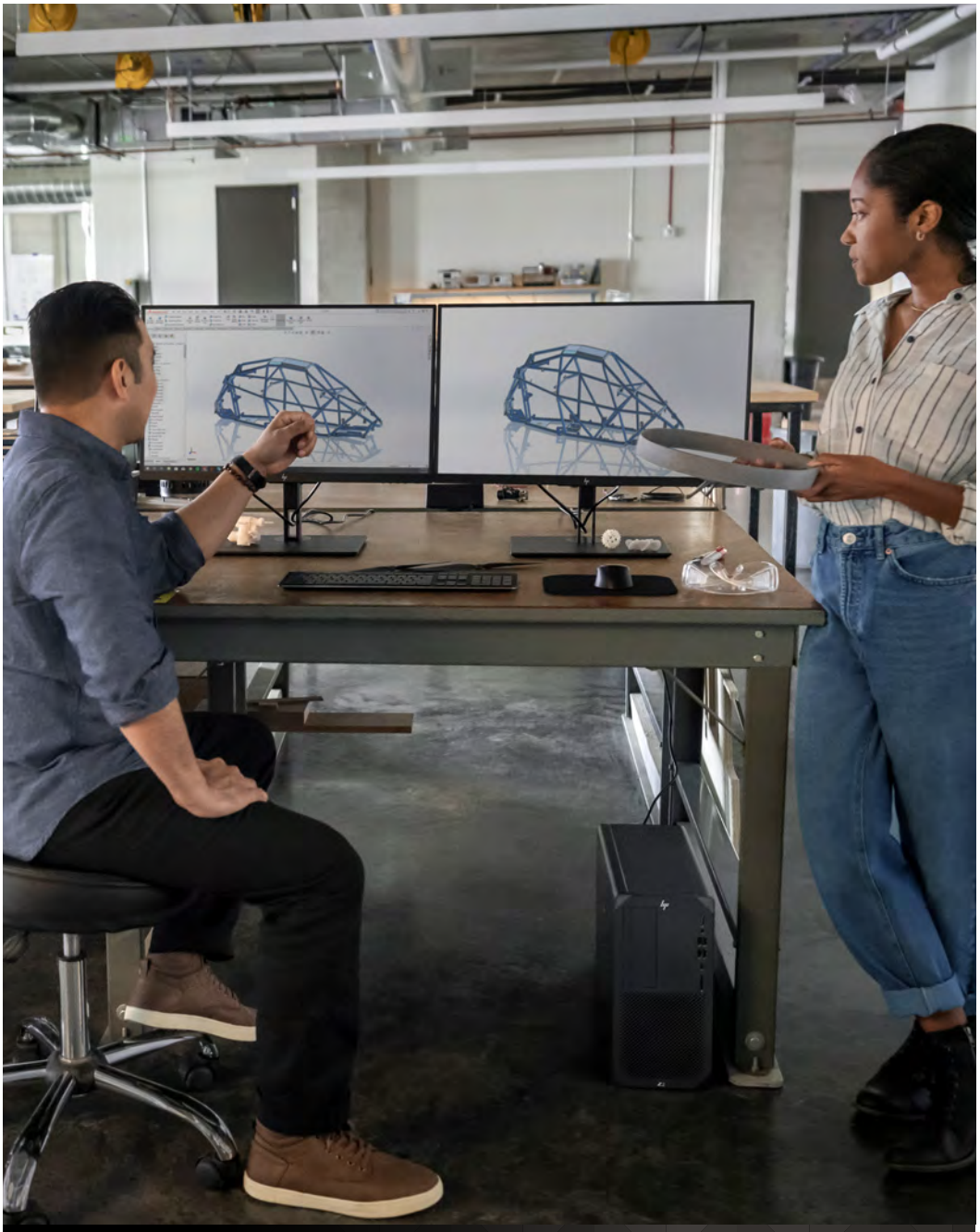
TECHNICAL WHITEPAPER

CONTENTS & NAVIGATION



SELF-ENCRYPTING DRIVES OVERVIEW

TECHNICAL WHITE PAPER

CONTENTS & NAVIGATION

WHAT IS A SELF-ENCRYPTING DRIVE?

A self-encrypting drive (SED) is a hard disk or a solid-state drive that provides hardware-based data encryption. All data that is committed to the media is encrypted with either a 128-bit or 256-bit key. Because all encryption is handled in hardware, there is a performance benefit to using an SED over software-based encryption. When using software-based encryption, all the data written and read from the drive must be encrypted and decrypted by the system processor. This extra processing work can lead to noticeable performance degradation. With hardware encryption using an SED, there is not a noticeable change in performance.

All SED devices use an internal Data Encryption Key (DEK), sometimes called a Media Encryption Key. The DEK is used to encrypt the data on the drive when written, and to decrypt the data when read. The DEK is not visible outside the drive and is stored in an encrypted format on the drive itself. In its factory-default state, the SED device is unlocked (accessible for reading and writing) when it is powered on, and the DEK is used to encrypt and decrypt writes and reads to the media. In other words, the encryption function is *always active*.

An SED also provides a set of security functions, include support for several passwords. Defining the most important of these passwords, called the Authentication Key (AK), is critical to making the drive protect the data in case it is physically accessed by a bad actor. We call this password-definition operation “provisioning”.

Once the password is defined and power is cycled, the drive starts in a locked state and the password must be provided in order to unlock it and allow read and operations to succeed. (For a boot drive, this unlocking must occur before the OS can be started.) The AK can actually be a long phrase. A value derived from it via a hash function is used to encrypt the DEK, so that it cannot be read off the media by nefarious means.

It is not until the drive is provisioned and locked that the data is fully secured.

Another benefit of using an SED is the device can be (in effect) securely erased in a matter of seconds. (Secure erasure can take several hours using traditional drive wipe methods.) The SED can be instructed to internally generate a new DEK, rendering all data on the drive unintelligible. The data remains in an encrypted format but can no longer be deciphered.

TCG and the Opal SSC

All SED devices sold by HP comply with the Opal SSC specification, created by the Trusted Computing Group (TCG). TCG is an organization of more than 100 member companies that develops open standards and specifications for secure computing.

TCG's Storage Working Group (SWG) has formulated the Opal Security Subsystem Class (SSC), one of the classifications of storage device security management specifications. It is mostly used in drives designed for desktop and notebook devices. In this specification, the data management of storage devices and the relevant details of the hierarchical management of data access permissions are defined to protect user data. Storage devices that are certified to comply with the Opal SSC specification are called trusted and secure storage devices with TCG Opal level.

A derivative specification called “Pyrite” describes an interface to manage security keys in the same way that Opal does, but without addressing encryption. In other words, it can be used to control read and write access to the media. It applies to non-SED drives.

SWG also defines certain “feature sets” that allow drives to show support for certain optional or extension features.

More information on the OPAL specification can be found on the Trusted Computing Group website: trustedcomputinggroup.org.

TECHNICAL WHITE PAPER

CONTENTS & NAVIGATION

SUPPORTED CONFIGURATIONS OF SED IN HP WORKSTATIONS

SED devices can be configured as both boot and data devices within HP workstations. Multiple SED can be provisioned within one HP workstation as standalone drives. The DEK and AK hash will be unique for each drive, despite using the same AK for multiple SED devices.

Several physical drive types may have SED capabilities: SATA HDDs (rotating media), SATA SSDs, and NVMe SSDs.

Configurations not supported in HP Workstations:

- RAID configurations with SED devices are not supported with Intel® iRST or RSTe/VROC.
- On older platforms: Flash Cache SSD modules used with the Intel® SRT software are not supported with the use of an SED HDD. The Intel® SRT software requires that the cache module and the HDD be configured in a RAID array, thus it cannot support an SED device.

PROVISIONING AND LOCKING AN SED

Provisioning an SED is normally accomplished using SED management software.

SED Management Software

SED Management software helps with the administration of SED in your specific environment. These tools offer features like security compliance, data protection policies, reporting, data recovery, and an interface which simplifies management. Provisioning an SED for boot (where unlocking has to precede the OS load) is made much easier by the right tool.

There are a variety of third-party software packages available for SED management. Features vary by manufacturer. In many cases, SED management is one function in an enterprise security solution suite. There are many articles discussing drive encryption as part of a security solution on the world wide web. A search string such as “TCG drive encryption software” can lead to some of the available software solutions.

The Linux community has converged on the sedutil boot image, provided by the Drive Trust Alliance, as a tool for SED provisioning. See www.drivetrust.com/sed-util/.

ATA Drive Lock (HP BIOS)

There is a method of defining an access lock for a SATA SED (or non-SED) that does not affect the DEK management. Drive Lock is a part of the ATA standard, and restricts access to any compliant drive unless the correct password is entered during BIOS Power-on Self-test (POST) to unlock the drive. Using ATA Drive Lock doesn’t require any additional software. When using ATA Drive Lock, an AK is not created on the SED. This means that the DEK is not encrypted and data is considered less secure. If possible, an SED drive should be properly provisioned.

The specific procedure to enable ATA Drive Lock can be found in the Workstations Maintenance and Service Guide. This guide can be found for all recent platforms at the HP Workstations Customer Support website: hp.com/go/workstationsupport.

In Linux, a SATA drive with ATA locking enabled can be manipulated further using the hdparm command.

NVMe devices do not support the ATA Drive Lock protocol.

NVMe SED Change Control (HP BIOS)

There is an important capability in HP system BIOS to prevent an SED from being provisioned unexpectedly, if the drive supports the Opal Feature Set item “Block SID Authentication,” as HP-provided drives do. (The SID is the security credential that must be presented to the drive in order to manage it.)

By default, the BIOS Setup item Security->Hard Drive Utilities->Allow OPAL Hard Drive SID Authentication is unchecked. That means that no changes to the drive setup can be made. When you are ready to provision your drive, you can check the box for this setting, and on the next bootup, the drive will be open to provisioning.

TECHNICAL WHITE PAPER

CONTENTS & NAVIGATION

SED SETUP AND OS BOOT PROCESS

During the provisioning process of an OS boot SED, the following occurs:

- Password (AK) is established.
- "Shadow Master Boot Record" created on SED.
  - -This establishes a drive-internal pre-boot OS to allow the entering of the password (AK) to unlock the drive, enabling access to the data stored on the device.

Note: Although "Master Boot Record" is the term used in TCG standards, it is misleading. Most storage drives of any size, and certainly any that support UEFI booting, use the GPT partition table format, not the older MBR format. The shadowing mechanism defined in the standard can support either type.

After completing the setup process for the SED, the boot flow of the Workstation is as follows:

- System BIOS attempts to read the boot record of the SED.
- System BIOS is redirected and loads the pre-boot OS.
- The user authenticates by entering the password defined during the setup process.
- If authentication is successful, the pre-boot interface passes control to the original boot record and the OS on the SED loads.
- If authentication is not successful, the machine is unable to boot from that drive.

REVERTING AN SED

It is possible to "reset" an SED to an accessible state without knowing the password. However, all the data is lost as one of the events in the reset is to trigger the internal generation of a new DEK. Most SED management software solutions will have a method for "deactivating" the password.

All TCG Opal Self-Encrypting drives show the Physical Security ID (PSID) on the label. This allows re-purposing of the drive without a master password while not exposing user data during the processing. Of course, physical access is required so one can read this string from the label.

PCIE NVME SED AND TCG OPAL

Standard security support for NVMe devices includes the TCG Pyrite subset of TCG commands for management of password security (for non-SED devices). The complete TCG Opal 2.0 set of TCG commands is implemented for encryption (for SED devices). The Storage Feature Set item "Block SID Authentication" is also supported on NVMe devices.

There are two types of NVMe devices used in HP Workstations:

- Non-SED: No TCG Opal support, TCG Pyrite support and Block SID Authentication support.
- SED: TCG Opal support and Block SID Authentication support.

On some workstations, the PCIe lane groups where NVMe storage devices are located can be in one of two modes, a BIOS setting managed per PCIe "slot." Some "slots" are actually M.2 sockets on the motherboard.

- Intel® VMD disabled: In this mode, the NVMe device(s) are directly visible to the OS. In Windows, a Microsoft-supplied NVMe driver is used.
- Intel® VMD enabled: In this mode, an Intel® capability in the PCIe root complex called a Volume Management Device is activated. In Windows, an Intel® VROC driver is loaded; the NVMe drives are not even seen by the normal Microsoft driver.

Slots for NVMe drives should be in VMD-disabled mode if they are to be managed. (Not all workstations have processors that support the VMD capability so this is not always an issue.)

TECHNICAL WHITE PAPER

CONTENTS & NAVIGATION

SATA SED AND SOFTWARE LIMITATIONS

In Intel®-based HP Workstations, each SATA port is connected to a SATA storage controller. Typical SATA controllers can be put in one of several modes via the BIOS setup interface. The mode set for the controller applies to all the ports under it. Some platforms have more than one SATA controller.

Depending on the platform vintage, these modes might be available:

- RAID: This is the default with greatest flexibility for most users. This mode triggers an Intel® RAID-supporting device driver to be loaded in Windows. In this mode, Intel® iRST or VROC RAID can be configured across non-SED drives.
- AHCI: An alternate mode that allows access to drive functionality, but not Intel® iRST or VROC RAID. In some platforms that only offer RAID and AHCI, unchecking the RAID checkbox in the BIOS enables this mode instead.
- IDE: A legacy mode that restricts SATA drives to functionality compatible with the old parallel ATA definition. Not recommended unless such compatibility is needed. Newer platforms do not support this mode.

SATA SEDs require AHCI mode if they are to be managed. Most key management software does not work when the SATA controller is in RAID mode as the SED security protocols are not supported by the RAID-capable driver. Software applications may disable management of SEDs if the software detects that the SED is attached to a RAID-mode controller.

Implications of switching SATA Modes

On HP systems, AHCI mode can be set in BIOS F10 setup interface; the details are platform-specific, but usually in the Advanced->System Options dialog.

CAUTION: Changing modes after the OS is installed is not advised. Most OSs use different storage drivers depending on the SATA controller mode. Changing modes may cause RAID arrays to become corrupt and unrecoverable and may lead to a failure to boot the OS. Be sure to back up your data before making any changes to the SATA mode. You may need to re-install the OS after the change.

Since the mode is a controller setting, all SATA drives attached to it are affected.

Note: The SAS controller on the HP Z840 is always a RAID controller and does not support SEDs.

AHCI Driver

An AHCI driver is required for AHCI support. If an AHCI driver is not installed, Windows may encounter a blue screen error when booting the system after switching the SATA mode to AHCI. HP workstations configured at the factory will have AHCI drivers preinstalled. If you are creating a new OS disk, download the latest storage driver SoftPaqs for your system from hp.com so you can have them available during the OS installation process. If you have an existing OS disk and are unsure if you have AHCI drivers, download the latest Intel® storage driver SoftPaqs from hp.com and use the executable install utility to install the drivers before switching controller modes.

TECHNICAL WHITE PAPER

CONTENTS & NAVIGATION

PLATFORM SPECIFICS

PLATFORM FAMILY	FORM FACTOR	NUMBER OF SATA PORTS	AVAILABLE MODES	VMD CAPABILITY	
HP Z1G5	Tower	4	RAID, AHCI	N	
HP Z2G4	Tower	4	RAID, AHCI	N	
	SFF	4	RAID, AHCI	N	
	Mini	1	AHCI	N	
HP Z2G5	Tower	4	RAID, AHCI	N	
	SFF	4	RAID, AHCI	N	
	Mini	1	AHCI	N	
HP Z440	Tower	Primary: 2 Secondary: 4	RAID, AHCI, IDE	N	
HP Z640	Tower	Primary: 2 Secondary: 4	RAID, AHCI, IDE	N	
HP Z840	Tower	Primary: 2 Secondary: 4	RAID, AHCI, IDE	N	Onboard LSI SAS: 8 ports that can accommodate SATA, but no SED support
HP ZCentral 4R	1U	Primary: 4	RAID, AHCI	Y	
HP Z4G4	Tower	6	RAID, AHCI	Y	
HP Z6G4	Tower	6	RAID, AHCI	Y	
HP Z8G4	Tower	Primary: 8 Secondary: 2	RAID, AHCI	Y	

FREQUENTLY ASKED QUESTIONS

- I just bought an SED from HP as an After Market Option, how can I move my boot image over to the new drive?
  - -To move your boot image to the new drive, you can use one of many available third-party imaging utilities. HP does not recommend any utility over another. Another way to make the new SED your boot drive would be to back up all of your data, install an operating system on your SED, and then recover your backed-up data to the SED.
  - -Make sure the controller for the new drive is in the SED-supporting mode before installing the OS. If the drive is SATA and the older source drive has been operating in RAID mode, you will have to use the second method with a new OS installation.
  - -Provision the new drive after the OS is booting correctly.
- What is the correct BIOS setting for my SED?
  - -For a SATA SED, you must set the SATA emulation mode to AHCI. Most of the 3rd party key management software packages will not correctly recognize the SED if SATA emulation is set to RAID.
  - -For an NVMe SED, make sure that VMD is disabled on the PCIe slot where it is located, if the platform supports VMD.
  - -When you're ready to provision the SED, make sure the SID Authentication box is checked in Security->Drive Utilities
- How do I set up an SED as a data drive?
  - -After installing your SED, you would use the key management software to provision the SED, much like you would if the SED was your boot drive.
- Can I have more than one data drive as an SED?
  - -This depends on the key management software that is being used to provision the SED. Contact the manufacturer of the key management software for further details.
- Can I RAID my SEDs?
  - -At present, you cannot use RAID in HP Workstations on SEDs and still retain the ability to provision/lock the SEDs.

TECHNICAL WHITE PAPER

CONTENTS & NAVIGATION

- Can I use a boot SED and a data SED? Can they use the same key?
  - -Supporting multiple SEDs depends on the key management software that is being used. Contact the manufacturer of the key management software for further details.
  - -The phrase you provide is hashed separately for each drive so normally you can use the same for multiple drives.
- How do I update the firmware on my SED?
  - -Firmware updates on SED are similar to firmware updates on non-SED storage devices. As with all firmware updates on storage devices, there is the possibility of data loss. Be sure to back up data stored on the drive prior to performing the firmware update.
  - -Technically, the authorization to modify the firmware is controlled by a different key than media access, but most SED management software should enable this operation either with the same key or with a special interface. However the authorization key for data access should not be affected by the update.
- I reset my BIOS to factory defaults and now I'm having problems. What can I do?
  - -For most HP desktop workstations, the default SATA emulation mode is RAID. This will have to be changed to AHCI mode to ensure proper recognition and management of the SED. Some older platforms offered a RAID+AHCI mode; those also must be set to AHCI.
  - -VMD is disabled by default on platforms that support it, so it is unlikely to interfere with NVMe SED operations.
- Does HP provide a software application for management of SEDs?
  - -In the past, HP offered an SED management software solution via HP Client Security Manager with the HP Drive Encryption adjunct software. It only addressed SATA storage drives. That software is now obsolete.

Additional Resources

hp.com/go/whitepapers

Solutions Guide for Data-At-Rest in PDF (2009)

NVM Express and TCG Joint White Paper (2015)

To learn more, visit hp.com

Sign up for updates
hp.com/go/getupdated

Share with colleagues

LET US HELP YOU CREATE AMAZING BUSINESS SOLUTIONS TODAY

LEARN MORE

4AA4-4992ENW, April 2021