PERC Self-Encrypting Drive (SED) Support and FAQs

Tech Note by:
Jeffrey Foss

SUMMARY

This tech note is designed to educate and inform about Self Encrypting Drive (SED) support in PERC and answer frequently asked questions.

Anyone who intends to use SEDs in their system along with a PERC card with enabled security can benefit from this information.

High level information is provided in this document. For more details on SED drives please see the *Additional Information* links at the end of this tech note.

Before jumping into the topic, level-setting on some acronyms can be helpful:

TERM	Description
PERC	PowerEdge RAID Controller
VD	PERC Virtual Disk
eHBA mode	Enhanced HBA mode
LKM	PERC Local Key Management
SED	Self-Encrypting Drive
TCG	Trusted Computing Group
AK or KEK	Authentication Key or Key Encryption Key
DEK or MEK	Data Encryption Key or Media Encryption Key
FIPS	Federal Information Processing Standardization
ISE	Instant Scramble Erase
IDRAC	Integrated Dell Remote Access Controller
HII	Human Interface Infrastructure Configuration Utility
PERCcli	PERC utility for managing storage controllers

Self-Encrypting Drives

Self-Encrypting Disks (SED) provide protection of data against physical loss or theft of disks only. Protection is achieved by requiring a key to unlock the drives before any data can be retrieved. The data on disks that support the SED feature is always encrypted and protection from theft is only available if the disks are secured.

NOTE: ISE capable drives have the same underlying encryption hardware that SED drives do, but they do not allow the drives to be secured.

Threat Models Covered by SED Drives

Secured SED protect against theft of the drives only and the drives are only locked after power is lost.

Support for SED drives on PERC (Local Key Management - LKM)

PERC controllers support the use of SED drives in all RAID levels. Virtual Disks can be secured when they are created or after a VD is already in use. All disks in the array must support SED to be secured. To enable the securing of Virtual Disks, security must also be enabled on the controller, as shown in Figure 1 below. See the PERC User Guide for detailed instructions for enabling security. A secured VD cannot be unsecured without erasing all data on the drive.

The user will be prompted to input and then confirm a passphrase, as shown in Figure 2 below. The user-provided passphrase is hashed and stored locally on the PERC controller. The key sent to the drive is derived from this hashed value.

If a secured disk is detected during boot or discovery of a new drive, the PERC controller will use the stored key to unlock the drive to allow data access. In the case of foreign configurations or drive migration where the drive requires a different passphrase than the one stored locally, the user will be required to enter the passphrase for that drive, after which the drive will be re-keyed with the local key.

Support for SED drives on PERC (OpenManage Secure Enterprise Key Management)

PERC 10 FW 50.5.1-2633 added support for enterprise key management. Secure enterprise key management mode has the same support for drives as LKM and secured Virtual Disks are also managed the same way as in LKM. The major difference between LKM and secure enterprise key management behavior is that the key used to unlock the drives is stored on an external server instead of the local controller. This enables PERC to protect the drives data from theft of an entire system. During boot, PERC will request a key from IDRAC. IDRAC will then communicate with the key management server and provide the key to the PERC. When a drive locked with secure enterprise key management is inserted during run time, the PERC will again request and wait for a key from IDRAC to unlock the drive. Please see latest PERC and IDRAC user guides for more details on the OpenManage Secure Enterprise Key Management.

PERC Security Management Applications

The PERC LKM controller passphrase can be managed from:

- HII
- PERCcli
- Open Manage
- IDRAC

The PERC enterprise key management controller passphrase can be managed from:

- IDRAC

NOTE: Enterprise key management mode must be managed from IDRAC. HII, PERCcli, & Open Manage only allow the user to disable the security mode if no secured Virtual Disks are present.

Threat Models Covered by PERC

PERC LKM protects against theft of drives. If an entire system is stolen, the key that is used to unlock the drive is still stored on the PERC controller allowing the drives to be unlocked at next boot.

PERC enterprise key management protects both theft of drives and theft of entire servers. If an entire system is stolen the key required to unlock the drives is located on a different physical server and the data will not be accessible until IDRAC is able to communicate with the key server and unlock the drives. Please see latest PERC and IDRAC user guides for more details.

Supported Security Protocol

PERC supports TCG Enterprise SSC for enabling secured encryption on SED Drives. See trustedcomputinggroup.org for more information. DELL's Enterprise drives that support SED follow this standard.

PERC 10 SED Support with Non-RAID disks

PERC 10 FW 50.5.0-1750 added support for eHBA mode allowing RAID and Non-RAID disks in the system. Under eHBA mode, both VDs and Non-RAID disks can be secured. See the latest PERC 10 User Guide for more information about eHBA mode and securing Non-RAID disks.

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries

LKM Passphrase Management in HII

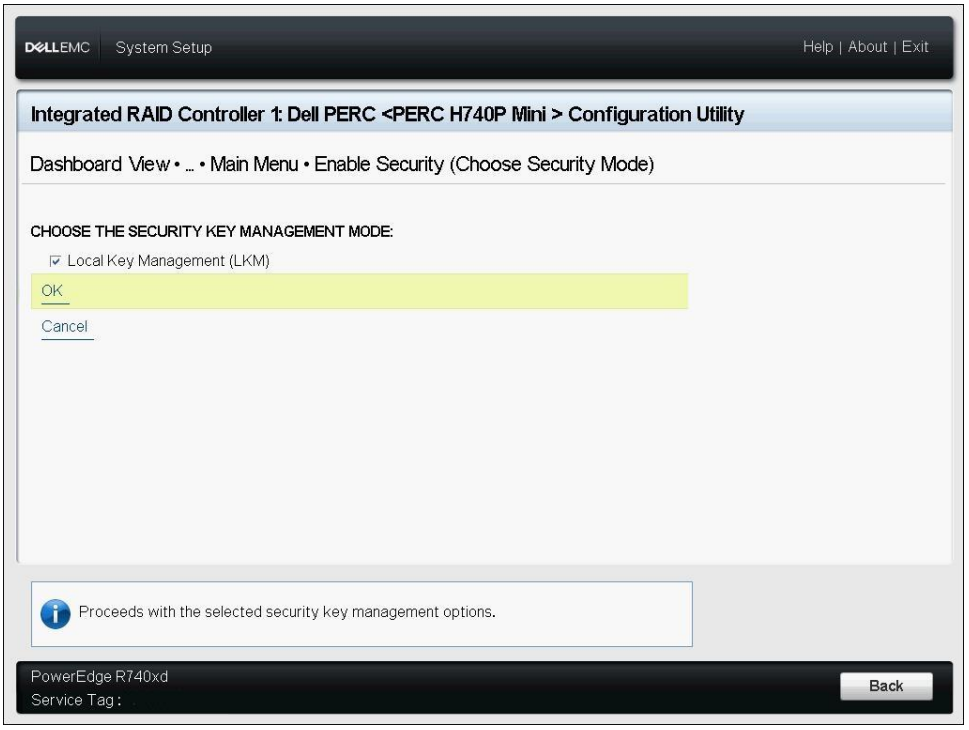

Figure 1: Selecting Local Key Management to enable security on the PERC.

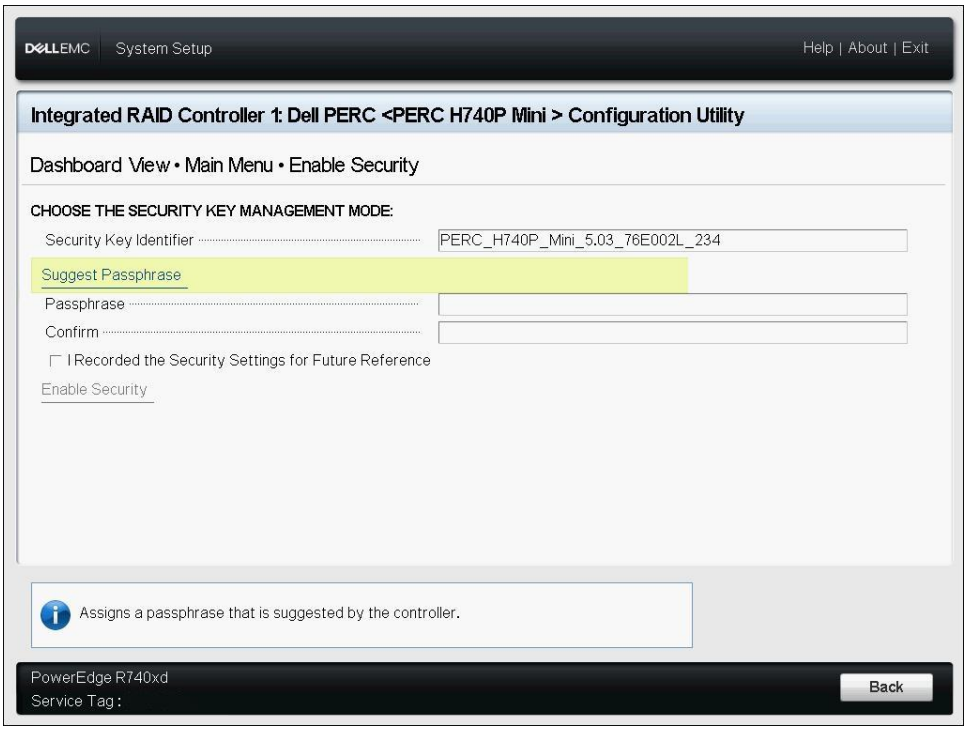

Figure 2: Creating a passphrase when enabling security on the PERC.

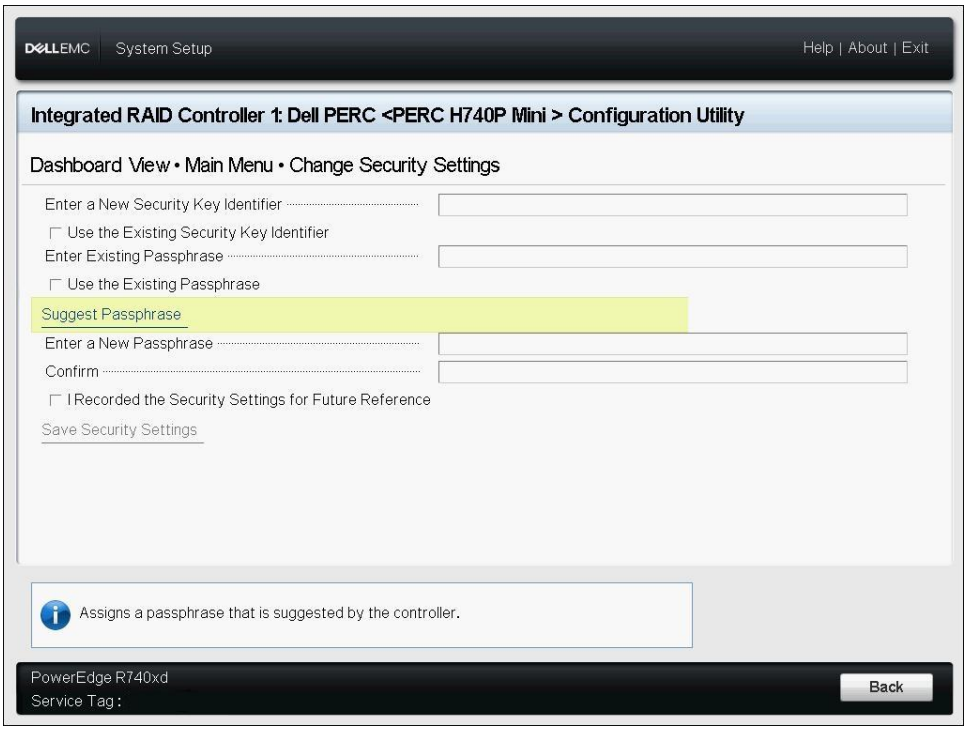

Figure 3: Changing security settings

Frequently Asked Questions:

Where does the encryption happen?

Encryption occurs on the drive whether the drive is secured or not. Any IO to the drive is encrypted/decrypted by hardware on the drive.

Where is the key stored, Drive or RAID controller?

KEK	Key Encryption Key
DEK	Data Encryption Key

There are multiple keys that are used between the drive and PERC. The DEK is what is used to encrypt the data on the drive, and it is stored on the drive itself. The KEK is used to unlock the drive so the drive can use the DEK. The hashed KEK is stored on the PERC controller.

The DEK is never revealed outside of the drive and the KEK is never revealed outside of the PERC controller.

Is the data encrypted by default?

The data is always encrypted but the drive needs to be secured to protect data from theft.

How to move disks between controllers, preserving the data?

Moving disks between different controllers is allowed and the passphrase that was originally used is needed to unlock the SEDs when importing them on the new controller. See Importing secure Virtual Disk section in the User Guide.

How to recover/access data in case of PERC card failure.

After replacing the failed controller with a working one and enabling security, the secured VDs can be imported using the original passphrase, allowing access to the data on the disks.

Can the passphrase be changed multiple times?

Yes, you can change the passphrase if you know the existing passphrase. This rekeys the KEK but does not change the DEK. See Changing Security Key section in the User Guide. The data will not be erased/lost when the new passphrase is established. The only thing that is changing is the passphrase that is used to unlock the drive.

If we lost a drive (and someone finds it) is the data accessible by default? What are the minimum steps required to ensure the data is protected?

If your drives are non-SED, then the data is accessible.
If your drives are SED and you did not secure them, then the data is accessible.
If your drives are SED and you secured them, then the data can only be accessed using the passphrase you have set.

By default, the data is not protected from theft. The minimum steps needed to secure a drive is to enable the controller security and securing the Virtual Disk. Please see Local Key Management section in the User Guide for more information.

What are performance implications of a SED. Would they perform faster/slower depending on if they are secured?

Data encryption occurs whether the drive is secured or not so there is no impact on performance.

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries

FAQ's, continued:

Can we mix RAID sets with some having normal drives and other RAID sets having SEDs?

Yes, you can mix SEDs and non-SEDs but you will not be able to secure those Virtual Disks. Securing a Virtual Disk requires all disks in the array to support SED.

Virtual Disk Drive Type	Controller Security Enabled	Controller Security Disabled
SEDs and Non-SEDs	Secured VD not allowed	Secured VD not allowed
SEDs	Secured VD allowed	Secured VD not allowed

What is Secure Erase or Cryptographic Erase?

Secure erase or Cryptographic erase allows you to scramble that data stored on the disk by changing the DEK. Preforming this erase operation will render that data on the device indecipherable and the data on the drive will not be able to be recovered. Secure erase or Cryptographic erase can only be done on a drive that is not configured in a Virtual Disk.

What is FIPS-140-2 level 2 compliance and does DELL EMC have supported drives?

FIPS stands for Federal Information Processing Standards and it is the mandatory standard required to protect sensitive or valuable data within Federal systems. Dell EMC offers SED drives with and without FIPS-140-2 level 2 certification, but it is not required for PERC secured VDs.

Additional Information

- https://en.wikipedia.org/wiki/Hardware-based_full_disk_encryption
- https://www.seagate.com/solutions/security/
- https://trustedcomputinggroup.org/resource/self-encrypting-drives-sed-overview/
- https://safenet.gemalto.com/data-encryption/enterprise-key-management/
- https://www.dellemc.com/en-us/solutions/openmanage/secure-enterprise-key-manager.htm

PowerEdge DfD Repository
For more technical learning

Contact Us
For feedback and requests

Follow Us
For PowerEdge news