://download.oracle.com/docs/cd/E19762-01/index.html

Sun Fire X4170, X4270, and X4275 Servers Service Manual at:
http://download.oracle.com/docs/cd/E19477-01/820-5830-13/index.html

Oracle Key Manager Overview at:

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf

Oracle Key Manager Version 2.X Security and Authentication White Paper at:
http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

National Institute of Standards and Technology Special Publication 800-60 Volume I Revision 1 at:

http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

Sun Cryptographic Accelerator 6000 FIPS 140-2 Security Policy at:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf