Intel® VROC Self-Encrypting Drive

High Level Architecture for Intel® Xeon® Scalable based Platforms
# Table of Contents

1 Revision History ................................................................................................................. 4  
2 Related Specifications ........................................................................................................ 4  
3 Introduction .......................................................................................................................... 5  
   3.1 Overview .......................................................................................................................... 5  
   3.2 Scope ..................................................................................................................................... 5  
   3.3 Document Audience/Purpose .............................................................................................. 5  
   3.4 Definitions .......................................................................................................................... 5  
4 Feature overview .................................................................................................................... 6  
   4.1 Background .......................................................................................................................... 6  
   4.2 Feature motivation ................................................................................................................. 6  
5 Architecture - Components Diagram ..................................................................................... 7  
   5.1 SED UEFI Component Model .............................................................................................. 7  
6 Key hierarchy and management ............................................................................................... 9  
   6.1 Cryptographic Algorithms .................................................................................................... 9  
   6.2 Cryptographic Keys and Their Properties ......................................................................... 10  
7 Architecture - OPAL datastore metadata ............................................................................. 11  
   7.1 Device Metadata Layout ..................................................................................................... 11  
8 Architecture - Functional Diagrams ....................................................................................... 13  
   8.1 System State (KMS available) ............................................................................................. 13  
   8.2 System State (KMS NOT available) .................................................................................... 14  
   8.3 Drive State .......................................................................................................................... 15  
   8.4 Manual System Setup from HII ......................................................................................... 16  
   8.5 Auto-Provisioning and Auto-Unlocking .............................................................................. 17  
   8.6 Re-key .................................................................................................................................. 18  
   8.7 Lock on Hot-plug .................................................................................................................. 19  
9 Architecture - EFI KMS protocol .......................................................................................... 20  
   9.1 Activity diagram for KMS.CreateKey() ............................................................................. 20  
   9.2 Activity diagram for KMS.DeleteKey() ............................................................................. 21  
   9.3 Activity diagram for KMS.GetKey() ................................................................................. 22  
10 UEFI HII Control Flow ......................................................................................................... 23  
11 UEFI HII Frameset ................................................................................................................. 24  
   11.1 Dashboard View ................................................................................................................. 24  
   11.2 Drive Management ............................................................................................................. 30  
   11.3 Error Pages ....................................................................................................................... 44  
   11.4 System Revert .................................................................................................................... 46  
   11.5 System Rotate Keys (Re-Key) ........................................................................................... 48  
   11.6 System Setup .................................................................................................................... 50  
22
1 Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td></td>
<td>Initial version</td>
</tr>
<tr>
<td>1.0</td>
<td>02/02/2022</td>
<td>Document format changes</td>
</tr>
</tbody>
</table>

2 Related Specifications

The following specifications are recommending reading and have been utilized in the creation of this document:

- **Intel Virtual RAID on CPU Rev 7.5 - Software Architecture Specification (SAS)**
  - The main SAS covers VROC architecture and management interfaces.
- **Intel VROC SW Licensing - Software Architecture Specification (SAS)**
  - This document outlines the software architecture of Licensing feature.
- **Unified Extensible Firmware Interface (UEFI) Specification**
  - The drivers support the UEFI 2.7 Specification and follow the UEFI driver model. It operates in the DXE system initialization phase. The document defines the EFI_KMS protocol.
- **System Management BIOS (SMBIOS) Reference Specification**
  - Describes details related to System UUID, which is used for drive migration detecting.
- **TCG Architecture Core Specification v2.01**
- **TCG Storage Security Subsystem Class: Opal Specification v2.01**
- **TCG Storage Application Note: Encrypting Drives Compliant with Opal SSC v1.00**
3 Introduction

3.1 Overview
This document describes the architecture of the Intel® Virtual RAID on CPU (Intel® VROC) Self-Encrypting Drive feature for the Intel® Virtual RAID on CPU (Intel® VROC) products based on Intel® Xeon® Scalable Generation 3, and higher, platforms.

Intel VROC is an Intel Xeon Scalable CPU Integrated RAID Hybrid (Hardware + Software) RAID solution for NVMe and SATA drives.

3.2 Scope
The document contains the information required to understand how the feature works. It also covers the dependencies, which have to be addressed on the OEM side.

3.3 Document Audience/Purpose
The primary audience of this document is OEMs, who would like to use the Intel VROC family of products included in their platform.

3.4 Definitions

3.4.1 Intel VROC
Intel VROC is an Intel Xeon Scalable CPU Integrated RAID (Redundant Array of Independent Disks) solution for CPU and PCH attached NVMe devices. The RAID solution is built on the Intel® Volume Management Device (Intel VMD) which is a hardware feature in the Intel® Xeon processors for 3rd Generation and higher platforms.

3.4.2 Acronyms and Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>HDA</td>
<td>Host Bus Adapter</td>
</tr>
<tr>
<td>HII</td>
<td>Human Interface Infrastructure</td>
</tr>
<tr>
<td>HLA</td>
<td>High Level Architecture</td>
</tr>
<tr>
<td>HSBP</td>
<td>Hot-Swap Back Plane</td>
</tr>
<tr>
<td>KDF</td>
<td>Key Derivation Function</td>
</tr>
<tr>
<td>KMIP</td>
<td>Key Management Interoperability Protocol</td>
</tr>
<tr>
<td>OASIS</td>
<td>Organization for the Advancement of Structured Information Standards</td>
</tr>
<tr>
<td>PSID</td>
<td>Physical Presence SID</td>
</tr>
<tr>
<td>SAS</td>
<td>Software Architecture Specification</td>
</tr>
<tr>
<td>SED</td>
<td>Self-Encrypting Drive</td>
</tr>
<tr>
<td>SID</td>
<td>Security Identifier</td>
</tr>
<tr>
<td>SP</td>
<td>Security provider</td>
</tr>
<tr>
<td>TPer</td>
<td>Trusted Peripheral</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
</tbody>
</table>
4 Feature overview

4.1 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.

4.2 Feature motivation

Intel VROC provides a compelling a RAID solution for NVMe SSDs. The goal is to provide a viable, cost effective, solution to Hardware RAID cards.

Booting the Operating System 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 solutions where SED Key Manager is only available during the UEFI phase.

The Intel VROC SED solution addresses the above by providing UEFI components with the following features supported:

- Automatic drive provisioning and unlocking on system boot in UEFI,
- Modular architecture in both UEFI and OS, to enable OEMs to implement their own Cryptographic Service Providers to use non-typical key managers,
- Human Interface Infrastructure (HII) includes manual management, diagnostic functionality, and integration into the existing VROC HII environment.

Figure: The HW HBA/RAID to VROC transition
5 Architecture - Components Diagram

5.1 SED UEFI Component Model

Component diagram in package ‘SED UEFI Component Model’

Two Intel VROC UEFI components provide UEFI support for SED (VROC SED Opal, VROC SED HII). Using the standardized EFI_KMS_PROTOCOL enables supporting multiple key managers, and the end-user can use its cryptographic service provider's UEFI driver to integrate SED support. Separating the HII and OPAL driver functionality allows Platform Vendors to support multiple use cases. For example, a traditional Hardware RAID card-like experience can be achieved where additional manual password and password hint functionality is expected, or fully automatic remote key management where no interaction with the user should occur.

Figure 1: SED UEFI Component Model
5.1.1 SED UEFI Components

5.1.1.1 VROC SED OPAL

A specific Intel VROC UEFI Driver is required to provide SED support and interact with the Intel VROC RAID management functionality. This specific Intel VROC UEFI Driver expects the available EFI_KMS_PROTOCOL services to generate and store the OPAL key. The Intel VROC UEFI Driver with SED support along with the appropriate Intel VROC license must be installed to enable the Intel VROC SED functionality.

5.1.1.2 VROC SED HII

The Intel VROC UEFI drivers with SED support must be incorporated in the platform BIOS. This will provide the Intel VROC SED HII interface functionality to allow access to the Intel VROC SED feature. All of the drives attached to the platform must be SED OPAL drives.

---

**Intel® VROC SED - Dashboard View**

**Intel® VROC SED Manager**

- Version: <1.0.0.1006>
- Status: <Disabled>

- System Setup
- Replace System Keys (Re-Key)
- System Revert
- Drive Management

---

Copyright (c) 2006-2020, Intel Corporation
6 Key hierarchy and management

Platform Encryption Key (PEK):
- A single PEK per server is used to generate DEK and create the key used to encrypt individual DEK_SALT.
- AES-256 bit

Disk Encryption Key (DEK):
- 256-bit wide generated using openssl RNG
- Unique per disk in the server
- Used for SID and Admin1 authorities
- Created from the PEK and DEK_SALT which is stored in encrypted (using the key derived from PEK) form in Opal datastore.

6.1 Cryptographic Algorithms

This section provides a listing of all cryptographic algorithms used in the project and shows their usage and cryptographic function for purposes of export classification.

<table>
<thead>
<tr>
<th>Algorithm (+key length +mode/padding scheme)</th>
<th>Usage</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES—256 GCM mode, no padding</td>
<td>wrapping/unwrapping SALT that is used for DEK creation</td>
<td>IV-randomly generated 12B In – randomly generated DEK in plain text 32B Key – PEK_HKDF_NO_SALT key derived form PEK that is retrieved from network-attached KMS appliance 32B Mode – ECP_aes_256_gcm() Padding – None</td>
</tr>
<tr>
<td>HMAC-based Key Derivation Function</td>
<td>Derivation of PEK_HKDF_NO_SALT</td>
<td>Key (SKM) – PEK key retrieved from network-attached KMS appliance</td>
</tr>
</tbody>
</table>
### 6.2 Cryptographic Keys and Their Properties

This section provides a listing of all cryptographic keys used in the project and shows their properties.

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Algorithm/Size</th>
<th>Usage</th>
<th>At rest location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Encryption Key (PEK)</td>
<td>HKDF 256</td>
<td>It is used as an argument to the HKDF derivation function. Two keys are derived from it. First, PEK_HKDF_NO_SALT is used to wrap/unwrap Disk Encryption Key Salt (DEK_SALT) by using AES-256 in GCM mode. The second one is DEK (see description below).</td>
<td>Stored persistently in 3rd party OASIS KMIP compliant Key Management Server</td>
</tr>
<tr>
<td>DEK</td>
<td>256 bits</td>
<td>Used as SID and Admin1 authentication key in Opal compliant disk</td>
<td>Created from PEK and DEK_SALT. DEK_SALT is stored on the drive in the Opal datastore region in encrypted form.</td>
</tr>
<tr>
<td>PEK_HKDF_NO_SALT</td>
<td>AES 256</td>
<td>Used to wrap/unwrap Disk Encryption Key Salt (DEK_SALT) by using AES-256 in GCM mode.</td>
<td>Created from PEK and “no-salt” (0’s - 32 zero bytes).</td>
</tr>
</tbody>
</table>
7 Architecture - OPAL datastore metadata

All OPAL compatible devices must provide a datastore that can be managed only by a security administrator. This area is used to store Intel VROC SED metadata. Anyone can perform the Read operation of the metadata. The Write operation is limited to security administrators. During the Re-key process, temporary data is stored in the OPAL datastore.

![Datastore Layout Diagram]

#### 7.1 Device Metadata Layout

<table>
<thead>
<tr>
<th>Section</th>
<th>Offset</th>
<th>Length</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata descriptor (9B)</td>
<td>0</td>
<td>0</td>
<td>Metadata identifier</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>8</td>
<td>Metadata version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>1</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>Encryption algorithm descriptor (7B)</td>
<td>9</td>
<td>1</td>
<td>Algorithm version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>6</td>
<td>Reserved</td>
<td></td>
</tr>
<tr>
<td>Encryption algorithm attributes (368B)</td>
<td>16</td>
<td>1</td>
<td>Platform Encryption Key (PEK) size in bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>255</td>
<td>Platform Encryption Key (PEK)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>272</td>
<td>1</td>
<td>IV size</td>
<td></td>
</tr>
<tr>
<td></td>
<td>273</td>
<td>64</td>
<td>Initial vector (IV) for encryption algorithm</td>
<td></td>
</tr>
<tr>
<td>UEFI/OS metadata (128B)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>337</td>
<td>47</td>
<td>Reserved</td>
<td>Align to 128B</td>
<td></td>
</tr>
<tr>
<td>384</td>
<td>2</td>
<td>Reserved for ReKey temporary data</td>
<td>number of drives</td>
<td></td>
</tr>
<tr>
<td>386</td>
<td>16</td>
<td>Platform UUID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>402</td>
<td>110</td>
<td>Reserved</td>
<td>Align to 128B</td>
<td></td>
</tr>
</tbody>
</table>

**Key section**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>1</td>
</tr>
<tr>
<td>513 + (N*dek_salt_entry_size)</td>
<td>16</td>
</tr>
<tr>
<td>529 + (N*dek_salt_entry_size)</td>
<td>2</td>
</tr>
<tr>
<td>5103 + (N*dek_salt_size)</td>
<td>32</td>
</tr>
<tr>
<td>5135 + (N*dek_salt_size)</td>
<td>16</td>
</tr>
<tr>
<td>17343</td>
<td>65</td>
</tr>
</tbody>
</table>

**dek_salt_entry_size** is equal to sum of DEK guid and DEK offset sizes.

**dek_salt_size** is equal to sum of DEK_SALT and AES-GCM tag values sizes
8 Architecture - Functional Diagrams

8.1 System State (KMS available)

System State (KMS available)
Version 1.1

Figure 2: System State (KMS available)
8.2 System State (KMS NOT available)

System State (KMS NOT available)
Version 1.0

Figure 3: System State (KMS NOT available)
8.3 Drive State

Figure 4: Drive State
8.4 Manual System Setup from HII

Figure 5: Manual System Setup from HII
8.5 Auto-Provisioning and Auto-Unlocking

Auto-Provisioning and Auto-Unlocking
Version 1.0

Figure 6: Auto-Provisioning and Auto-Unlocking
8.6 Re-key

Figure 7: Re-key
8.7 Lock on Hot-plug

Figure 8: Lock on Hot-plug
9 Architecture - EFI KMS protocol

9.1 Activity diagram for KMS.CreateKey()

Activity diagram for KMS.CreateKey()
Version 1.0

Figure 9: Activity diagram for KMS.CreateKey()
9.2 Activity diagram for KMS.DeleteKey()

Activity diagram for KMS.DeleteKey()

Version 1.1

Figure 10: Activity diagram for KMS.DeleteKey()
9.3 Activity diagram for KMS.GetKey()

Activity diagram for KMS.GetKey()
Version 1.0

Figure 11: Activity diagram for KMS.GetKey()
10 UEFI HII Control Flow

The diagram below shows the flow between the individual forms in the HI UI. The Formset Guid which is used to install all pages described in this document is {0x6b737f11, 0x7ba8, 0x434d, { 0x8c, 0x55, 0xe6, 0xfe, 0x21, 0x7c, 0x85, 0xf0}}.

![Diagram showing UEFI HII Control Flow](image-url)

*Figure 12: UI Navigation, Version 1.1*
11 UEFI HII Frameset

11.1 Dashboard View

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

![Dashboard View](image)

Figure 13: Dashboard View, Version 1.6

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Id</td>
<td>0x0001</td>
<td>A 16-bit unsigned integer, which uniquely identifies the form within the form set. The Form Identifier, along with the device path and Form Set Identifier, uniquely identifies a form within a system.</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - Dashboard View</td>
<td>Title text for the form. The Forms Browser may use this text to describe the nature and purpose of the form in a window title.</td>
</tr>
<tr>
<td>Warning Message Area</td>
<td>See the table with warning messages below. The element is hidden when no warning conditions met.</td>
<td>A text message that alerts the user of a condition that might cause a problem in the future.</td>
</tr>
<tr>
<td>Actions Message Area</td>
<td>See the table with actions' messages below. The element is hidden when no actions required.</td>
<td>A text message to inform user about required actions.</td>
</tr>
</tbody>
</table>
Unique Version numbers X.Y.Z.B that defines all SED UEFI components versions. Where X is a major release number, Y is a minor release number, Z is a “fix” number, B is a build number.

Indicate if SED Security is enabled or disabled for the system. It is referred to as “System Status” in the document.

The element is hidden when no PEK_IDs found in drives' metadata.

Go to Form "Show Key Identifiers".

PEK_ID can be used by the user to identify the system key (PEK) on Remote KMS.

"DISABLED" means here that the element is "greyed out" and the operation cannot be executed.

Go to Form "System Setup".

"DISABLED" means here that the element is "greyed out" and the operation cannot be executed.

Go to Form "System Revert".

"DISABLED" means here that the element is "greyed out" and the operation cannot be executed.

Go to Form "Drive Management".

"DISABLED" means here that the element is "greyed out" and the operation cannot be executed.

The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Setup</td>
<td>Go to Form &quot;System Setup&quot;</td>
</tr>
<tr>
<td>Replace System Keys</td>
<td>Go to Form &quot;Replace System Keys (Re-Key)&quot;</td>
</tr>
<tr>
<td>System Revert</td>
<td>Go to Form &quot;System Revert&quot;</td>
</tr>
<tr>
<td>Drive Management</td>
<td>Go to Form &quot;Drive Management&quot;</td>
</tr>
<tr>
<td>Key identifier</td>
<td>Text with Selected PEK_ID value</td>
</tr>
</tbody>
</table>

The table below describes help text area per selected element.
The table below describes **warning** messages area

<table>
<thead>
<tr>
<th>Warning Text</th>
<th>Help message</th>
<th>Conditions</th>
</tr>
</thead>
</table>
| Can't connect to Key Management Service           | Can't connect to Key Management Service!                                     | • System Status != "Internal Error"  
• KMS status == "DISCONNECTED"                                                                 |
| Can't find any Key Management Service             | Can't find any Key Management Service!                                       | • System Status != "Internal Error"  
• KMS status == "NOT_FOUND"                                                                 |
| Unsupported configuration detected                | Unsupported configuration detected!                                          | • Non-Opal device detected  
(MixedConfigDetected)                                                                 |
| Automatic unlocking or provisioning has failed    | Automatic unlocking or provisioning of Self-Encrypting drive(s) has failed!  | At least one of the following must be true:  
• System Status == "Enabled - Incompatible device detected"  
• "Disabled - Incompatible device detected" && Unknown Security Owner flag is set (3rd party managed drive) |
| Non-Intel Drive detected                          | Intel SSD Only" license is used.                                              | • There is any device with a "non-supported-drive" flag set.  
The SED support is disabled when non-Intel drive(s) detected. |
| System Re-Key completed                           | The Re-Key was continued after reset. The operation has completed successfully. | • Value of system variable STARTUP_REKEY_STATUS is equal to STARTUP_REKEY_CONTINUED_SUCCEEDED |
| System Re-Key failed                              | The Re-Key was continued after reset and has failed. The recovery procedure has been executed. | • Value of system variable STARTUP_REKEY_STATUS is equal to STARTUP_REKEY_CONTINUED_FAILED |
| Foreign Key Identifier detected                   | Key Identifier from a different platform is detected. Re-Key operation is recommended. | PEK_ID from a different platform detected.  
Key Identifier from a different platform is detected. |
| Multiple Key Identifiers detected                  | Multiple Key Identifiers are detected. Re-Key operation is recommended.       | Multiple PEK_IDs detected.                                                                                                               |

The table below describes **actions** messages area

<table>
<thead>
<tr>
<th>ActionText</th>
<th>Help message</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot required</td>
<td>The system reboot is required due to configuration change(s).</td>
<td>• Reset required UEFI HII flag is set</td>
</tr>
</tbody>
</table>
| Unencrypted drive(s) detected           | Unencrypted drive(s) detected. Please provision all drives to secure the system and enable all maintenance operations. | • Drive in "Unencrypted" state detected.  
• System Status is NOT equal "Disabled" or "Disabled - Incompatible device detected" |

**Example Screenshots:**
Intel® VROC Self-Encrypting Drive

Intel® VROC SED - Dashboard View

Intel® VROC SED Manager
Version: 1.0.0.1086
Status: Disabled

Go to form "System Setup"

System Setup
Replace System Keys (Re-Key)
System Revert
Drive Management

F9=Reset to Defaults  F10=Save
↑↓=Move Highlight  <Enter>=Select Entry  Esc=Exit

Copyright (c) 2006-2020, Intel Corporation

Intel® VROC SED - Dashboard View

Intel® VROC SED Manager
Version: 1.0.0.1086
Status: Enabled

Key Identifiers

System Setup
Replace System Keys (Re-Key)
System Revert
Drive Management

F9=Reset to Defaults  F10=Save
↑↓=Move Highlight  <Enter>=Select Entry  Esc=Exit

Copyright (c) 2006-2020, Intel Corporation
11.1.1 Show Key Identifiers

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Id</td>
<td>0x000A</td>
<td>A 16-bit unsigned integer, which uniquely identifies the form within the form set. The Form Identifier, along with the device path and Form Set Identifier, uniquely identifies a form within a system.</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - Show Key Identifiers</td>
<td>Title text for the form. The Forms Browser may use this text to describe the nature and purpose of the form in a window title.</td>
</tr>
<tr>
<td>Key Identifiers(s)</td>
<td>A list of PEK_IDs detected on the drives. The element is hidden when no PEK_IDs found in drives' metadata. If PEK_ID not fit in a single line, it should be truncated and ended with &quot;...&quot;. Full PEK_ID shall be printed in the Help Text Area.</td>
<td>PEK_ID can be used by the user to identify the system key (PEK) on Remote KMS.</td>
</tr>
</tbody>
</table>

The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key identifier</td>
<td>Text with Selected PEK_ID value</td>
</tr>
<tr>
<td>Back to Main Menu</td>
<td>Back to Main Menu</td>
</tr>
</tbody>
</table>

Example Screenshots:
# Intel® VROC SED - Key Identifiers

### Key Identifier(s):

<table>
<thead>
<tr>
<th>Addr</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>6E DD D9 BB</td>
</tr>
<tr>
<td>0x01</td>
<td>1A C8 11 3F</td>
</tr>
<tr>
<td>0x02</td>
<td>77 23 F5 41</td>
</tr>
<tr>
<td>0x03</td>
<td>0x04 1A C8 11</td>
</tr>
<tr>
<td>0x05</td>
<td>77 23 F5 41</td>
</tr>
<tr>
<td>0x06</td>
<td>0x0C D1 B4 D2</td>
</tr>
<tr>
<td>0x07</td>
<td>0x10 1E A8 49</td>
</tr>
<tr>
<td>0x08</td>
<td>0x14 10 F8 76</td>
</tr>
<tr>
<td>0x09</td>
<td>0x18 EF 62 D1</td>
</tr>
<tr>
<td>0x0A</td>
<td>0x1C 03 50 9E</td>
</tr>
<tr>
<td>0x0B</td>
<td>0x20 C2 AF C6</td>
</tr>
<tr>
<td>0x0C</td>
<td>0x24 2F BD C2</td>
</tr>
<tr>
<td>0x0D</td>
<td>0x28 2A 02 DD</td>
</tr>
<tr>
<td>0x0E</td>
<td>0x2C 99 A5 F2</td>
</tr>
<tr>
<td>0x0F</td>
<td>0x30 BE 6B A1</td>
</tr>
</tbody>
</table>

More (D/d)

---

**T↓=Move Highlight**
**Esc=Exit**

Copyright (c) 2006-2020, Intel Corporation
11.2 Drive Management

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Id</td>
<td>0x0004</td>
<td>Unique Id for the form within the form set</td>
</tr>
<tr>
<td>Title</td>
<td>Intel® VROC SED - Drive Management</td>
<td>Title text for the form.</td>
</tr>
<tr>
<td>Warning Message Area</td>
<td>See the table with warning messages below. The element is hidden when no warning conditions met.</td>
<td>A text message that alerts the user of a condition that might cause a problem in the future.</td>
</tr>
<tr>
<td>Physical Drives with Self-Encrypting:</td>
<td>A list of SED capable drives (Model, SN, Capacity). When no SED devices found following text shall be displayed instead: &quot;No Self-Encrypting capable drives connected to the system&quot;.</td>
<td></td>
</tr>
<tr>
<td>Selected Drive (Action)</td>
<td>Go to Form &quot;Drive Detail&quot;</td>
<td></td>
</tr>
<tr>
<td>Physical Drives (Non-supported or without Self-Encrypting):</td>
<td>A list of Non-SED capable drives (Model, SN, Capacity). When IntelSSDOnly license found then, non-Intel drives should be displayed in the list too. When no Non-SED devices found following text shall be displayed instead: &quot;No Drives that are non-supported or without Self-Encrypting capability are connected to the system.&quot;</td>
<td></td>
</tr>
</tbody>
</table>
The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Selected Drive&gt;</td>
<td>View the drive details</td>
</tr>
<tr>
<td>Back to Main Menu</td>
<td>Back to Main Menu</td>
</tr>
</tbody>
</table>

Example Screenshots:

```
Intel(R) VROC SED - Drive Management

Physical Drives with Self-Encrypting:
- INTEL SSDPF2X003BTZ SN:PHAC0151001Q3P8AGN 3.84TB
  Port 5:5, Slot 11, CPU0, VMD0, BDF 02:00.0
  State: Unlocked
- INTEL SSDPF2X003BTZ SN:PHAC0150061Q3P8AGN 3.84TB
  Port 5:9, Slot 12, CPU0, VMD0, BDF 03:00.0
  State: Unlocked

Physical Drives (Non-supported or without Self-Encrypting):
No Drives that are non-supported or without Self-Encrypting capability are connected to the system.

Back to Main Menu
```

Press F1=Move Highlight  <Enter>=Select Entry  Esc=Exit

Copyright (c) 2006-2020, Intel Corporation
11.2.1 Drive Details (Foreign)

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

![Drive Details (Foreign), Version 1.3](image)

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Id</td>
<td>0x0005</td>
<td>Unique Id for the form within the form set</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - Drive details</td>
<td>Title text for the form.</td>
</tr>
<tr>
<td>State</td>
<td>&quot;Unlocked&quot;</td>
<td>&quot;Locked&quot;</td>
</tr>
<tr>
<td>PSID Revert</td>
<td>The action shall be ENABLED when the following conditions are met:</td>
<td>Go to Form &quot;PSID Revert&quot;</td>
</tr>
<tr>
<td></td>
<td>• KMS status is &quot;Connected&quot;</td>
<td></td>
</tr>
<tr>
<td>Back to Drive Management</td>
<td></td>
<td>Go to Form &quot;Drive Management&quot;</td>
</tr>
<tr>
<td>Back to Main Menu</td>
<td></td>
<td>Go to Form &quot;Dashboard View&quot;</td>
</tr>
<tr>
<td>Drive details</td>
<td></td>
<td>Model Number • Serial Number • Size in GB • Root Port Number • Root Port Offset • Slot Number • Socket Number</td>
</tr>
</tbody>
</table>
The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSID Revert</td>
<td>Go to Form &quot;PSID Revert&quot;</td>
</tr>
<tr>
<td>Back to Drive Management</td>
<td>Go back to &quot;Drive Management&quot; form.</td>
</tr>
<tr>
<td>Back to Main Menu</td>
<td>Back to Main Menu</td>
</tr>
</tbody>
</table>

Example Screenshots:
### 11.2.2 Drive Details (Locked/Unlocked)

**NOTE:** The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

![Figure 17: Drive Details (Locked/Unlocked), Version 1.5](image)

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Id</td>
<td>0x05</td>
<td>Unique Id for the form within the form set</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - Drive details</td>
<td>Title text for the form.</td>
</tr>
<tr>
<td>State</td>
<td>&quot;Unlocked&quot;</td>
<td>&quot;Locked&quot;</td>
</tr>
<tr>
<td>Secure Erase Drive for Removal (Action)</td>
<td>The action shall be ENABLED when the following conditions are met:</td>
<td>Go to Form &quot;Drive Revert&quot;</td>
</tr>
<tr>
<td></td>
<td>- KMS status is &quot;Connected&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- System Status is &quot;Enabled&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Drive Status is &quot;Locked&quot; or &quot;Unlocked&quot;</td>
<td></td>
</tr>
<tr>
<td>Back to Drive Management</td>
<td>Go to Form &quot;Drive Management&quot;</td>
<td></td>
</tr>
</tbody>
</table>
Back to Main Menu | Go to Form "Dashboard View"
---|---
Drive details | • Model Number
| • Serial Number
| • Size in GB
| • Root Port Number
| • Root Port Offset
| • Slot Number
| • Socket Number
| • VMD controller
| • PCI BDF

The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Erase Drive for Removal</td>
<td>Secure Erase Drive for Removal</td>
</tr>
<tr>
<td>Back to Drive Management</td>
<td>Go back to “Drive Management” form.</td>
</tr>
<tr>
<td>Back to Main Menu</td>
<td>Back to Main Menu</td>
</tr>
</tbody>
</table>

Example Screenshots:
## Intel® VROC SED - Drive Details

**INTEL SSDPF2X030TZ SN:PHAC015G001Q3P6AGN 3.04TD**

**Status:** <Locked>  
**Go to Form "Secure Erase Drive for Removal"**

**Drive Actions:**
- Secure Erase Drive for Removal
- Back to Drive Management
- Back to Main Menu

<table>
<thead>
<tr>
<th>Model Number</th>
<th>INTEL SSDPF2X030TZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Number</td>
<td>PHAC015G001Q3P6AGN</td>
</tr>
<tr>
<td>Size</td>
<td>3.04TB</td>
</tr>
<tr>
<td>Root Port Number</td>
<td>5</td>
</tr>
<tr>
<td>Root Port Offset</td>
<td>9</td>
</tr>
<tr>
<td>Slot Number</td>
<td>12</td>
</tr>
</tbody>
</table>

---

Copyright (c) 2006-2020, Intel Corporation
11.2.3 Drive Details (Unencrypted)

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

Figure 18: Drive Details (Unencrypted), Version 1.4

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form id</td>
<td>0x05</td>
<td>Unique Id for the form within the form set</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - Drive details</td>
<td>Title text for the form.</td>
</tr>
<tr>
<td>State</td>
<td>&quot;Unencrypted&quot;</td>
<td>Indicate security status for the drive.</td>
</tr>
</tbody>
</table>
| Setup Security Key | The action shall be ENABLED when the following conditions are met:  
                      • KMS status is "Connected"  
                      • System Status is "Enabled"  
                      • Drive Status is "Unencrypted" | Enables encryption on the drive. |
| Back to Drive Management | Go to Form "Drive Management" |                                               |
| Back to Main Menu  | Go to Form "Dashboard View" |                                                 |
The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup Security Key</td>
<td>Take ownership of security on the drive and enable automatic drive unlocking during system boot. A configuration changing like hot-remove or hot-add during the operation is not recommended.</td>
</tr>
<tr>
<td>Back to Drive Management</td>
<td>Go back to &quot;Drive Management&quot; form.</td>
</tr>
<tr>
<td>Back to Main Menu</td>
<td>Back to Main Menu</td>
</tr>
</tbody>
</table>

The table below describes popup details.

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Setup Security completed successfully&quot;</td>
<td>Setup Security configuration on the drive completed successfully.</td>
<td>When the operation completed successfully.</td>
</tr>
<tr>
<td>&quot;Setup Security failed&quot;</td>
<td>Setup security configuration on the drive failed.</td>
<td>When the operation failed.</td>
</tr>
</tbody>
</table>

Example Screenshots:
### 11.2.4 Drive Revert

**NOTE:** The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

![Figure 19: Secure Erase - Prepare drive for removal, Version 1.5](image)

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Id</td>
<td>0x0007</td>
<td>Unique Id for the form within the form set</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - Secure Erase Drive for Removal</td>
<td>Title text for the form.</td>
</tr>
<tr>
<td>Warning Message Area</td>
<td>See the table with warning messages below. The element is hidden when no warning conditions met.</td>
<td>A text message that alerts the user of a condition that might cause a problem in the future.</td>
</tr>
<tr>
<td>Confirm</td>
<td>“OFF” (Default)</td>
<td></td>
</tr>
</tbody>
</table>
| Execute Secure Erase Drive for Removal (Action) | The action shall be ENABLED when the following conditions are met:  
- KMS status is “Connected”  
- System Status is “Enabled” | Perform the revert operation. Go to dialogue box “Secure Erase Drive for Removal is In-Progress”. |
• Drive Status is "Locked" or "Unlocked"
• "Confirm" checkbox is set to "ON"

Back to Drive Details | Go to Form "Drive Details"
Back to Main Menu | Go to Form "Dashboard View"

Drive details
• Model Number
• Serial Number
• Size in GB
• Root Port Number
• Root Port Offset
• Slot Number
• Socket Number
• VMD controller
• PCI BDF

The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute Secure Erase Drive for Removal</td>
<td>The drive will be reverted to OPAL manufacturing-inactive state (all data on the drive will be securely erased). A configuration changing like hot-remove or hot-add during the operation is not recommended.</td>
</tr>
</tbody>
</table>

Back to Drive Details | Go back to "Drive Details" form of this drive
Back to Main Menu | Back to Main Menu

The table below describes popup details.

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Erase Drive for Removal is In-Progress</td>
<td>Reverting security from device could take several minutes. Do not restart platform, wait until operation is completed.</td>
<td>Shall be shown until reverting operation is completed.</td>
</tr>
<tr>
<td>Secure Erase Drive for Removal completed successfully</td>
<td>Reverting Security configuration from the drive completed successfully.</td>
<td>When the operation completed successfully</td>
</tr>
<tr>
<td>&quot;Secure Erase Drive for Removal failed&quot;</td>
<td>Reverting drive security operation failed.</td>
<td>When the operation failed.</td>
</tr>
</tbody>
</table>

The table below describes warning messages area.

<table>
<thead>
<tr>
<th>Warning Message</th>
<th>Description</th>
</tr>
</thead>
</table>
| KMS not connected | The message shall be displayed when the following conditions met:
  • KMS status is NOT equal "Connected"
| System Security not enabled | The message shall be displayed when the following conditions met:
  • System Status is NOT equal "Enabled"

Example Screenshots:
INTEL SSDPF2KX030TZ SN:PHAC0151001Q3P8AGN 3.84TB

Security Reverting will delete Key and configuration. All drive’s data will be erased.
The operation could take several minutes

Confirm

Back to Drive Details
Back to Main Menu

Model Number: INTEL SSDPF2KX030TZ
Serial Number: PHAC0151001Q3P8AGN
Size: 3.84TB
Root Port Number: [5]

F9=Reset to Defaults F10=Save
↑↓=Move Highlight 〈Spacebar〉=Toggle Checkbox Esc=Exit

Intel® VROC Self-Encrypting Drive - Secure Erase Drive for Removal

INTEL SSDPF2KX030TZ SN:PHAC0151001Q3P8AGN 3.84TB

The drive will be reverted to OPAL manufacturing-inactive state (all data on the drive will be securely erased). A configuration changing like hot-remove or hot-add during the operation is not recommended.

Confirm [X]

Back to Drive Details
Back to Main Menu

Model Number: INTEL SSDPF2KX030TZ
Serial Number: PHAC0151001Q3P8AGN
Size: 3.84TB
11.2.5 PSID Revert

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form id</td>
<td>0x0006</td>
<td>Unique Id for the form within the form set</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - PSID Revert</td>
<td>Title text for the form.</td>
</tr>
<tr>
<td>Enter PSID</td>
<td></td>
<td>Physical Presence SID.</td>
</tr>
<tr>
<td>Execute PSID Revert (Action)</td>
<td>Disabled if PSID field not filled with 32 characters.</td>
<td>Operate. Go to dialogue box &quot;PSID Revert In-Progress&quot;. On Success - if System is not in &quot;Disabled&quot; state then Set Reset required UEFI HII flag.</td>
</tr>
<tr>
<td>Back to Drive Details</td>
<td></td>
<td>Go to Form &quot;Drive Details&quot;</td>
</tr>
<tr>
<td>Back to Main Menu</td>
<td></td>
<td>Go to Form &quot;Dashboard View&quot;</td>
</tr>
</tbody>
</table>
The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter PSID</td>
<td>Physical Presence SID. PSID should be printed on the disk label as a 32-character string.</td>
</tr>
<tr>
<td>Execute PSID Revert</td>
<td>The drive will be reverted to OPAL manufacturing-inactive state (all data on the drive will be securely erased). Reset will be required to enable security on the drive. A configuration changing like hot-remove or hot-add during the operation is not recommended.</td>
</tr>
</tbody>
</table>

The table below describes popup details.

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“PSID Revert In-Progress”</td>
<td>Reverting security from device could take several minutes. Do not restart platform, wait until operation is completed.</td>
<td>Shall be shown until reverting operation is completed.</td>
</tr>
<tr>
<td>“PSID Revert completed successfully”</td>
<td>PSID Revert completed successfully.</td>
<td>When the operation completed successfully.</td>
</tr>
<tr>
<td>“PSID Revert failed”</td>
<td>PSID Revert failed.</td>
<td>When the operation failed.</td>
</tr>
</tbody>
</table>

Example Screenshots:

![Example Screenshot](image-url)
11.3 Error Pages

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

![Diagram of error page]

System configuration has changed, please enter the form again to reload data.

Figure 21: Re-enumeration detected error page, Version 1.4

Example Screenshots:
System configuration has changed, please enter the form again to reload data.

Back to Main Menu
11.4 System Revert

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Id</td>
<td>0x0003</td>
<td>Unique Id for the form within the form set</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - System Revert</td>
<td>Title text for the form.</td>
</tr>
<tr>
<td>Physical Drives to Revert</td>
<td>A list of SED capable drives with provisioned security (Model, SN, Capacity)</td>
<td>List of drives with provisioned security.</td>
</tr>
<tr>
<td>Confirm</td>
<td>“OFF” (Default)</td>
<td></td>
</tr>
<tr>
<td>Execute System Revert</td>
<td>The action shall be ENABLED when the following conditions are met:</td>
<td>Operate. Go to dialogue box “Revert System In-Progress”</td>
</tr>
<tr>
<td></td>
<td>• KMS status is &quot;Connected&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• System Status is &quot;Enabled&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &quot;Confirm&quot; checkbox is set to &quot;ON&quot;</td>
<td></td>
</tr>
<tr>
<td>Back to the Main Menu</td>
<td>Go to Form &quot;Dashboard View&quot;</td>
<td></td>
</tr>
</tbody>
</table>

The table below describes help text area per selected element.

Figure 22: System Revert, Version 1.3
Execute Revert System

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute Revert System</td>
<td>Destroys the System Key. All secured drives will be reverted to OPAL manufacturing inactive state (erase all data). A configuration changing like hot-remove or hot-add during the operation is not recommended.</td>
<td></td>
</tr>
</tbody>
</table>

The table below describes popup details.

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Revert System In-Progress&quot;</td>
<td>Reverting security from devices could take several minutes. Do not restart platform, wait until operation is completed.</td>
<td>Shall be shown until reverting operation is completed.</td>
</tr>
<tr>
<td>&quot;Reverting Security completed successfully&quot;</td>
<td>Reverting Security configuration from the system completed successfully.</td>
<td>When the operation completed successfully. Refresh Physical Drives to Revert List.</td>
</tr>
<tr>
<td>&quot;Reverting Security failed&quot;</td>
<td>Reverting system security operation failed.</td>
<td>When the operation failed. Refresh Physical Drives to Revert List.</td>
</tr>
</tbody>
</table>

Example Screenshots:

Revert security configuration from the system.

Physical Drives to Revert:
INTEL SSDPF2K03T2 SN:PHAC0151001Q3P8AGN 3.84TB
INTEL SSDPF2K03T2 SN:PHAC0150001Q3P8AGN 3.84TB

All secured drives will be reverted and data erased. Reverting security from all drives could take several minutes.

Confirm [X]
Execute System Revert

Back to Main Menu

F9-Reset to Defaults  F10-Save
†1-Move Highlight  †—Select Entry  Esc-Exit

Copyright (c) 2006-2020, Intel Corporation
11.5 System Rotate Keys (Re-Key)

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

Figure 23: System Rotate Keys (Re-Key), Version 1.4

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Id</td>
<td>0x0002</td>
<td>Unique Id for the form within the form set</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - Replace System Keys (Re-Key)</td>
<td>Title text for the form.</td>
</tr>
<tr>
<td>Physical Drives to provision (List)</td>
<td>A list of SED capable drives to Re-Key (Model, SN, Capacity). If no drives to shown display &quot;No drives to Re-Key found&quot;.</td>
<td>List of drives to re-keys. Only drives with state equal to &quot;Unlocked&quot; or &quot;Locked&quot;.</td>
</tr>
<tr>
<td>Execute System Re-Key(Action)</td>
<td>The action shall be ENABLED when the following conditions are met: KMS status is &quot;Connected&quot; System Status is &quot;Enabled&quot;</td>
<td>Perform a change of all keys used by the VROC SED. Go to dialogue box &quot;Re-Key in progress&quot;.</td>
</tr>
</tbody>
</table>

The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute System Re-Key</td>
<td>Execute the operation. Perform a change of all keys used by the VROC SED. A configuration changing like hot-remove or hot-add during the operation is not recommended.</td>
</tr>
</tbody>
</table>

Do not restart the platform. Wait until the operation is completed.

System Re-key completed successfully.

Setup Re-key operation has been interrupted due to failing on the following device: <device details>
The table below describes popup details.

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Re-Key in progress&quot;</td>
<td>Do not restart the platform. Wait until the operation is completed.</td>
<td>Shall be shown until re-key operation is completed.</td>
</tr>
<tr>
<td>&quot;System Re-Key completed successfully&quot;</td>
<td>System Re-Key completed successfully.</td>
<td>When the operation completed successfully</td>
</tr>
<tr>
<td>&quot;System Re-Key failed&quot;</td>
<td>System Re-Key operation has been interrupted due to failing on the following device: INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB</td>
<td>When the operation failed and there is issue connected with a particular drive.</td>
</tr>
<tr>
<td>&quot;System Re-Key failed&quot;</td>
<td>System Re-Key operation has been interrupted due to a general failure.</td>
<td>When the operation failed, and there is NO information which drive has failed.</td>
</tr>
</tbody>
</table>

Example Screenshots:

```
Intel® VROC Self-Encrypting Drive
27 June, 2022

Back to Main Menu

The table below describes popup details.

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Re-Key in progress&quot;</td>
<td>Do not restart the platform. Wait until the operation is completed.</td>
<td>Shall be shown until re-key operation is completed.</td>
</tr>
<tr>
<td>&quot;System Re-Key completed successfully&quot;</td>
<td>System Re-Key completed successfully.</td>
<td>When the operation completed successfully</td>
</tr>
<tr>
<td>&quot;System Re-Key failed&quot;</td>
<td>System Re-Key operation has been interrupted due to failing on the following device: INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB</td>
<td>When the operation failed and there is issue connected with a particular drive.</td>
</tr>
<tr>
<td>&quot;System Re-Key failed&quot;</td>
<td>System Re-Key operation has been interrupted due to a general failure.</td>
<td>When the operation failed, and there is NO information which drive has failed.</td>
</tr>
</tbody>
</table>

Example Screenshots:

```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
11.6 System Setup

NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.

The table below describes the attributes of the form.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form id</td>
<td>0x0008</td>
<td>Unique id for the form within the form set</td>
</tr>
<tr>
<td>Title</td>
<td>Intel(R) VROC SED - Setup</td>
<td>Title text for the form.</td>
</tr>
<tr>
<td>Physical Drives to provision (List)</td>
<td>A list of SED capable drives to provision security (Model, SN, Capacity). When no SED devices found following text shall be displayed instead: &quot;No Self-Encrypting capable drives connected to the system&quot;.</td>
<td>List of drives to provisioned security on</td>
</tr>
<tr>
<td>Execute System Setup (Action)</td>
<td>The action shall be ENABLED when the following conditions are met: • KMS status is &quot;Connected&quot; • System Status is &quot;Disabled&quot; • There is at least one VMD attached drive with OPAL capability.</td>
<td>Generates the System Key and prepares the system for secured RAID arrays and drives. It also enables encryption on all the NVMe drives in the system. Go to dialogue box &quot;Setup in progress&quot;.</td>
</tr>
<tr>
<td>Back to the Main Menu</td>
<td></td>
<td>Go to Form &quot;Dashboard View&quot;</td>
</tr>
</tbody>
</table>

The table below describes help text area per selected element.

<table>
<thead>
<tr>
<th>Element</th>
<th>Help message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute System Setup</td>
<td>Generates the System Key and prepares the system for secured RAID arrays and drives. It also enables encryption on all the NVMe drives in the system.</td>
</tr>
</tbody>
</table>
A configuration changing like hot-remove or hot-add during the operation is not recommended.

<table>
<thead>
<tr>
<th>Element</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Setup in progress&quot;</td>
<td>Do not restart the platform. Wait until the operation is completed.</td>
<td>Shall be shown until setup operation is completed.</td>
</tr>
<tr>
<td>&quot;Setup Security completed successfully&quot;</td>
<td>Setup Security configuration on the system completed successfully.</td>
<td>When the operation completed successfully</td>
</tr>
<tr>
<td>&quot;Setup Security failed&quot;</td>
<td>Setup system security operation has been interrupted due to failing on the following device: INTEL SSDPE21K375GA SN:PHKE71S1005Q375AGN, 349.32GB</td>
<td>When the operation failed and there is issue connected with a particular drive.</td>
</tr>
<tr>
<td>&quot;Setup Security failed&quot;</td>
<td>Setup system security operation has been interrupted due to a general failure.</td>
<td>When the operation failed, and there is NO information which drive has failed.</td>
</tr>
</tbody>
</table>

Example Screenshots:

Enable security on the system.

Physical Drives to provision:
INTEL SSDP2K8038T2 SN:PHAC0151001Q3P8AGN 3.84TB
INTEL SSDP2K8038T2 SN:PHAC0150001Q3P8AGN 3.84TB

Execute System Setup

Back to Main Menu

Generates the System Key and prepares the system for secured RAID arrays and drives. It also enables encryption on all the NUMA drives in the system.
A configuration changing like hot-remove or hot-add during the operation is not recommended.