# Oracle® Key Manager 3

Guida per la sicurezza

Release 3.1

**E52206-02**

**Aprile 2016**

ORACLE®

**Oracle® Key Manager 3**
Guida per la sicurezza

**E52206-02**

# Indice

# Lista delle tabelle

# Prefazione

In questo documento vengono descritte le funzioni di sicurezza di Oracle Key Manager 3 (OKM 3).

## Destinatari

Il presente manuale è rivolto a chiunque sia coinvolto nell'uso delle funzioni di sicurezza nonché nell'installazione e configurazione sicure di OKM 3.

## Accesso facilitato alla documentazione

Per informazioni sull'impegno di Oracle riguardo l'accesso facilitato, visitare il sito Web Oracle Accessibility Program su http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

**Accesso al supporto Oracle**
I clienti Oracle che hanno acquistato l'assistenza, hanno accesso al supporto elettronico mediante My Oracle Support. Per informazioni, visitare http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info o http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs per i non udenti.

# 1

# Capitolo 1. Panoramica

Questa sezione contiene una panoramica sul prodotto e una descrizione dei principi generali di sicurezza dell'applicazione.

## 1.1. Panoramica sul prodotto

Oracle Key Manager (OKM) crea, memorizza e gestisce chiavi di cifratura. È composto dai componenti elencati di seguito.

- Key Management Appliance (KMA): dispositivo dotato di sicurezza potenziata che offre servizi basati su criteri per la gestione, l'autenticazione, il controllo dell'accesso e il provisioning delle chiavi. Allo stesso modo di un'autorità attendibile per le reti di storage, la KMA controlla che tutti i dispositivi di storage siano registrati e autenticati e che tutte le operazioni di creazione, provisioning ed eliminazione delle chiavi di cifratura siano conformi ai criteri stabiliti.
- Interfaccia GUI di Oracle Key Manager: interfaccia utente grafica eseguita su una workstation che comunica con la KMA su una rete IP per configurare e gestire OKM. L'interfaccia GUI di Oracle Key Manager deve essere installata su una workstation fornita dall'utente.
- Interfacce CLI di Oracle Key Manager: due interfacce a riga di comando eseguite su una workstation che comunicano con la KMA su una rete IP per automatizzare le operazioni amministrative effettuate di frequente. Le interfacce CLI di Oracle Key Manager devono essere installate su una workstation fornita dall'utente.
- Cluster di OKM: l'insieme completo delle KMA nel sistema. Tutte queste KMA sono consapevoli l'una dell'altra e replicano le informazioni tra di loro.
- Agente: dispositivo o software che esegue la cifratura, utilizzando le chiavi gestite dal cluster di OKM. Un esempio di agente è un'unità nastro per la cifratura StorageTek. Gli agenti comunicano con le KMA utilizzando il protocollo per gli agenti KMS. L'interfaccia API dell'agente è un insieme di interfacce software incorporate nell'hardware o nel software dell'agente.

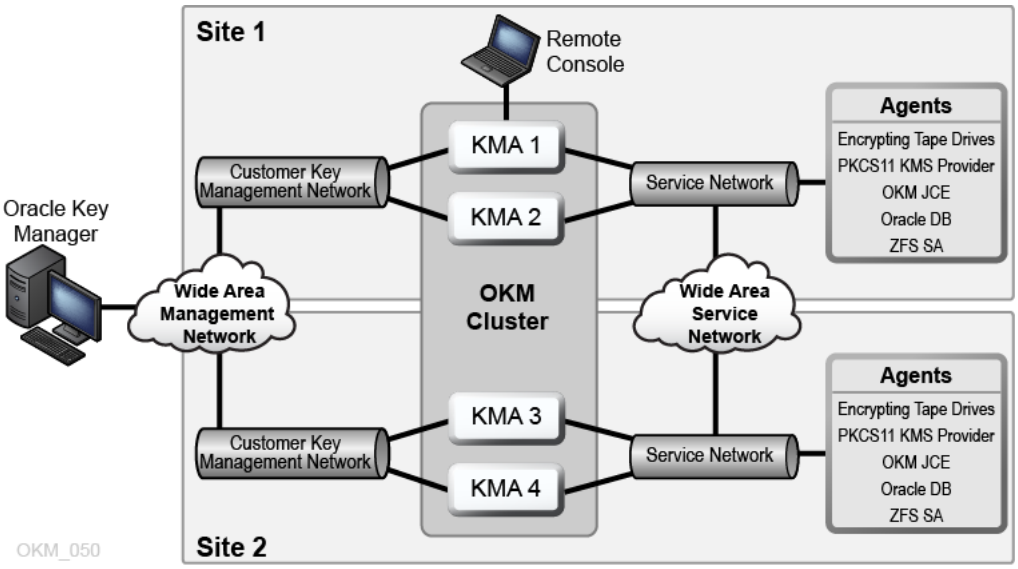
OKM utilizza le reti TCP/IP per la connessione tra le KMA, gli agenti e le workstation su cui sono in esecuzione le interfacce GUI e CLI di Oracle Key Manager. Per offrire connessioni di rete flessibili, sono disponibili tre apposite interfacce su ciascuna KMA.

- Connessione di gestione: per la connessione alla rete dell'utente.
- Connessione di servizio: per la connessione agli agenti.

- Connessione a ILOM/ELOM: per la connessione all'ILOM o all'ELOM sulla KMA.

Vedere l'esempio nell'immagine seguente.

**Figura 1.1.**




# 1.2. Principi di sicurezza generali

I principi indicati di seguito sono fondamentali per utilizzare in sicurezza qualsiasi applicazione.

## 1.2.1. Mantenere il software aggiornato

Uno dei principi alla base delle procedure di sicurezza consigliate consiste nel mantenere aggiornate tutte le versioni e le patch del software. Gli ultimi pacchetti di aggiornamento e programmi di installazione di Oracle Key Manager sono disponibili sul sito Web My Oracle Support all'indirizzo: `http://support.oracle.com`.

## 1.2.2. Limitare l'accesso di rete ai servizi critici

Proteggere le applicazioni aziendali con un firewall. Il firewall garantisce che l'accesso a questi sistemi sia limitato a un percorso di rete noto, che è possibile monitorare e limitare, se necessario. Un router dotato di firewall costituisce una valida alternativa a più firewall indipendenti.

## 1.2.3. Attenersi al principio di privilegio minimo

Il principio di privilegio minimo richiede che agli utenti venga assegnata la minore quantità di privilegi per eseguire le operazioni. Responsabilità, ruoli e concessioni troppo elevati,

soprattutto nelle fasi iniziali del ciclo di vita di un'organizzazione in cui il personale è ridotto e il lavoro deve essere svolto rapidamente, spesso portano a rischi di abusi del sistema. I privilegi dell'utente devono essere verificati periodicamente per stabilire l'importanza delle responsabilità del lavoro corrente.

### 1.2.4. Monitorare l'attività del sistema

La sicurezza del sistema si basa su tre elementi: protocolli di sicurezza validi, configurazione di sistema appropriata e monitoraggio del sistema. Il controllo e l'analisi dei record di controllo soddisfano il terzo requisito. Ciascun componente all'interno di un sistema prevede qualche tipo di funzionalità di monitoraggio. Seguire il suggerimento sui controlli nel presente documento e monitorare i record di controllo a intervalli regolari.

### 1.2.5. Mantenersi aggiornati sulle ultime informazioni sulla sicurezza

Oracle apporta continui miglioramenti ai prodotti software e alla documentazione. Controllare una volta l'anno il sito Web My Oracle Support per le revisioni.

2

# Capitolo 2. Configurazione e installazione sicure

In questa sezione viene descritto il processo di pianificazione per un'installazione sicura e vengono illustrate le diverse topologie di distribuzione consigliate per i sistemi.

## 2.1. Informazioni sull'ambiente

Per comprendere al meglio le proprie esigenze di sicurezza, è necessario rispondere alle domande riportate di seguito.

### 2.1.1. Quali risorse desidero proteggere?

Nell'ambiente di produzione è possibile proteggere molte risorse. Identificare le risorse che si desidera proteggere quando si stabilisce il livello di sicurezza che occorre ottenere.

In genere, la principale risorsa da proteggere è costituita dai dati. In questa sede vengono descritte altre risorse in quanto associate alla gestione e alla protezione dei dati. I diversi problemi che riguardano la protezione dei dati includono la perdita di dati (ossia, dati resi non disponibili) e il danneggiamento o la divulgazione dei dati a parti non autorizzate.

Per proteggere i dati dalla divulgazione non autorizzata, spesso vengono utilizzate le chiavi di cifratura. Esse costituiscono pertanto un'altra risorsa da proteggere. Una gestione delle chiavi altamente affidabile è fondamentale per garantire l'alta disponibilità dei dati. Un altro livello di risorse da proteggere è costituito da quelle incluse nel cluster di Oracle Key Manager stesso, tra cui le Key Management Appliance.

### 2.1.2. Da chi desidero proteggere le risorse?

Queste risorse devono essere protette da chiunque non disponga dell'autorità necessaria all'accesso. Queste risorse devono essere protette fisicamente. È necessario considerare a quali dipendenti è opportuno concedere l'accesso a queste risorse. Quindi, identificare i tipi di operazione che ciascun dipendente deve poter eseguire nell'ambiente Oracle Key Manager.

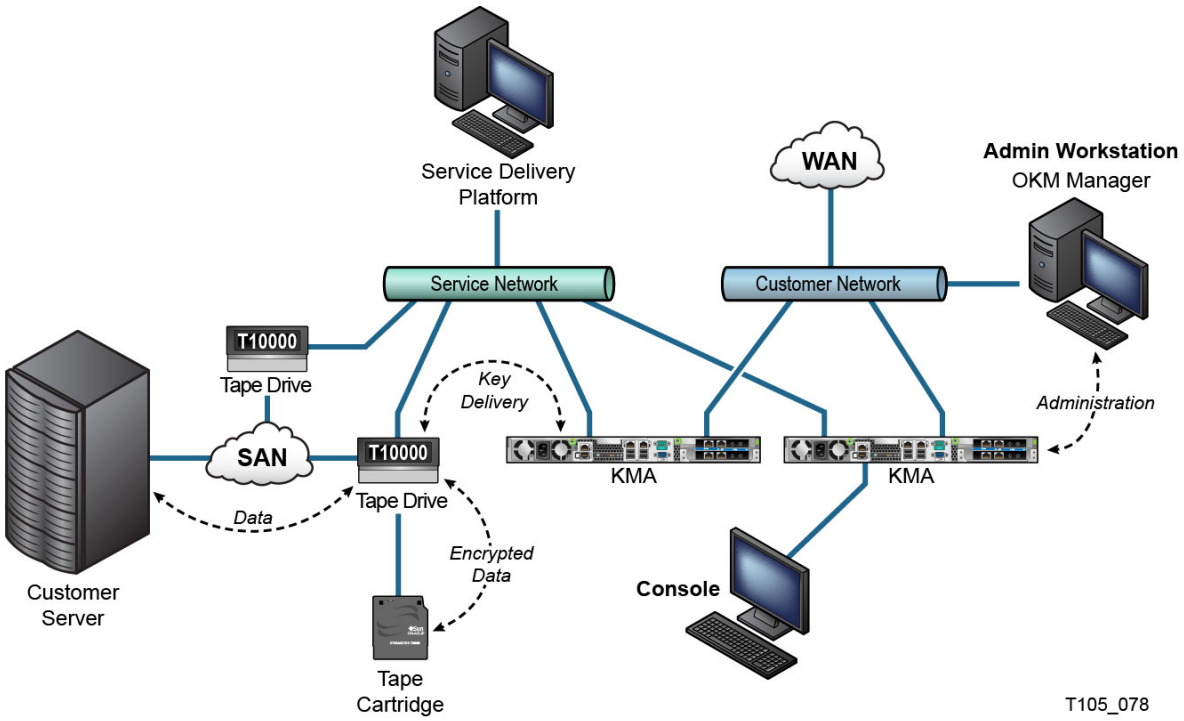
### 2.1.3. Cosa accade se la protezione delle risorse strategiche fallisce?

In alcuni casi, un problema nello schema di sicurezza viene rilevato facilmente e considerato semplicemente un'inconveniente. In altri casi, un problema potrebbe causare un grave danno alle aziende o ai singoli clienti che utilizzano le risorse. Per proteggere correttamente ogni risorsa, è necessario comprenderne le ramificazioni in termini di sicurezza.

## 2.2. Topologie di distribuzione consigliate

Nella figura riportata di seguito viene illustrata una distribuzione tipica di una soluzione Oracle Key Manager.

**Figura 2.1. Distribuzione tipica di una soluzione OKM**




## 2.3. Installazione di una Key Management Appliance

In questa sezione viene descritto come installare e configurare in sicurezza una Key Management Appliance di OKM.

Le KMA vengono prodotte come appliance potenziate con la funzionalità Oracle Key Manager già disponibile.

L'installazione e la configurazione delle KMA in un cluster di OKM includono le operazioni elencate di seguito.

1. Installare ciascuna KMA in un rack.
2. Proteggere l'ILOM di ciascuna KMA.
3. Configurare la prima KMA nel cluster di OKM.
4. Aggiungere altre KMA al cluster di OKM.

Per ulteriori informazioni sulla pianificazione della distribuzione di un cluster di OKM, consultare il manuale *Overview and Planning Guide* di OKM.

### 2.3.1. Installazione di una KMA in un rack

Un tecnico del servizio clienti Oracle installa una KMA in un rack, in base alle procedure indicate nel documento *Oracle Key Manager Installation and Service Manual*. Per informazioni più dettagliate, il personale dell'assistenza Oracle può fare riferimento a questo manuale.

### 2.3.2. Protezione dell'ILOM di una KMA

Le KMA di Oracle Key Manager sono prodotte con il recente firmware ILOM. L'ILOM di una KMA deve essere protetto da un tecnico del servizio clienti Oracle o dall'utente. L'ILOM deve essere protetto anche dopo l'aggiornamento del firmware.

La protezione dell'ILOM comporta la definizione di determinate impostazioni dell'ILOM in modo da impedire modifiche all'ILOM che possano compromettere la sicurezza. Per le istruzioni, vedere "ILOM Security Hardening" nell'appendice Service Processor Procedures del manuale OKM *Administration Guide*.

### 2.3.3. Configurazione della prima KMA in un cluster di OKM

Prima di configurare la prima KMA, identificare le credenziali di suddivisione della chiave, nonché gli ID utente e le passphrase da definire in questo cluster di OKM. A questo scopo è possibile utilizzare un foglio di lavoro, come quello presente nel documento OKM *Installation and Service Manual* (solo interno). Chiedere al rappresentante del supporto Oracle.

Fornire le credenziali di suddivisione della chiave, gli ID utente e le passphrase al personale appropriato. Per ulteriori informazioni, consultare «Protezione del quorum» più avanti in questo documento.

**Nota:**

**Conservare e proteggere le credenziali di suddivisione della chiave, gli ID utente e le passphrase.**

Aprire un browser Web, avviare la console remota, quindi avviare la utility OKM QuickStart nella console remota. Per inizializzare il cluster di OKM su questa KMA, seguire la procedura di inizializzazione del cluster descritta nel manuale *Oracle Key Manager Administration Guide* incluso nella libreria della documentazione di Oracle Key Manager.

Durante questa procedura vengono definite le credenziali di suddivisione della chiave e un utente con privilegi di Security Officer. Una volta completata la procedura QuickStart, il Security Officer deve eseguire il login alla KMA e definire ulteriori utenti di OKM.

### 2.3.4. Considerazioni per la definizione delle credenziali di suddivisione della chiave

La definizione di un numero ridotto di ID utente e passphrase per la suddivisione della chiave e di una soglia minima è più conveniente ma meno sicura. La definizione di un numero

maggiore di ID utente e passphrase per la suddivisione della chiave e di una soglia superiore è meno conveniente ma più sicura.

### 2.3.5. Considerazioni per la definizione di ulteriori utenti di OKM

La definizione di pochi utenti di OKM, alcuni dei quali con più ruoli assegnati, è più conveniente ma meno sicura. La definizione di più utenti di OKM, la maggior parte dei quali con un solo ruolo assegnato, è meno conveniente ma più sicura in quanto facilita la registrazione delle operazioni eseguite da un determinato utente di OKM.

### 2.3.6. Aggiunta di ulteriori KMA al cluster di OKM

Aprire un browser Web, avviare la console remota, quindi avviare la utility OKM QuickStart nella console remota. Per aggiungere una KMA al cluster di OKM, seguire la procedura "Join Cluster" descritta in *Oracle Key Manager Administration Guide* all'indirizzo:

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

### 2.3.7. Considerazioni per l'aggiunta di ulteriori KMA

Oracle Key Manager offre la conveniente opzione Autonomous Unlock per ciascuna KMA. Questa opzione viene definita durante la procedura QuickStart per la prima KMA e le KMA aggiuntive in un cluster e può essere modificata in un secondo momento dal Security Officer.

Se l'opzione Autonomous Unlock è abilitata, la KMA si sbloccherà automaticamente al momento dell'avvio e potrà fornire chiavi senza richiedere l'approvazione in base al quorum. Se l'opzione Autonomous Unlock è disabilitata, la KMA rimarrà bloccata al momento dell'avvio e non fornirà alcuna chiave finché il Security Officer non emetterà una richiesta di sblocco e questa richiesta non verrà approvata in base al quorum.

Per la massima sicurezza, Oracle sconsiglia di abilitare l'opzione Autonomous Unlock. Per ulteriori informazioni sull'opzione Autonomous Unlock, consultare *Oracle Key Manager Version 2.x Security and Authentication White Paper* all'indirizzo:

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

### 2.3.8. Caratteristiche delle KMA potenziate

Come indicato in precedenza, le KMA vengono prodotte come appliance potenziate con la funzionalità Oracle Key Manager già disponibile. In qualità di appliance potenziate, sono dotate delle caratteristiche elencate di seguito.

- I pacchetti Solaris non necessari non sono inclusi nell'immagine di Solaris. Ad esempio, i servizi e le utility ftp e telnet non compaiono nell'immagine di Solaris.

- Le KMA non producono file core.
- La utility login(1) standard di Solaris è stata sostituita dalla console di OKM. Pertanto gli utenti non possono eseguire il login alla console di Solaris.
- Il servizio ssh è disabilitato per impostazione predefinita. Ai fini dell'assistenza clienti, il Security Officer può abilitare il servizio ssh e definire un account di assistenza per un periodo di tempo limitato. Questo account di assistenza è l'unico account disponibile e prevede accesso e autorizzazioni limitate. Il controllo di Solaris tiene traccia dei comandi richiamati dall'account di assistenza.
- L'account root è disabilitato e configurato come un ruolo.
- Le KMA non sono dotate di alcuna unità DVD.
- Le porte USB sono completamente disabilitate.
- Le porte di rete inutilizzate sono chiuse.
- Gli stack non eseguibili sono abilitati.
- La casualità di ricerca nello spazio degli indirizzi è configurata.
- Gli heap non eseguibili sono abilitati.
- Per i file system in cui la sicurezza è un fattore determinate viene utilizzata la cifratura ZFS.
- Solaris è configurato per garantire la conformità al benchmark SCAP PCI-DSS.
- I servizi SMF non necessari sono disabilitati.
- Il boot verificato di Oracle Solaris è configurabile nelle KMA basate su SPARC T7-1 per proteggere il processo di boot del sistema, proteggendo dal danneggiamento dei moduli kernel, dall'inserimento di kit root o da altri programmi malevoli.
- Le nuove KMA basate sui server SPARC T7-1 e Netra SPARC T4-1 prevedono il rilevamento delle manomissioni (errore ILOM) in caso di accesso allo sportello dello chassis quando l'alimentazione è collegata.
- Il firmware ILOM 3.2 è ora certificato in base a FIPS 140-2 livello 1 e può essere configurato in modalità FIPS.
- Lo strumento di controllo di base e di reportistica viene eseguito periodicamente per facilitare le analisi. Questi report sono inclusi nei dump di sistema di OKM.
- La funzione Solaris Cryptographic Security Framework è configurata per i criteri di sicurezza FIPS 140-2 livello 1 (documentato per Solaris 11.1) in presenza o meno di un Hardware Security Module.

## 2.4. Connessioni TCP/IP e KMA

Quando tra le entità (OKM Manager, agenti e altre KMA nello stesso cluster) e la KMA è presente un firewall, è necessario che questo consenta all'entità di stabilire connessioni TCP/IP con la KMA sulle porte riportate di seguito.

- La comunicazione da OKM Manager a KMA richiede le porte 3331, 3332, 3333, 3335.
- La comunicazione da agente a KMA richiede le porte 3331, 3332, 3334, 3335.

- La comunicazione da KMA a KMA richiede le porte 3331, 3332, 3336.

**Nota:**

Per gli utenti che configurano le rispettive KMA per l'utilizzo degli indirizzi IPv6, configurare i firewall perimetrali basati su IPv4 in modo da escludere tutti i pacchetti IPv4 del protocollo 41 in uscita e i pacchetti UDP della porta 3544 per impedire agli host Internet di utilizzare il traffico in tunnelling IPv6 su IPv4 per raggiungere gli host interni.

Per ulteriori informazioni, consultare la documentazione di configurazione del firewall. Nella Tabella 2.1, «Connessioni alle porte delle KMA » sono elencate le porte che le KMA utilizzano in modo esplicito o le porte alle quali le KMA forniscono servizi.

### Tabella 2.1. Connessioni alle porte delle KMA

| Numero porta | Protocollo | Direzione | Descrizione |
|---|---|---|---|
| 22 | TCP | Ascolto | SSH (solo quando il supporto tecnico è abilitato) |
| 123 | TCP/UDP | Ascolto | NTP |
| 3331 | TCP | Ascolto | Servizio OKM CA |
| 3332 | TCP | Ascolto | Servizio certificati di OKM |
| 3333 | TCP | Ascolto | Servizio di gestione di OKM |
| 3334 | TCP | Ascolto | Servizio agenti di OKM |
| 3335 | TCP | Ascolto | Servizio di ricerca automatica di OKM |
| 3336 | TCP | Ascolto | Servizio di replica di OKM |

Nella Tabella 2.2, «Altri servizi » vengono elencati altri servizi in ascolto su porte che potrebbero non essere utilizzate.

### Tabella 2.2. Altri servizi

| Numero porta | Protocollo | Direzione | Descrizione |
|---|---|---|---|
| 53 | TCP/UDP | Connessione | DNS (solo quando la KMA è configurata per utilizzare DNS) |
| 68 | UDP | Connessione | DHCP (solo quando la KMA è configurata per utilizzare DHCP) |
| 111 | TCP/UDP | Ascolto | RPC (le KMA rispondono alle query rpcinfo). Questa porta è aperto alle richieste esterne solo su KMS 2.1 e versioni precedenti |
| 161 | UDP | Connessione | SNMP (solo quando sono definiti gli SNMP Manager) |
| 161 | UDP | Ascolto | SNMP (solo quando Hardware Management Pack è abilitato) |
| 514 | TCP | Connessione | Syslog remoto (solo quando i server syslog remoto vengono definiti e configurati per l'utilizzo di TCP senza cifratura) |
| 546 | UDP | Connessione | DHCPv6 (solo quando la KMA è configurata per utilizzare DHCP e IPv6) |
| 4045 | TCP/UDP | Ascolto | Daemon di blocco NFS (solo KMS 2.0) |

| Numero porta | Protocollo | Direzione | Descrizione |
|---|---|---|---|
| 6514 | TLS su TCP | Connessione | Syslog remoto (solo quando i server syslog remoto vengono definiti e configurati per l'utilizzo di TLS) |

**Nota:**

La porta 443 deve essere aperta per consentire agli utenti di accedere all'interfaccia Web del processore di servizio e alla console OKM attraverso il firewall. Consultare *Oracle Key Manager Installation and Service Manual* (solo interno) per informazioni sulle porte ELOM e ILOM.

Nella Tabella 2.3, «Porte ELOM/ILOM » vengono elencate le porte ELOM/ILOM delle KMA. Se occorre accedere a ELOM/ILOM esternamente al firewall, è necessario che queste porte siano abilitate; in caso contrario, non è necessario che siano abilitate per gli indirizzi IP ELOM/ILOM.

### Tabella 2.3. Porte ELOM/ILOM

| Numero porta | Protocollo | Direzione | Descrizione |
|---|---|---|---|
| 22 | TCP | Ascolto | SSH (per l'interfaccia a riga di comando ELOM/ILOM) |
| 53 | TCP/UDP | Connessione | DNS (necessaria solo quando è configurato DNS) |
| 68 | UDP | Connessione | Se DHCP è necessario per ELOM/ILOM.<br><br>**Nota**: la documentazione per DHCP e ELOM/ILOM non è disponibile, sebbene siano supportati. |
| 80 | TCP | Ascolto | HTTP (per l'interfaccia Web ELOM/ILOM)<br><br>Se HTTP è necessario; in caso contrario, gli utenti possono fare riferimento alle istruzioni sulla connessione alla console remota all'indirizzo riportato di seguito.<br><br>ELOM:<br><br>`http://docs.oracle.com/cd/E19121-01/sf.x2100m2/819-6588-14/819-6588-14.pdf`<br><br>ILOM:<br><br>`http://docs.oracle.com/cd/E19860-01/index.html` |
| 161 | UDP | Ascolto/ Connessione | SNMPv3 (configurabile, è la porta predefinita) |
| 443 | TCP/TLS | Ascolto | Embedded/Integrated Lights Out Manager<br><br>Servizi Web DMTF (Desktop Management Task Force) per protocollo di gestione (WS-Man) su TLS (Transport Layer Security) |
| 623 | UDP | Ascolto | IPMI (Intelligent Platform Management Interface) |

# 3

# Capitolo 3. Funzioni di sicurezza

In questa sezione vengono descritti i meccanismi di sicurezza specifici offerti dal prodotto.

## 3.1. Potenziali minacce

Di seguito sono elencati i principali problemi che preoccupano gli utenti che dispongono di agenti che supportano la cifratura.

- Divulgazione di informazioni in violazione dei criteri
- Perdita o danneggiamento dei dati
- Ritardo inaccettabile nel ripristino dei dati in caso di errore irreversibile (ad esempio, in sede di continuità aziendale)
- Modifica dei dati non rilevata.

## 3.2. Obiettivi delle funzioni di sicurezza

Gli obiettivi delle funzioni di sicurezza di Oracle Key Manager sono riportati di seguito.

- Protezione dei dati cifrati dalla divulgazione.
- Riduzione dell'esposizione agli attacchi.
- Offerta di affidabilità e disponibilità sufficientemente alte.

## 3.3. Modello di sicurezza

In questa sezione della guida per la sicurezza viene offerta una panoramica di alto livello delle minacce che il sistema è progettato per affrontare e di come si combinano le singole funzioni di sicurezza per impedire gli attacchi.

Le funzioni di sicurezza fondamentali che offrono questa protezione sono riportate di seguito.

- Autenticazione: garantisce che solo le persone autorizzate ottengano l'accesso al sistema e ai dati.
- Autorizzazione: controllo dell'accesso ai privilegi e ai dati del sistema. Questo controllo dell'accesso si basa sull'autenticazione per garantire che ai singoli utenti sia consentito solo l'accesso appropriato.

- Controllo: consente agli amministratori di rilevare i tentativi di violazione del meccanismo di autenticazione e i tentativi o le violazioni al controllo dell'accesso.

Per ulteriori informazioni sugli aspetti correlati alla sicurezza e all'autenticazione in Oracle Key Manager, consultare *Oracle Key Manager Version 2.x Security and Authentication White Paper* all'indirizzo:

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

## 3.4. Autenticazione

L'architettura di Oracle Key Manager offre l'autenticazione reciproca tra tutti gli elementi del sistema: da KMA a KMA, dall'agente alla KMA e dall'interfaccia GUI o CLI di Oracle Key Manager alla KMA per le operazioni dell'utente.

Ciascun elemento del sistema (ad esempio, un nuovo agente di cifratura) deve essere iscritto nel sistema tramite la creazione di un ID e una passphrase in OKM che vengono quindi inseriti nell'elemento da aggiungere. Ad esempio, quando si aggiunge un'unità nastro al sistema, l'agente e la KMA eseguono automaticamente un protocollo challenge-response basato sulla passphrase condivisa che consente all'agente di ottenere il certificato dall'autorità di certificazione root (CA, Certificate Authority), nonché una nuova coppia di chiavi e un certificato firmato per l'agente. Una volta ottenuti il certificato CA root, il certificato dell'agente e una coppia di chiavi, l'agente può eseguire il protocollo TLS (Transport Layer Security) per tutte le comunicazioni successive con le KMA. Tutti i certificati sono X.509.

OKM si comporta come un'autorità di certificazione root per generare un certificato root utilizzato dalle KMA per derivare (autofirmare) i certificati utilizzati da agenti, utenti e nuove KMA.

## 3.5. Controllo dell'accesso

Di seguito sono elencati i tipi di controllo dell'accesso disponibili.

- Controllo dell'accesso basato su utenti e ruoli
- Protezione del quorum.

### 3.5.1. Controllo dell'accesso basato su utenti e ruoli

Oracle Key Manager consente di definire più utenti, ciascuno con un ID utente e una passphrase diversi. A ciascun utente vengono assegnati uno o più ruoli predefiniti. Questi ruoli determinano le operazioni consentite a un utente in un sistema Oracle Key Manager. Di seguito sono elencati i ruoli disponibili.

- Security Officer: esegue le operazioni di configurazione e gestione di Oracle Key Manager.

- Operator: esegue la configurazione dell'agente e le operazioni quotidiane.
- Compliance Officer: definisce i gruppi di chiavi e controlla l'accesso dell'agente a tali gruppi.
- Backup Operator: esegue le operazioni di backup.
- Auditor: visualizza gli audit trail del sistema.
- Quorum Member: visualizza e approva le operazioni di quorum in sospeso.

Durante il processo QuickStart viene definito un Security Officer, che configura una KMA in un cluster di OKM. In seguito, un utente deve eseguire il login al cluster come Security Officer utilizzando l'interfaccia GUI di Oracle Key Manager per definire ulteriori utenti. Il Security Officer può scegliere di assegnare più ruoli a un determinato utente e può anche scegliere di assegnare un determinato ruolo a più utenti.

Per ulteriori informazioni sulle operazioni consentite da ciascun ruolo e su come un Security Officer crea gli utenti e assegna loro i ruoli, consultare il manuale *Oracle Key Manager Administration Guide* incluso nella libreria della documentazione di Oracle Key Manager all'indirizzo:

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

Questo controllo dell'accesso basato sul ruolo supporta i ruoli operativi elencati nel documento Special Publication (SP) 800-60 del National Institute of Standards and Technology (NIST) per distinguere le funzioni operative.

## 3.5.2. Protezione del quorum

Alcune operazioni sono sufficientemente critiche per richiedere un livello di sicurezza aggiuntivo. Queste operazioni includono l'aggiunta di una KMA a un cluster di OKM, lo sblocco di una KMA, la creazione di utenti e l'aggiunta di ruoli agli utenti. Per implementare questa funzione di sicurezza, il sistema utilizza un insieme di credenziali di suddivisione della chiave oltre all'accesso basato sul ruolo descritto in precedenza.

Le credenziali di suddivisione della chiave sono costituite da un insieme di coppie di ID utente e passphrase, insieme al numero minimo di queste coppie necessario al sistema per consentire il completamento di determinate operazioni. Le credenziali di suddivisione della chiave vengono anche denominate "quorum" e il numero minimo "soglia di quorum".

Oracle Key Manager consente di definire un massimo di 10 coppie di ID utente/passphrase per la suddivisione della chiave e una soglia. Esse vengono definite durante il processo QuickStart, quando si configura la prima KMA in un cluster di OKM. Gli ID utente e le passphrase per la suddivisione della chiave sono diversi da quelli utilizzati per il login al sistema. Quando un utente tenta di eseguire un'operazione che richiede l'approvazione in base al quorum, prima che il sistema esegua questa operazione, è necessario che venga approvata in base alla soglia definita di utenti e passphrase per la suddivisione della chiave.

## 3.6. Controlli

Ciascuna KMA registra gli eventi di controllo per le operazioni eseguite, incluse quelle effettuate da agenti, utenti e altre KMA nel cluster di OKM. Le KMA registrano gli eventi di controllo anche ogni volta che un agente, un utente o un'altra KMA non riesce a eseguire l'autenticazione. Gli eventi di controllo che indicano una violazione della sicurezza vengono annotati. Una mancata autenticazione è un esempio di evento di controllo che indica una violazione della sicurezza. Se nel cluster di OKM vengono identificati agenti SNMP, le KMA inviano SNMP INFORM anche a tali agenti SNMP in caso di violazione della sicurezza. Se la funzione di syslog remoto è configurata, una KMA inoltrerà anche questi messaggi di controllo ai server configurati. Vedere Capitolo 5, *Syslog remoto* .

Per poter visualizzare gli eventi di controllo, è prima necessario che l'utente esegua correttamente il login al cluster di OKM e disponga di un ruolo assegnato.

Le KMA gestiscono i propri eventi di controllo. Le KMA rimuovono gli eventi di controllo precedenti in base ai termini e ai limiti (numerici) impostati per la conservazione. Se necessario, il Security Officer può modificare questi termini e limiti di conservazione.

## 3.7. Altre funzioni di sicurezza

In Oracle Key Manager sono disponibili altre funzioni di sicurezza. Per ulteriori informazioni su queste e altre funzioni di OKM, consultare il documento *Oracle Key Manager Overview* all'indirizzo:

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

### 3.7.1. Comunicazione sicura

Il protocollo di comunicazione tra un agente e una KMA, un utente e una KMA oppure una KMA e un'altra KMA è lo stesso. In ogni caso, il sistema utilizza la passphrase per l'entità che avvia la comunicazione per eseguire un protocollo challenge-response. In caso di successo, all'entità viene fornito un certificato e la chiave privata corrispondente. Il certificato e la chiave privata possono stabilire un canale TLS (Transport Layer Security) (socket sicuri). Viene eseguita l'autenticazione reciproca; ciascuna estremità di una connessione esegue l'autenticazione dell'altra parte. Le KMA di OKM 3.1+ utilizzeranno sempre TLS 1.2 per il relativo traffico di replica peer to peer.

### 3.7.2. Hardware Security Module

Le KMA dispongono di un Hardware Security Module, ordinato separatamente. Tale Hardware Security Module, una scheda SCA (Sun Cryptographic Accelerator) 6000, era conforme alla certificazione FIPS 140-2 livello 3 e fornisce chiavi di cifratura AES (Advanced Encryption Standard) a 256 bit (questo certificato è scaduto il 31/12/2015 e non è stato rinnovato; un HSM alternativo verrà fornito nelle release successive). La scheda SCA

6000 supporta una modalità di funzionamento conforme alla certificazione FIPS 140-2 livello 3 e viene sempre utilizzata in questa modalità in OKM. Quando il cluster di OKM opera in modalità conforme alla certificazione FIPS, le chiavi di cifratura nascondono il limite di cifratura della scheda SCA 6000. La scheda SCA 6000 utilizza un generatore di numeri casuali approvato in base alla certificazione FIPS, come specificato in FIPS 186-2 DSA Random Number Generator, utilizzando SHA-1 per la creazione delle chiavi di cifratura.

Quando una KMA non è configurata con una scheda SCA 6000, la cifratura viene eseguita utilizzando il token SCF (Solaris Cryptographic Framework) PKCS#11. SCF è configurato in modalità FIPS 140 in base ai più recenti criteri di sicurezza Solaris FIPS 140-2 pubblicati.

### 3.7.3. AES Key Wrapping

Oracle Key Manager utilizza la funzionalità AES Key Wrapping (RFC 3994) con le chiavi di cifratura a 256 bit per proteggere le chiavi simmetriche quando vengono create, memorizzate sulla KMA, trasmesse agli agenti o nei file di trasferimento della chiave.

### 3.7.4. Replica delle chiavi

Quando viene inizializzata la prima KMA di un cluster di OKM, la KMA genera un grande pool di chiavi. Quando vengono aggiunte ulteriori KMA al cluster, le chiavi vengono replicate nelle nuove KMA e possono essere quindi utilizzate per la cifratura dei dati. Ciascuna KMA aggiunta al cluster genera un pool di chiavi e le replica nelle altre KMA del cluster. Tutte le KMA generano le nuove chiavi necessarie per mantenere la dimensione del pool di chiavi in modo che siano sempre disponibili chiavi per gli agenti. Per richiedere una nuova chiave, un agente contatta una KMA nel cluster e la richiede. La KMA estrae una chiave dal pool di chiavi e la assegna al gruppo di chiavi predefinito dell'agente e all'unità dati. La KMA replica quindi questi aggiornamenti al database attraverso la rete sulle altre KMA nel cluster. In seguito, l'agente può contattare un'altra KMA nel cluster per recuperare la chiave. La trasmissione nella rete di materiale correlato alla chiave in testo leggibile non è mai consentita.

### 3.7.5. Criteri di sicurezza di Solaris FIPS 140-2

In dicembre 2013, il National Institute of Standards and Technology (NIST) ha conferito il certificato di convalida FIPS 140-2 livello 1 n. 2061 per il modulo Oracle Solaris Kernel Cryptographic Framework in Solaris 11. In gennaio 2014, NIST ha conferito il certificato FIPS 140-2 livello 1 n. 2076 per Oracle Solaris Userland Cryptographic Framework con SPARC T4 e SPARC T5. La KMA di Oracle Key Manager 3.1.0 è ora basata su Solaris 11.3 che è ancora in fase di test di convalida per FIPS 140-2. Oracle Solaris Kernel Cryptographic Framework in una KMA di Oracle Key Manager 3.1.0 viene configurato in base a quanto riportato nel documento *Oracle Kernel Cryptographic Framework Security Policy*. Allo stesso modo, anche la KMA viene configurata in base a quando riportato nel documento *Oracle Solaris Userland Cryptographic Framework with SPARC T4 and SPARC T5 Security Policy*. OKM effettuerà l'aggiornamento ai più recenti criteri di sicurezza Solaris non appena diventeranno disponibili.

### 3.7.6. Aggiornamenti software

Tutti i bundle di aggiornamento del software delle KMA sono firmati in modalità digitale per evitare il caricamento di software dannoso da origini non approvate.

# 4

# Capitolo 4. Endpoint

OKM supporta diversi endpoint di cifratura, elencati di seguito.

- Unità nastro che supportano la cifratura
- Oracle Transparent Database Encryption (TDE) 11g e versioni successive
- Oracle ZFS Storage Appliance
- File system Oracle Solaris 11 ZFS

Inoltre, sono disponibili strumenti endpoint per gli sviluppatori di applicazioni oppure, nel caso di PKCS#11, per l'uso con Transparent Database Encryption (TDE) di Oracle Database.

## 4.1. Provider di Linux PKCS#11 KMS

Per gli utenti che desiderano comunicare con OKM utilizzando PKCS#11, è disponibile il provider di Linux PKCS#11 KMS. Un amministratore può scaricare il provider di Linux PKCS#11 KMS dal sito Web My Oracle Support e installarlo su un server Oracle Enterprise Linux. Il provider di Linux PKCS#11 KMS ha le stesse caratteristiche di sicurezza e supporta l'autenticazione con le appliance di Oracle Key Manager allo stesso modo degli altri agenti. Il provider di Linux PKCS#11 KMS memorizza un file di log e le informazioni sul profilo nella directory */var/opt/kms/username*. L'utente e/o l'amministratore possono gestire questo file di log manualmente o con una utility quale logrotate. Il controllo dell'accesso alla directory */var/opt/kms/username* deve essere limitato tramite le autorizzazioni appropriate. Nella directory del profilo le credenziali di autenticazione per l'agente vengono salvate in un file PKCS#12. Il file PKCS#12 è protetto con una password. Per ulteriori informazioni sul provider di Linux PKCS#11 KMS, consultare il manuale *Oracle Key Manager Administration Guide* incluso nella libreria della documentazione di Oracle Key Manager all'indirizzo:

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

## 4.2. Provider PKCS#11 KMS per Solaris

Un provider PKCS#11 KMS simile è disponibile con Solaris 10 e Solaris 11.

## 4.3. Provider di JCE KMS

Per gli sviluppatori che desiderano implementare le applicazioni client Java in grado di ottenere le chiavi da OKM, è disponibile un provider di JCE (Java Cryptographic Environment). Questo prodotto è stato integrato con diversi prodotti Oracle ed è disponibile in Oracle Technology Network.

## 4.4. Plugin OKM per Oracle Enterprise Manager

Il plugin dell'appliance Oracle Key Manager (OKM) per Oracle Enterprise Manager (OEM) Cloud Control fornisce il monitoraggio dei cluster OKM. Ciascuna KMA appartenente a un cluster viene monitorata dal plugin. Per questo strumento viene fornita una guida per la sicurezza.

# 5

# Capitolo 5. Syslog remoto

Oracle Key Manager supporta il syslog remoto. Le KMA possono essere configurate per inviare messaggi in formato RFC 3164 o RFC 5424 a un server syslog remoto tramite TCP senza cifratura o TLS (Transport Layer Security). RFC 5425 descrive l'utilizzo di TLS per fornire una connessione sicura per il trasporto dei messaggi syslog nel formato RFC 5424.

Il Security Officer può configurare una KMA per l'invio di messaggi tramite TCP senza cifratura o TLS. L'utilizzo di TLS per autenticare e cifrare la comunicazione tra la KMA e un server syslog remoto presenta un livello di sicurezza più elevato. La KMA effettua l'autenticazione del server syslog remoto richiedendo il relativo certificato e la relativa chiave pubblica. Facoltativamente, è possibile configurare il server syslog remoto per l'utilizzo dell'autenticazione reciproca. Questo tipo di autenticazione garantisce che il server syslog remoto accetterà i messaggi solo dai client autorizzati, ad esempio le KMA. Quando viene configurato per l'utilizzo dell'autenticazione reciproca, il server syslog remoto richiede un certificato alla KMA per verificarne l'identità.

# 6

# Capitolo 6. Hardware Management Pack

Oracle Key Manager supporta Oracle Hardware Management Pack (HMP) sulle KMA SPARC T7-1, Netra SPARC T4-1 e Sun Fire X4170 M2. Il prodotto HMP è un membro di Oracle Single System Management insieme a ILOM. Il Security Officer può abilitare HMP su una KMA in modo da utilizzare un agente di gestione in Solaris e abilitare il monitoraggio in banda della KMA su SNMP. Il software HMP è preinstallato ma disabilitato nella configurazione dell'agente SNMP. Di conseguenza, la porta di ascolto dell'agente SNMP non è aperta finché HMP non viene abilitato. HMP è disabilitato per impostazione predefinita.

L'abilitazione di HMP consente di ottenere quanto riportato di seguito.

- Notifica degli eventi relativi a problemi hardware prima che si manifestino come notifiche SNMP specifiche di Oracle Key Manager o come interruzione del servizio di una KMA.
- Possibilità di abilitare HMP su qualsiasi KMA supportata o su tutte le KMA supportate in un cluster di OKM.
- Possibilità di utilizzare le operazioni Get SNMP di sola lettura su SNMP MIBS nella KMA, incluso MIB-II, SUN-HW-MONITORING-MIB e SUN-STORAGE-MIB.
- Integrazione di Oracle Red Stack con Oracle Enterprise Manager tramite i receivelet e i fetchlet SNMP.

Quando si sceglie di abilitare HMP su una KMA, occorre tenere a mente le seguenti considerazioni sulla sicurezza. Quando abilitato, HMP effettua le operazioni riportate di seguito.

- Utilizza qualsiasi manager di protocollo SNMP v2c abilitato, configurato nel cluster di Oracle Key Manager. Il protocollo SNMP v2c non dispone dei miglioramenti alla sicurezza presenti nel protocollo SNMP v3.
- Abilita un agente di gestione SNMP nella KMA, consentendo l'accesso di rete in sola lettura alle informazioni SNMP MIB presenti su tale KMA.
- I rischi alla sicurezza identificati nel manuale *Guida per la sicurezza di Oracle Hardware Management Pack (HMP)* (`http://docs.oracle.com/cd/E40072_01/pdf/E39914.pdf`) sono mitigati da quanto riportato di seguito.
  - "I prodotti di gestione del sistema possono essere utilizzati per ottenere un ambiente root di boot": il potenziamento delle KMA disabilita l'accesso root agli utenti del sistema. SNMP viene configurato per l'accesso di sola lettura. Pertanto, le operazioni Put SNMP vengono rifiutate.

- "I prodotti di gestione del sistema includono potenti strumenti la cui esecuzione richiede privilegi di amministratore o root": l'accesso root alle KMA è disabilitato. Pertanto, gli utenti del sistema non possono eseguire questi strumenti.

# Appendice A

## Appendice A. Elenco di controllo per la distribuzione sicura

L'elenco di controllo di sicurezza riportato di seguito include le linee guida per la protezione del sistema di gestione delle chiavi.

1. Installare ciascuna KMA in un ambiente sicuro dal punto di vista fisico.
2. Proteggere OpenBoot PROM o BIOS in ciascuna KMA.
3. Proteggere Lights Out Manager in ciascuna KMA.
4. Definire la configurazione di suddivisione della chiave per questo cluster di Oracle Key Manager.
5. Definire l'impostazione di sblocco autonomo appropriata per ciascuna KMA.
6. Definire gli utenti di Oracle Key Manager e i ruoli ad essi associati.
7. Attenersi al principio del privilegio minimo.
    a. Concedere a ciascun utente di Oracle Key Manager solo i ruoli necessari.
8. Monitorare l'attività sul cluster di Oracle Key Manager.
    a. Individuare le cause di eventuali errori, in particolare le violazioni alla sicurezza, registrati nel log di controllo di Oracle Key Manager.
9. Eseguire il backup della sicurezza di base durante la definizione iniziale e a ogni modifica della configurazione di suddivisione della chiave.
10. Eseguire regolarmente i backup di Oracle Key Manager.
11. Memorizzare i file di backup della sicurezza di base e di Oracle Key Manager in una posizione sicura.

# Appendice B

## Appendice B. Riferimenti

- Documentazione per l'utente di Oracle Key Manager

  http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto
- *Oracle Enterprise Manager System Monitoring Plug-in for Oracle Key Manager Security Guide*
- *Oracle Key Manager Installation and Service Manual* (solo interno)
- *Oracle Key Manager Overview*

  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*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf
- Documentazione di Oracle Integrated Lights Out Manager (ILOM)

  http://docs.oracle.com/cd/E37444_01/
- Documentazione relativa al server SPARC T7-1 https://docs.oracle.com/cd/E54976_01/
- Documentazione relativa al server Netra SPARC T4-1

  http://docs.oracle.com/cd/E23203_01/
- Documentazione di Oracle Hardware Management Pack
  - Libreria della documentazione di Oracle Hardware Management Pack

    http://docs.oracle.com/cd/E20451_01/
  - Oracle Single System Management

    http://www.oracle.com/technetwork/server-storage/servermgmt/overview/index.html
- Documentazione NIST:
  - *National Institute of Standards and Technology Special Publication 800-60 Volume I Revision 1*

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

- Documentazione sui criteri di sicurezza per i prodotti Oracle:
  - *Oracle Solaris Kernel Cryptographic Framework Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2061.pdf
  - *Oracle Solaris Kernel Cryptographic Framework with SPARC T4 and T5 Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2060.pdf
  - *Sun Cryptographic Accelerator 6000 FIPS 140-2 Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Oracle StorageTek T10000D Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Oracle StorageTek T10000C Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Oracle StorageTek T10000B Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Oracle StorageTek T10000A Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf
  - *Oracle StorageTek T9480D Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf
- Certificati di convalida FIPS per i prodotti Oracle:
  - Sun Crypto Accelerator 6000 - Certificato n. 1026 (scaduto)

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1026.pdf