Intel® VROC Self-Encrypting Drive

High Level Architecture for Intel® Xeon® Scalable based Platforms

Document Revision 1.0

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Intel products are not intended for use in medical, life saving, or life sustaining applications.
Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.
No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware and/or software optimized to use the technologies. Consult your system manufacturer and/or software vendor for more information.
Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. Check with your system manufacturer or retailer to learn more at intel.com.
The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.
Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.
All products, computer systems, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Table of Contents

1 Revision History

Revision	Date	Description
0.1		Initial version
1.0	02/02/2022	Document format changes

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

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

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 equality 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.

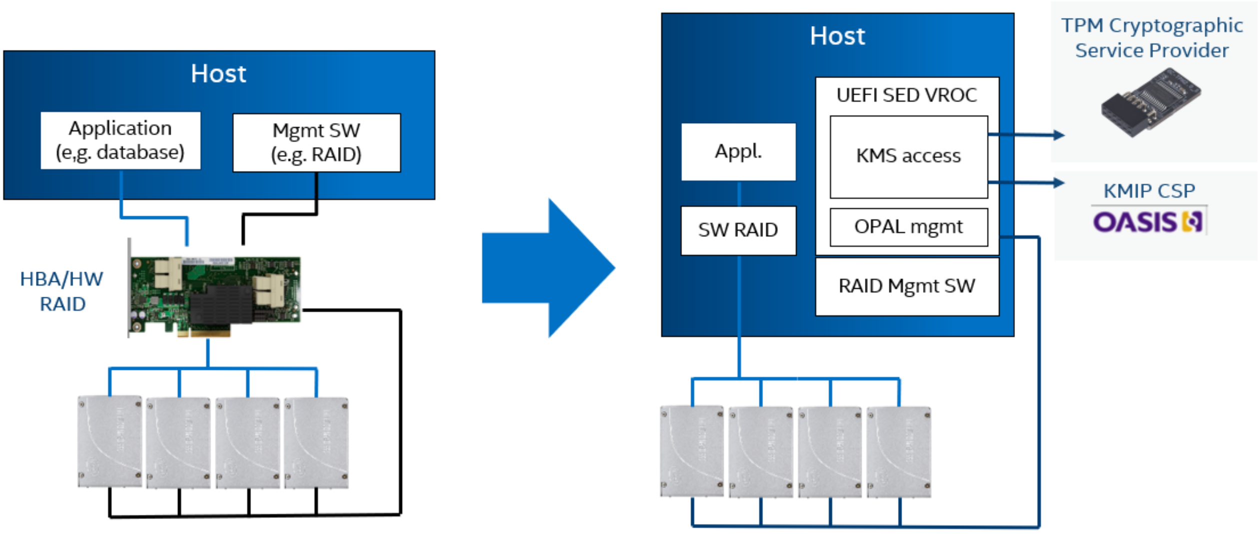


Figure: The HW HBA/RAID to VROC transition

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.

SED UEFI Component Model
Version 1.0

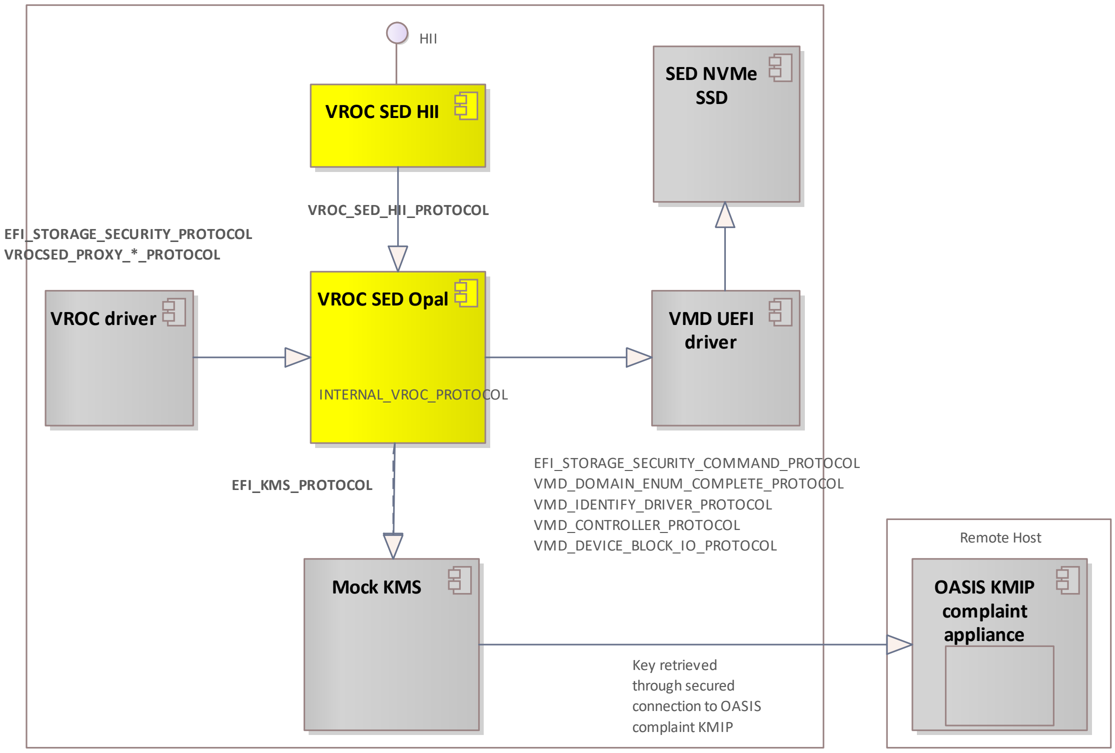

HII
VROC SED HII
SED NVMe SSD
VROC_SED_HII_PROTOCOL
EFI_STORAGE_SECURITY_PROTOCOL
VROCSED_PROXY_*_PROTOCOL
VROC driver
VROC SED Opal
INTERNAL_VROC_PROTOCOL
VMD UEFI driver
EFI_KMS_PROTOCOL
EFI_STORAGE_SECURITY_COMMAND_PROTOCOL
VMD_DOMAIN_ENUM_COMPLETE_PROTOCOL
VMD_IDENTIFY_DRIVER_PROTOCOL
VMD_CONTROLLER_PROTOCOL
VMD_DEVICE_BLOCK_IO_PROTOCOL
Remote Host
Mock KMS
OASIS KMIP complaint appliance
Key retrieved through secured connection to OASIS complaint KMIP

Figure 1: SED UEFI Component Model

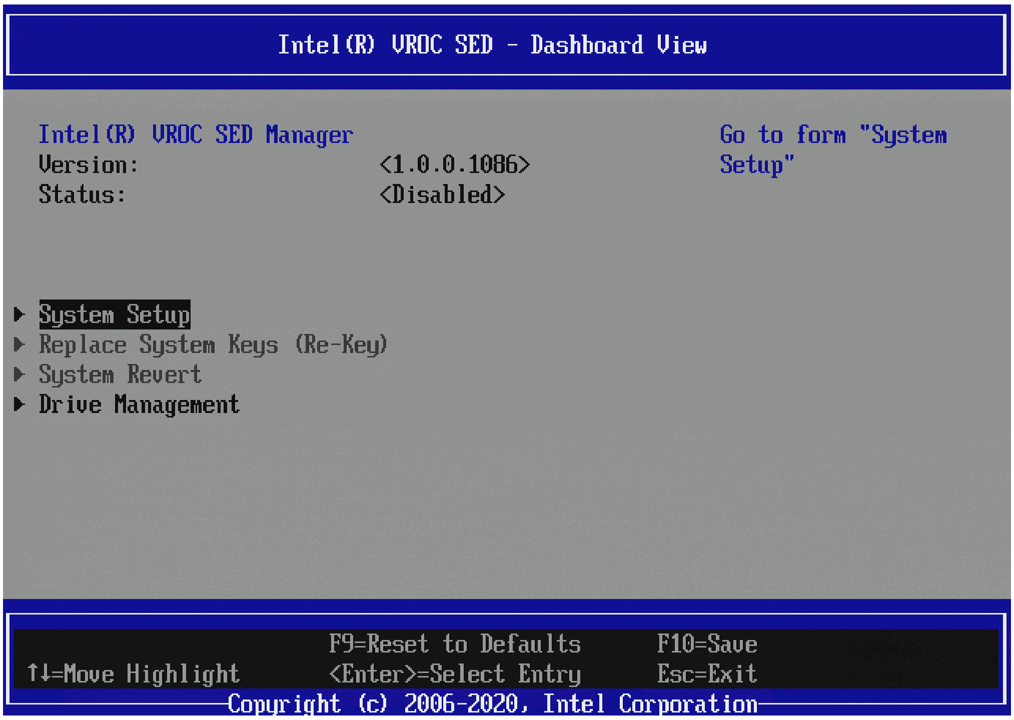
5.1.1 SED UEFI Components

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(R) VROC SED - Dashboard View

Intel(R) VROC SED Manager                         Go to form "System
Version:                  <1.0.0.1086>            Setup"
Status:                   <Disabled>


▶ 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
```

6 Key hierarchy and management

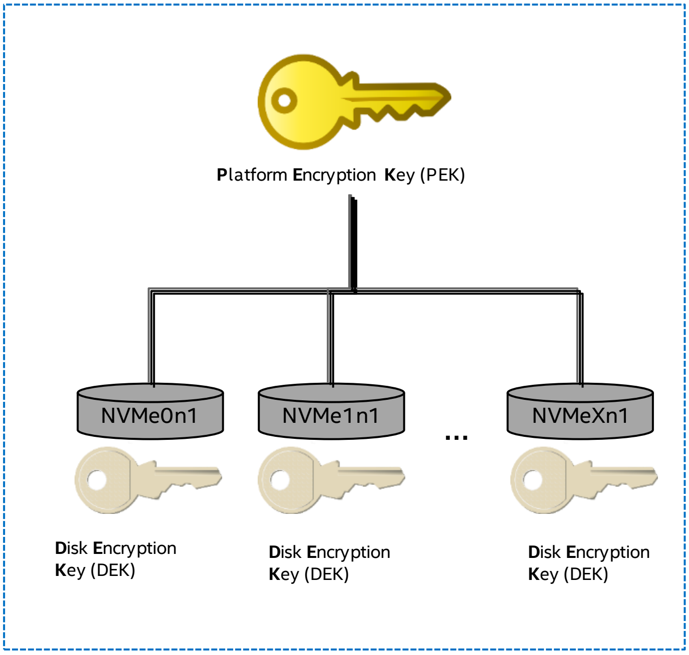
Platform Encryption Key (PEK):

- 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.

Single server perspective


Platform Encryption Key (PEK)
NVMe0n1
NVMe1n1
...
NVMeXn1
Disk Encryption Key (DEK)
Disk Encryption Key (DEK)
Disk Encryption Key (DEK)

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.

Algorithm (+key length +mode/padding scheme)	Usage	Parameters
AES—256 GCM mode, no padding	wrapping/unwrapping SALT that is used for DEK creation	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
HMAC-based Key Derivation Function	Derivation of PEK_HKDF_NO_SALT	Key (SKM) – PEK key retrieved from network-attached KMS appliance

(HKDF)	from PEK.	Salt (XTSALT) – 0's (32 zero bytes) CTXInfo – "SALT PROTECTION KEY DERIVATION" L – 32 bytes
HMAC-based Key Derivation Function (HKDF)	Derivation of DEK from PEK and Salt	Key (SKM) – PEK key retrieved from network-attached KMS appliance Salt (XTSALT) – Generated by the product and stored in encrypted form in the drive OPAL DataStore CTXInfo – "DISK ENCRYPTION KEY DERIVATION" L – 32 bytes

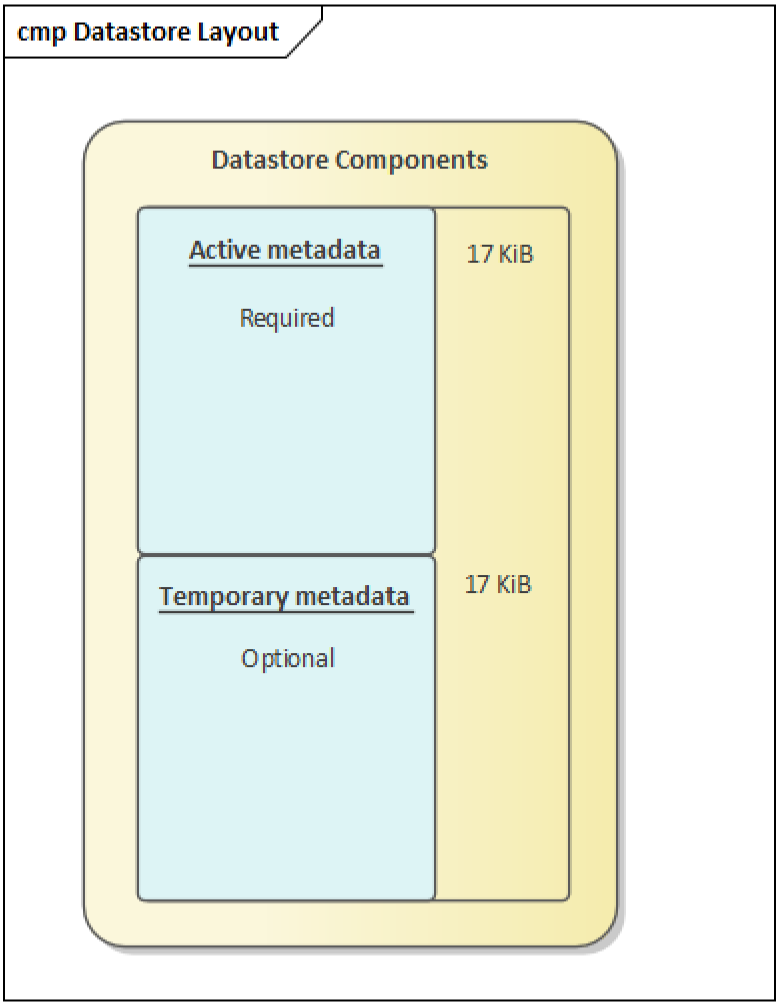
6.2 Cryptographic Keys and Their Properties

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

Key Name	Algorithm/Size	Usage	At rest location
Platform Encryption Key (PEK)	HKDF 256	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).	Stored persistently in 3rd party OASIS KMIP compliant Key Management Server
DEK	256 bits	Used as SID and Admin1 authentication key in Opal compliant disk	Created from PEK and DEK_SALT. DEK_SALT is stored on the drive in the Opal datastore region in encrypted form.
PEK_HKDF_NO_SALT	AES 256	Used to wrap/unwrap Disk Encryption Key Salt (DEK_SALT) by using AES-256 in GCM mode.	Created from PEK and "no-salt" (0's - 32 zero bytes).

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.



7.1 Device Metadata Layout

Section	Offset	Length	Description	Notes
Metadata descriptor (9B)	0			
	0	8	Metadata identifier	
	8	1	Metadata version	
Encryption algorithm descriptor (7B)	9	1	Algorithm version	
	10	6	Reserved	
Encryption algorithm attributes (368B)	16	1	Platform Encryption Key (PEK) size in bytes	
	17	255	Platform Encryption Key (PEK)	
	272	1	IV size	
	273	64	Initial vector (IV) for encryption algorithm	

	337	47	Reserved	Align to 128B
UEFI/OS metadata (128B)	384	2	Reserved for ReKey temporary data	number of drives
	386	16	Platform UUID	
	402	110	Reserved	Align to 128B
Key section	512	1	Key entries count	
	513 + (N*dek_salt_entry_size)	16	Entry "N" DEK_SALT guid	
	529 + (N*dek_salt_entry_size)	2	Entry "N" DEK_SALT offset	
	5103 + (N*dek_salt_size)	32	Encrypted "N" DEK_SALT value	
	5135 + (N*dek_salt_size)	16	Encrypted "N" DEK_SALT AES-GCM tag	
	17343	65	Reserved	Align to 128B

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)

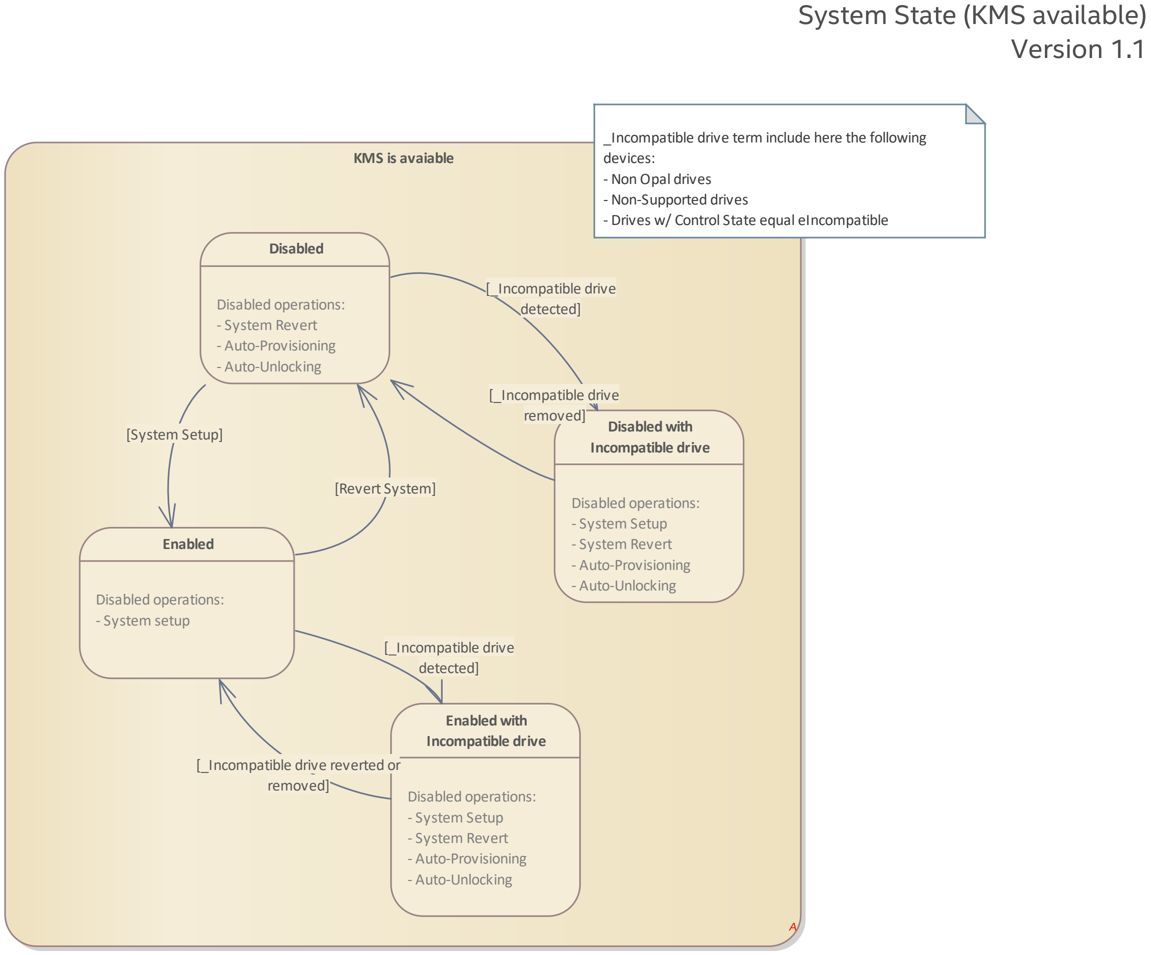


Figure 2: System State (KMS available)

8.2 System State (KMS NOT available)

System State (KMS NOT available)
Version 1.0

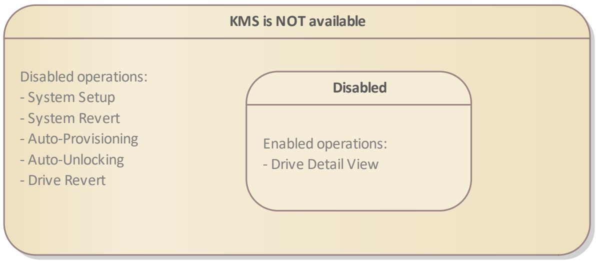


Figure 3: System State (KMS NOT available)

8.3 Drive State

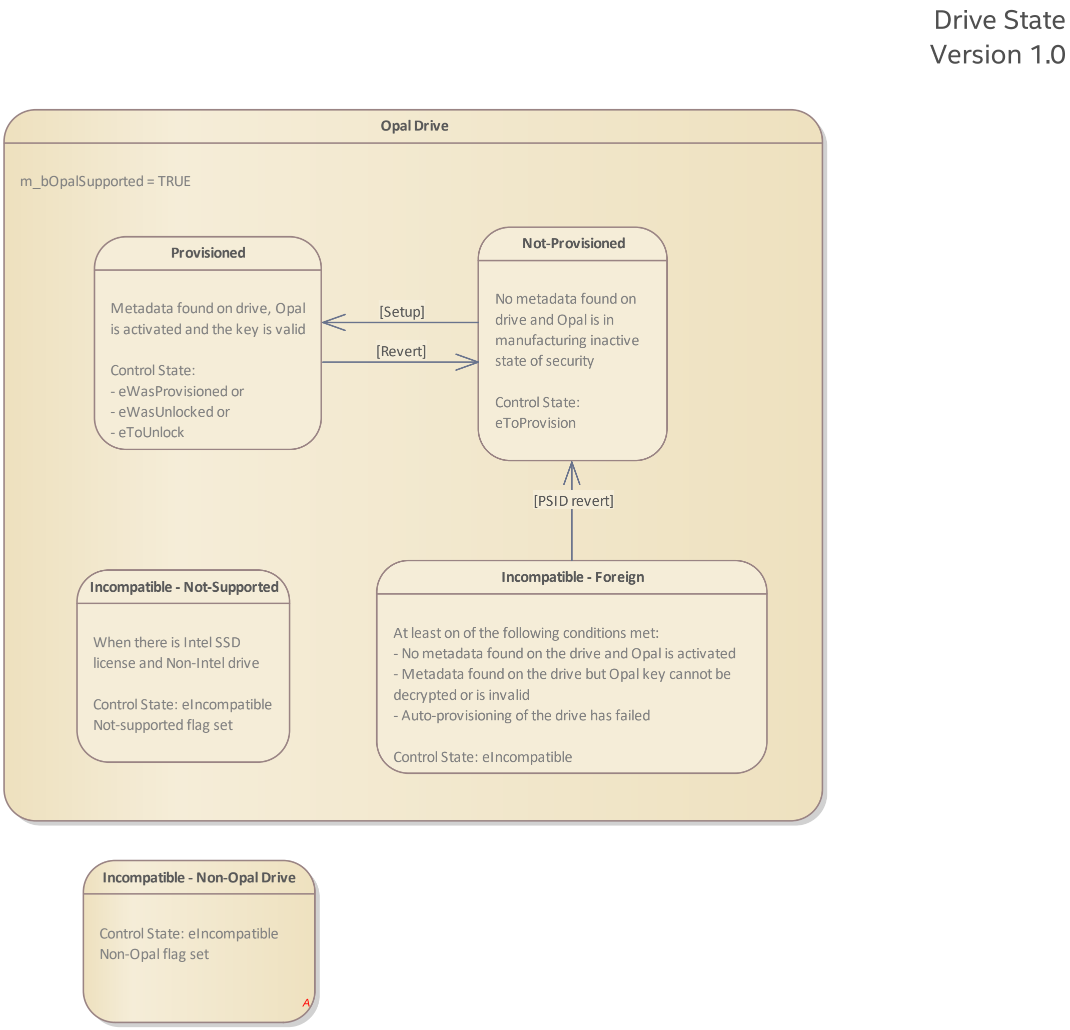

Drive State
Version 1.0
Opal Drive
m_bOpalSupported = TRUE
Provisioned
Metadata found on drive, Opal is activated and the key is valid
Control State:
- eWasProvisioned or
- eWasUnlocked or
- eToUnlock
[Setup]
[Revert]
Not-Provisioned
No metadata found on drive and Opal is in manufacturing inactive state of security
Control State:
eToProvision
[PSID revert]
Incompatible - Not-Supported
When there is Intel SSD license and Non-Intel drive
Control State: eIncompatible Not-supported flag set
Incompatible - Foreign
At least on of the following conditions met:
- No metadata found on the drive and Opal is activated
- Metadata found on the drive but Opal key cannot be decrypted or is invalid
- Auto-provisioning of the drive has failed
Control State: eIncompatible
Incompatible - Non-Opal Drive
Control State: eIncompatible
Non-Opal flag set

Figure 4: Drive State

8.4 Manual System Setup from HII

Manual System Setup from HII
Version 1.0

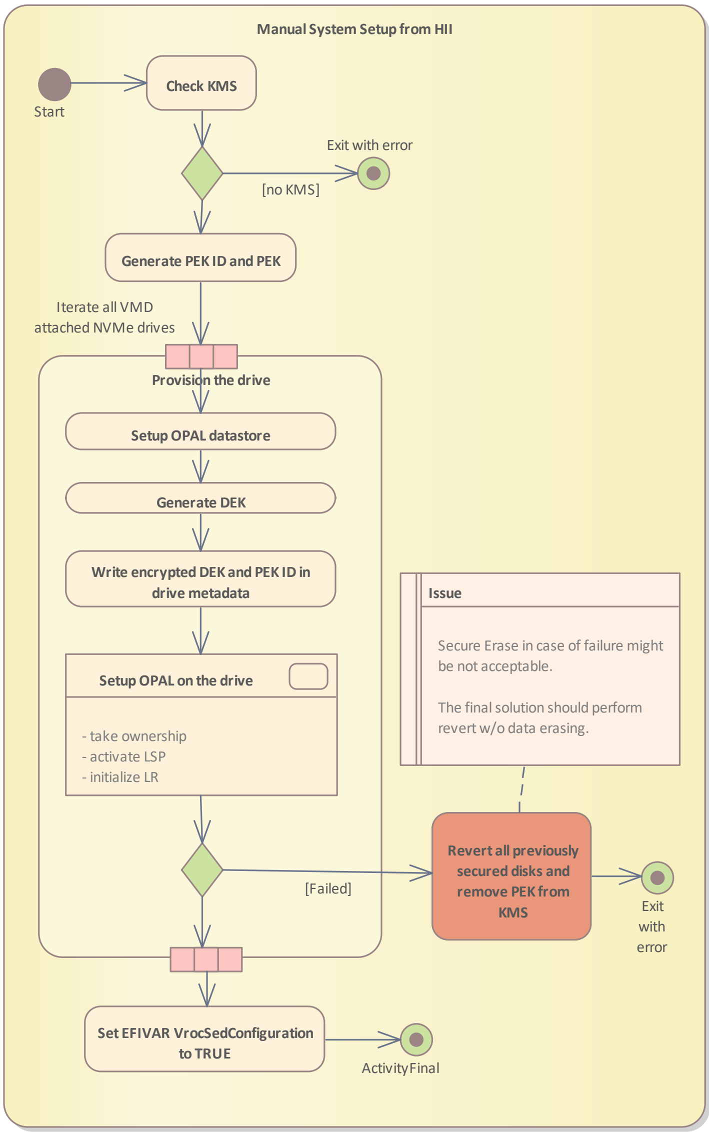

Manual System Setup from HII
Start
Check KMS
Exit with error
[no KMS]
Generate PEK ID and PEK
Iterate all VMD attached NVMe drives
Provision the drive
Setup OPAL datastore
Generate DEK
Write encrypted DEK and PEK ID in drive metadata
Setup OPAL on the drive
- take ownership
- activate LSP
- initialize LR
Issue
Secure Erase in case of failure might be not acceptable.
The final solution should perform revert w/o data erasing.
[Failed]
Revert all previously secured disks and remove PEK from KMS
Exit with error
Set EFIVAR VrocSedConfiguration to TRUE
ActivityFinal

Figure 5: Manual System Setup from HII

8.5 Auto-Provisioning and Auto-Unlocking

Auto-Provisioning and Auto-Unlocking
Version 1.0

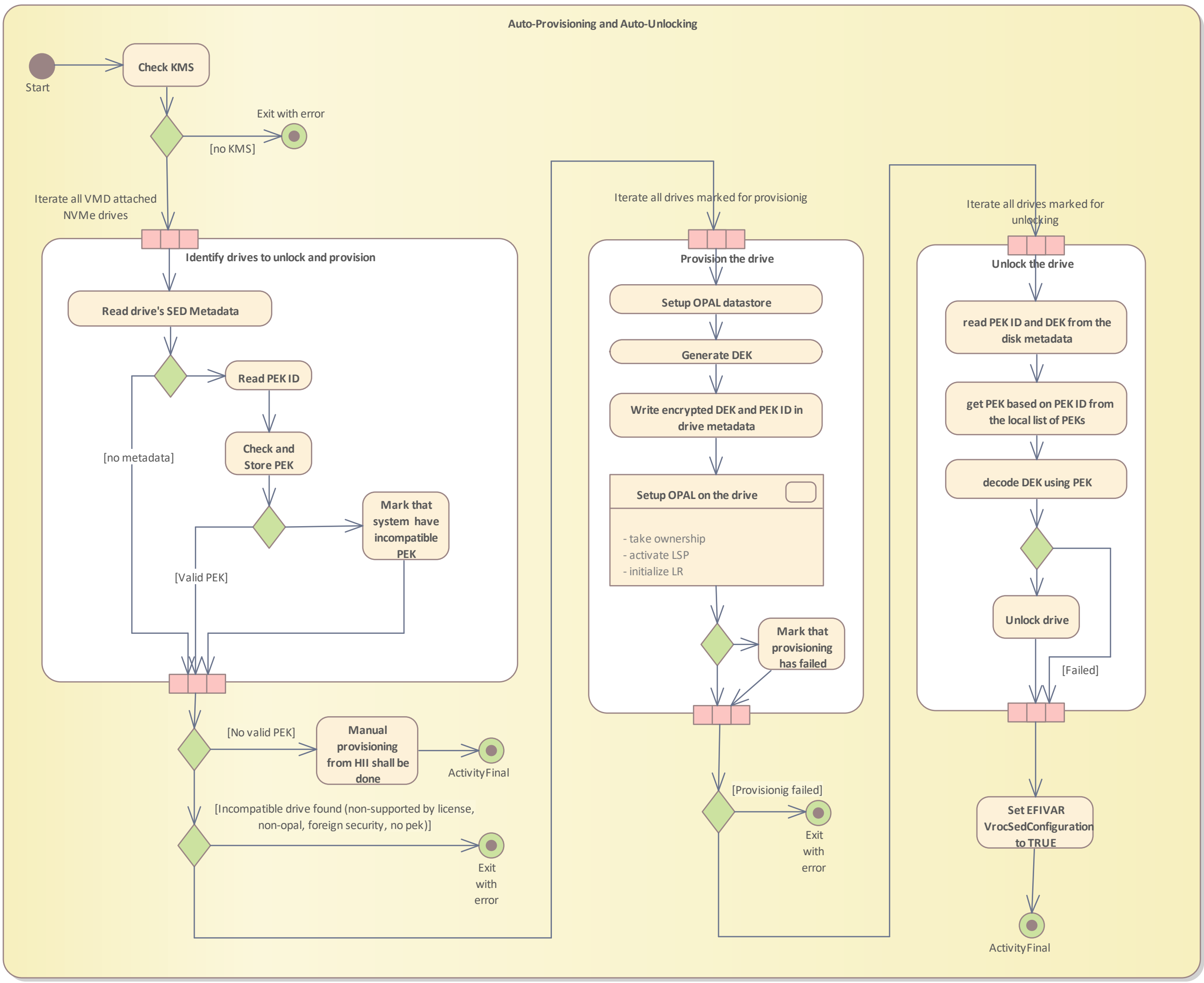

Auto-Provisioning and Auto-Unlocking
Start
Check KMS
Exit with error
[no KMS]
Iterate all VMD attached NVMe drives
Identify drives to unlock and provision
Read drive's SED Metadata
Read PEK ID
[no metadata]
Check and Store PEK
Mark that system have incompatible PEK
[Valid PEK]
[No valid PEK]
Manual provisioning from HII shall be done
ActivityFinal
[Incompatible drive found (non-supported by license, non-opal, foreign security, no pek)]
Exit with error
Iterate all drives marked for provisionig
Provision the drive
Setup OPAL datastore
Generate DEK
Write encrypted DEK and PEK ID in drive metadata
Setup OPAL on the drive
- take ownership
- activate LSP
- initialize LR
Mark that provisioning has failed
[Provisionig failed]
Exit with error
Iterate all drives marked for unlocking
Unlock the drive
read PEK ID and DEK from the disk metadata
get PEK based on PEK ID from the local list of PEKs
decode DEK using PEK
Unlock drive
[Failed]
Set EFIVAR VrocSedConfiguration to TRUE
ActivityFinal

Figure 6: Auto-Provisioning and Auto-Unlocking

8.6 Re-key

Re-key
Version 1.0

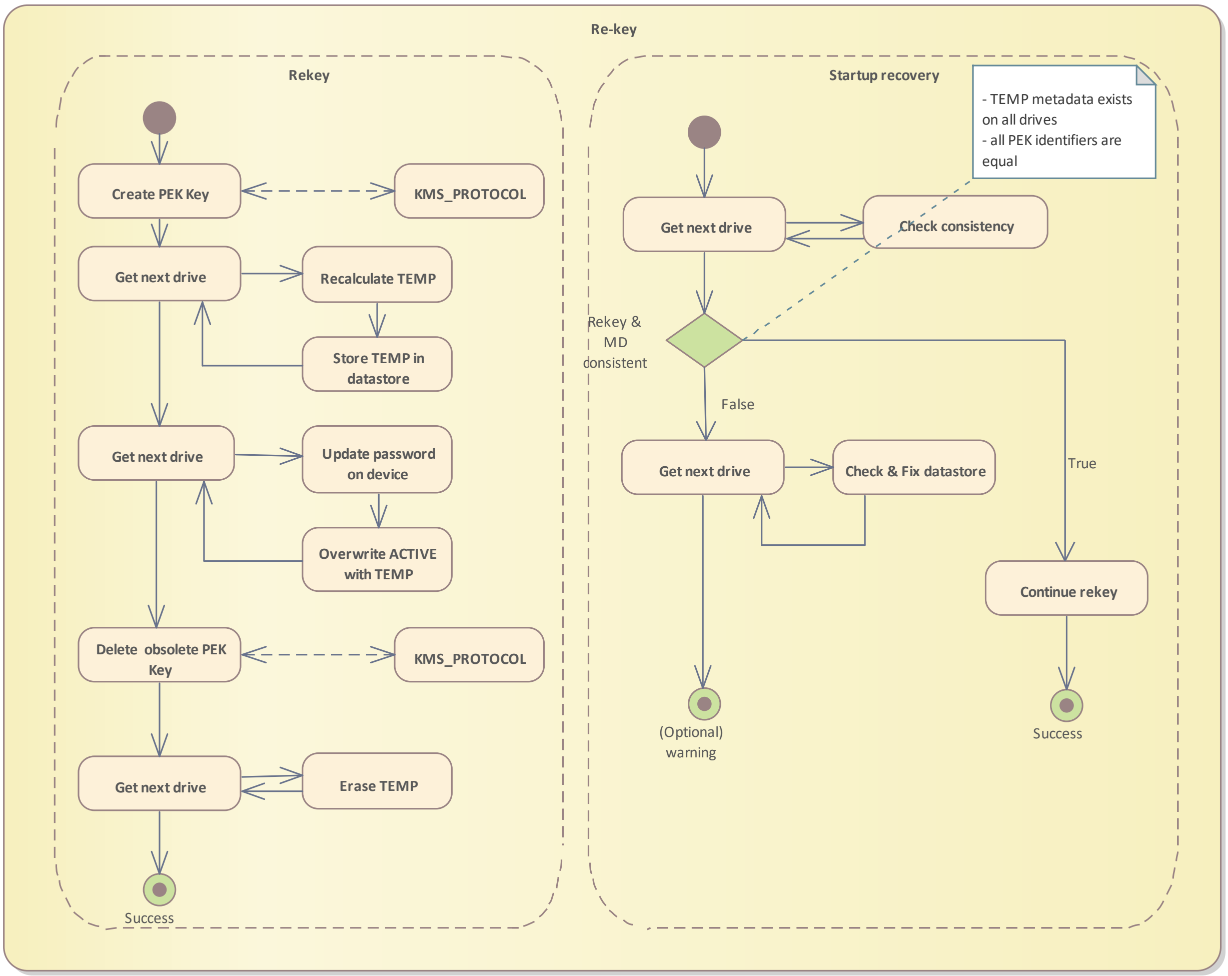


Figure 7: Re-key

8.7 Lock on Hot-plug

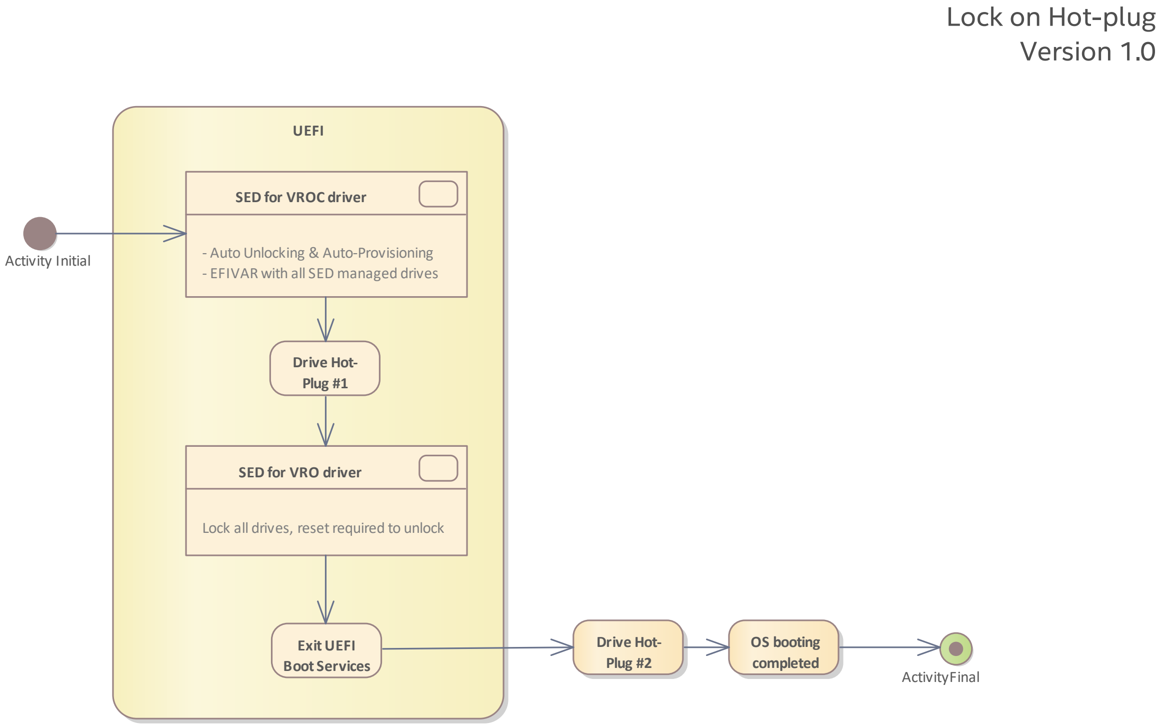


Figure 8: Lock on Hot-plug

9 Architecture - EFI KMS protocol

9.1 Activity diagram for KMS.CreateKey()

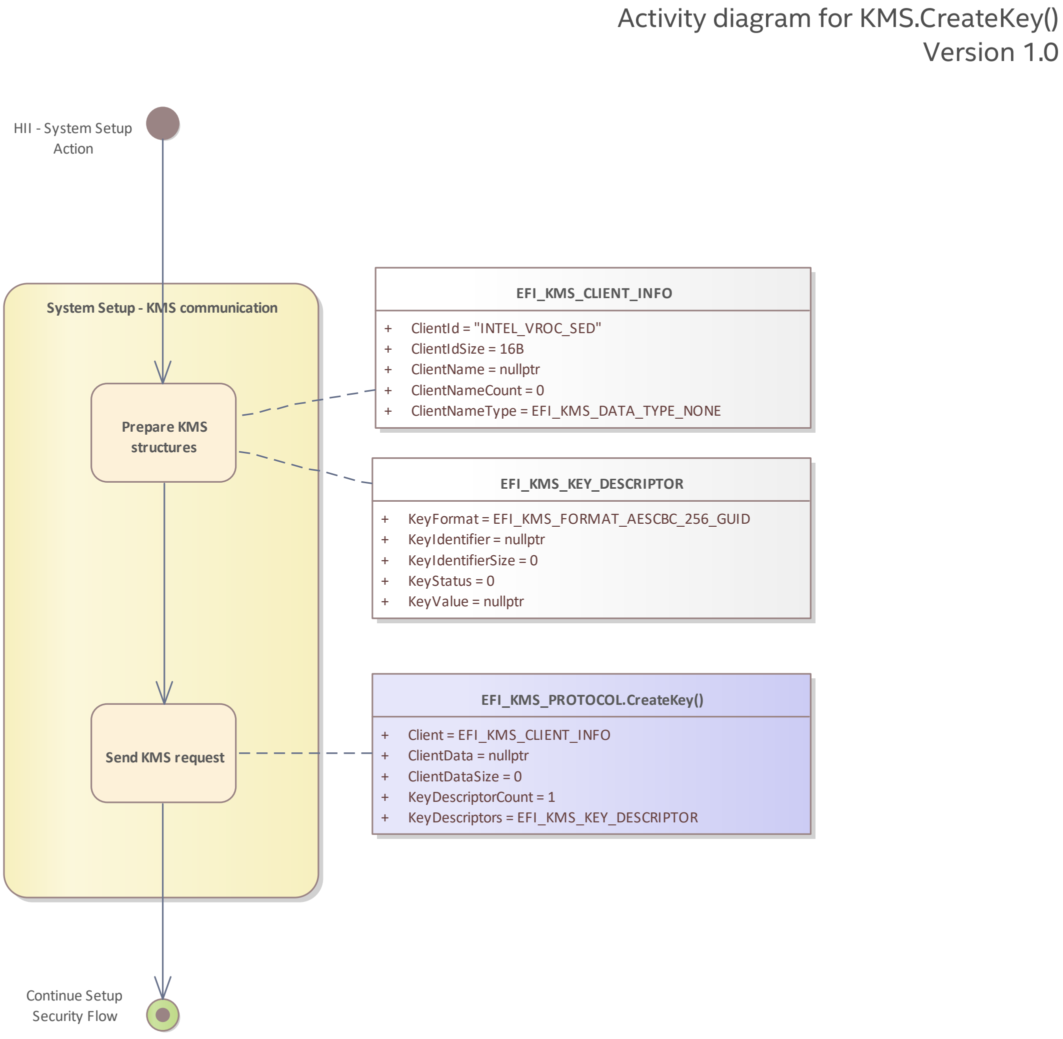

Activity diagram for KMS.CreateKey()
Version 1.0
HII - System Setup Action
System Setup - KMS communication
Prepare KMS structures
Send KMS request
Continue Setup Security Flow
EFI_KMS_CLIENT_INFO
+ ClientId = "INTEL_VROC_SED"
+ ClientIdSize = 16B
+ ClientName = nullptr
+ ClientNameCount = 0
+ ClientNameType = EFI_KMS_DATA_TYPE_NONE
EFI_KMS_KEY_DESCRIPTOR
+ KeyFormat = EFI_KMS_FORMAT_AESCBC_256_GUID
+ KeyIdentifier = nullptr
+ KeyIdentifierSize = 0
+ KeyStatus = 0
+ KeyValue = nullptr
EFI_KMS_PROTOCOL.CreateKey()
+ Client = EFI_KMS_CLIENT_INFO
+ ClientData = nullptr
+ ClientDataSize = 0
+ KeyDescriptorCount = 1
+ KeyDescriptors = EFI_KMS_KEY_DESCRIPTOR

Figure 9: Activity diagram for KMS.CreateKey()

9.2 Activity diagram for KMS.DeleteKey()

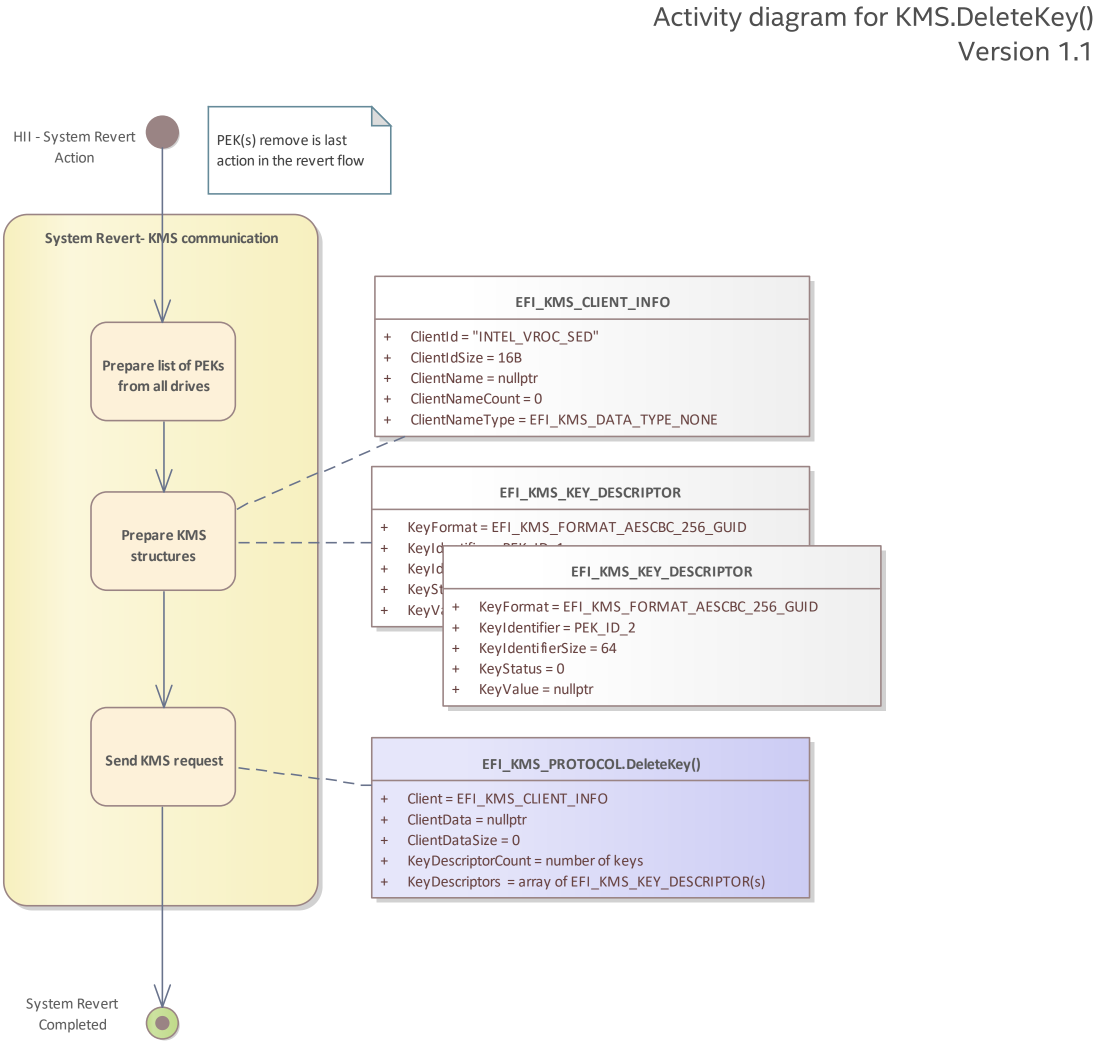

Activity diagram for KMS.DeleteKey()
Version 1.1
HII - System Revert Action
PEK(s) remove is last action in the revert flow
System Revert- KMS communication
Prepare list of PEKs from all drives
Prepare KMS structures
Send KMS request
EFI_KMS_CLIENT_INFO
+ ClientId = "INTEL_VROC_SED"
+ ClientIdSize = 16B
+ ClientName = nullptr
+ ClientNameCount = 0
+ ClientNameType = EFI_KMS_DATA_TYPE_NONE
EFI_KMS_KEY_DESCRIPTOR
+ KeyFormat = EFI_KMS_FORMAT_AESCBC_256_GUID
+ KeyId
+ KeyId
+ KeySt
+ KeyV
EFI_KMS_KEY_DESCRIPTOR
+ KeyFormat = EFI_KMS_FORMAT_AESCBC_256_GUID
+ KeyIdentifier = PEK_ID_2
+ KeyIdentifierSize = 64
+ KeyStatus = 0
+ KeyValue = nullptr
EFI_KMS_PROTOCOL.DeleteKey()
+ Client = EFI_KMS_CLIENT_INFO
+ ClientData = nullptr
+ ClientDataSize = 0
+ KeyDescriptorCount = number of keys
+ KeyDescriptors = array of EFI_KMS_KEY_DESCRIPTOR(s)
System Revert Completed

Figure 10: Activity diagram for KMS.DeleteKey()

9.3 Activity diagram for KMS.GetKey()

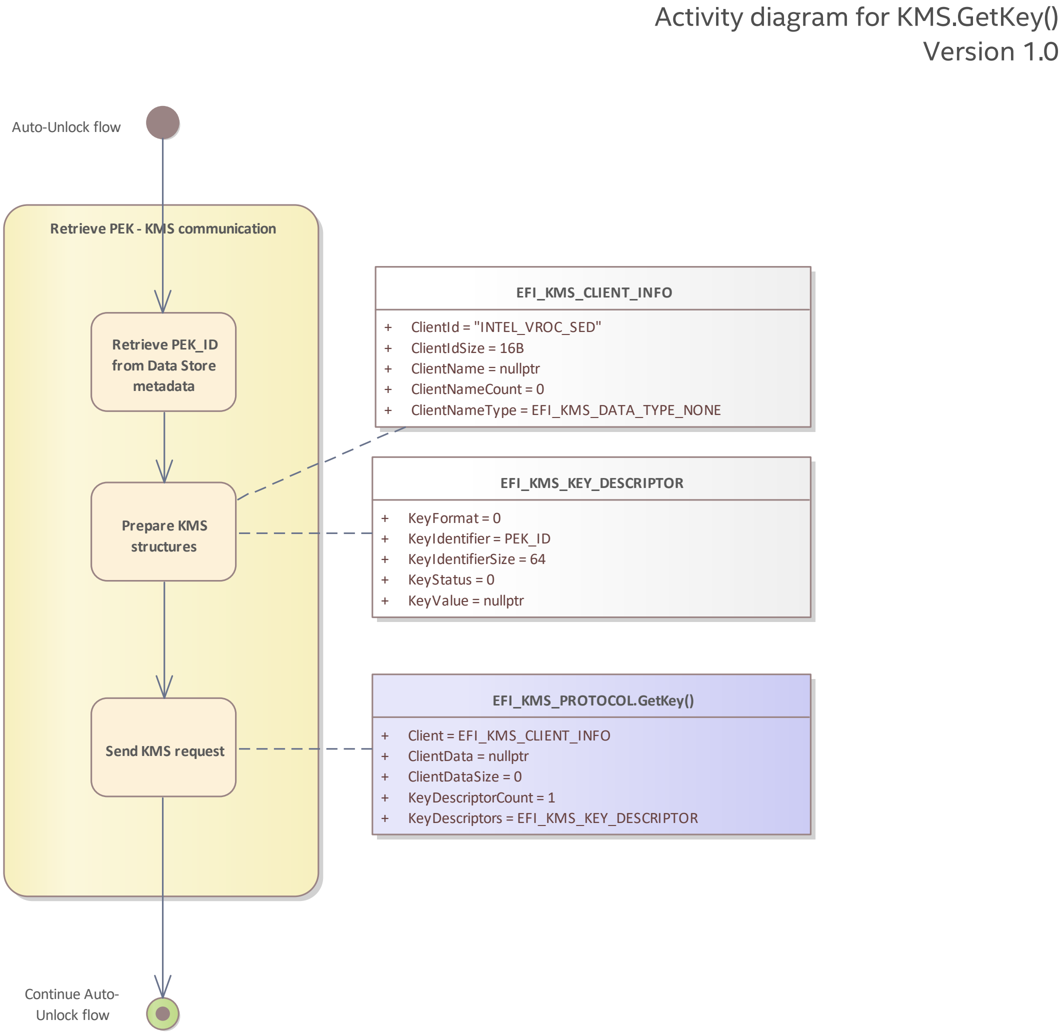


Figure 11: Activity diagram for KMS.GetKey()

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}.

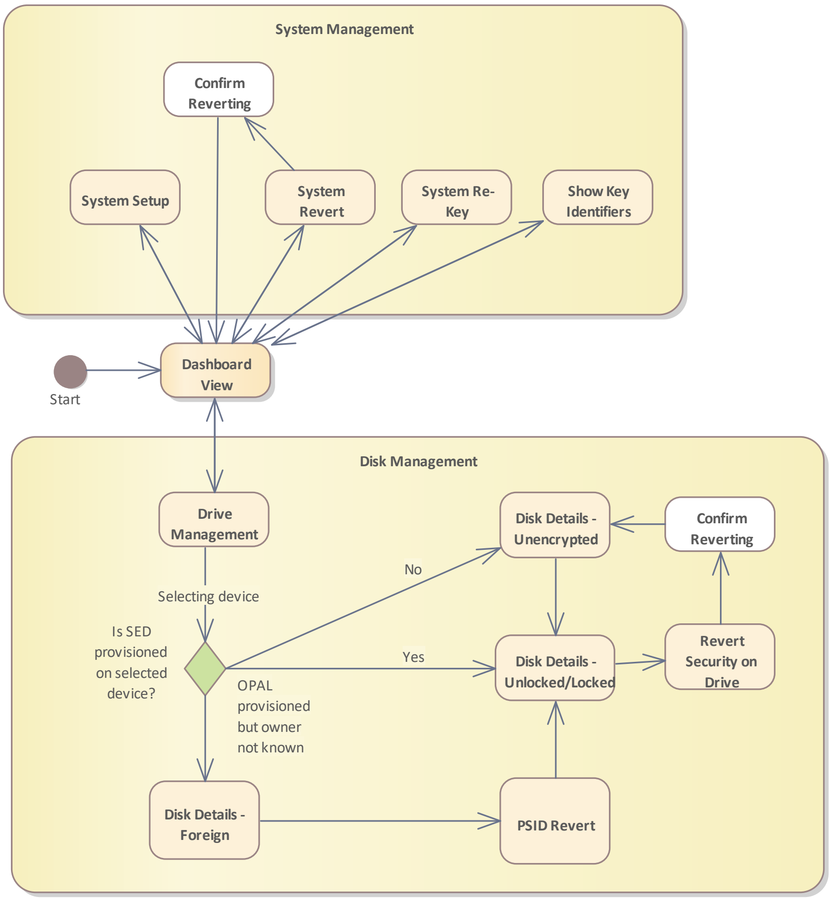
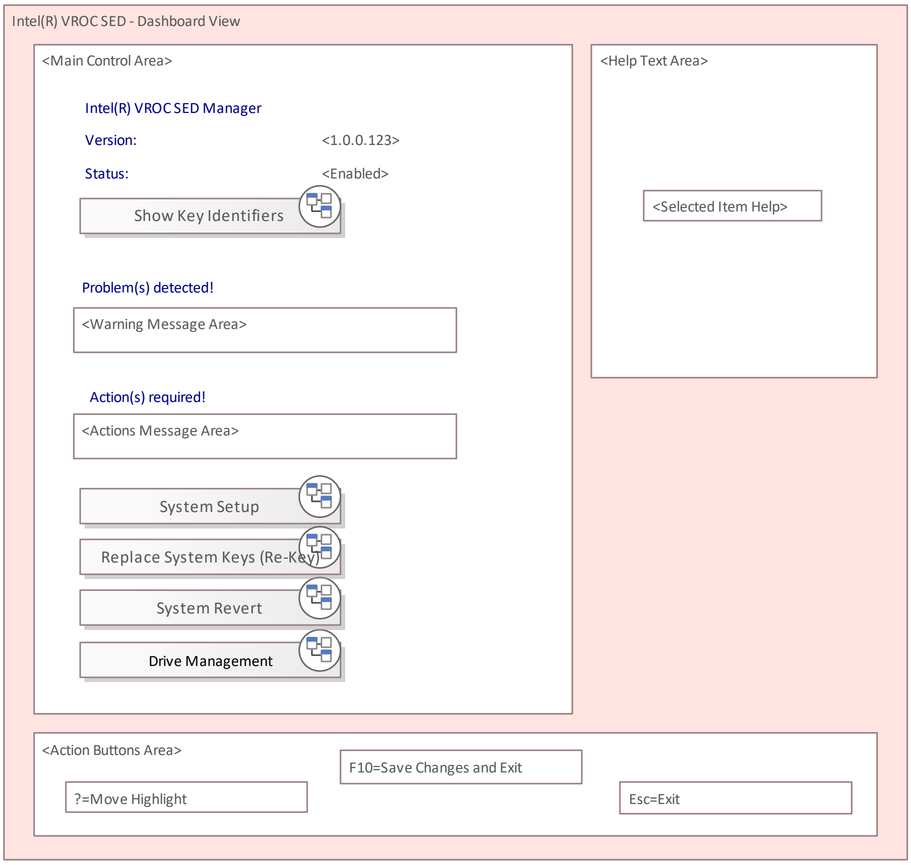


Figure 12: UI Navigation , Version 1.1

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.



Intel(R) VROC SED - Dashboard View

<Main Control Area>

Intel(R) VROC SED Manager

Version: <1.0.0.123>

Status: <Enabled>

Show Key Identifiers

Problem(s) detected!

<Warning Message Area>

Action(s) required!

<Actions Message Area>

System Setup

Replace System Keys (Re-Key)

System Revert

Drive Management

<Help Text Area>

<Selected Item Help>

<Action Buttons Area>

?=Move Highlight

F10=Save Changes and Exit

Esc=Exit

Figure 13: Dashboard View , Version 1.6

The table below describes the **attributes** of the form.

Attribute	Value	Description
Form Id	0x0001	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
Title	Intel(R) VROC SED - Dashboard View	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.
Warning Message Area	See the table with warning messages below. The element is hidden when no warning conditions met.	A text message that alerts the user of a condition that might cause a problem in the future.
Actions Message Area	See the table with actions' messages below. The element is hidden when no actions required.	A text message to inform user about required actions.

Version	e.g. 1.0.1.123	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.
Status	"Disabled" | "Disabled - Incompatible device detected" | "Enabled" | "Enabled - Incompatible device detected" | "Internal Error"	Indicate if SED Security is enabled or disabled for the system. It is referred to as "System Status" in the document.
Show Key Identifiers (Action)	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.
System Setup (Action)	The action shall be DISABLED when any of the following conditions is met: • KMS status is NOT equal "Connected" • System Status is NOT equal "Disabled" • Mixed configuration flag is TRUE (Non OPAL device found) • There is any device with a "non-supported-drive" flag set. • There is no VMD attached drive with OPAL capability. (Note: In case of hot remove, the re-enumeration flow need to be detected which is done when action executed)	Go to Form "System Setup" "DISABLED" means here that the element is "greyed out" and the operation cannot be executed.
Replace System Keys (Re-Key) (Action)	The action shall be DISABLED when any of the following conditions is met: • KMS status is NOT equal "Connected" • System Status is NOT equal "Enabled" • Mixed configuration flag is TRUE (Non OPAL device found) • There is any device with a "non-supported-drive" flag set. • There is any device in "Unencrypted" state	Go to Form "System Rotate Keys (Re-Key)" "DISABLED" means here that the element is "greyed out" and the operation cannot be executed.
System Revert (Action)	The action shall be DISABLED when any of the following conditions is met: • KMS status is NOT equal "Connected" • System Status is NOT equal "Enabled" • Mixed configuration flag is TRUE (Non OPAL device found) • There is any device with a "non-supported-drive" flag set.	Go to Form "System Revert" "DISABLED" means here that the element is "greyed out" and the operation cannot be executed.
Drive Management	The action shall be DISABLED when any of the following conditions is met: • KMS status is NOT equal "Connected"	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.

Element	**Help message**
System Setup	Go to Form "System Setup"
Replace System Keys (Re-Key)	Go to Form "Replace System Keys (Re-Key)"
System Revert	Go to Form "System Revert"
Drive Management	Go to Form "Drive Management"
Key identifier	Text with Selected PEK_ID value

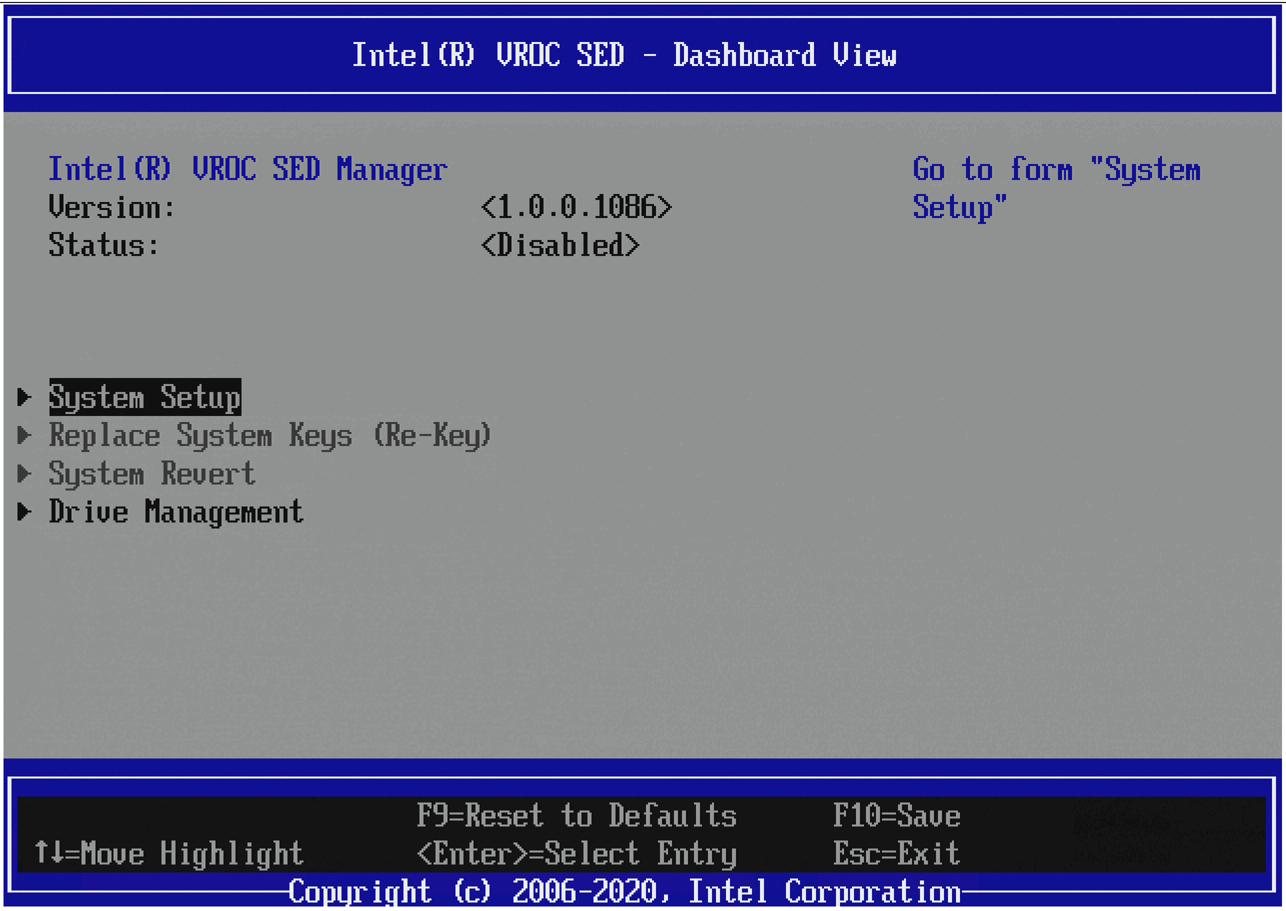
The table below describes **warning** messages area

Warning Text	**Help message**	**Conditions**
Can't connect to Key Management Service	Can't connect to Key Management Service! Please verify if the system is healthy and correctly configured.	• System Status != "Internal Error" • KMS status == "DISCONNECTED"
Can't find any Key Management Service	Can't find any Key Management Service! Please verify if the system is healthy and correctly configured.	• System Status != "Internal Error" • KMS status == "NOT_FOUND"
Unsupported configuration detected	Unsupported configuration detected! Please verify if all drives support the OPAL 2.0.	• Non-Opal device detected (MixedConfigDetected)
Automatic unlocking or provisioning has failed	Automatic unlocking or provisioning of Self-Encrypting drive(s) has failed! Please verify if all drives are healthy and correctly configured.	**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. The SED support is disabled when non-Intel drive(s) detected.	• There is any device with a "non-supported-drive" flag set.
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_SUCCEED
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.
Multiple Key Identifiers detected	Multiple Key Identifiers are detected. Re-Key operation is recommended.	Multiple PEK_IDs detected.

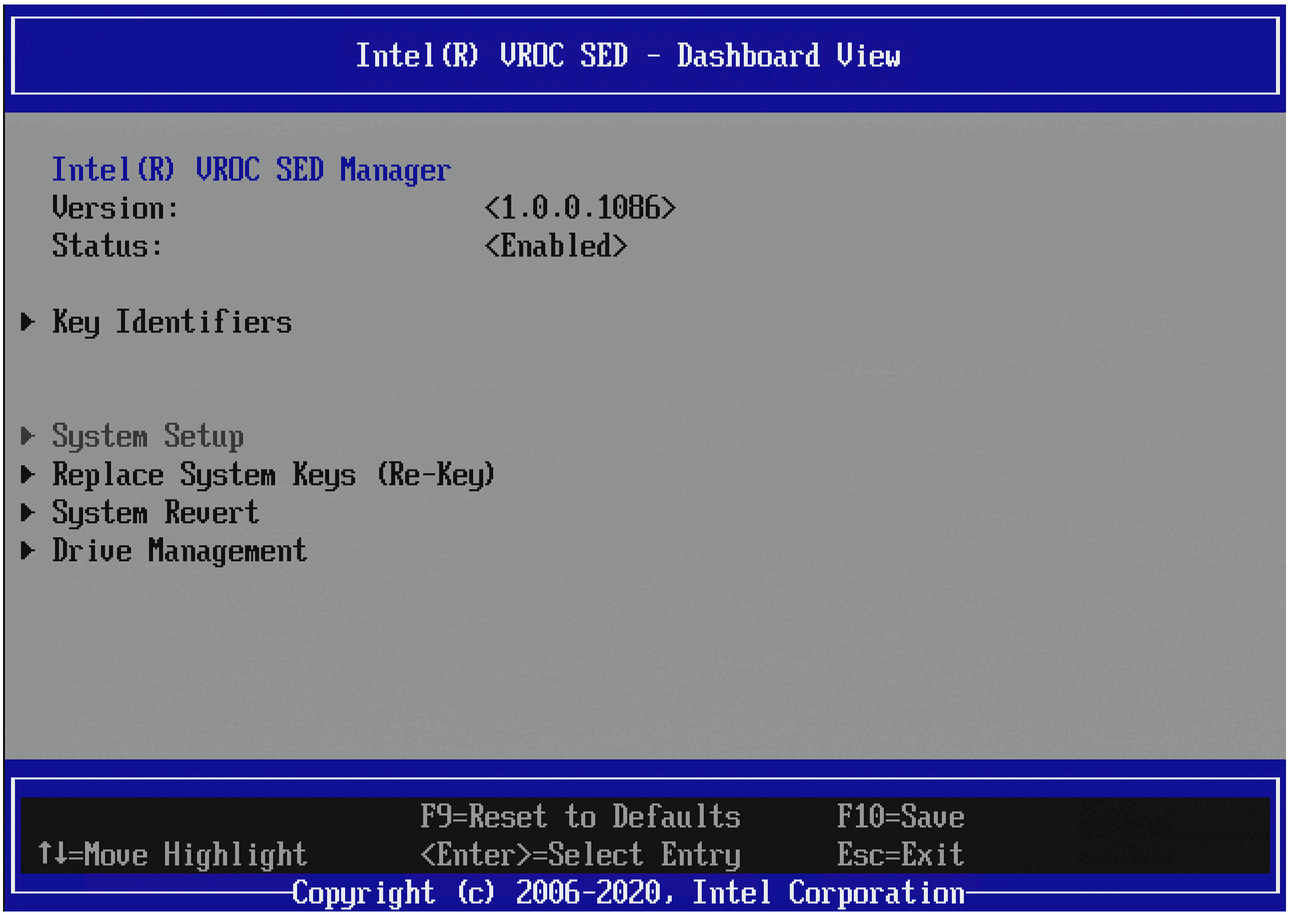
The table below describes **actions** messages area

ActionText	**Help message**	**Conditions**
Reboot required	The system reboot is required due to configuration change(s).	• Reset required UEFI HII flag is set
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:



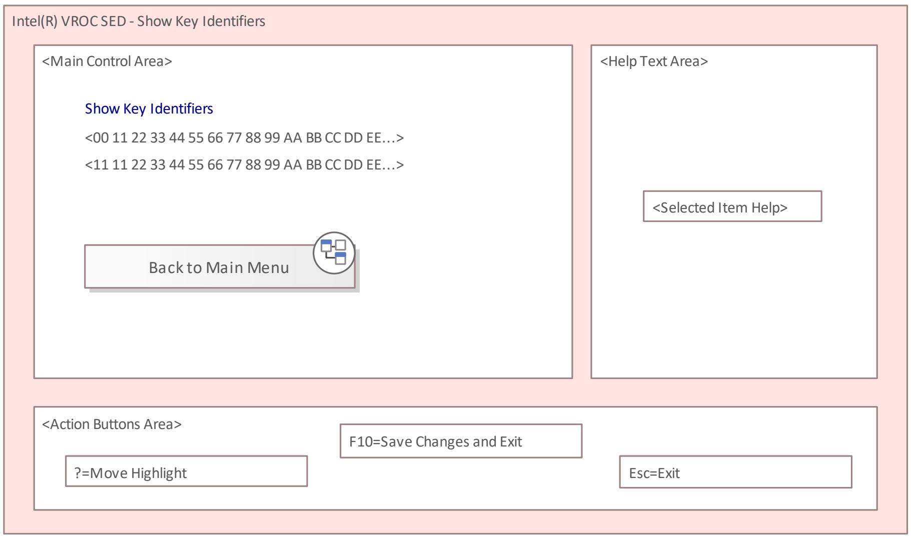
```
Intel(R) VROC SED - Dashboard View

Intel(R) VROC SED Manager                                  Go to form "System
Version:                    <1.0.0.1086>                   Setup"
Status:                     <Disabled>


▶ 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(R) VROC SED - Dashboard View

Intel(R) 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.



Intel(R) VROC SED - Show Key Identifiers

Show Key Identifiers

<00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE…>

<11 11 22 33 44 55 66 77 88 99 AA BB CC DD EE…>

Figure 14: Show Key Identifiers , Version 1.0

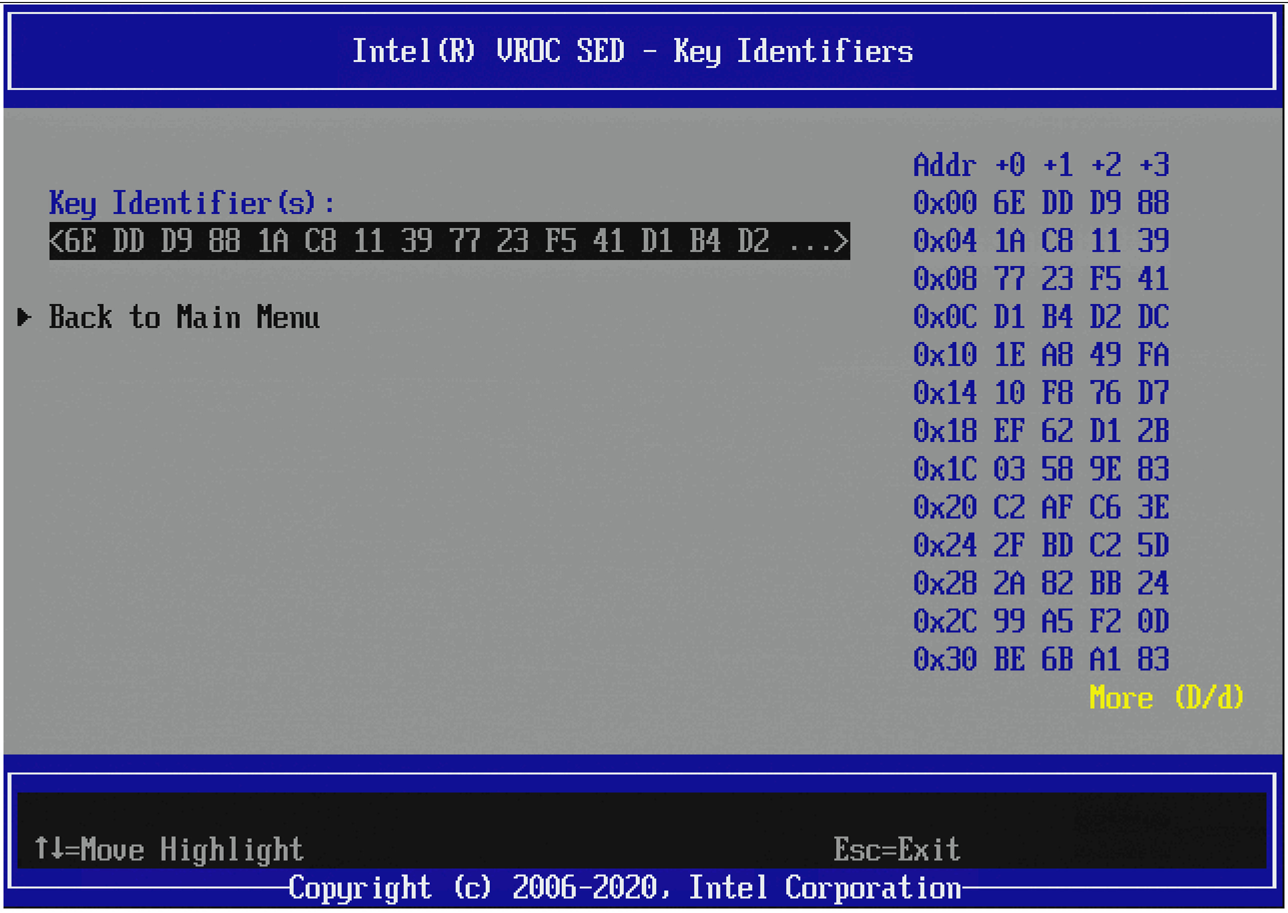
The table below describes the **attributes** of the form.

Attribute	**Value**	**Description**
Form Id	0x000A	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
Title	Intel(R) VROC SED - Show Key Identifiers	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.
Key Identifiers(s)	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 "…". Full PEK_ID shall be printed in the Help Text Area.	PEK_ID can be used by the user to identify the system key (PEK) on Remote KMS.
Back to Main Menu		Go to Form "Dashboard View"

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

Element	**Help message**
Key identifier	Text with Selected PEK_ID value
Back to Main Menu	Back to Main Menu

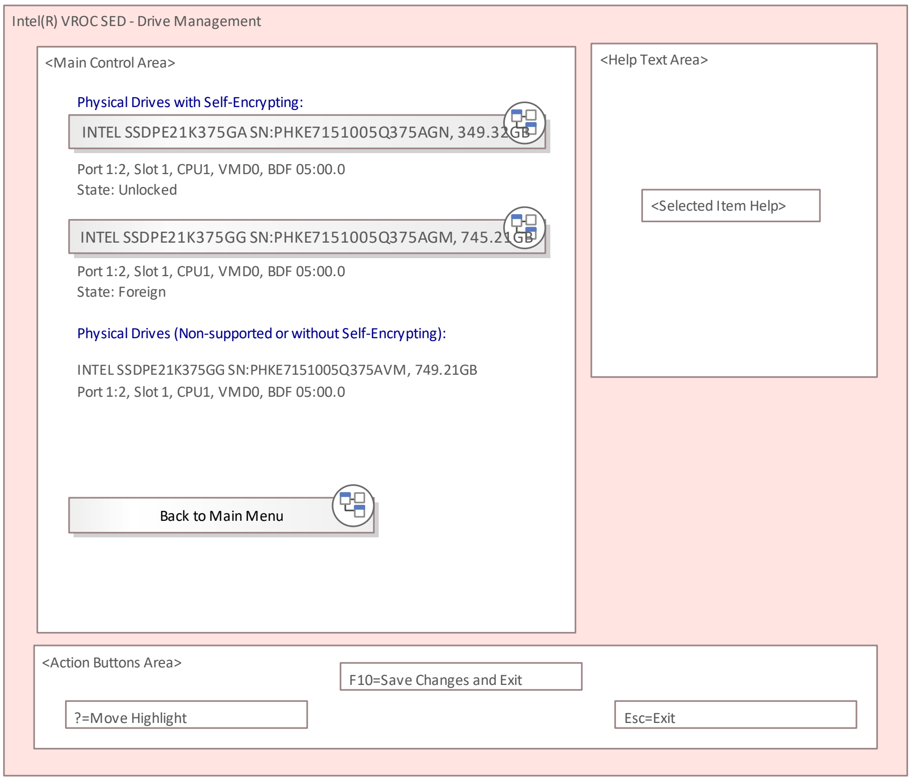
Example Screenshots:



```
                    Intel(R) VROC SED - Key Identifiers

                                                     Addr +0 +1 +2 +3
  Key Identifier(s):                                 0x00 6E DD D9 88
  <6E DD D9 88 1A C8 11 39 77 23 F5 41 D1 B4 D2 ...> 0x04 1A C8 11 39
                                                     0x08 77 23 F5 41
▶ Back to Main Menu                                  0x0C D1 B4 D2 DC
                                                     0x10 1E A8 49 FA
                                                     0x14 10 F8 76 D7
                                                     0x18 EF 62 D1 2B
                                                     0x1C 03 58 9E 83
                                                     0x20 C2 AF C6 3E
                                                     0x24 2F BD C2 5D
                                                     0x28 2A 82 BB 24
                                                     0x2C 99 A5 F2 0D
                                                     0x30 BE 6B A1 83
                                                              More (D/d)

 ↑↓=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.



Intel(R) VROC SED - Drive Management

<Main Control Area>

Physical Drives with Self-Encrypting:

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

Port 1:2, Slot 1, CPU1, VMD0, BDF 05:00.0
State: Unlocked

INTEL SSDPE21K375GG SN:PHKE7151005Q375AGM, 745.21GB

Port 1:2, Slot 1, CPU1, VMD0, BDF 05:00.0
State: Foreign

Physical Drives (Non-supported or without Self-Encrypting):

INTEL SSDPE21K375GG SN:PHKE7151005Q375AVM, 749.21GB
Port 1:2, Slot 1, CPU1, VMD0, BDF 05:00.0

Figure 15: Drive Management , Version 1.5

The table below describes the **attributes** of the form.

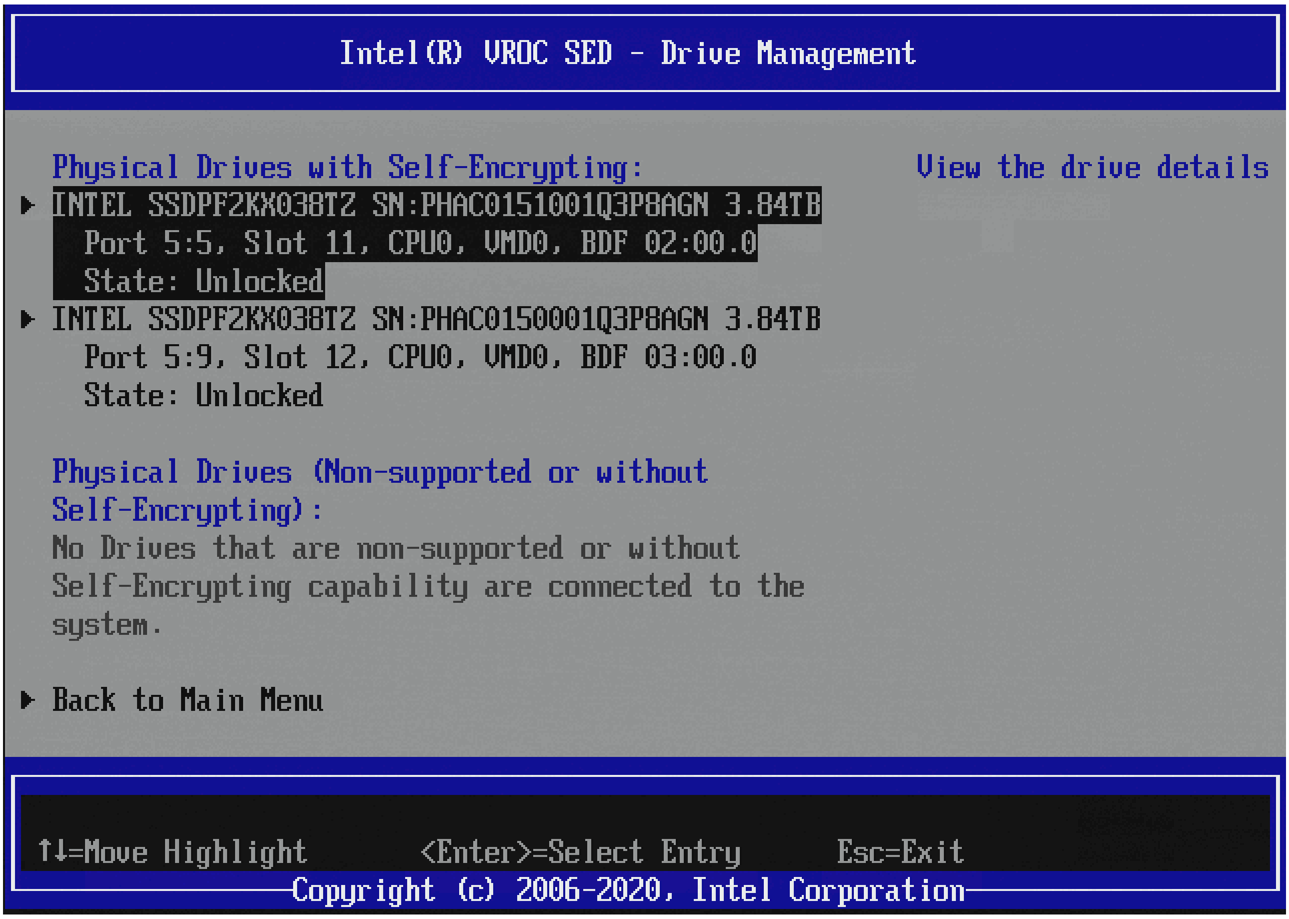
Attribute	**Value**	**Description**
Form Id	0x0004	Unique Id for the form within the form set
Title	Intel(R) VROC SED - Drive Management	Title text for the form.
Warning Message Area	See the table with warning messages below. The element is hidden when no warning conditions met.	A text message that alerts the user of a condition that might cause a problem in the future.
Physical Drives with Self-Encrypting:	A list of SED capable drives (Model, SN, Capacity). When no SED devices found following text shall be displayed instead: "No Self-Encrypting capable drives connected to the system".	
Selected Drive (Action)		Go to Form "Drive Detail"
Physical Drives (Non-supported or without Self-Encrypting):	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: "No Drives that are non-supported or without Self-Encrypting capability are connected to the system."	

Back to Main Menu		Go to Form "Dashboard View"

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

Element	Help message
<Selected Drive>	View the drive details
Back to Main Menu	Back to Main Menu

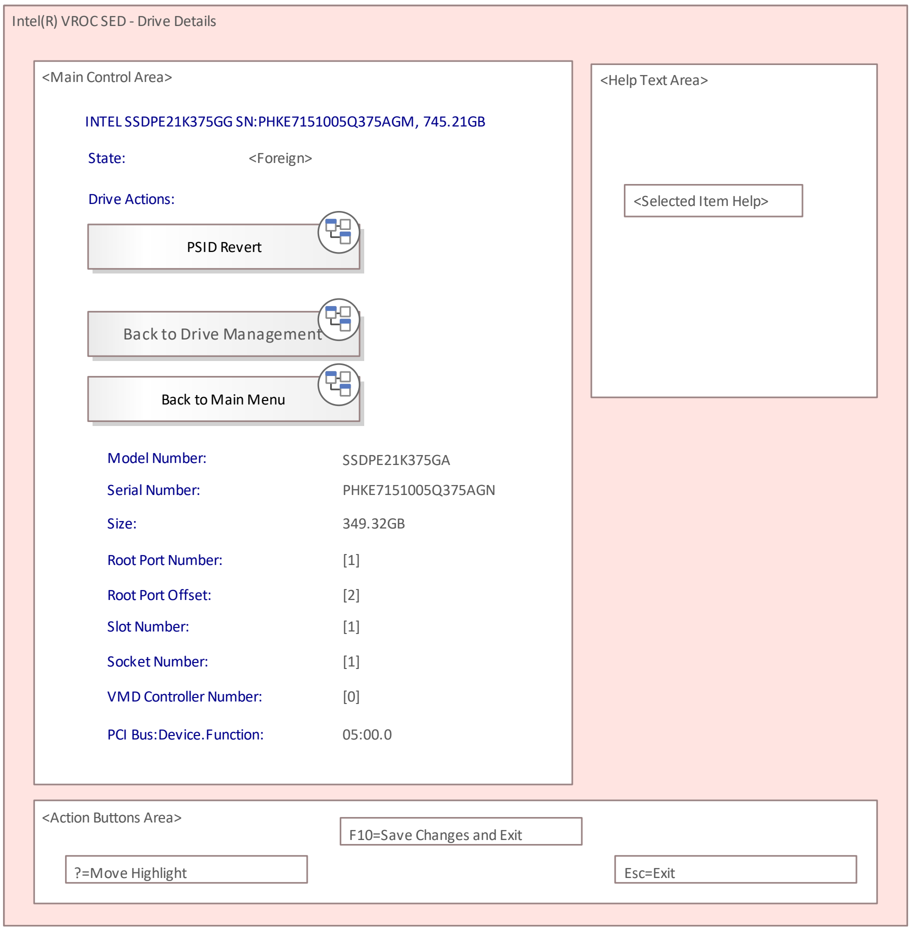
Example Screenshots:



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

  Physical Drives with Self-Encrypting:              View the drive details
▶ INTEL SSDPF2KX038TZ SN:PHAC0151001Q3P8AGN 3.84TB
    Port 5:5, Slot 11, CPU0, VMD0, BDF 02:00.0
    State: Unlocked
▶ INTEL SSDPF2KX038TZ SN:PHAC0150001Q3P8AGN 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

 ↑↓=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.



Intel(R) VROC SED - Drive Details

<Main Control Area>

INTEL SSDPE21K375GG SN:PHKE7151005Q375AGM, 745.21GB

State: <Foreign>

Drive Actions:

PSID Revert

Back to Drive Management

Back to Main Menu

Model Number:	SSDPE21K375GA
Serial Number:	PHKE7151005Q375AGN
Size:	349.32GB
Root Port Number:	[1]
Root Port Offset:	[2]
Slot Number:	[1]
Socket Number:	[1]
VMD Controller Number:	[0]
PCI Bus:Device.Function:	05:00.0

<Help Text Area>

<Selected Item Help>

<Action Buttons Area>

F10=Save Changes and Exit

?=Move Highlight

Esc=Exit

Figure 16: Drive Details (Foreign) , Version 1.3

The table below describes the **attributes** of the form.

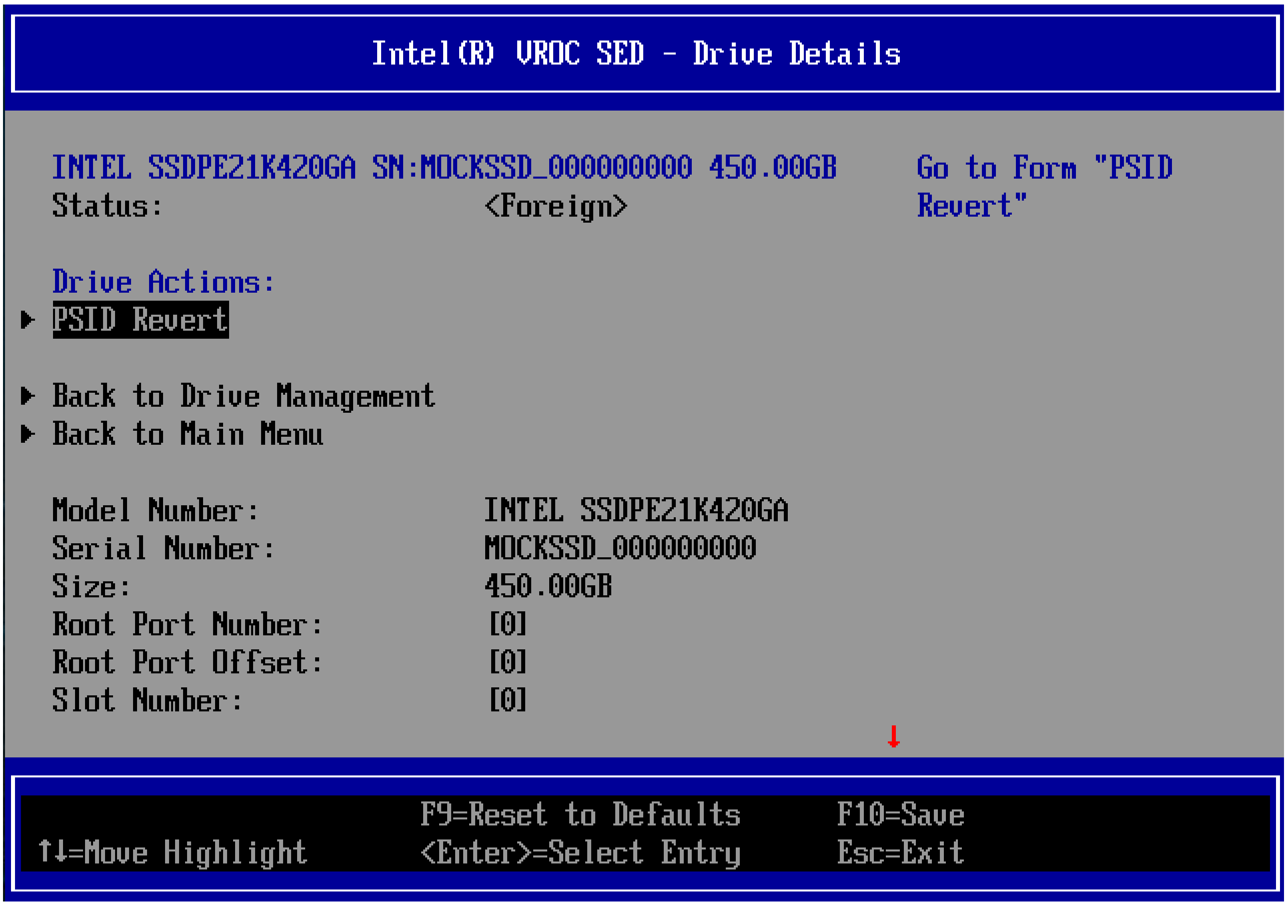
Attribute	**Value**	**Description**
Form Id	0x0005	Unique Id for the form within the form set
Title	Intel(R) VROC SED - Drive details	Title text for the form.
State	"Unlocked" | "Locked" | "Foreign" | "Unencrypted"	Indicate security status for the drive.
PSID Revert	The action shall be ENABLED when the following conditions are met: • KMS status is "Connected"	Go to Form "PSID Revert"
Back to Drive Management		Go to Form "Drive Management"
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.

Element	**Help message**
PSID Revert	Go to Form "PSID Revert"
Back to Drive Management	Go back to "Drive Management" form.
Back to Main Menu	Back to Main Menu

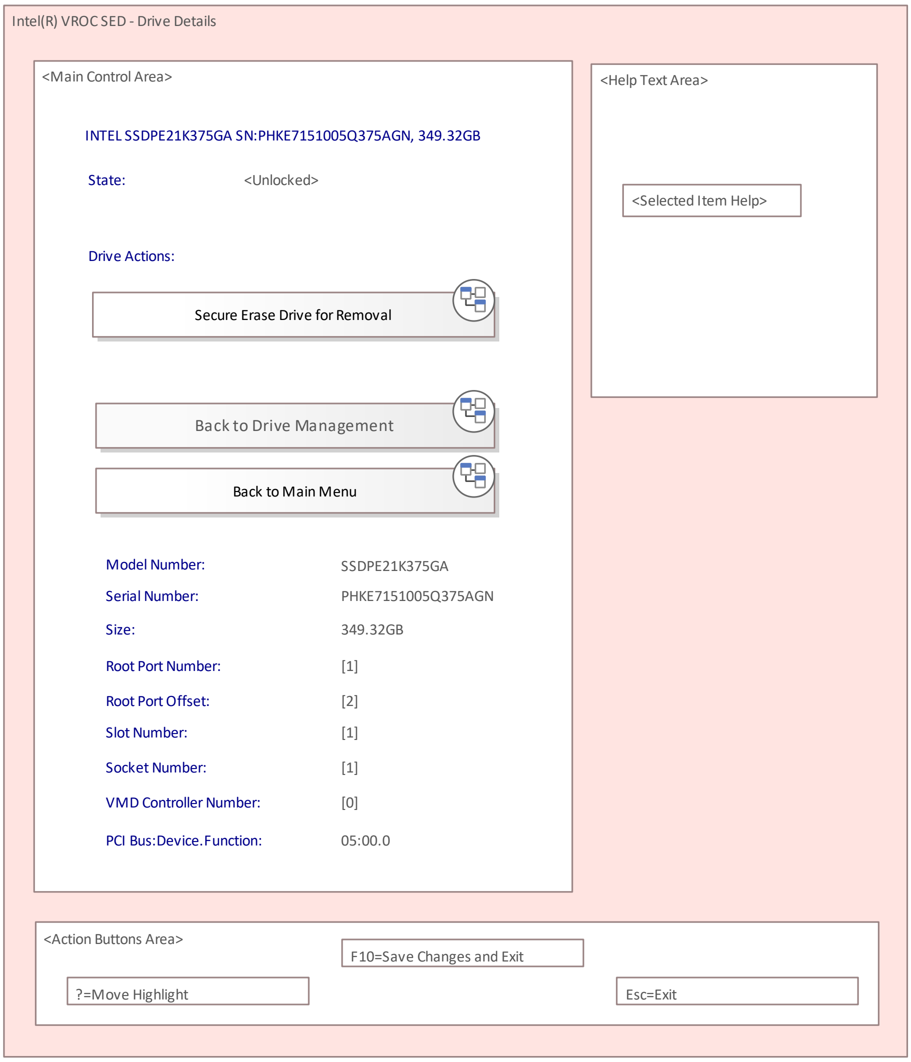
Example Screenshots:



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

  INTEL SSDPE21K420GA SN:MOCKSSD_000000000 450.00GB     Go to Form "PSID
  Status:                    <Foreign>                  Revert"

  Drive Actions:
▶ PSID Revert

▶ Back to Drive Management
▶ Back to Main Menu

  Model Number:              INTEL SSDPE21K420GA
  Serial Number:             MOCKSSD_000000000
  Size:                      450.00GB
  Root Port Number:          [0]
  Root Port Offset:          [0]
  Slot Number:               [0]

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

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.



INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

State: <Unlocked>

Drive Actions:

Model Number:	SSDPE21K375GA
Serial Number:	PHKE7151005Q375AGN
Size:	349.32GB
Root Port Number:	[1]
Root Port Offset:	[2]
Slot Number:	[1]
Socket Number:	[1]
VMD Controller Number:	[0]
PCI Bus:Device.Function:	05:00.0

Figure 17: Drive Details (Locked/Unlocked) , Version 1.5

The table below describes the **attributes** of the form.

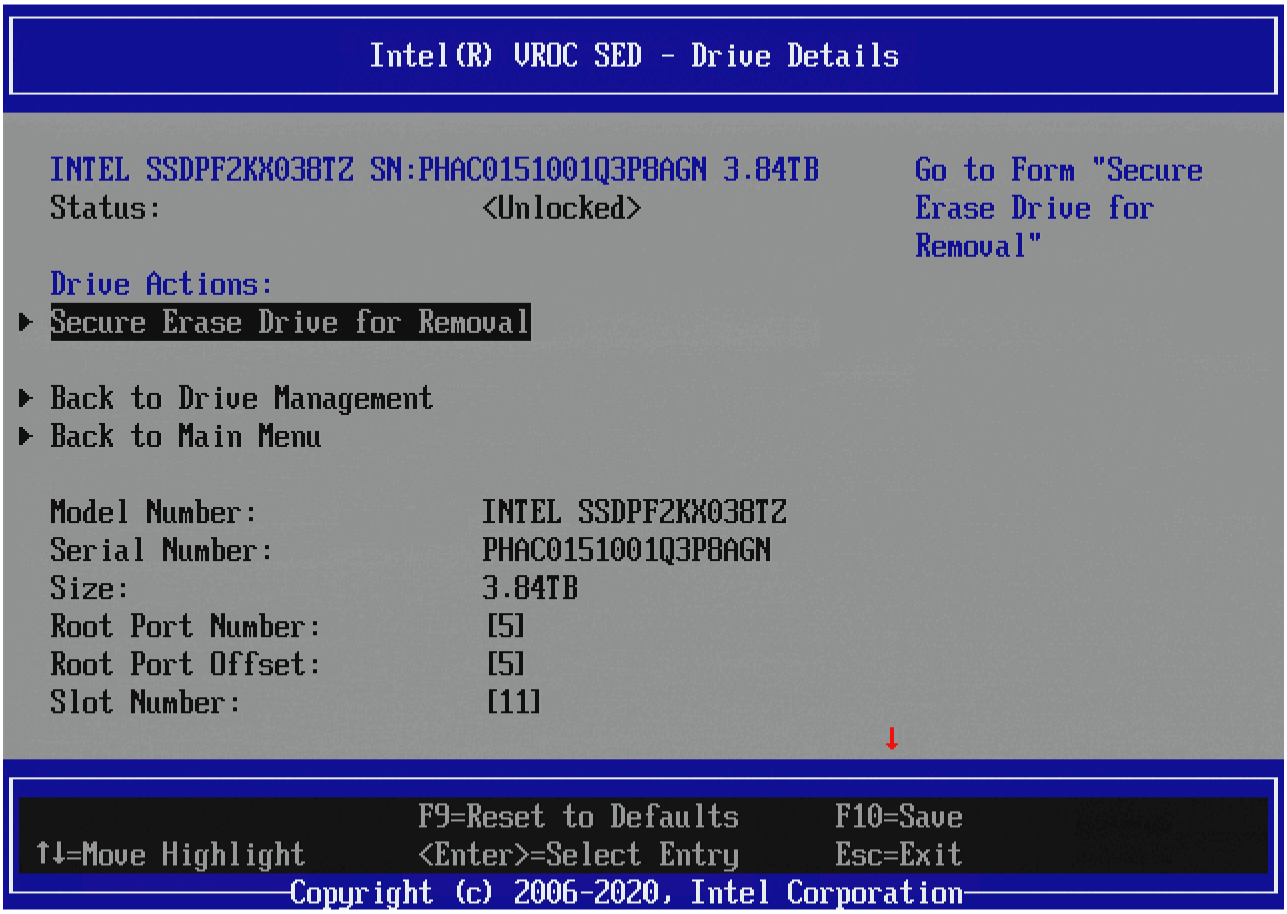
Attribute	**Value**	**Description**
Form Id	0x05	Unique Id for the form within the form set
Title	Intel(R) VROC SED - Drive details	Title text for the form.
State	"Unlocked" | "Locked" | "Foreign" | "Unencrypted"	Indicate security status for the drive.
Secure Erase Drive for Removal (Action)	The action shall be ENABLED when the following conditions are met: • KMS status is "Connected" • System Status is "Enabled" • Drive Status is "Locked" or "Unlocked"	Go to Form "Drive Revert"
Back to Drive Management		Go to Form "Drive Management"

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

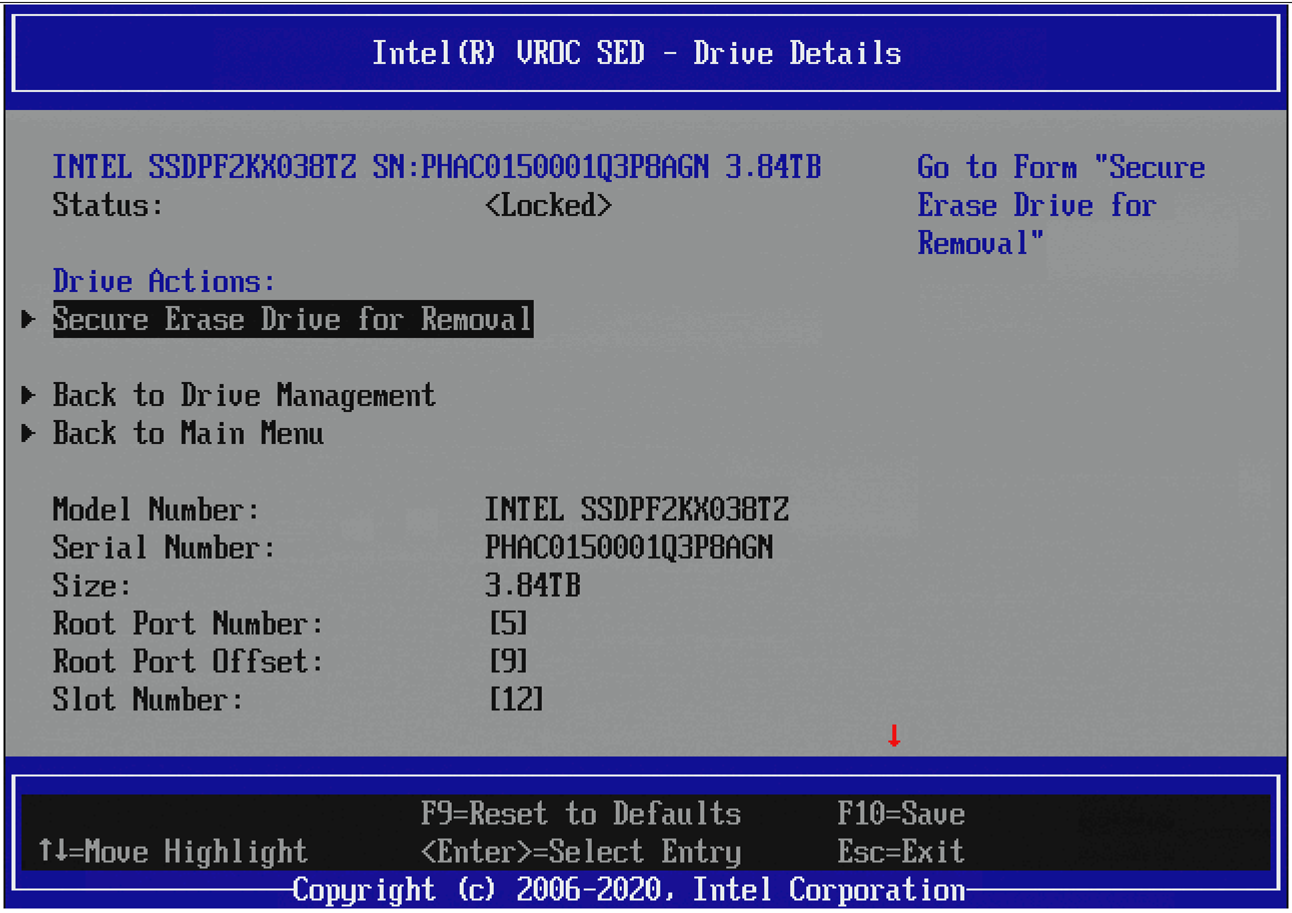
The table below describes **help** text area per selected element.

Element	**Help message**
Secure Erase Drive for Removal	Secure Erase Drive for Removal
Back to Drive Management	Go back to "Drive Management" form.
Back to Main Menu	Back to Main Menu

Example Screenshots:



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

INTEL SSDPF2KX038TZ SN:PHAC0151001Q3P8AGN 3.84TB      Go to Form "Secure
Status:                    <Unlocked>                 Erase Drive for
                                                      Removal"
Drive Actions:
▶ Secure Erase Drive for Removal

▶ Back to Drive Management
▶ Back to Main Menu

Model Number:              INTEL SSDPF2KX038TZ
Serial Number:             PHAC0151001Q3P8AGN
Size:                      3.84TB
Root Port Number:          [5]
Root Port Offset:          [5]
Slot Number:               [11]

                     F9=Reset to Defaults     F10=Save
↑↓=Move Highlight    <Enter>=Select Entry     Esc=Exit
             Copyright (c) 2006-2020, Intel Corporation
```



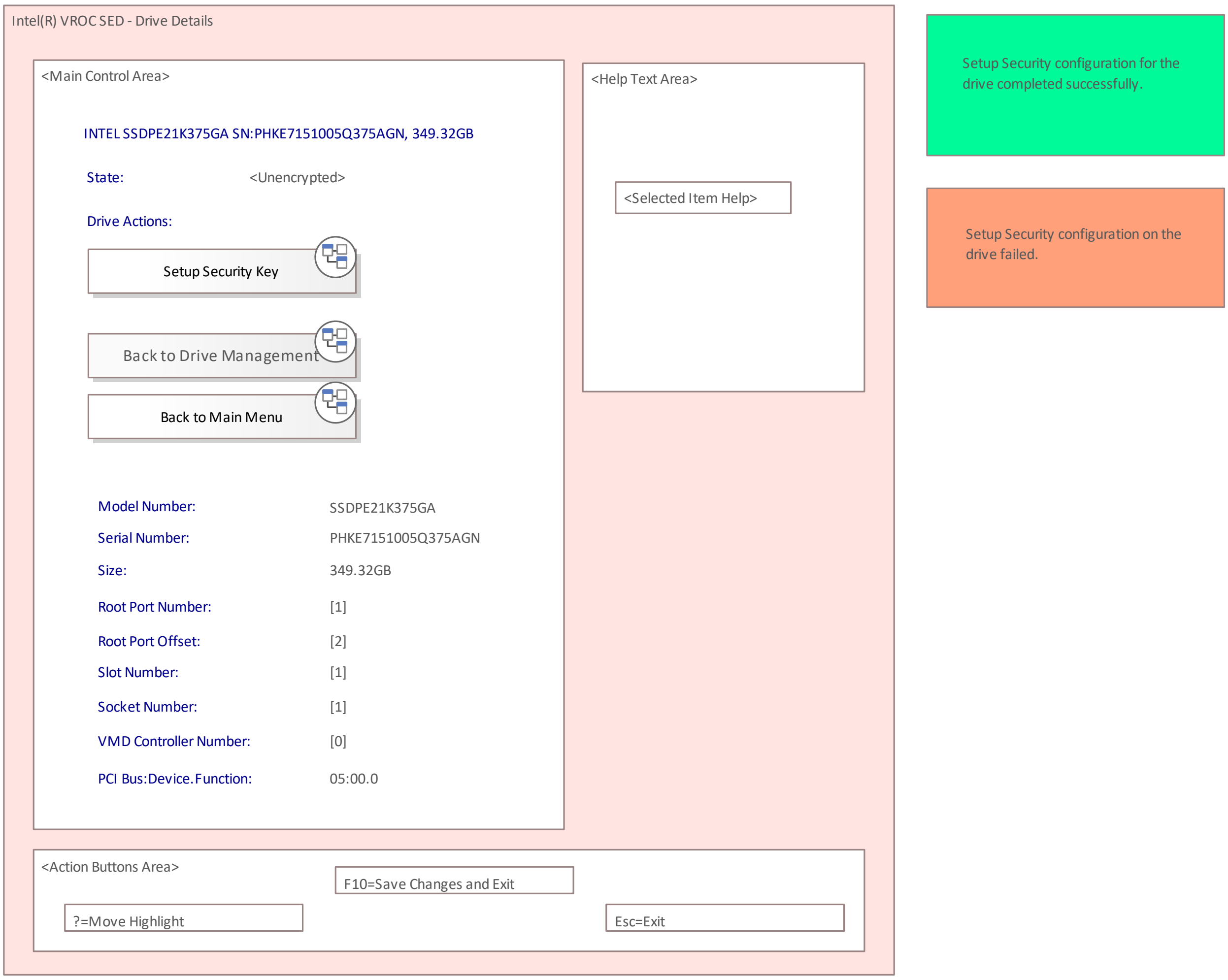
Intel(R) VROC SED - Drive Details

```
INTEL SSDPF2KX038TZ SN:PHAC0150001Q3P8AGN 3.84TB     Go to Form "Secure
Status:                    <Locked>                  Erase Drive for
                                                     Removal"
Drive Actions:
▶ Secure Erase Drive for Removal

▶ Back to Drive Management
▶ Back to Main Menu

Model Number:              INTEL SSDPF2KX038TZ
Serial Number:             PHAC0150001Q3P8AGN
Size:                      3.84TB
Root Port Number:          [5]
Root Port Offset:          [9]
Slot Number:               [12]
```

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



INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

State: <Unencrypted>

Drive Actions:

Model Number: SSDPE21K375GA

Serial Number: PHKE7151005Q375AGN

Size: 349.32GB

Root Port Number: [1]

Root Port Offset: [2]

Slot Number: [1]

Socket Number: [1]

VMD Controller Number: [0]

PCI Bus:Device.Function: 05:00.0

Setup Security configuration for the drive completed successfully.

Setup Security configuration on the drive failed.

Figure 18: Drive Details (Unencrypted) , Version 1.4

The table below describes the **attributes** of the form.

Attribute	**Value**	**Description**
Form Id	0x05	Unique Id for the form within the form set
Title	Intel(R) VROC SED - Drive details	Title text for the form.
State	"Unlocked" | "Locked" | "Foreign" | "Unencrypted"	Indicate security status for the drive.
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"

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

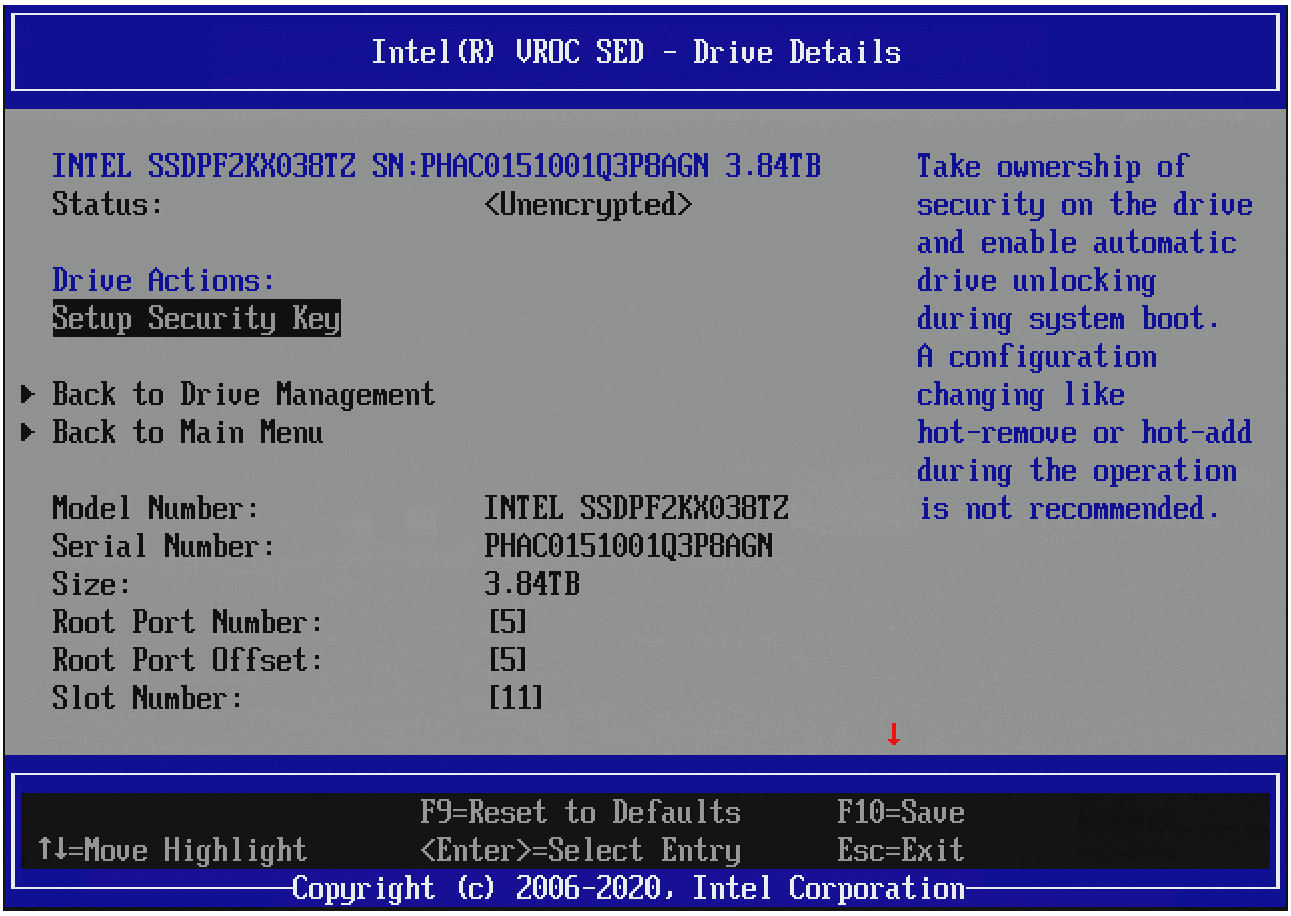
The table below describes **help** text area per selected element.

Element	Help message
Setup Security Key	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.
Back to Drive Management	Go back to "Drive Management" form.
Back to Main Menu	Back to Main Menu

The table below describes **popup** details.

Element	Value	Description
"Setup Security completed successfully"	Setup Security configuration on the drive completed successfully.	When the operation completed successfully
"Setup Security failed"	Setup security configuration on the drive failed.	When the operation failed.

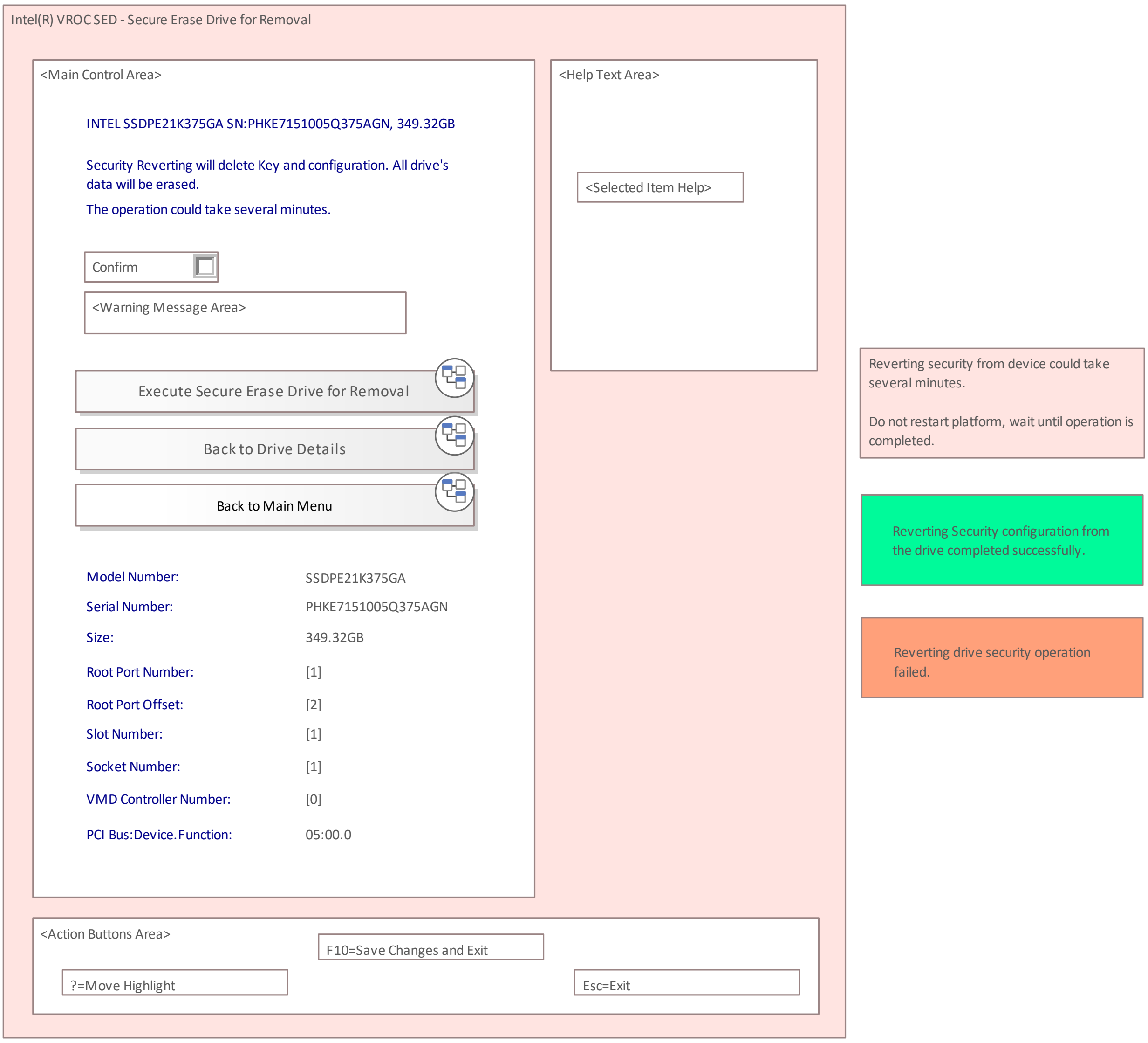
Example Screenshots:



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

  INTEL SSDPF2KX038TZ SN:PHAC0151001Q3P8AGN 3.84TB    Take ownership of
  Status:                  <Unencrypted>              security on the drive
                                                      and enable automatic
  Drive Actions:                                      drive unlocking
  Setup Security Key                                  during system boot.
                                                      A configuration
▶ Back to Drive Management                            changing like
▶ Back to Main Menu                                   hot-remove or hot-add
                                                      during the operation
  Model Number:            INTEL SSDPF2KX038TZ        is not recommended.
  Serial Number:           PHAC0151001Q3P8AGN
  Size:                    3.84TB
  Root Port Number:        [5]
  Root Port Offset:        [5]
  Slot Number:             [11]
                                                      ↓
                        F9=Reset to Defaults      F10=Save
  ↑↓=Move Highlight     <Enter>=Select Entry      Esc=Exit
                Copyright (c) 2006-2020, Intel Corporation
```

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.



Intel(R) VROC SED - Secure Erase Drive for Removal

<Main Control Area>

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

Security Reverting will delete Key and configuration. All drive's data will be erased.

The operation could take several minutes.

Confirm □

<Warning Message Area>

Model Number:	SSDPE21K375GA
Serial Number:	PHKE7151005Q375AGN
Size:	349.32GB
Root Port Number:	[1]
Root Port Offset:	[2]
Slot Number:	[1]
Socket Number:	[1]
VMD Controller Number:	[0]
PCI Bus:Device.Function:	05:00.0

<Help Text Area>

<Selected Item Help>

<Action Buttons Area>

Reverting security from device could take several minutes.

Do not restart platform, wait until operation is completed.

Reverting Security configuration from the drive completed successfully.

Reverting drive security operation failed.

Figure 19: Secure Erase - Prepare drive for removal , Version 1.5

The table below describes the **attributes** of the form.

Attribute	Value	Description
Form Id	0x0007	Unique Id for the form within the form set
Title	Intel(R) VROC SED - Secure Erase Drive for Removal	Title text for the form.
Warning Message Area	See the table with warning messages below. The element is hidden when no warning conditions met.	A text message that alerts the user of a condition that might cause a problem in the future.
Confirm	"OFF" (Default)	
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.

Element	**Help message**
Execute Secure Erase Drive for Removal	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.
Back to Drive Details	Go back to "Drive Details" form of this drive
Back to Main Menu	Back to Main Menu

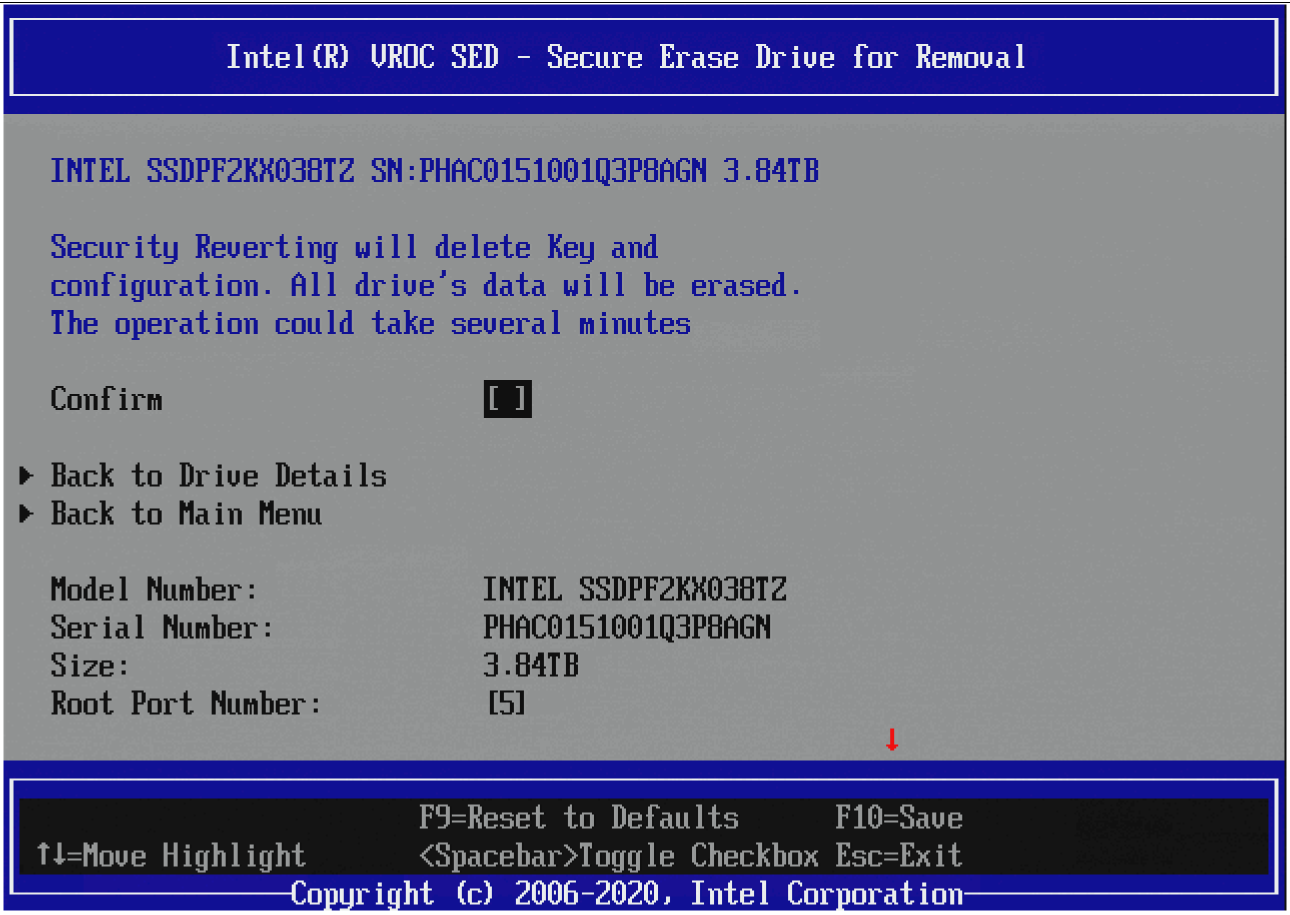
The table below describes **popup** details.

Element	**Value**	**Description**
Secure Erase Drive for Removal is In-Progress"	Reverting security from device could take several minutes. Do not restart platform, wait until operation is completed.	Shall be shown until reverting operation is completed.
Secure Erase Drive for Removal completed successfully"	Reverting Security configuration from the drive completed successfully.	When the operation completed successfully
"Secure Erase Drive for Removal failed"	Reverting drive security operation failed.	When the operation failed.

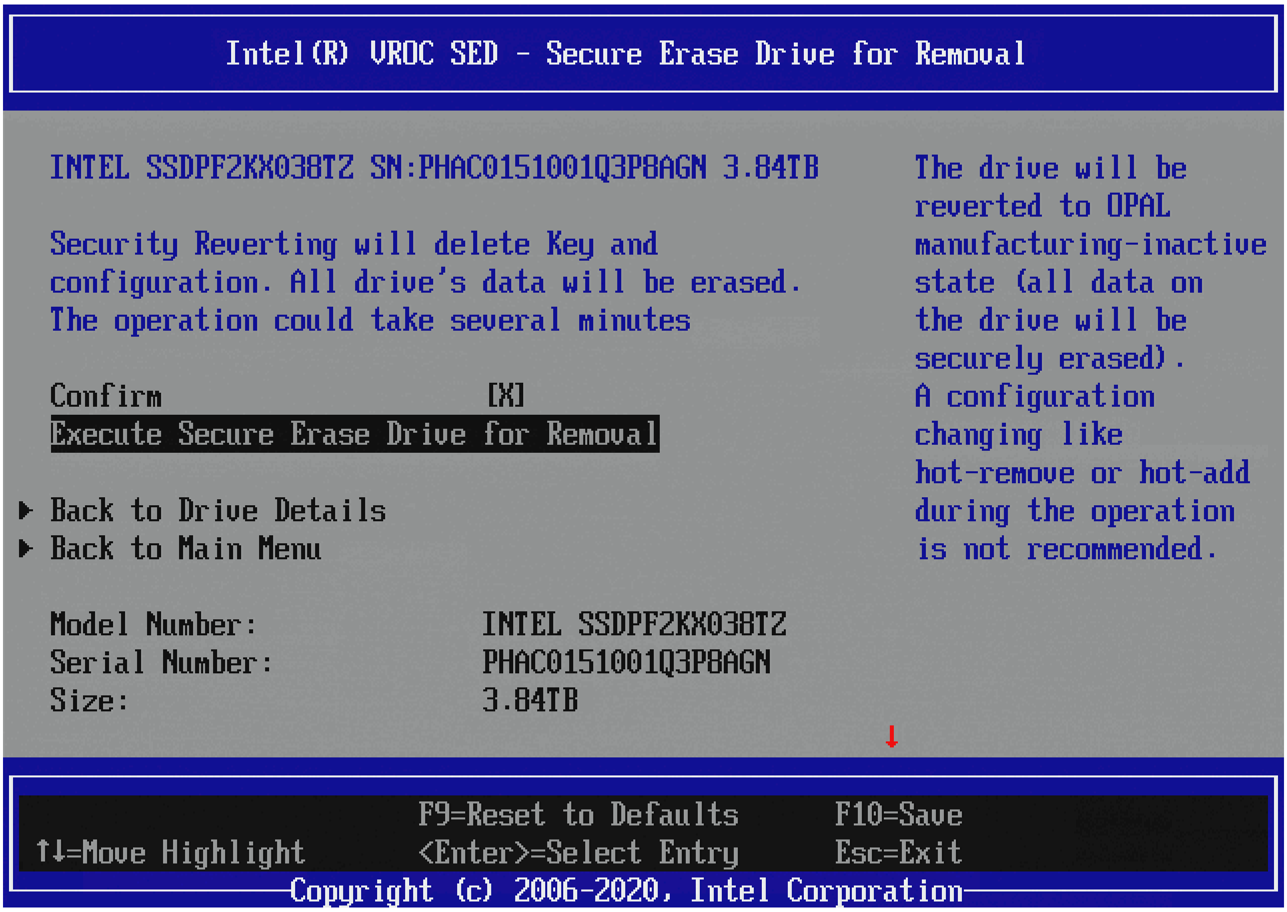
The table below describes **warning** messages area

Warning Message	**Description**
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:



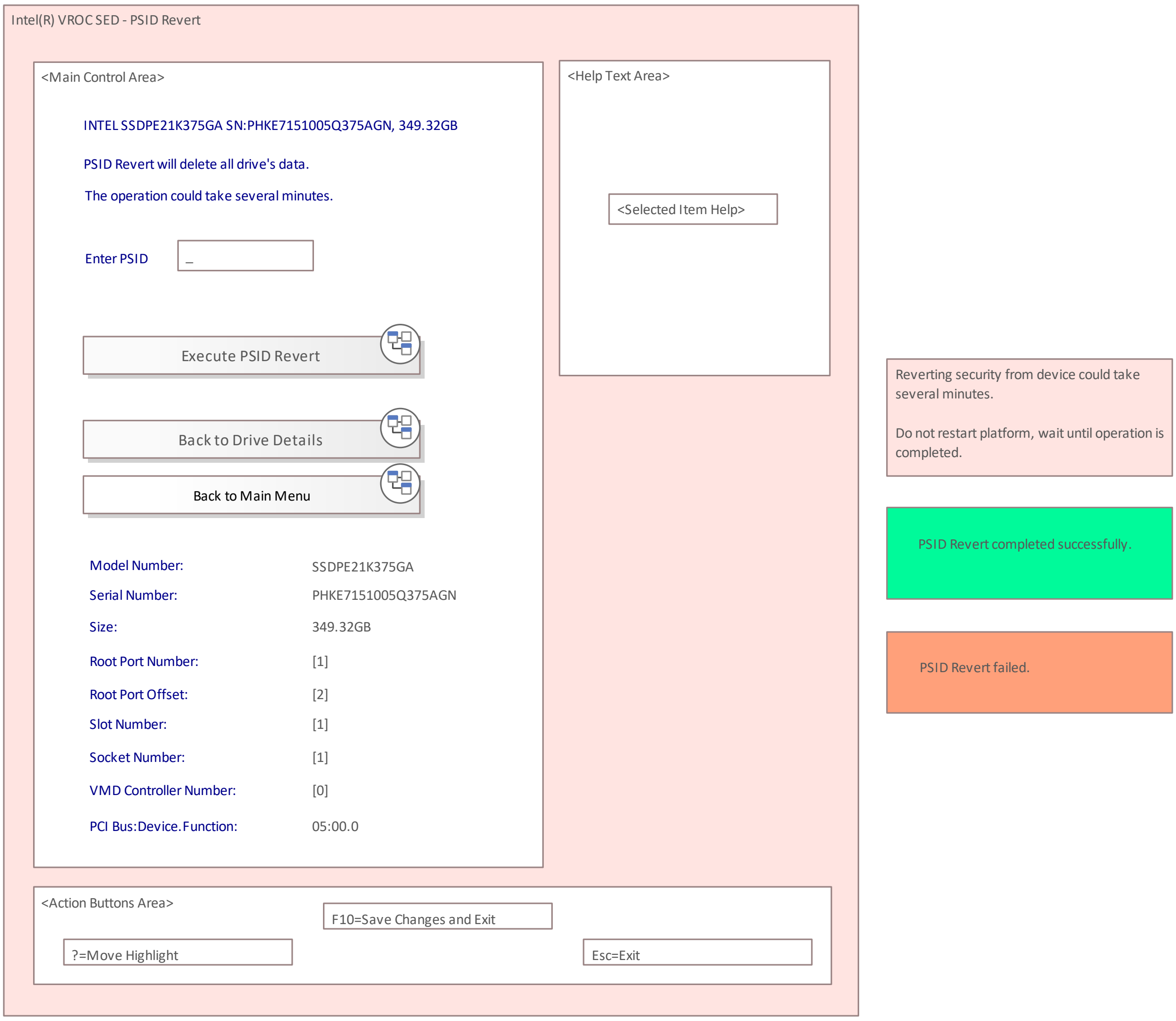
```
              Intel(R) VROC SED - Secure Erase Drive for Removal

  INTEL SSDPF2KX038TZ 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 SSDPF2KX038TZ
  Serial Number:             PHAC0151001Q3P8AGN
  Size:                      3.84TB
  Root Port Number:          [5]

                         F9=Reset to Defaults       F10=Save
 ↑↓=Move Highlight       <Spacebar>Toggle Checkbox  Esc=Exit
                Copyright (c) 2006-2020, Intel Corporation
```



```
              Intel(R) VROC SED - Secure Erase Drive for Removal

  INTEL SSDPF2KX038TZ SN:PHAC0151001Q3P8AGN 3.84TB      The drive will be
                                                        reverted to OPAL
  Security Reverting will delete Key and                manufacturing-inactive
  configuration. All drive's data will be erased.       state (all data on
  The operation could take several minutes              the drive will be
                                                        securely erased).
  Confirm                    [X]                        A configuration
  Execute Secure Erase Drive for Removal                changing like
                                                        hot-remove or hot-add
▶ Back to Drive Details                                 during the operation
▶ Back to Main Menu                                     is not recommended.

  Model Number:              INTEL SSDPF2KX038TZ
  Serial Number:             PHAC0151001Q3P8AGN
  Size:                      3.84TB

                         F9=Reset to Defaults       F10=Save
 ↑↓=Move Highlight       <Enter>=Select Entry       Esc=Exit
                Copyright (c) 2006-2020, Intel Corporation
```

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.



Intel(R) VROC SED - PSID Revert

<Main Control Area>

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

PSID Revert will delete all drive's data.

The operation could take several minutes.

Enter PSID _

Execute PSID Revert

Back to Drive Details

Back to Main Menu

Model Number:	SSDPE21K375GA
Serial Number:	PHKE7151005Q375AGN
Size:	349.32GB
Root Port Number:	[1]
Root Port Offset:	[2]
Slot Number:	[1]
Socket Number:	[1]
VMD Controller Number:	[0]
PCI Bus:Device.Function:	05:00.0

<Help Text Area>

<Selected Item Help>

<Action Buttons Area>

F10=Save Changes and Exit

?=Move Highlight

Esc=Exit

Reverting security from device could take several minutes.

Do not restart platform, wait until operation is completed.

PSID Revert completed successfully.

PSID Revert failed.

Figure 20: PSID Revert , Version 1.5

The table below describes the **attributes** of the form.

Attribute	Value	Description
Form Id	0x0006	Unique Id for the form within the form set
Title	Intel(R) VROC SED - PSID Revert	Title text for the form.
Enter PSID		Physical Presence SID.
Execute PSID Revert (Action)	Disabled if PSID field not filled with 32 characters.	Operate. Go to dialogue box "PSID Revert In-Progress". On Success - if System is not in "Disabled" state then Set Reset required UEFI HII flag.
Back to Drive Details		Go to Form "Drive Details"
Back to Main Menu		Go to Form "Dashboard View"

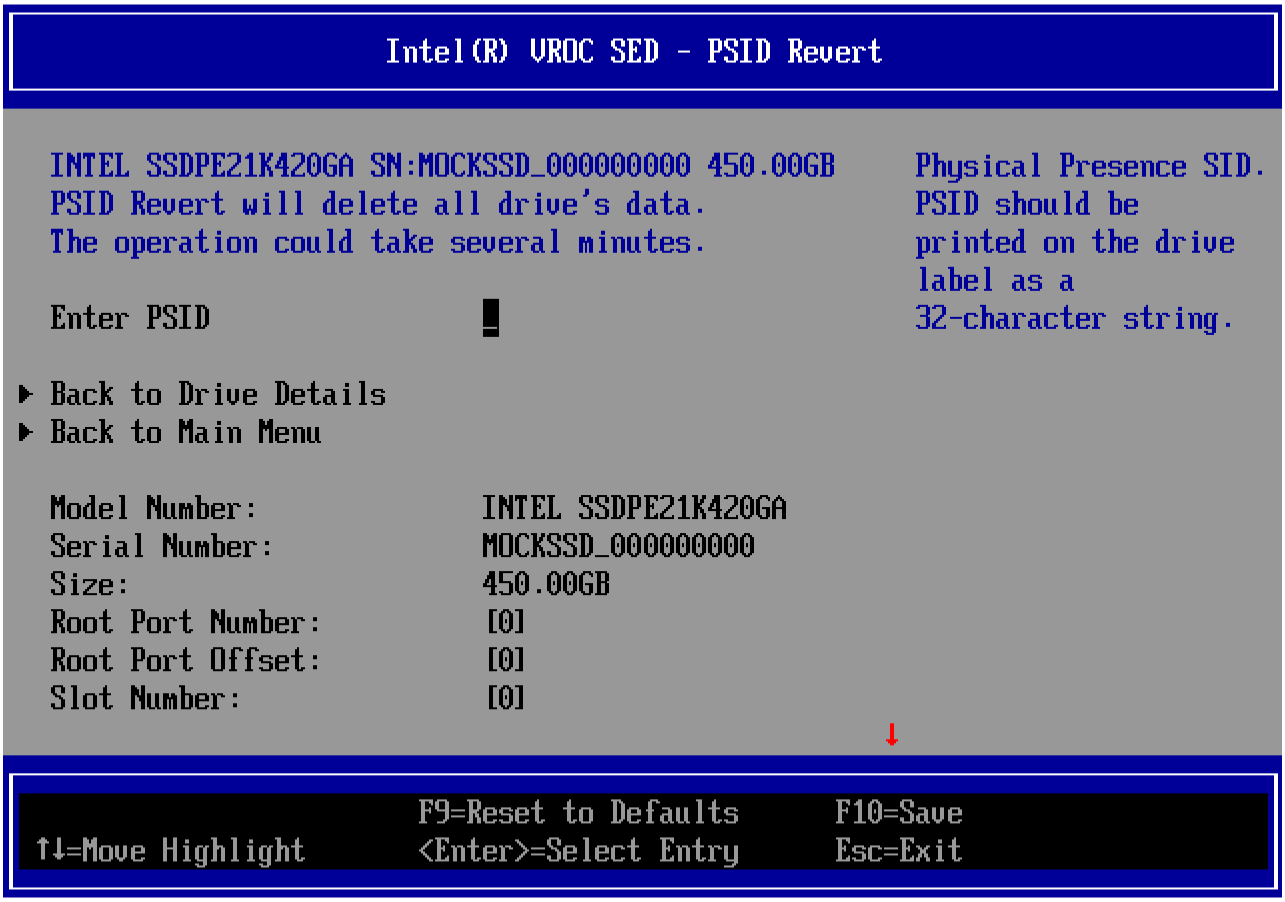
The table below describes **help** text area per selected element.

Element	Help message
Enter PSID	Physical Presence SID. PSID should be printed on the disk label as a 32-character string.
Execute PSID Revert	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.
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.

Element	Value	Description
"PSID Revert In-Progress"	Reverting security from device could take several minutes. Do not restart platform, wait until operation is completed.	Shall be shown until reverting operation is completed.
"PSID Revert completed successfully"	PSID Revert completed successfully.	When the operation completed successfully.
"PSID Revert failed"	PSID Revert failed.	When the operation failed.

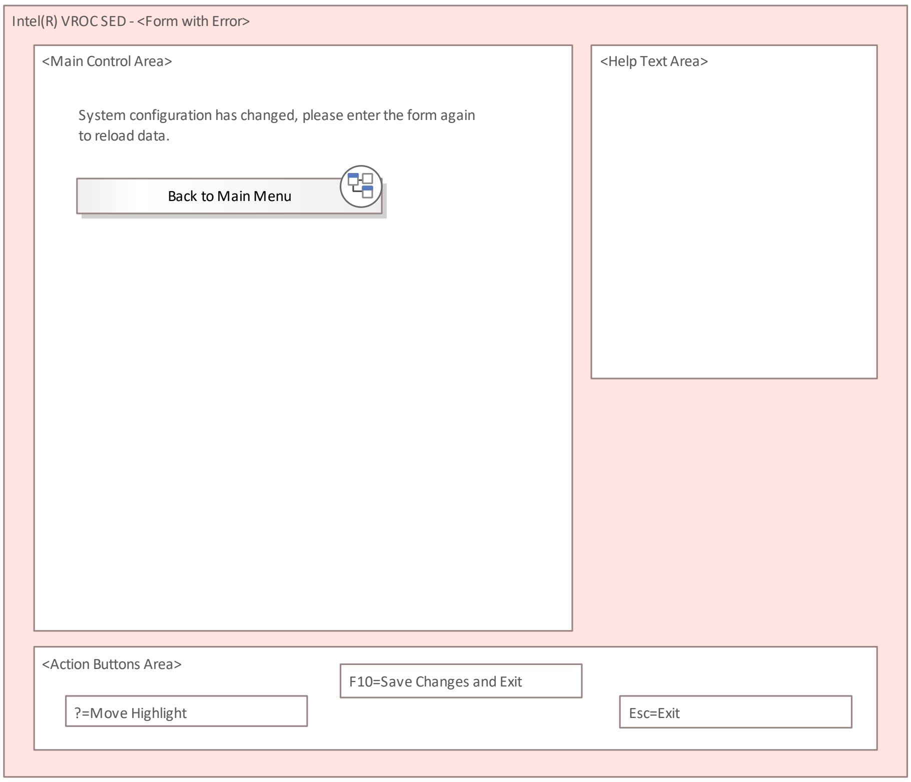
Example Screenshots:



```
                 Intel(R) VROC SED - PSID Revert

  INTEL SSDPE21K420GA SN:MOCKSSD_000000000 450.00GB     Physical Presence SID.
  PSID Revert will delete all drive's data.             PSID should be
  The operation could take several minutes.             printed on the drive
                                                        label as a
  Enter PSID                 _                          32-character string.

▶ Back to Drive Details
▶ Back to Main Menu

  Model Number:              INTEL SSDPE21K420GA
  Serial Number:             MOCKSSD_000000000
  Size:                      450.00GB
  Root Port Number:          [0]
  Root Port Offset:          [0]
  Slot Number:               [0]

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

11.3 Error Pages

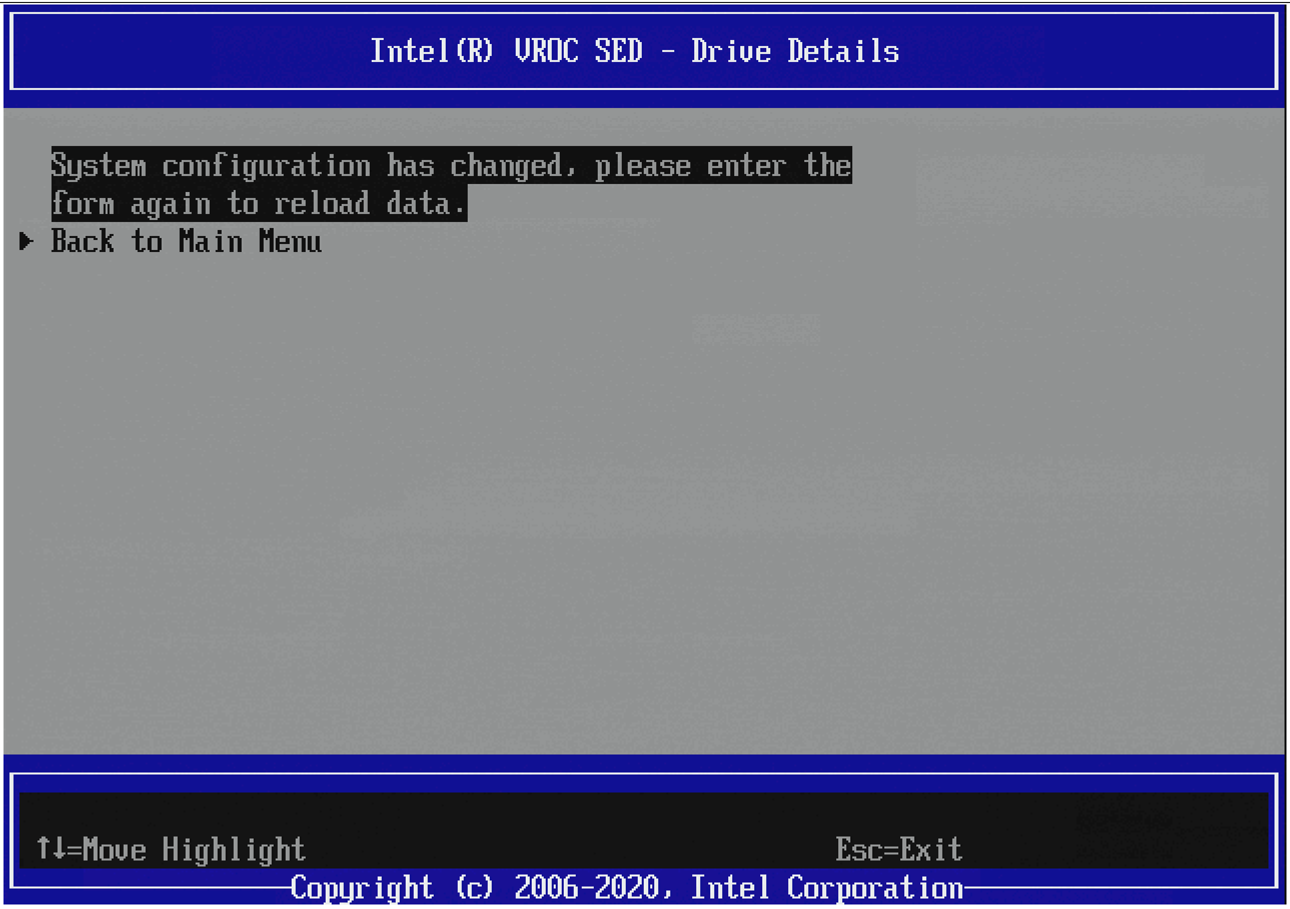
NOTE: The layout of the forms is the responsibility of the browser. The figures shown below are mockups of a possible layout.



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

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

Example Screenshots:

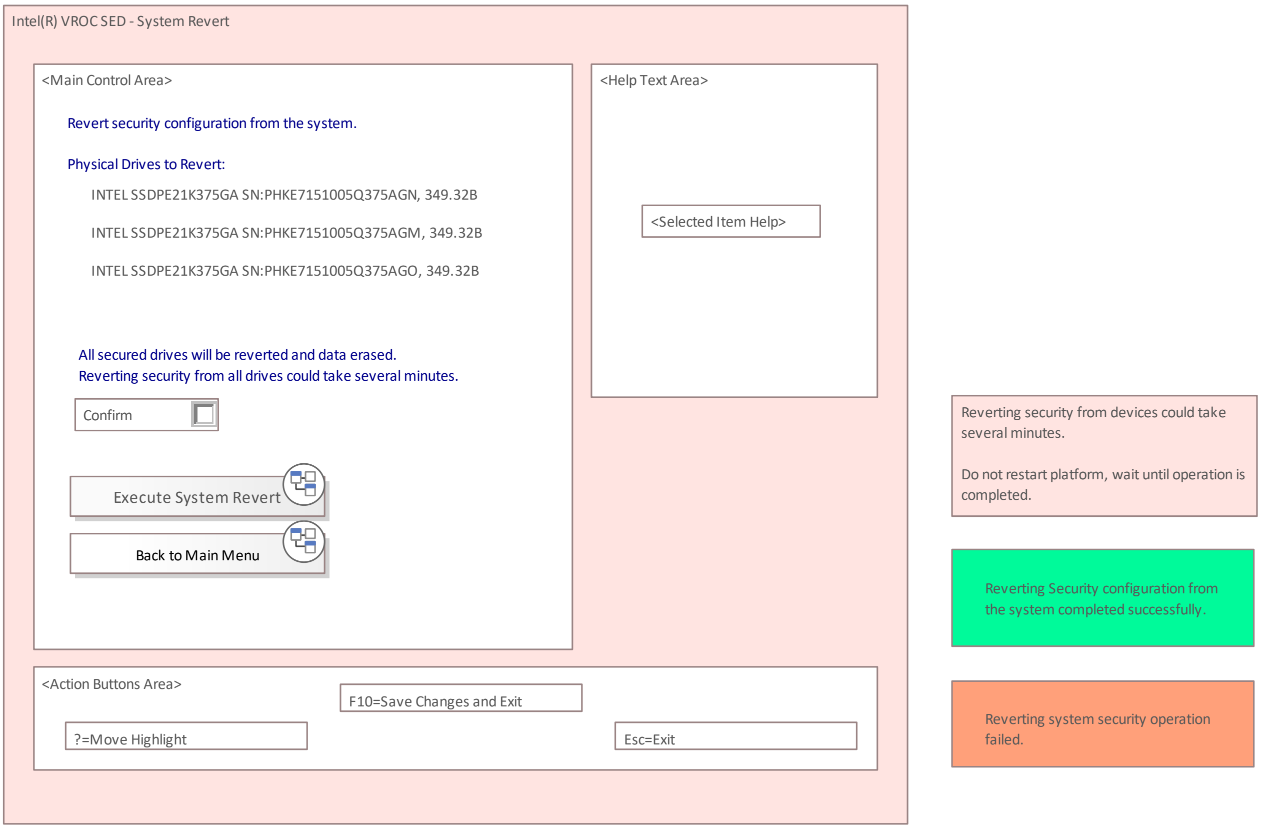


Intel(R) VROC SED - Drive Details

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

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.



Revert security configuration from the system.

Physical Drives to Revert:

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32B

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGM, 349.32B

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGO, 349.32B

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

Reverting security from devices could take several minutes.

Do not restart platform, wait until operation is completed.

Reverting Security configuration from the system completed successfully.

Reverting system security operation failed.

Figure 22: System Revert , Version 1.3

The table below describes the **attributes** of the form.

Attribute	**Value**	**Description**
Form Id	0x0003	Unique Id for the form within the form set
Title	Intel(R) VROC SED - System Revert	Title text for the form.
Physical Drives to Revert (List)	A list of SED capable drives with provisioned security (Model, SN, Capacity) If no drives to shown display "No drives to revert found".	List of drives with provisioned security.
Confirm	"OFF" (Default)	
Execute System Revert	The action shall be ENABLED when the following conditions are met: • KMS status is "Connected" • System Status is "Enabled" • "Confirm" checkbox is set to "ON"	Operate. Go to dialogue box "Revert System In-Progress"
Back to the Main Menu		Go to Form "Dashboard View"

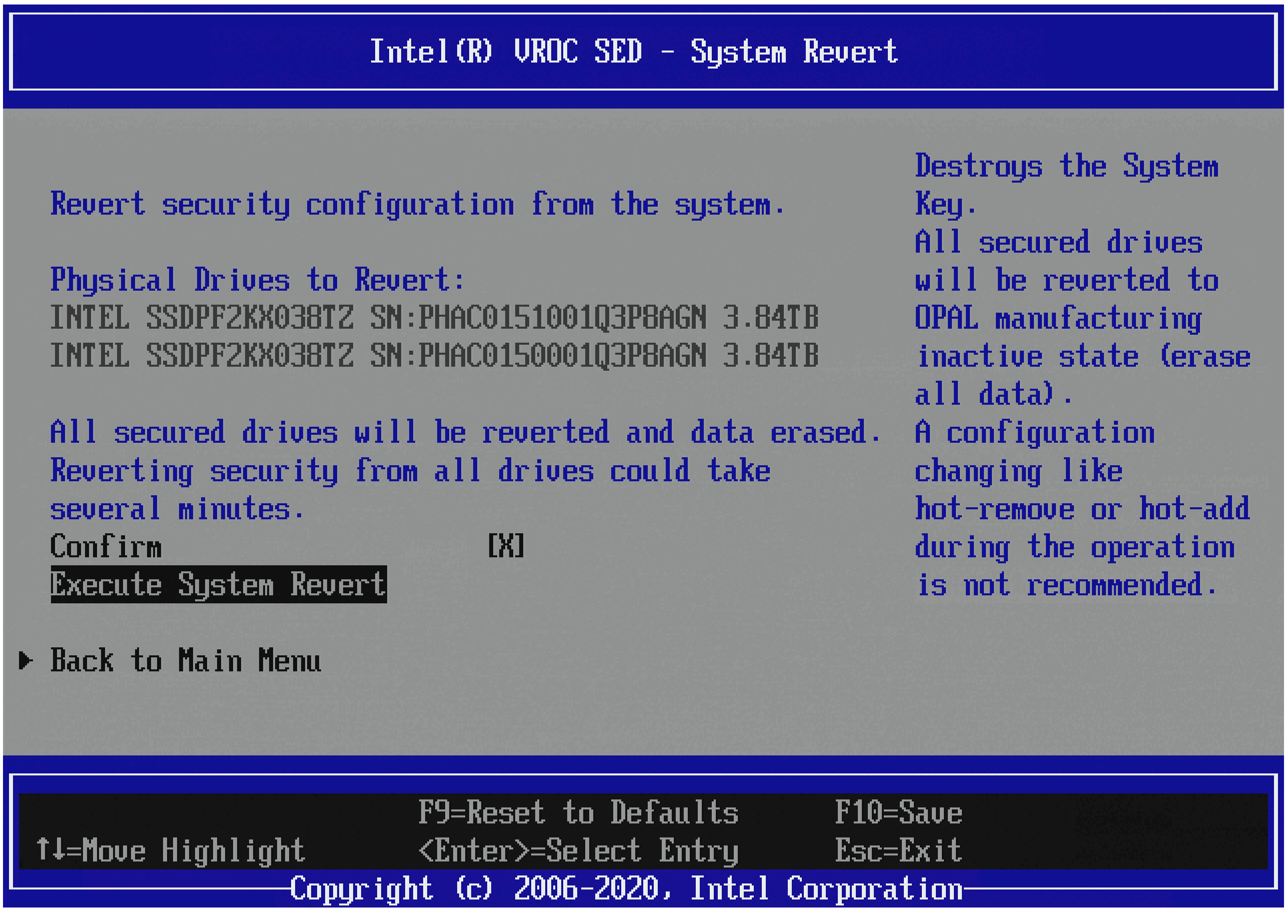
The table below describes **help** text area per selected element.

Element	Help message
Execute Revert System	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.
Back to Main Menu	Back to Main Menu

The table below describes **popup** details.

Element	Value	Description
"Revert System In-Progress"	Reverting security from devices could take several minutes. Do not restart platform, wait until operation is completed.	Shall be shown until reverting operation is completed.
"Reverting Security completed successfully"	Reverting Security configuration from the system completed successfully.	When the operation completed successfully. Refresh Physical Drives to Revert List.
"Reverting Security failed"	Reverting system security operation failed.	When the operation failed. Refresh Physical Drives to Revert List.

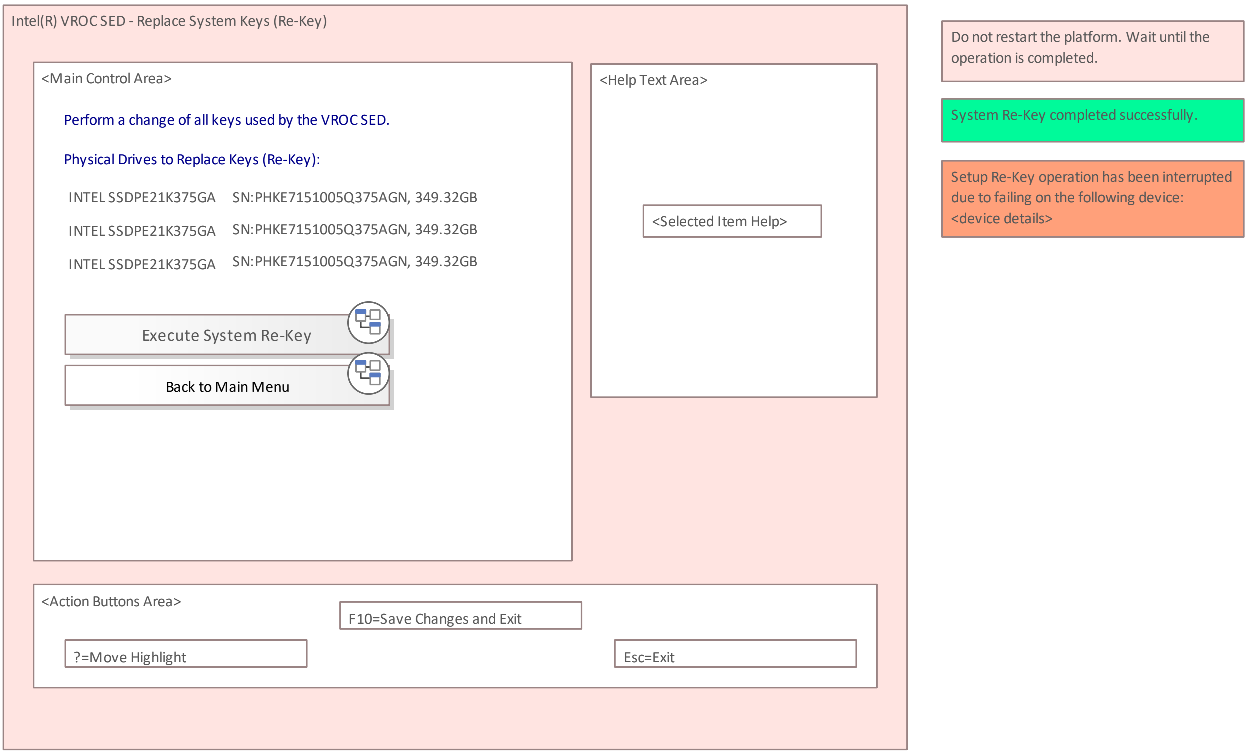
Example Screenshots:



```
Intel(R) VROC SED - System Revert

Revert security configuration from the system.        Destroys the System
                                                      Key.
Physical Drives to Revert:                            All secured drives
INTEL SSDPF2KX038TZ SN:PHAC0151001Q3P8AGN 3.84TB      will be reverted to
INTEL SSDPF2KX038TZ SN:PHAC0150001Q3P8AGN 3.84TB      OPAL manufacturing
                                                      inactive state (erase
                                                      all data).
All secured drives will be reverted and data erased.  A configuration
Reverting security from all drives could take         changing like
several minutes.                                      hot-remove or hot-add
Confirm                           [X]                 during the operation
Execute System Revert                                 is not recommended.

▶ Back to Main Menu

                     F9=Reset to Defaults      F10=Save
↑↓=Move Highlight    <Enter>=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.



Intel(R) VROC SED - Replace System Keys (Re-Key)

Perform a change of all keys used by the VROC SED.

Physical Drives to Replace Keys (Re-Key):

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

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>

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

The table below describes the **attributes** of the form.

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

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

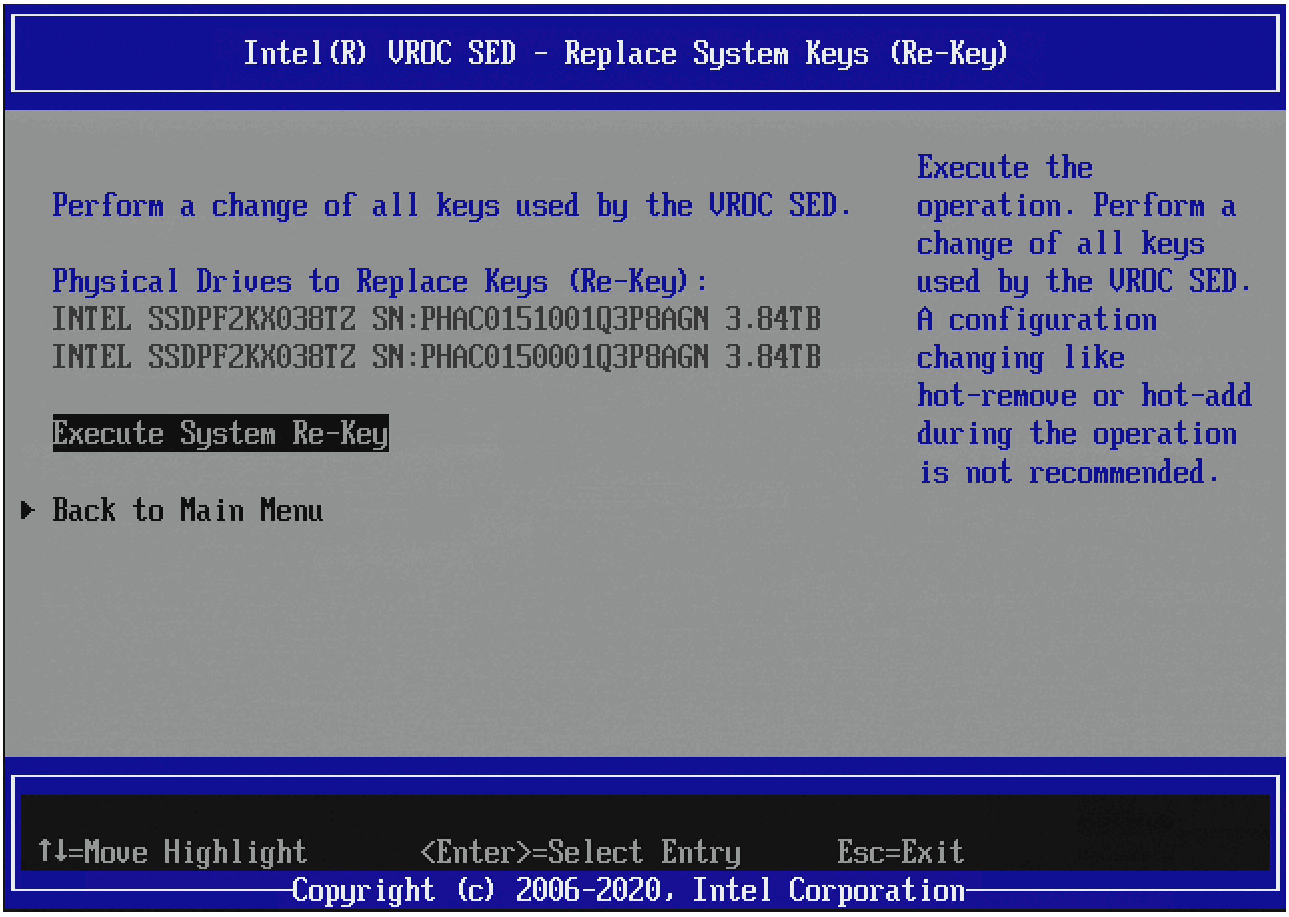
Element	**Help message**
Execute System Re-Key	Execute the operation. Perform a change of all keys used by the VROC SED. A configuration changing like hot-remove or hot-add during the operation is not recommended.

Back to Main Menu	Back to Main Menu

The table below describes **popup** details.

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

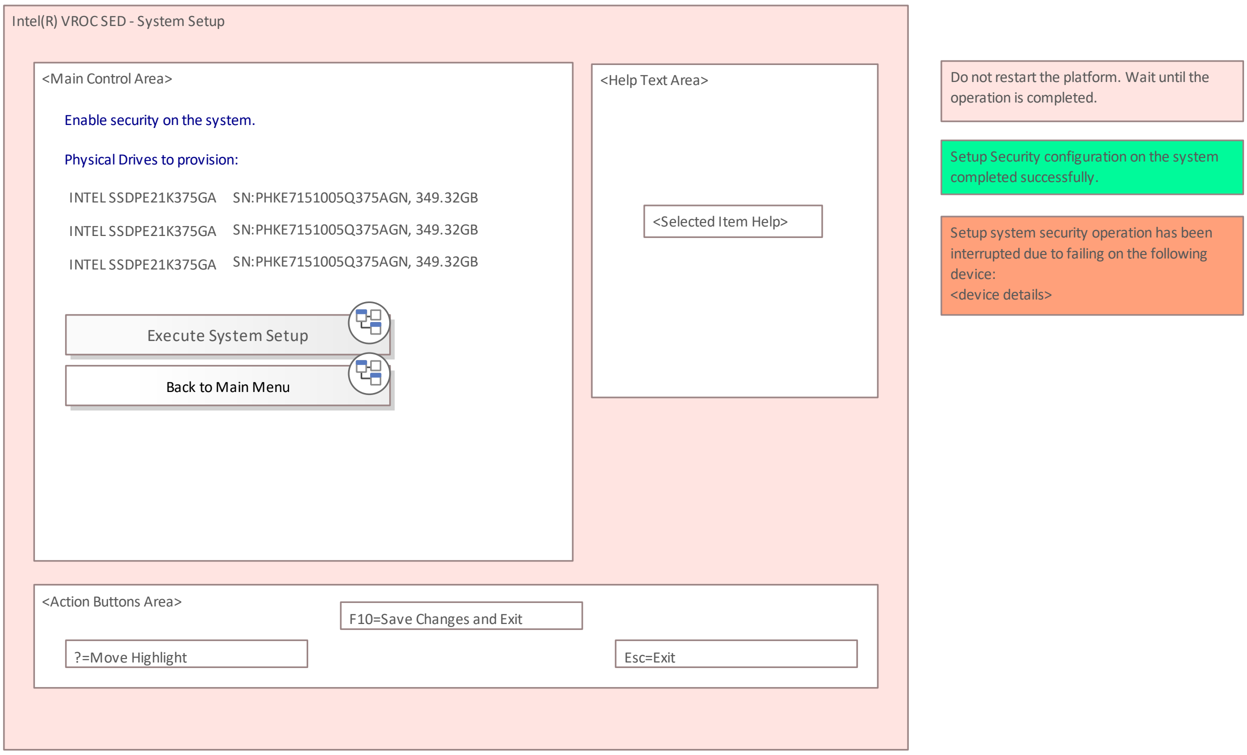
Example Screenshots:



```
                Intel(R) VROC SED - Replace System Keys (Re-Key)

  Perform a change of all keys used by the VROC SED.    Execute the
                                                        operation. Perform a
  Physical Drives to Replace Keys (Re-Key):             change of all keys
  INTEL SSDPF2KX038TZ SN:PHAC0151001Q3P8AGN 3.84TB      used by the VROC SED.
  INTEL SSDPF2KX038TZ SN:PHAC0150001Q3P8AGN 3.84TB      A configuration
                                                        changing like
  Execute System Re-Key                                 hot-remove or hot-add
                                                        during the operation
▶ Back to Main Menu                                     is not recommended.

 ↑↓=Move Highlight      <Enter>=Select Entry      Esc=Exit
              Copyright (c) 2006-2020, Intel Corporation
```

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.



Enable security on the system.

Physical Drives to provision:

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB

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

Setup Security configuration on the system completed successfully.

Setup system security operation has been interrupted due to failing on the following device:
<device details>

Figure 24: System Setup , Version 1.4

The table below describes the **attributes** of the form.

Attribute	Value	Description
Form Id	0x0008	Unique Id for the form within the form set
Title	Intel(R) VROC SED - Setup	Title text for the form.
Physical Drives to provision (List)	A list of SED capable drives to provision security (Model, SN, Capacity). When no SED devices found following text shall be displayed instead: "No Self-Encrypting capable drives connected to the system".	List of drives to provisioned security on
Execute System Setup (Action)	The action shall be ENABLED when the following conditions are met: • KMS status is "Connected" • System Status is "Disabled" • There is at least one VMD attached drive with OPAL capability.	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 "Setup in progress".
Back to the Main Menu		Go to Form "Dashboard View"

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

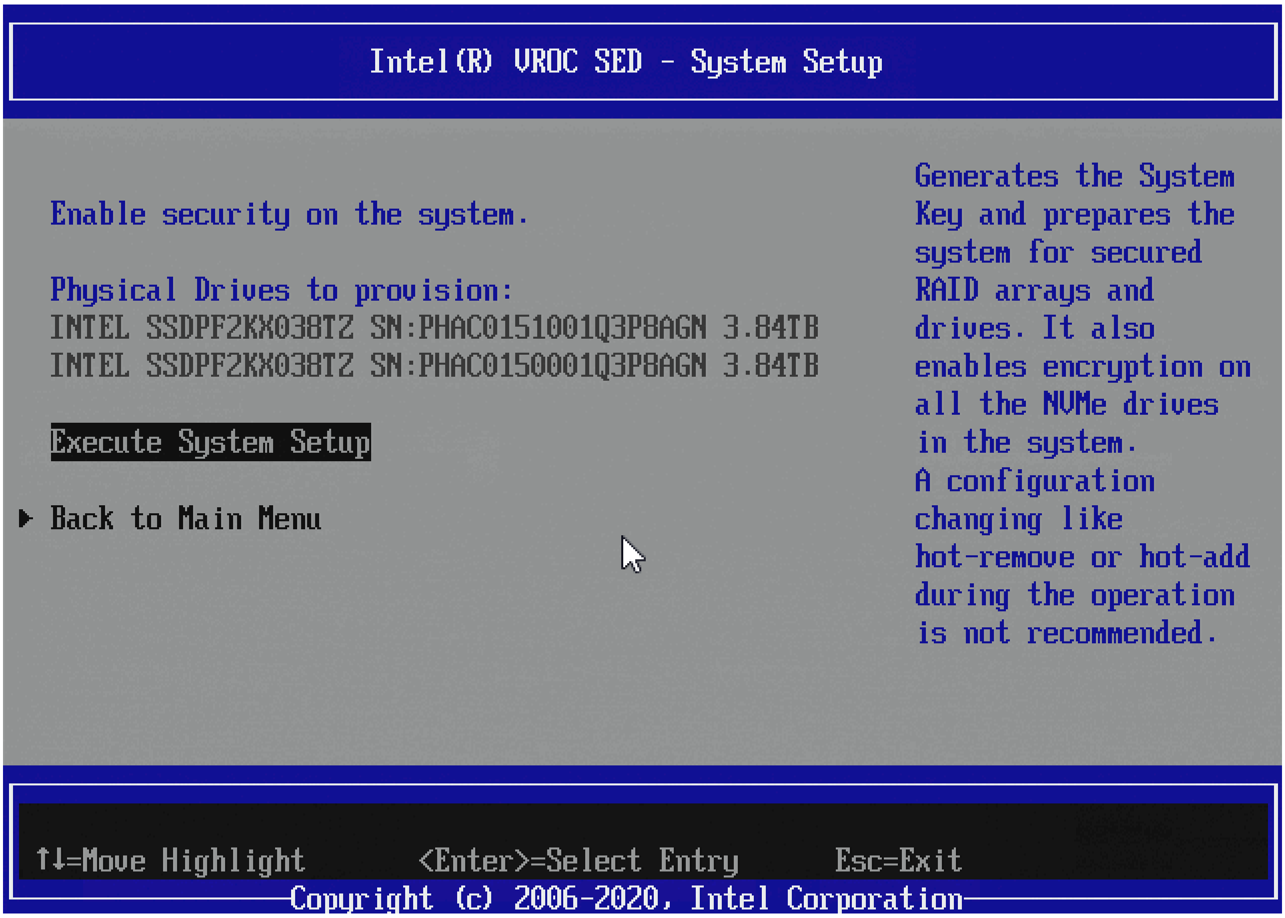
Element	Help message
Execute System Setup	Generates the System Key and prepares the system for secured RAID arrays and drives. It also enables encryption on all the NVMe drives in the system.

	A configuration changing like hot-remove or hot-add during the operation is not recommended.
Back to Main Menu	Back to Main Menu

The table below describes **popup** details.

Element	Value	Description
"Setup in progress"	Do not restart the platform. Wait until the operation is completed.	Shall be shown until setup operation is completed.
"Setup Security completed successfully"	Setup Security configuration on the system completed successfully.	When the operation completed successfully
"Setup Security failed"	Setup system security operation has been interrupted due to failing on the following device: INTEL SSDPE21K375GA SN:PHKE7151005Q375AGN, 349.32GB	When the operation failed and there is issue connected with a particular drive.
"Setup Security failed"	Setup system security operation has been interrupted due to a general failure.	When the operation failed, and there is NO information which drive has failed.

Example Screenshots:



Intel(R) VROC SED - System Setup

Enable security on the system.

Physical Drives to provision:
INTEL SSDPF2KX038TZ SN:PHAC0151001Q3P8AGN 3.84TB
INTEL SSDPF2KX038TZ 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 NVMe drives in the system. A configuration changing like hot-remove or hot-add during the operation is not recommended.

↑↓=Move Highlight <Enter>=Select Entry Esc=Exit
Copyright (c) 2006-2020, Intel Corporation