Best Practices

OpenManage Secure Enterprise Key Manager- Best Practices Guide

This whitepaper outlines some recommended best practice guidelines for the use of Secure Enterprise Key Manager in Dell EMC PowerEdge servers.

March 2019

Document ID

Revisions

Date	Description
March 2019	Initial release

Acknowledgements

This paper was produced by the following:

Author: Caroline Covington, Lisa Scheuplein and Michael Linane

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Table of contents

Executive summary

The purpose of this document is to provide information about Dell PowerEdge Data At Rest Encryption offerings and guidance on the Best Practices for using Secure Enterprise Key Manager.

1 Overview

The Dell Technologies whitepaper "*Cyber Resilient Security in 14th generation of Dell EMC PowerEdge servers*" describes the numerous threats and the Dell Technologies design and tools that are used to address them. Table 1 describes how Dell Technologies addresses common threat vectors.

Table 1 Common Threat Vectors

Security layer	Threat vector	Dell Technologies Solution	Addressed by Local Key Manager	Addressed by Secure Enterprise Key Manager
Physical server	Server tampering	Physical deterrents including…	Yes	Yes
	Server theft	Secure Enterprise Key Manager protects your data when the server is removed from the network, the keys required to unlock the drives will not be available from the central key server.	No	Yes
Firmware and software	Firmware corruption, malware injection	• Silicon-based Root of Trust; Intel Boot Guard; AMD Secure Root-of-Trust • Cryptographically signed and validated firmware;	Yes	Yes
	Software	Updates provided by Dell Technologies	Yes	Yes
Attestation trust features	Server identity spoofing	TPM, TXT, Chain of Trust	Yes	Yes
Server management	Rogue configuration and updates, unauthorized open-port attacks	iDRAC9	Yes	Yes

Table 2 Server Environment Layers

Security layer	Threat vector	Dell Technologies Solution
Data	**Data breach**	• **SED (Self-Encrypting Drives) – FIPS or Opal/TCG** • **ISE-only (Instant Secure Erase) drives Secure Key Management** • **Secure User Authentication**
Supply Chain Integrity	**Counterfeit components**	**ISO9001 certification for all global server manufacturing sites**
	Malware Threats	**Security measures implemented as part of Secure Development Lifecycle (SDL) process**
Supply Chain Security	**Physical security in Manufacturing sites**	**Transported Asset Protection Association (TAPA) facility security requirements**
	Theft and tempering during transport	**Customs-Trade Partnership Against Terrorism (C-TPAT)**

To combat data breach, Dell Technologies offer the Secure Enterprise Key Manager that uses the Key Management Interoperability Protocol (KMIP) standard to implement. Secure Enterprise Key Manager enables a centralized key manager to store and securely deliver keys that lock/unlock drives to authenticated servers. Combined with Self-Encrypting Drives (SEDs), Secure Enterprise Key Manager provides greater security from physical threat/theft of a PowerEdge server.

2 Reference Architecture

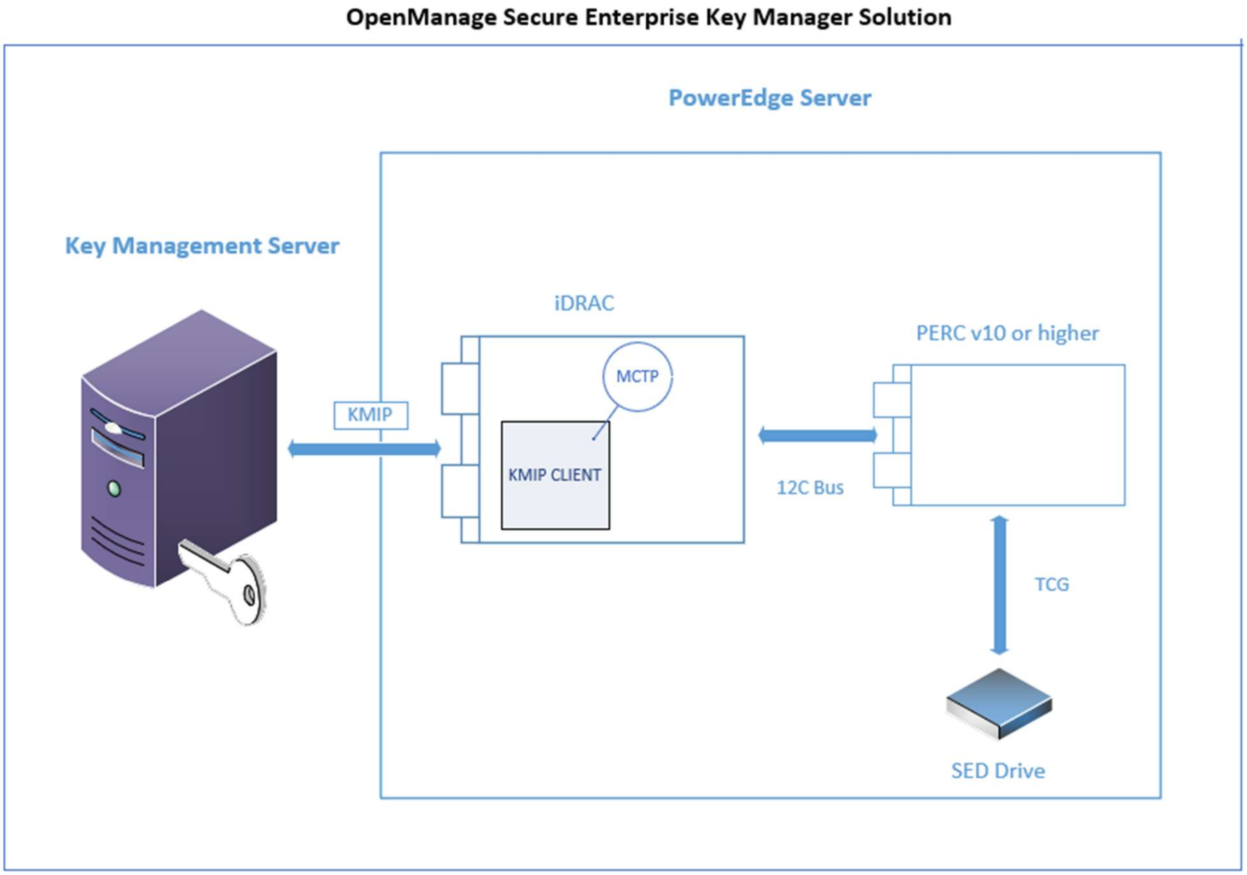


Figure 1 Secure Enterprise Key Manager

2.1 Definitions

- D@RE – Data At Rest Encryption
- Locking - Cryptographically locking
- LKM – Local Key Management
- PERC – PowerEdge RAID Controller
- iDRAC – Integrated Dell Remote Access Controller
- KMIP – Key Management Interoperability Protocol
- SED – Self-Encrypting Drive
- FIPS – Federal Information Processing Standard
- ISE – Instant Secure Erase
- SAS – Serial Attached SCSI
- SATA – Serial AT Attachment

- HDD – Hard Disk Drive
- SSD – Solid State Drive
- HA – High Availability (cluster)

3 Dell PowerEdge D@RE Offerings

Keys to lock and unlock drives must be managed. PowerEdge provides two optional mechanisms for this:

- LKM – managed by the PERC
- Secure Enterprise Key Manager – Subject of this paper, managed by iDRAC

3.1 How to Choose Between LKM and Secure Enterprise Key Manager

The decision to use LKM or Secure Enterprise Key Manager can be based on the following criteria:

- Budget
  - LKM is a standard feature of PERC. Therefore, there is no additional licensing or hardware required.
  - Secure Enterprise Key Manager requires additional licensing and also an external key store server (with associated licensing).
- Threat Vectors
  - One of the primary Threat Vectors addressed by Secure Enterprise Key Manager is server theft (see While LKM protects data, if a drive or entire server is removed the data would still be accessible. This is because the key is stored on the LKM PERC).
  - With Secure Enterprise Key Manager, server possession does not allow access to data.
- Day-to-day administration
  - LKM - Customers must maintain PERC passwords in the event of PERC failure and replacement.
  - Secure Enterprise Key Manager– Keys are stored in a central repository (KMIP server) that could be at a different physical location than the nodes which contain the drives. All that is required monitoring the health of KMIP server.
- Secure Enterprise Key Manager Integration across several Dell Solutions
  - Secure Enterprise Key Manager has the ability to integrate PowerEdge with a Key Management Server that is also managing keys for other Dell EMC products -
    - Avamar Backup and Recovery
    - Data Domain
    - Disk Library for Mainframe (DLm)
    - Elastic Cloud Storage (ECS)
    - ML3 Tape Library
    - SC Series Storage (formerly Compellent)
    - Unity Storage
    - VMAX Storage (formerly Symmetrix)
    - VxRail VMware Hyper-Converged Appliance
    - XC Series Hyper-Converged Appliance

3.2 Compliance

Compliance and governance requirements, whether they be government mandated, industry standards, or corporate policy, contain multiple requirements regarding encrypting data at rest and protection of the corresponding cryptographic keys. Evaluation of compliance requirements should always be done to determine if LKM is sufficient or if the features (high assurance key protection, centralize audit and reporting, robust access control, etc.) offered through use of Secure Enterprise Key Manager with a Key Management Servermeets compliance requirements.

–

–

4 Components of Secure Enterprise Key Manager

4.1 Secure Enterprise Key Manager Server

The Secure Enterprise Key Manager server acts as the key store and resides on the management network. Initial release of Secure Enterprise Key Manager was validated with Gemalto and SafeNet AT KeySecure.

This solution is compatible with the following PowerEdge Servers:

R640

R740, R740XD

R840

R940, R940 XA

R540

R440

R6415

R7415, R7425

R6515

R7515

T440

T640

C6420

M640, MX740C, MX840C

4.2 iDRAC

- For Secure Enterprise Key Manager, Dell Technologies embedded a KMIP-compliant client into iDRAC for communication with the KMIP server.
- iDRAC is the control center of Dell Technologies Secure Enterprise Key Manager. iDRAC provides authentication with the KMIP server, enable/disable options, and key rotation.
- PERC firmware version must be 10.3 or higher.

4.3 PERC H740, H740P

- Must be v10.3 or higher.

4.4 Storage devices (HDD/SSD)

Dell Technologies supports industry-standard storage devices in PowerEdge Data At Rest applications.

Table 3 – Storage Devices Supported by Secure Enterprise Key Manager

Storage Device Type	**Supported by Secure Enterprise Key Manager**	**Supported by LKM**
ISE	No	Yes
SED	Yes	Yes
FIPS	Yes	Yes

- ISE

  All Dell drives are ISE enabled and have an encryption engine. All data is automatically encrypted on write and decrypted on read. All data on the media is encrypted but is not encrypted at the interface.

  This architecture is used to better enable repurposing drives without elaborate procedures. Simply issue the ISE command and any data on the drive is no longer recoverable.

  ISE drives cannot be secured. Secure Enterprise Key Manager ignores them and cannot be part of a secure raid virtual disk.

- SED

  Additionally, SED drives add the ability to secure the data requiring a key to decrypt the data at the interface. Like ISE drives, the data on the media is always encrypted but SED also enables auto-locking to secure active data.

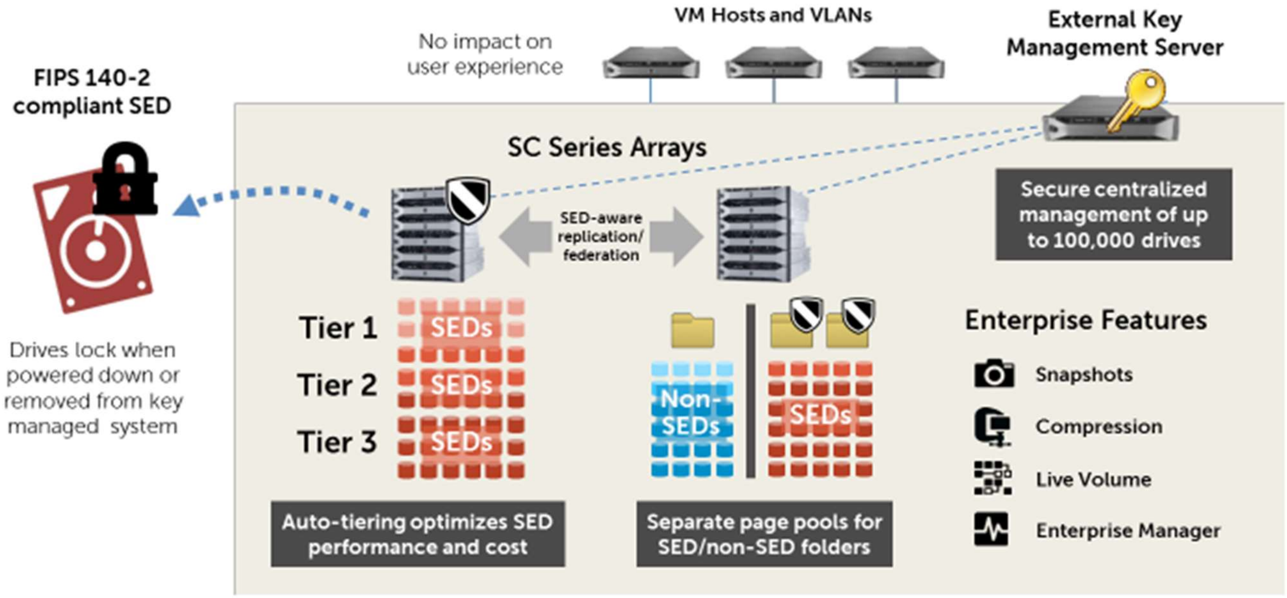
  SED can be part of a Secure Enterprise Key Manager solution.

- FIPS

  FIPS extends SED to include the Federal certification, tamper-proof labels, etc.

  FIPS drives can also be part of the Secure Enterprise Key Manager solution.

Components of Secure Enterprise Key Manager


VM Hosts and VLANs
No impact on user experience
External Key Management Server
FIPS 140-2 compliant SED
SC Series Arrays
SED-aware replication/ federation
Secure centralized management of up to 100,000 drives
Drives lock when powered down or removed from key managed system
Tier 1
Tier 2
Tier 3
SEDs
SEDs
SEDs
Non-SEDs
SEDs
Enterprise Features
Snapshots
Compression
Live Volume
Enterprise Manager
Auto-tiering optimizes SED performance and cost
Separate page pools for SED/non-SED folders

5 Best Practices for Secure Enterprise Key Manager Implementation

5.1 Protect and Ensure your Key Availability

Without associated lock/unlock key(s), data is protected and will not be accessible. Therefore, use of a high-availability, redundant KMIP server configuration is strongly recommended. With a redundant KMIP server, should one KMIP server be down and a node needs to retrieve keys to unlock drives, keys would still be available from another in its cluster. Without this redundancy, if a KMIP server is not available, the requesting node will not be able to unlock drives to access data.

Additional best practices, such as regular backing up of the keys from the key server to another server/site/locale, is also recommended. This would enable recovery in the event of loss of the key server/cluster/site.

Like equipment in the data center, best practices for monitoring the health of the KMIP server and keeping it current are also recommended to prevent unexpected downtime (and associated potential data unavailability) of the key server.

5.2 Other Considerations

5.2.1 Grouping

Grouping is done at KeySecure. Segregating of server/drive keys per department/project might be beneficial to prevent unwanted moving of physical drives (and associated data) to a different physical location that would still provide access of the data. If your application does not segregate keys, the central KMIP server can unlock a drive no matter where it is physically located within the network.

To determine if this would benefit your organization, consider your internal data sharing policies across projects and groups.

For example, consider an environment where data related to specific projects must be kept private from a different project. In this case, a drive that is removed from the lab of one project should not be unlocked if relocated to a different lab on the same network. By setting up a key grouping for that private project, a drive that is removed from one lab would remain locked if placed into a different node in a different lab.

5.2.2 Key Rotation

It is important to limit the amount of data encrypted with a single key because using the same key over a long duration increases the chances of the key to be compromised. Key rotation reduces the risk of key compromise and limits the amount of time a stolen drive would be accessible.

Once a key is assigned from the central KMIP server, the drives that are attached to that PERC will remain unlocked until the next reboot because the key remains unchanged. If you are concerned about the physical drive node being stolen from your network while the node retains powered, a mitigation is to periodically change the keys. This would lock a drive if power remains but becomes disconnected from your network. A new key would not be available, and the drive would lock and become inaccessible.

Key rotation is initiated by iDRAC. Scripting can be also used to schedule the rotation.

5.2.3 Secure Enterprise Key Manager to iDRAC Authentication

iDRAC and Gemalto/SafeNet AT KeySecure. Secure Enterprise Key Manager servers support varying levels of authentication for communication.

- None
- User ID
- PW
- Certificates
- IP

The more authentication that is utilized, the more trustworthy the communication and resistance to spoofing.

5.2.4 Cryptographic Erase

Cryptographic Erase is a NIST approved technique to sanitize media. By using capabilities of the Key Management Server to erase the lock/unlock key for a drive, the encrypted data on the drive is unrecoverable, effectively sanitizing the data. Cryptographic Erase can be used for normal reprovisioning of drives, active data sanitization in hostile situations, or in response to a stolen drive or server.

6 Other References

6.1.1 NIST Guidelines for Media Sanitization (Cryptographic Erase) - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

6.1.2 SafeNet Best Practices for Cryptographic Key Management white paper - www.safenetat.com/best-practices-for-key-management