Intel® Virtual RAID on CPU (Intel® VROC) 9.3 Production Version (PV) Self-Encrypting Drive (SED)

Release Notes

Revision 1.6

October 2025

Document Number: 787385

Contents

Figures

Revision History

Revision Number	Description	Revision Date
1.6	• Updated issue list.	October 2025
1.5	• Initial public release of the document.	April 2025
1.4	• Updated issue list in Chapter 4 for VROC 9.1 PV.	February 2025
1.3	• Updated issue list.	June 2024
1.2	• Updated issue list.	March 2024
1.1	• Updated issue list.	November 2023
1.0	• Initial release of the document.	March 2023

§§

1 Introduction

1.1 Overview

This document contains the release notes for the Self-Encrypting drive (SED) feature for the Intel® Virtual RAID on CPU (Intel® VROC) product. The Intel VROC Self-Encrypting Drive feature targets the Intel® Xeon® Scalable Generation 3, and higher, platforms.

A SED is a Storage Device that integrates encryption of user data at rest, all user data written to the Storage Device is encrypted by specialized hardware implemented inside the Storage Device controller. The data is decrypted as it is read.

Booting the Operating System (OS) from a secured RAID volume or secured single drive is one of the important functionalities available in an SED Solutions. Another function that is equally important is supporting a solution where SED Key Manager is only available during the UEFI phase.

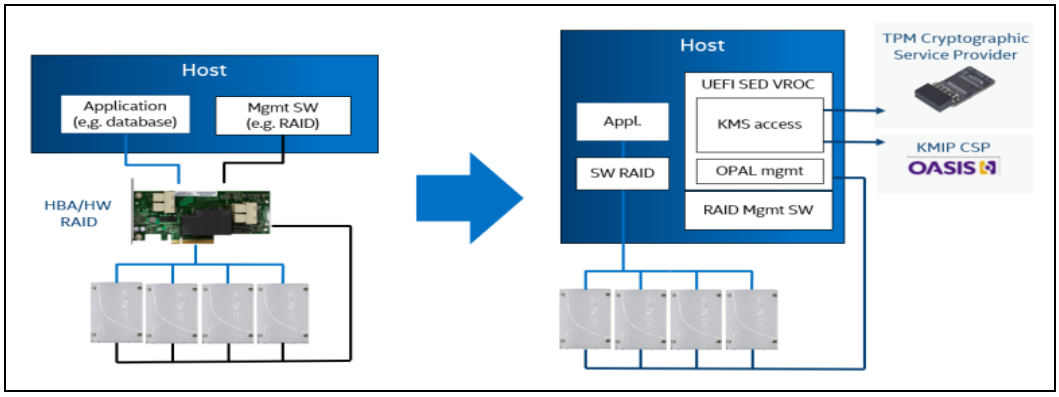
Intel VROC provides a compelling RAID solution for NVMe SSDs. The generic goal for the solution is to behave like HW RAID cards. There are already HW products that support Self-Encrypting Drives (SED).

Boot the OS from a secured RAID volume or secured single drive is one of the functionalities available in such devices. Another one that is maybe even more important is supporting the end-user solutions where the Key Manager is accessible only in the PreOS phase.

1.2 Background

Data-at-rest security is a critical requirement for Data Center deployments. For example, Data-At-Rest security reduces the cost of retiring and repurposing storage via cryptographic erasure, while methods like physical destruction or degaussing are used for legacy solutions. The Trusted Computing Group (TCG) Opal Family of specifications introduces a set of standards allowing the management of user data encryption in a storage device flexibly. Opal is the developing industry standard to address security concerns in storage. Hardware RAID Cards have a Hardware-based automatic key management for SED drives but may have performance limitations and additional Hardware costs**.**

Figure 1-1. HW HBA/RAID to VROC Transition



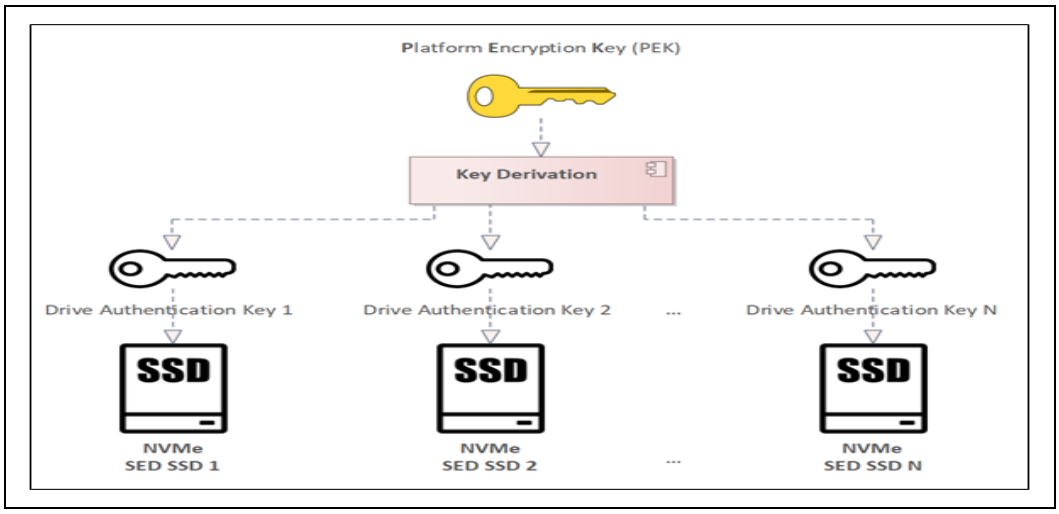
1.3 Architecture-Components Diagram

Intel® VROC SED solution uses different keys for each SSD to guarantee that breaking protection of one NVMe SSD does not affect other NVMe SSDs. But, for ease of use, only one key per server is required to manage all NVMe SSDs. This is to address cases like plugging additional drives into system without need of providing additional key to server.

VROC UEFI SED drivers uses the following keys, on each server (as presented on below figure):

- Platform Encryption Key (PEK) – single key per server. It is provided and managed by UEFI Cryptographic Service Provider driver, which is implemented outside Intel by the OEM or BIOS vendor.
- Drive Authentication Key (DAK) – single key per NVMe SSD. DAK is derived from PEK locally on the server node. It is used as password for the NVMe SSD (Security Identifier (SID) and Admin1 authentication key as defined in Opal standard).

Figure 1-2. Keys used by VROC SED in Single Server



Components

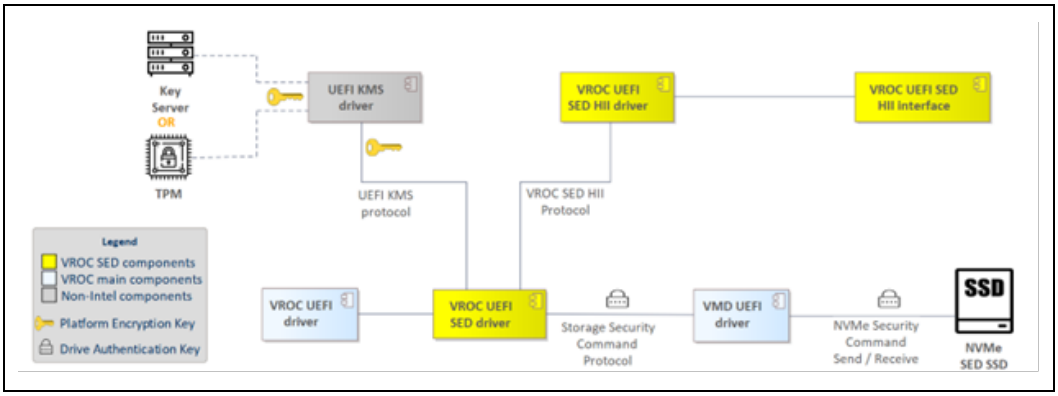
Intel® VROC UEFI SED driver retrieves the key from the third-party component implemented by BIOS vendor (typically implemented by OEMs, outside Intel), called UEFI KMS Driver. UEFI KMS driver implements standard API, which is UEFI Key Management Service (KMS) protocol, defined by UEFI specification. The UEFI KMS protocol is used by VROC UEFI SED driver to create new key and then get this key.

Intel® VROC UEFI SED solution consists of two UEFI drivers:

1. VROC UEFI SED driver, which provisions and unlocks NVMe SED SSDs
2. VROC UEFI SED Human Interface Infrastructure (HII) driver, which provides BIOS user interface for manual management and diagnostic purposes.

Below figure presents the diagram of VROC UEFI SED components, providing SED features.

Figure 1-3. VROC UEFI SED Components



The usage of standardized UEFI KMS protocol enables supporting multiple key managers, the OEM can use its cryptographic service provider UEFI driver to integrate VROC SED support.

Separation of VROC UEFI SED HII driver and VROC UEFI SED driver provides flexibility to OEMs to support multiple end-users use cases. For example, one can achieve the user experience compared to HW RAID card, where additional manual password and password hind functionality is expected, or fully automatic remote key management one where no interaction with the user should occur.

TPM is supported by UEFI KMS driver, from the third-party component implemented by BIOS vendor (typically implemented by OEMs, outside Intel), called UEFI KMS Driver

1.4 Defect Submission Support

With this release, Intel receives, and processes issues reported by customers via the Intel® Premier Support portal.

The Intel® Premier Support tool to submit an issue. Information, training, and details can be found in http://www.intel.com/content/www/us/en/design/support/ips/training/welcome.html.

Your local Field Application Engineer (FAE) can also provide you the necessary requirements to enable you to submit an Intel® Premier Support issue (also known as a "case"), including an account setup if you do not have one already.

When submitting a case, the following information needs to be included in the corresponding fields to flag Intel® VROC Application Engineering (AE) support:

```
Product/Project Info → Case Category = TechnologyInitiative
Product/Project Info → Case Subcategory = Intel® Virtual RAID on CPU
(Intel ® VROC)
```

1.5 Supported Platforms

The Intel® VROC 9.3 Platform Validation (PV) package was designed to work on customer platforms that are based on the following Intel reference platforms starting with 6th Gen Intel® Xeon® Scalable processors codenamed Granite Rapids.

1.6 Reference Documents

Document	Document Number
Intel® Virtual RAID on CPU (Intel® VROC) Self-Encrypting Drive Feature User Guide	https://www.intel.com/content/www/us/en/support/articles/000098587/memory-and-storage/datacenter-storage-solutions.html

§§

2 Drivers, Images, and Intel® VROC SED Utilities

PreOS: `Intel® VROC Pre-OS SED version 9.3.0.1132.`

The SED UEFI package relies on the UEFI package from the `Intel® VROC 9.3.0.1132 PV` release Package.

2.1 How to Use in UEFI

SED PreOS drivers and their dependency files (`VrocSedHii.efi`, `VrocSedDxe.efi`, `VrocSedDxe.depex`, `VMDVROC_1_sk_sed.depex`, `VMDVROC_1_sk_sed.efi`, `VMDVROC_2.efi` and `HwKeySedDxe.efi`) should be integrated into BIOS if SED feature is needed and VROC H/W key is used. `HwKeySedDxe.efi` is used for VROC H/W key. `HwKeySedDxe.efi` should be excluded from the BIOS if VROC H/W key is not used. `VrocSedDxe.depex` and `VMDVROC_1_sk_sed.depex` are their drivers' dependency files.

SED function is enabled in UEFI. More details are available in the Intel® Virtual RAID on CPU (Intel® VROC) User Guide for the Self-Encrypting Drive (SED) Feature.

§§

3 Intel® VROC SED Limitations

3.1 Support for NVMe* Driver Only

If no NVMe driver is present in system, Intel® VROC SED manager and Intel® Virtual RAID on CPU HII won't be displayed.

3.2 SED and Non-SED Drives Should Not be Mixed to Use

Intel® VROC SED exclusively supports arrays made up of SED drives. Combining SED and non-SED drives will prevent the Intel VROC SED manager HII from being displayed.

3.3 Intel® VROC OS Interfaces Limitation with SED OPAL Devices.

Intel VROC OS interfaces (Windows* GUI CLI, Linux mdadm, Linux*/Windows* OOB) may not forbid performing operations that use Self Encrypting Drives in locked/foreign state:

RAID Volume operations with locked / foreign device will be failed (e.g., RAID volume creation will be failed).

RAID Volume hot-plug related operations with locked / foreign device will be failed as well (Example: RAID volume rebuild may not be blocked; hot-inserted device detection will be failed).

§§

4 Intel® VROC Issues

This section outlines the issues reported -and internally found- that customers need to be aware of. The issues are broken down into “Known Issues”.

4.1 Known Issues in Intel® VROC 9.3 PV

These are the known issues in this PV release package.

ID	Title

4.2 Resolved Issues in Intel® VROC 9.3 PV

These are the resolved issues in this PV release package.

ID	Title
15017895846	The SED manager always shows "Reboot required"

§§