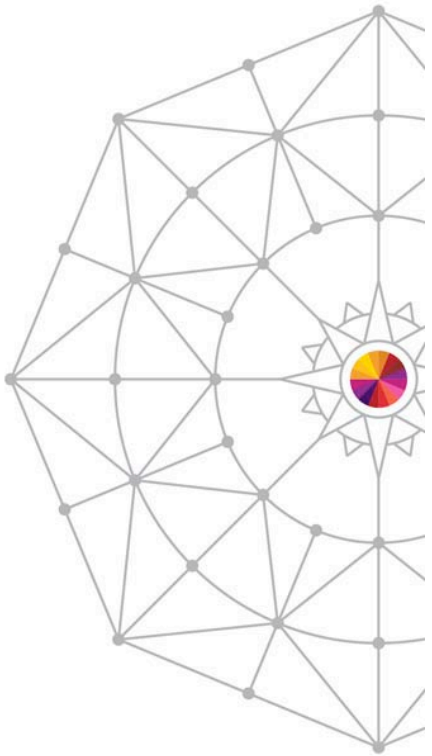
Securing Your Data at Rest With Encryption

Session 15913

Steve Aaker

Sr. Principal Product Strategy Manager



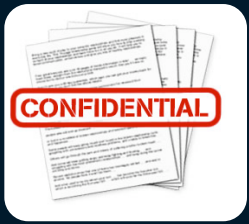
#SHAREorg

SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.

SHARE in Pittsburgh 2014

Why encryption?

Confidential Data



- Intellectual Property
- Personally Identifiable Information (PII)
- Company confidential or private information

Why Encryption

- Regulatory compliance
- Increasing mobility of sensitive information
- Protection from Data Breach, Brand Damage, Fines

Data Security Regulations

- Payment Card Industry Data Security Standards
- California Senate Bill 1386

Data Loss Happens

Data Loss Happens

*Data from Open Security Foundation Data Loss DB, http://datalossdb.org Also see: http://www.privacyrights.org

67% Records breached from servers

76% Breached using weak or stolen credentials

69% Discovered by an external party

97% Preventable with basic controls

Impact of Security Breaches

#1 Direct Losses	Customer Data	Company Data	Loss of
	Customers		
	Employee Data	Digital Assets	Fines
#2 Indirect Losses	Loss of sales/market share	Competitive Disadvantage	
	Negative Brand Impact	Loss of Customer Trust	
#3 Ongoing Expenses	Corruption of Data	Notification Costs	
	Recovery Costs	Continuity Costs	
#4 Legal Exposure	Regulations Violation	Executive Liabilities	
	Disclosure Requirements	Lawsuits / Settlements	

Data Security Drivers

PCI DSS v2.0
October 2010

3.5.2	Store cryptographic keys securely in the fewest possible locations and forms
3.6.4	Verify that key-management procedures are implemented for periodic key changes

And more!

- Payment Card Industry Data Security Standards (PCI-DSS)
  - 12 requirements to meet security control objectives
- California Senate Bill 1386
  - Requires notification to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person
  - 40+ states have adopted similar legislation
- HIPAA Security Rule and HITECH Act
  - Security Rule requires appropriate safeguards to ensure the confidentiality, integrity, and security of electronic protected health information
  - HITECH Act requires HIPAA covered entities to provide notification following a breach of unsecured protected health information
- Sarbanes-Oxley, EU Data Protection Directive, Japan's Personal Information Protection Law…and many others

Would you risk 60% of your business?

"20% of people who were notified of a privacy breach involving their data immediately terminated their accounts with the firm suffering the data breach. 40% more were considering termination."

* Consumers' Report Card on Data Breach Notification, Ponemon Institute LLC

Encryption solves the problem

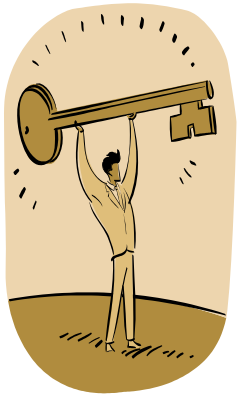
- Data encryption uses algorithms to transform plaintext into cyphertext, a form that is non-readable to unauthorized parties
- Customer or regulatory body notification is not required as information is not accessible to unauthorized parties
- Provides protection from both off-site and on-premise information loss
- Enables secure shipment of data
- Supports time-based data expiration and secure data disposal

It's All About the Keys

- Encryption keys determine the functional output of a given encryption algorithm
- Keys convert the data into cyphertext and are used to convert the data back to a readable form (cleartext)
- Keys must be 'strong'
  - Randomly and securely generated
  - Securely managed
  - The longer the key length, the more secure the encryption method
- AES 256 is most secure encryption standard available today
  - Symmetric, block cipher-based method
  - 256 bit key length
- Lose the keys and you lose the data!

Key Management Best Practices

- Keys must be always available
  - Redundant servers with Backup/recovery
- Keys must be secure
  - Proper access control: quorum, role-based, separation of duty for administration
  - Hardened solution with FIPS certification
- Key management system must scale economically
  - Easy-to-use interface with Simple client enrollment & setup
- Key management system must be openly architected
  - Wide range of environments and client-end points, Standard protocols
- Key management system must offer auditing/reporting tools
  - Key lifecycle, policy compliance, alerts



Data Encryption Models

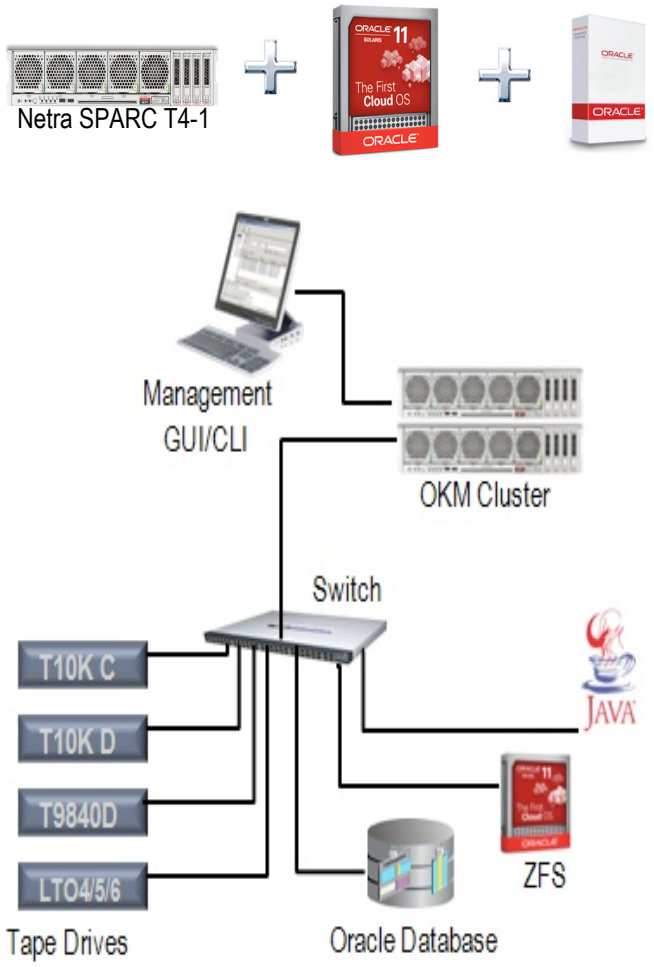
	Application/Server-based	In-band/Network-based	Storage-Based
Definition	Data encrypted at data creation and/or as the application processes the data	Data encrypted by switch or appliance as it travels across the network	Data encrypted by storage device (disk or tape)
Sample Products	• IBM Tivoli Storage Manager • Oracle 11gR2 Transparent Data Encryption	• Cisco MDS 9000 Storage Media Encryption (SME) • NetApp / Decru DataFort (now EOL)	• Oracle Sun S6780 disk array • Oracle StorageTek T10000C tape drive
Pros	✔Data can encrypted throughout its lifecycle ✔Data is secure wherever it travels in the environment	✔Works with any storage device (including legacy devices) ✔Application/OS/server agnostic ✔Quick implementation	✔Application/OS/server agnostic ✔Compression/de-dupe enabled ✔No performance degradation ✔Economic scaling
Cons	✘Processor-intensive ✘Must compress before encrypting ✘Disables storage compression and de-dupe ✘Application dependency for life of the data	✘Expensive to scale ✘Easy to bypass (poor security) ✘Disables storage compression and de-dupe ✘Obsolescence of early wave of appliances	✘Storage device-specific ✘Does not address upstream data security

Encryption Key Management Models

	Key Management Appliance	Software-Based Key Manager
Definition	Dedicated security server / network	Application that can be co-hosted with other applications
Sample Products	• Oracle Key Manager (OKM) • RSA Key Manager for the Data Center	• NetApp Lifetime Key Manager (LKM) • IBM Tivoli Lifetime Key Manager (TLKM)
Pros	✔Increased security ✔Dedicated / isolated hardware ✔Resistant to tampering / hacking ✔Performance and availability ✔Simplified deployment	✔Can be integrated with backup application ✔No hardware investment
Cons	✘ Dedicated hardware	✘ Complex installation and setup ✘ Less secure ✘ Potential for interoperability issues ✘ Risk of CPU resource contention and performance issues

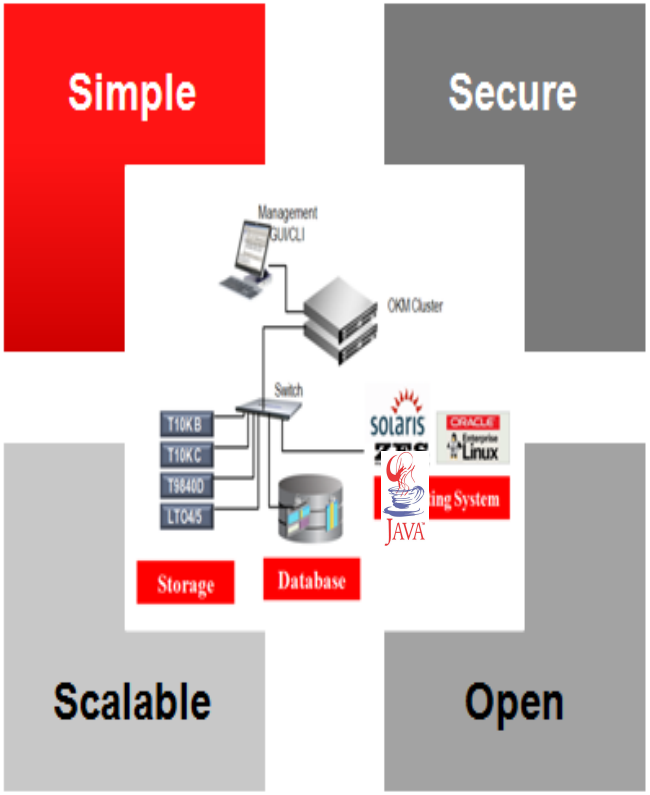
Oracle Key Manager 3 (OKM 3) Overview

- Key management appliance (KMA)
  - Solaris 11 on Netra SPARC T4-1 server
  - Oracle key management software
  - Crypto Accelerator Card (optional)
- OKM management server
  - OKM management GUI
- OKM cluster
  - 2 to 20 KMAs, connected via Ethernet network
- Attach Kits
  - Switches and cabling
- Encryption end-points
  - Java applications
  - Oracle Database & ZFS
  - Tape drives & libraries



Oracle Key Manager 3

- Simple to Install and Operate
  - Automated, policy-driven system
  - Server, O/S, application neutral
- Secure
  - Strongest encryption (AES-256) end-to-end
  - Strong key protection mechanisms
  - Conforms to federal security certifications (FIPS)
- Scales Economically
  - Supports large sites & multiple storage technologies
  - Easily adds more key management appliances, sites and drives as needed



FIPS 140-2 Level 3

- Supporting Federal Information Processing Standards (FIPS 140)
- Level 1 = No security mechanism but uses approved algorithm
  - Oracle LTO tape drives
- Level 2 = Temper evident, role-based authentication
  - Select Oracle StorageTek Enterprise tape drives
- Level 3 = Tamper detection and response (i.e., zeroizes all cleartext)
  - SCA 6000 card

Tape Drives - Enterprise

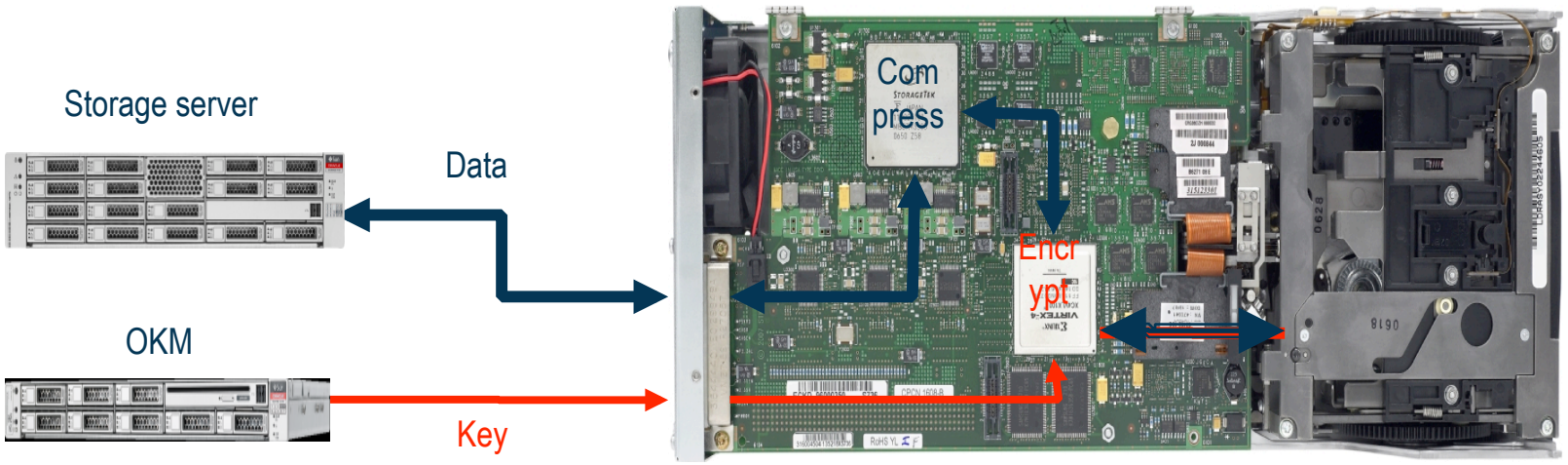
- T10K A, B, C, D & T9840D
  - All drives shipped crypto-ready
  - FIPS 140-2 Certified
- T10000D:
  - 8.5TB native capacity, 250MB/s native transfer rate
  - Re-use media from T10000 A, B, and C
- T9840D:
  - 75GB capacity, 30MB/s transfer rate
  - Re-use media from T9840A/B/C
- No performance impact with encryption
  - Drive-level compression maintained

Tape Drives - Midrange

- LTO4
  - 800GB capacity, 120MB/s transfer rate
  - OKM communication is supported by interface board mounted on the library tray (“Belisarius” or “Dionne” card)
- LTO5
  - 1.5TB capacity, 140MB/s transfer rate
  - HP LTO5 has Dionne card built in, IBM LTO5 requires a Belisarius card
- LTO6
  - 2.5TB capacity, 160MB/s transfer rate
  - HP LTO6 has Dionne card built in, IBM LTO6 requires a Belisarius card
- No performance impact with encryption; Drive-level compression maintained

Separate Key and Data Paths

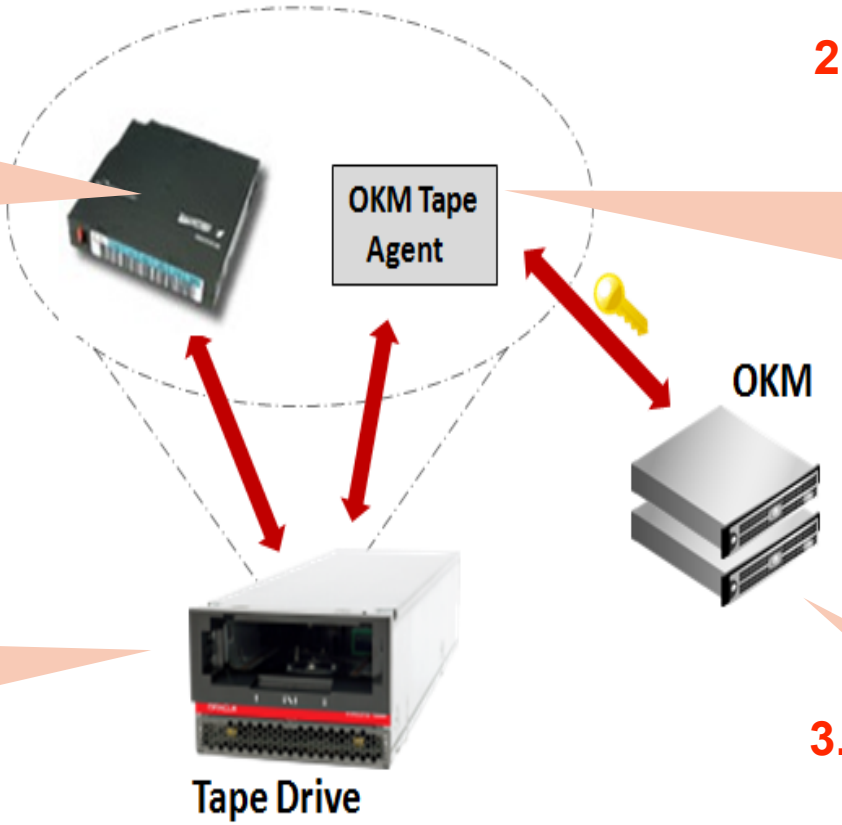
- Key communication over dedicated Ethernet port
- Drive compresses data before encrypting
- Non-disruptive
  - Coexist with non-encrypting devices
  - No changes/awareness required in storage server and data network



How OKM Works

1. new tape cartridge is mounted, drive sends a request to create a new encryption key

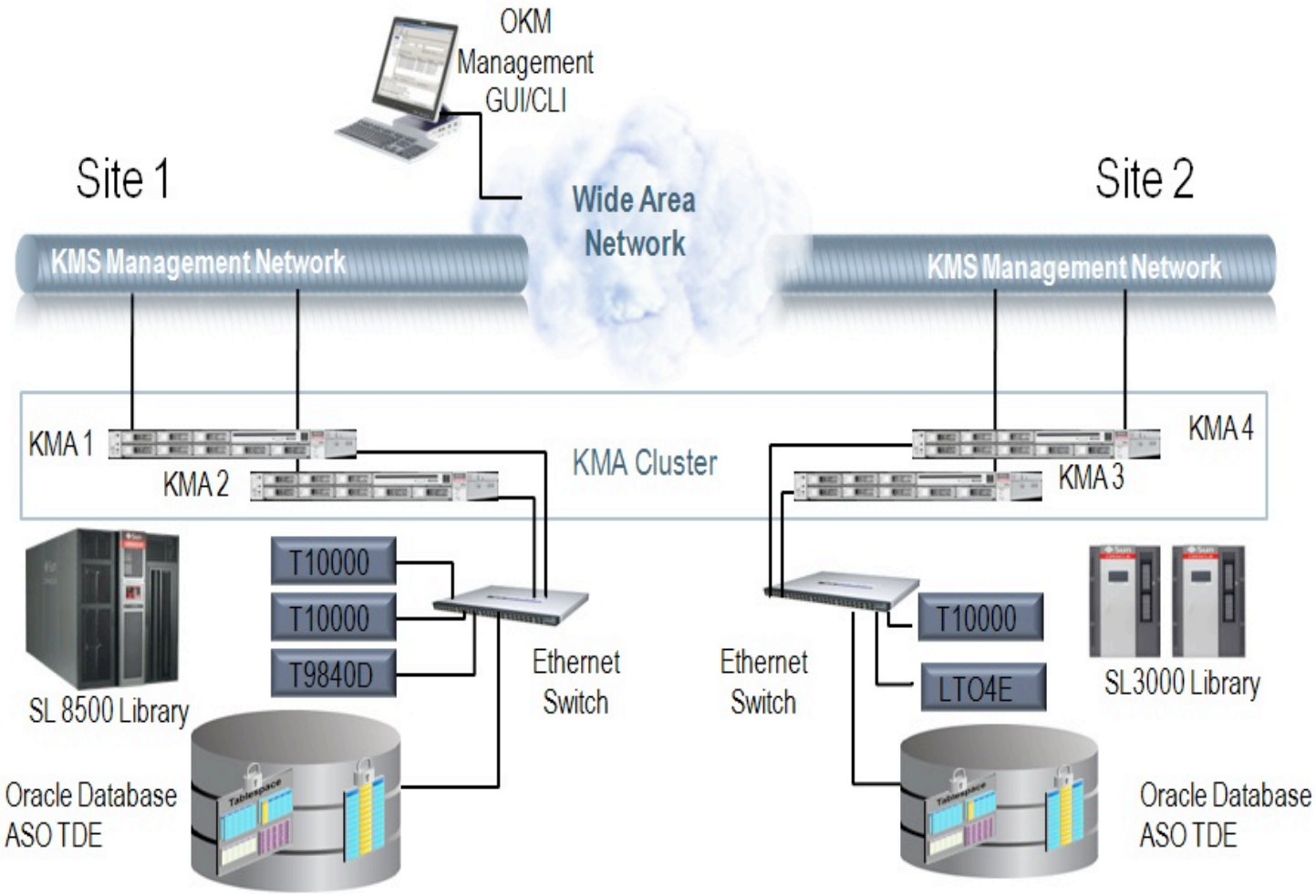
2. Agent interacts with OKM to generate and retrieve keys on behalf of tape drive



3. OKM generates and forwards the key to OKM agent

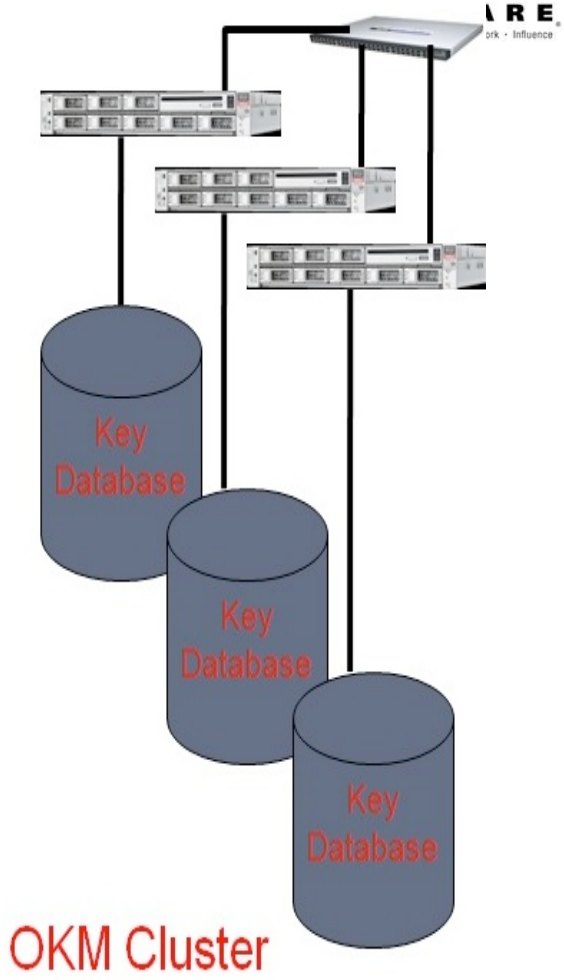
4. drive caches the encryption key until tape unload, encrypts data with the key

High Level Architecture



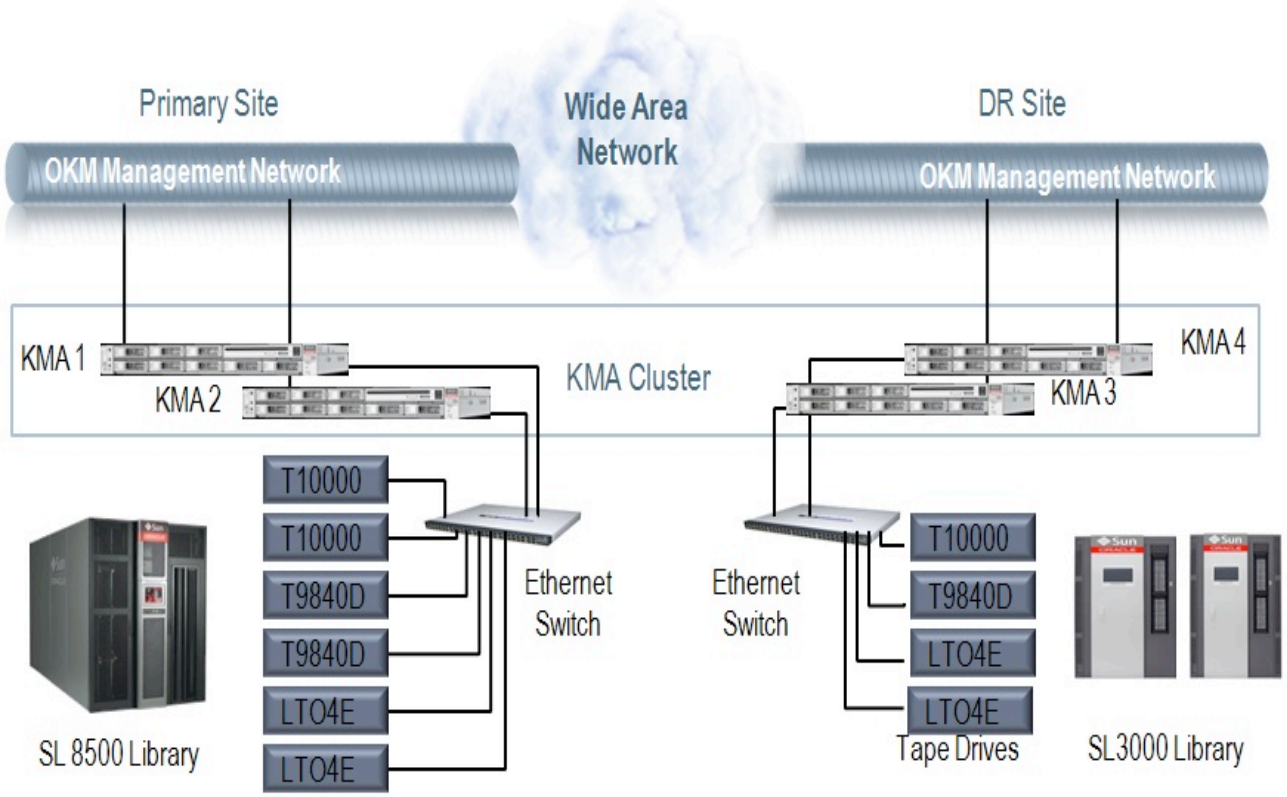
Mirroring

- Key, policy and administration changes made in single KMA are automatically propagated to all parts of the cluster
- Key database is replicated across entire cluster
  - Robust fault tolerance
- Any KMA can supply keys to any device in its' cluster



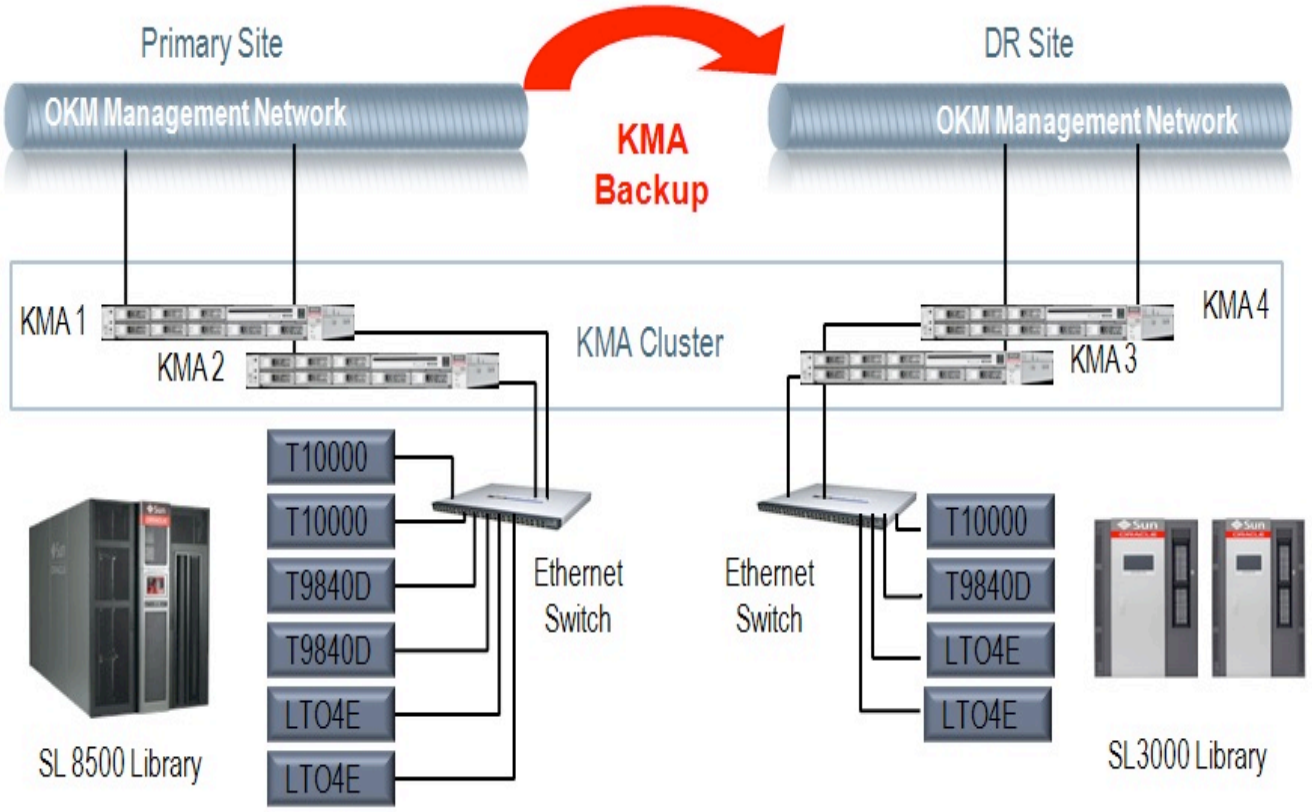
Disaster Recovery – Live DR Site

- Pair of KMAs at DR site included in the production cluster
- DR site KMAs always have latest copy of all keys



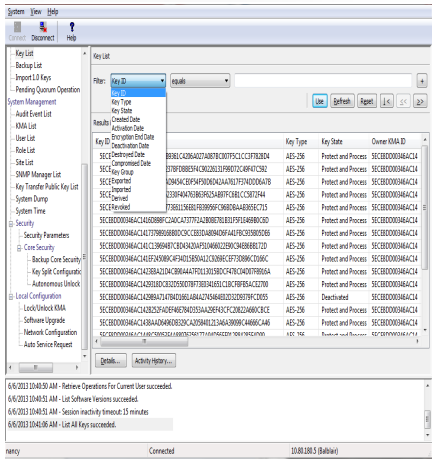
Disaster Recovery – Backup DR

- Use DR provider's KMAs, restored from latest backup
- Avoids dedicated DR KMAs and WAN link



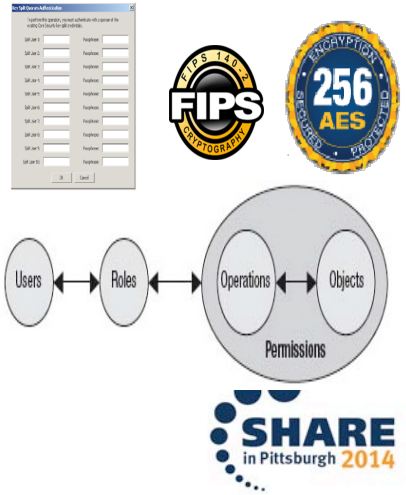
Simple

- Easy to install and set-up
- Intuitive User Interface and CLI
- Unattended, policy-driven appliance system
  - Lights-out system
  - No manual intervention required once properly installed
  - No administration required for appliance
- Fully automated
  - Automatic key generation & retrieval
  - Automatic key replication across cluster
  - Automatic policies and settings replication across cluster
  - Automated event logging



Secure

- Dedicated key management and key transport (service) networks
- Hardened solution; No other applications, patches/upgrades and/or administration settings to compromise security
- Conforms to stringent federal security certifications (FIPS 140-2 level 3)
- Strong key protection mechanisms
- Strong encryption (AES-256) end-to-end
- Role & access control
- Quorum functionality



Scalable

- Scales economically
  - Supports multiple sites/devices concurrently
  - Tested with up to 2,000 drives and 1,000,000 keys
- Transparent/non-disruptive growth
  - Add more OKM appliances, sites and drives as needed
- Flexible management
  - Supports managing multi-site installation from any single location
  - Supports multiple user roles

Oracle's Storage Portfolio

Data Security is Table Stakes for Long-term Storage

Engineered Systems

Exadata Exalogic SPARC SuperCluster Big Data Appliance

NAS Storage

ZFS Storage Appliances

SAN Storage

2500-M2 Pillar Axiom 600

Tape and Virtual Tape

Cloud Storage

Deployment Options: Private, Public, Hybrid

Services: IaaS, PaaS, SaaS

Consumption Options: Build, Manage, Subscribe

Storage Software

Storage Management: OEM, ASM, Storage Analytics, CAM, ACSLS, ELS
Automated Tiering: Partitions, SAM QFS, Hybrid Storage Pools, VSM
Data Reduction: 11g ACO, HCC, RMAN, ZFS Storage Appliance Dedup/Comp
Data Protection: Data Guard, RMAN, OSB, ZFS Storage Appliance Snap/Rep, MaxRep
Security/Encryption: ASO, Oracle Key Manager, Disk/Tape Encryption

Learn More About Storage and Virtual Tape

Monday

- 4:15pm
  Securing Your Data at Rest With Encryption
  Steve Aaker, Room 305 (Session 15913)

Tuesday

- **7:00pm Free Wine at the Oracle Booth!**

Learn More About Storage and Virtual Tape

Wednesday

- 8:30am
  Modern Long-Term Data Storage Realities: Tape, Disk, or the Cloud?
  Kevin Horn, Room 318, Session 15916
- 10:00am
  Announcing Oracle's New StorageTek T10000D Tape Drive
  Record-Breaking Capacity and Performance to Help You Consolidate, Simplify, and Save Money
  Kevin Horn, Room 302, Session 16246
- 4:15pm
  Ensure Your Data is Available When You Need It With Proactive Monitoring
  Steve Aaker, Room 305, Session 15915

Learn More About Storage and Virtual Tape

Thursday

- 10:00am
  How to Ensure Your Disaster Recovery Plan Really Works
  Damon Clark, Room 405, Session 15907
- 1:30pm
  Revolutionary New Storage Architectures Designed to Meet Mainframe High Availability Requirements
  Damon Clark, Room 318, Session 15917

Thank you!