Key Management Guide 9.1.0.5

Created on: Nov 19, 2024

Notice

Copyright

Protegrity products are protected by and subject to patent protections;

Patent: *https://www.protegrity.com/patents*.

The Protegrity logo is the trademark of Protegrity Corporation.

NOTICE TO ALL PERSONS RECEIVING THIS DOCUMENT

Some of the product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective owners.

Windows, Azure, MS-SQL Server, Internet Explorer and Internet Explorer logo, Active Directory, and Hyper-V are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SCO and SCO UnixWare are registered trademarks of The SCO Group.

Sun, Oracle, Java, and Solaris are the registered trademarks of Oracle Corporation and/or its affiliates in the United States and other countries.

Teradata and the Teradata logo are the trademarks or registered trademarks of Teradata Corporation or its affiliates in the United States and other countries.

Hadoop or Apache Hadoop, Hadoop elephant logo, Hive, and Pig are trademarks of Apache Software Foundation.

Cloudera and the Cloudera logo are trademarks of Cloudera and its suppliers or licensors.

Hortonworks and the Hortonworks logo are the trademarks of Hortonworks, Inc. in the United States and other countries.

Greenplum Database is the registered trademark of VMware Corporation in the U.S. and other countries.

Pivotal HD is the registered trademark of Pivotal, Inc. in the U.S. and other countries.

PostgreSQL or Postgres is the copyright of The PostgreSQL Global Development Group and The Regents of the University of California.

AIX, DB2, IBM and the IBM logo, and z/OS are registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

Table of Contents

Chapter 1

Introduction to this Document

This document is intended to provide a general overview of Key Management and to explain its importance and impact on Protegrity products.

1.1 Sections contained in this Guide

The guide is broadly divided into the following sections.

- Section 1 *Introduction to this Document* defines the purpose and scope for this guide. In addition, it explains how information is organized in this guide.
- Section 2 *What is Key Management* provides information about why key management is important to an organization.
- Section 3 *Protegrity Key Management* provides information about key elements that Protegrity Key Management includes and how to assist in maintaining data integrity.
- Section 4 *Key Management Web UI* provides information about the Key Management Web UI options and supporting screens for different types of keys that are part of the Protegrity Key Management.
- Section 5 *Working with Keys* describes each option that you can perform, such as rotating keys and changing key states for each of the keys in Protegrity Key Management.
- Section 6 *Appendix A: Best Practices* provides information about best practices that must be followed for efficient key management.
- Section 7 *Appendix B: Keys-Related Terminology* provides information terminology related to Protegrity Key Management.

1.2 Accessing the Protegrity documentation suite

This section describes the methods to access the *Protegrity Documentation Suite* using the *My.Protegrity* portal.

Chapter 2

What is Key Management

In an IT infrastructure, many disparate business functions work together. Each of these functions use security features in form of point solutions within themselves to protect sensitive data that they consume. The data is protected by these point solutions using keys that cannot be used interchangeably among point solutions, thus risking the integrity of data. Enterprises need to implement data protection using Key Management (KM) solutions that manage keys comprehensively.

A KM solution that an enterprise selects must ensure that data encryption does not disrupt organizational functions. KM solutions must provide secure administration of keys through their life cycle, which includes generation, use, distribution, storage, recovery, rotation, termination, auditing, and archival.

Chapter 3

Protegrity Key Management

The Protegrity Data Security platform uses many keys to protect your sensitive data. The Protegrity Key Management solution manages these keys and this system is embedded into the fabric of the Protegrity Data Security Platform. For example, the creation of a cryptographic or data protection key is a part of the process of how you define the way sensitive data is to be protected. There is not a specific user visible function to create a data protection key.

With key management as a part of the platform's core infrastructure, the security team can focus on protecting data and not the low-level mechanics of key management. This platform infrastructure-based key management technique eliminates the need for any human to be a custodian of keys. This holds true for any of the functions included in key management.

The following keys are a part of the Protegrity Key Management solution:

- **Key Encryption Key (KEK)**: The cryptographic key used to protect other keys. The KEKs are categorized as follows:
  - **Master Key**: It protects the Data Store Keys, Repository Key, and Signing Key. In the ESA, only one active Master Key is present at a time.
  - **Repository Key**: It protects policy information in the ESA. In the ESA, only one active Repository Key is present at a time.
  - **Data Store Key**: It encrypts the audit logs on the protection endpoint. In the ESA, multiple active Data Store keys can be present at a time.
- **Signing Key**: The protector utilizes the Signing Key to sign the audit logs for each data protection operation. The signed audit log records are then sent to the ESA, which authenticates and displays the signature details received for the log records.

  For more information about the signature details for the log records, refer to the *Log Management Guide 8.0*.
- **Data Encryption Key (DEK)**: The cryptographic key used to encrypt the sensitive data for the customers.
- **Codebooks**: The lookup tables used to tokenize the sensitive data.

3.1 Key Encryption Keys (KEKs) in Protegrity

Protegrity Key Encryption Keys (KEKs) are made of three keys, namely Master Key (MK), Repository Key (RK), and Data Store Key (DSK). All three keys are AES 256-based keys and are collectively referred to as the KEKs. The MK, RK, and DSKs are generated from a FIPS 140-2 Level 1 non-certified Protegrity Soft HSM module using PKCS#11 API specification in ESA.

The MK is responsible for protecting RK and DSK. The MK protects the Policy-Key repository that holds key value and properties for RK, DSK, and only key properties of MK. The MK is non-exportable and stored in the Protegrity Soft HSM. Both the MK and RK are generated when ESA is installed. The RK protects the Policy-Key repository for DEKs.

When we create a Data Store (DS), ESA creates a DSK for that DS and encrypts it with the MK. This protected DSK is stored in the Policy-Key repository. A single DS can be associated with multiple DSKs, out of which only one DSK is in the Active state at a time.

3.2 DEKs in Protegrity

Based on the protection method that you want to apply to sensitive data, you can either use encryption or tokenization.

When encryption is selected as the protection method, a Data Element (DE) linked to an encryption algorithm is created. Along with the DE, a Data Encryption Key (DEK) is also created. When tokenization is selected as the protection method, a data element linked to a tokenizer is created. The logic about how protect and unprotect methods with tokenization should work is stored in codebooks.

The DEK protects the actual sensitive data. The policy and the codebooks are stored in ESA's Policy-Key repository.

3.3 Codebooks

Codebooks are generated when a data element uses tokenization as the method of performing security operations. Codebooks are stored in clear in the shared memory of the PEP server.

Tokenization does not involve use of algorithms for protection but relies on randomized tables known as look up tables to protect and unprotect sensitive information. Since random values are used for data security operations, the strength of data protection is also improved.

When the PEP server of the protector connected with the ESA is started, it requests for policy information. This policy information includes codebooks required for tokenization data elements.

3.4 Policy Key Integration

In the Protegrity Data Security Platform, *endpoint* protection is implemented through policies. Keys form a part of the underlying infrastructure of a policy and are not explicitly visible.

The following figure provides an overview of the key management workflow.

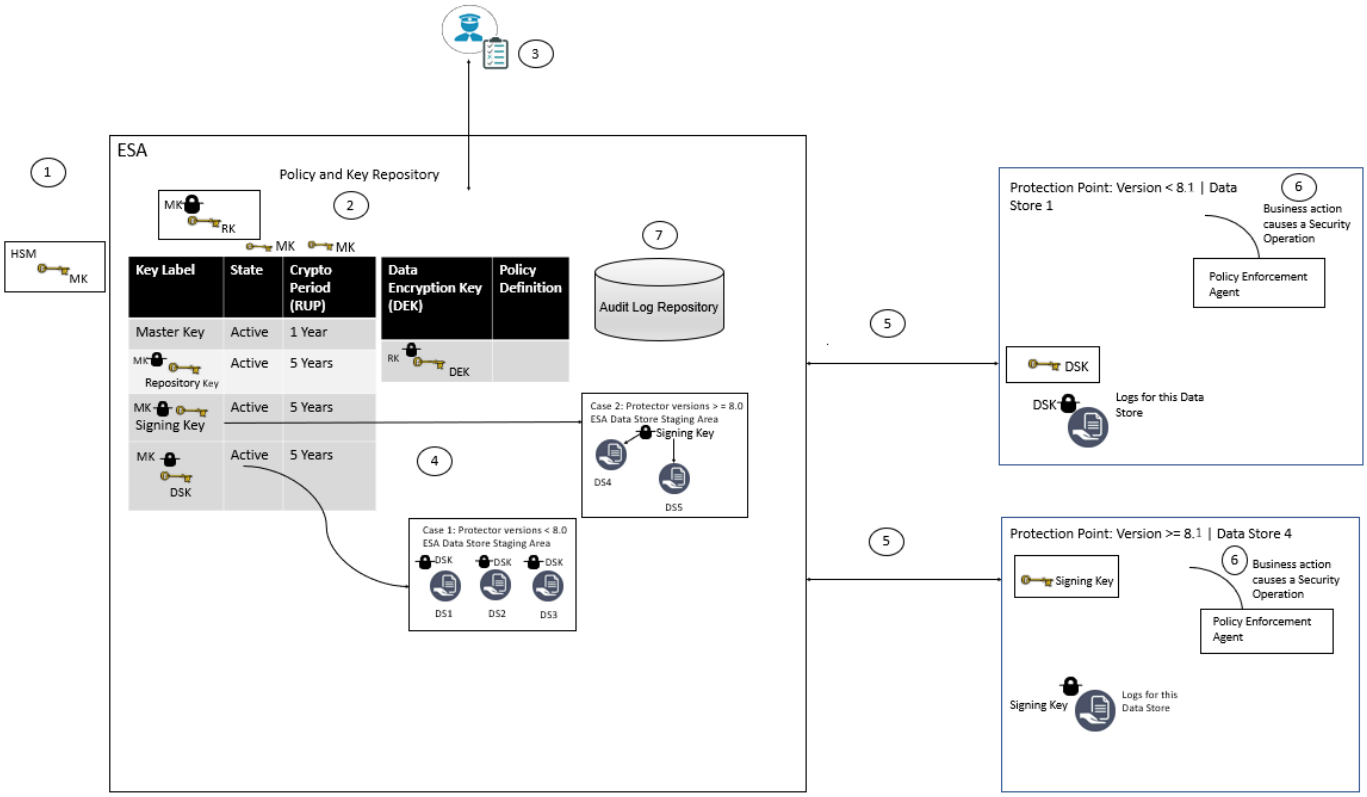


Figure 3-1: Protegrity Key Management Workflow

1. When the ESA is installed and the Key Management is initialized, the *Protegrity Soft HSM* generates the Master key. The *Master key* protects the *Policy-Key Repository*, which stores the internal Master Key properties, Signing Key, Repository Key, and Data Store Key. The Master key resides in the Soft Hardware Security Module (HSM) and never moves out of it. You must use the switch Key Store module option to switch to an external HSM or Key Store. After switching, a new master key is generated, which is then used to re-protect the other KEKs.

   For more information about initializing the Key Management, refer to the section *Initializing the Key Management*.

   For more information about switching Key Store modules, refer to the section *Switching Key Store Modules* in the section *HSM Integration Guide 9.1.0.0*.

2. The *Repository Key (RK)* is also generated in the Protegrity Soft HSM when the Key Management data is initialized. After generation, it is exported to the policy-key repository. It is encrypted using the Master key, which is used to protect the policy-key repository.

3. Starting from the version 8.1.0.0 release, when the ESA v8.1.0.0 is installed and policy management is initialized, a Signing Key is created. It is encrypted by the Master Key. When a Security Administrator creates a policy, as part of the policy creation process, a Data Store is created. When a Data Store is created in the ESA 8.1.0.0, the Signing Key is linked to the data store and is deployed with the data store. The Signing Key is used to add a signature to the log records generated for each data protection operation, which are then sent from the Protection Endpoint to the ESA.

   For more information about the Signing Key, refer to the section *Signing Key*.

   In case of data store deployment to protectors with version lower than 8.0, a related *Data Store Key (DSK)* is generated. This DSK is protected by the Master key.

4. When a policy is deployed, the HubController service makes the policy-related information available to the protectors for download. It verifies the registered nodes for the data stores from the repository. It also reads the policy information and routes the information to the protection point.

5. At the protection endpoint, the PEP server receives the policy information and data store information. When the PEP server finds information related to the data store to which it belongs, it pulls the relevant policy information.

   The policy and codebooks are sent to the protector. Since this transfer is through Transport Layer Security (TLS), the line is encrypted.

   The DSK is sent to the protector in case of protectors with version lower than 8.1.0.0. It is used to encrypt the audit logs on the protector, which reside on the disk. The Signing Key is deployed with the data store in case of protectors with version starting from 8.1.0.0.

6. When a security operation is performed at the protection endpoint, the enforcement agent in the protector pulls the required policy information and completes the security operation.

   The Signing Key adds a signature to the log record for each data protection operation.

7. The audit logs are sent to the ESA Audit Log repository periodically. In addition, the signed log records are then sent to the ESA for additional analysis.

   For more information about the signature details for the log records, refer to the *Protegrity Log Forwarding Guide 9.1.0.5*.

For more information about policy, DS, and Data elements, refer to the *Policy Management Guide 9.1.0.3*.

3.5 Certificates

Certificates in Protegrity are generated when the ESA is installed. These certificates and their related keys are used for internal communication between various components in the ESA and between ESA and the PEP servers.

For more information about certificates, refer to the *Certificate Management Guide 8.1.0.0*.

3.6 Key Store

A Hardware Security Module (HSM) is a device used to store keys. The keys stored in the HSM are used to protect and un-protect data. The protection and un-protection of data takes place inside the HSM. These keys cannot be exported.

Protegrity Soft HSM: The Protegrity Soft HSM is an internal Soft HSM bundled with the ESA. The Protegrity Soft HSM provides all the functionalities that a HSM provides. Using the Protegrity Soft HSM provided with the ESA ensures that the keys remain within the secure perimeter of the data security solution. When an enterprise decides to implement a data protection solution in their infrastructure, careful consideration about the type of the HSM device to be used needs to be taken as part of the implementation strategy.

The Protegrity Data Security Platform provides you the flexibility, if needed, to switch between HSMs. When the ESA is installed, the internal Protegrity Soft HSM generates the Master Key (MK). When switching an external HSM, a new MK is generated in the new HSM. The existing KEKs are re-protected using this new MK and the old MK is deactivated.

> **Warning:** Ensure that the HSM supports the PKCS#11 interface.

For more information about switching from the Protegrity Soft HSM to HSM, refer to the *HSM Integration Guide 9.1.0.0*.

Cloud HSM: The Cloud-hosted Hardware Security Module (Cloud HSM) service allows you to host encryption keys and perform cryptographic operations in a cloud hosted HSM cluster. Protegrity supports the Google Cloud Platform (GCP) Cloud

HSM. The GCP console is used to define a project where keyrings, keys, and key versions can be created. You can use the GCP Cloud HSM to ensure that the life cycles of keys work the same as they would on-premise.

> **Important:** The GCP support is available with the additional patch ESA_PAP-ALL-64_x86-64_9.1.0.0.2156.FE-1 on the ESA release 9.1.0.0.

> **Warning:** Ensure that the project location supports creating HSM level keys.

For more information about switching from the Protegrity Cloud HSM to Soft HSM, refer to the *Google Cloud platform (GCP) Key Management Service (KMS) Integration Guide for ESA 9.1.0.0.*

3.7 Key Rotation

Key rotation involves putting the new encryption key into active use and ensure that the data encrypted with the older key is now encrypted with the new key. Key rotation can take place either when the key is about to expire or needs to be deactivated due to malicious threats.

The key rotation for KEKs, Signing Key, and DEKs in the Protegrity Data Security Platform can be described as follows:

- **Master Key (MK)**: The Master Key(MK) can be rotated using the ESA Web UI. The supported states for the MK are *Active*, *Deactivated*, *Compromised*, and *Destroyed*. When the ESA is installed, the MK is in *Active* state. It moves to *Deactivated* state, when rotated. As soon as MK is rotated, the RK and DSK are reprotected by first decrypting using the old MK and re-encrypted using the new MK.

  The MK is set for automatic rotation ten days prior to the *Originator Usage Period (OUP)* expiration date by default. On the ESA Web UI, navigate to **Key Management** > **Master Keys** to check the automatic rotation date.

- **Repository Key (RK)**: The Repository Key (RK) can be rotated using the ESA Web UI. The supported states for the RK are *Active*, *Deactivated*, *Compromised*, and *Destroyed*. After the RK is rotated, it is decrypted using the MK. The old decrypted RK is then used to decrypt the policy data residing in the database and is then deactivated. Thus, the RK in *Active* state moves to *Deactivated* state, when rotated. The newly generated RK is encrypted using the MK and is used to encrypt the policy data residing in the database. Thus, with rotation, the newly generated RK moves to the *Active* state.

  The RK is set for automatic rotation ten days prior to the *Originator Usage Period (OUP)* expiration date by default. On the ESA Web UI, navigate to **Key Management** > **Repository Keys** to check the automatic rotation date.

  > **Note:** It is recommended that token elements are not created when the RK is in the *Deactivated* state.

- **Data Store Key (DSK)**: The Data Store Key (DSK) can be rotated using the ESA Web UI. The supported states for the DSK are *Preactive*, *Active*, *Deactivated*, *Compromised*, and *Destroyed*. When the ESA is installed, the DSK is in the *Preactive* state and encrypts the policy information in the ESA Data Store staging area. It moves to *Active* state when the policy is deployed.

  When the DSK is rotated, it is marked as *Deactivated*. As soon as the DSK is rotated, the MK decrypts the old DSK. The old DSK is used to decrypt the policy package in the ESA Data Store staging area. The new DSK is generated in the Protegrity Soft HSM. The new DSK encrypts the policy package, and then the active MK encrypts the new DSK.

  When the protection endpoint polls the ESA, it notices that the policy package has changed. It pulls the new package along with the new DSK. The Audit logs that are generated after key rotation are encrypted with the new DSK.

  > **Note:**
  > - Starting from version 7.1, the manual rotation for the RK, MK, and DSK from the ESA Web UI requires the user to be assigned with the *KeyManager* role.

> - It is recommended that the RK, MK, and DSK are not rotated simultaneously.

The DSK is set for automatic rotation ten days prior to the *Originator Usage Period (OUP)* expiration date by default. On the ESA Web UI, navigate to **Key Management** > **Data Store Keys** to check the automatic rotation date.

- **Signing Key**: The Signing Key can be rotated using the ESA Web UI. The supported states for Signing Key are *Active*, *Deactivated*, *Compromised*, and *Destroyed*. When the ESA 8.0 is installed and policy management is initialized, a Signing Key is created, which is in the *Active* state.

  When it is rotated, the data stores that are already deployed are updated with the new Signing Key details, such as, Unique Identifier (UID). The old Signing Key is marked as *Deactivated*. The PEP server downloads the new Signing Key during a subsequent policy update and the Protector starts utilizing it to sign the audit logs for each data protection operation.

  The Signing Key is set for automatic rotation ten days prior to the *Originator Usage Period (OUP)* expiration date by default. On the ESA Web UI, navigate to **Key Management** > **Signing Keys** to check the automatic rotation date.

  > **Note:**
  > - The manual rotation for the Signing Key from the ESA Web UI requires the user to be assigned with the *KeyManager* role.
  > - It is recommended that the Signing Key and Key Encryption Keys (KEKs) are not rotated simultaneously.

- **Data Element Key (DEK)**: If key ID is enabled for a data element, then multiple keys can be created for a single data element, but only one key at a time is used for encryption.

3.8 Key Cryptoperiod and States

Cryptoperiods can be defined as the time span for which the key remains available for use across an enterprise. Setting cryptoperiods ensures that the probability of key compromise by external threats is limited. Shorter cryptoperiods ensure that the strength of security is greater.

In the ESA, the Master Key, Repository Key, Signing Key, and the Data Store Key are governed by cryptoperiods. For these keys in the ESA, the validity is dictated by the Originator Usage Period (OUP) and the Recipient Usage Period (RUP). The OUP is the period until when the key can be used for protection, while the RUP is the period when the key can be used to unprotect only.

For keys in Protegrity, the following table provides the OUP and RUP information.

Table 3-1: Cryptoperiod

Key Name	OUP	RUP
Master Key	1 Year	1 Year
Repository Key	<=2 Years	<=5 Years
Data Store Key	<=2 Years	<=5 Years
Signing Key	<=2 Years	<=5 Years

For more information about key states, refer to *Changing DSK States*, *Changing Signing Key States*, and *Changing ERK States*.

Chapter 4

Key Management Web UI

The Key Management Web UI lets you initialize, view, and manage key information.

4.1 Initializing the Key Management

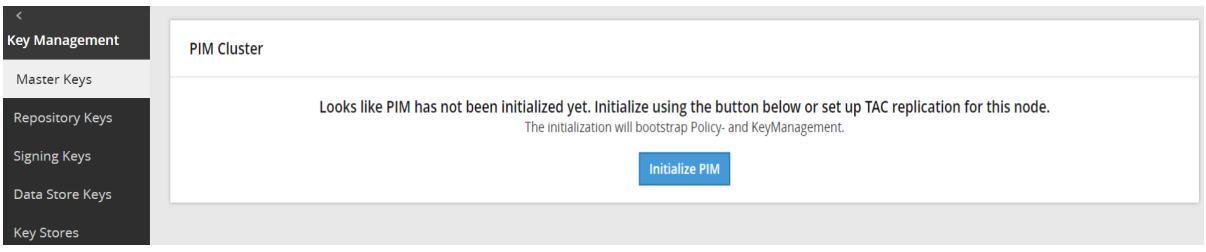
When you install and log in to the ESA for the first time, you must initialize the Policy Management (PIM), which creates the keys-related data and the policy repository. In a Cloud-based installation, this step helps to create a new instance of the required keys-related data instead of inheriting the data from the virtual image template. This section describes the steps to initialize the Policy Management (PIM) to load the Policy Management-specific information on the ESA Web UI.

Before you begin

> **Note:**
> When you try to access any of the Policy Management or Key Management screens on the ESA Web UI, a request to initialize the PIM appears.

> **Caution:** Prior to the installation of protectors, ensure that you perform the following steps to initialize the Policy Management.

1. On the ESA Web UI, click **Key Management**.
2. Click any option available in the Key Management area.
   The following screen to initialize PIM appears.



3. Click **Initialize PIM**.
   A confirmation message box appears.

4. Click **Ok**.
   The information for the keys appears in the Key Management area.

If you are working with protector versions 6.6.x, then the following additional steps must be performed to ensure the backward compatibility of the ESA v8.1.0.0 with the v6.6.x protectors.

1. On the ESA Web UI, navigate to **System** > **Services**.
2. In the *Policy Management* area, restart the *Logfacade Legacy* service.

4.2 Master Keys Web UI

Information related to Master Keys such as state, timestamps for key creation and modification, and so on is available on the Master Keys Web UI.

The following image shows the Master Keys UI.

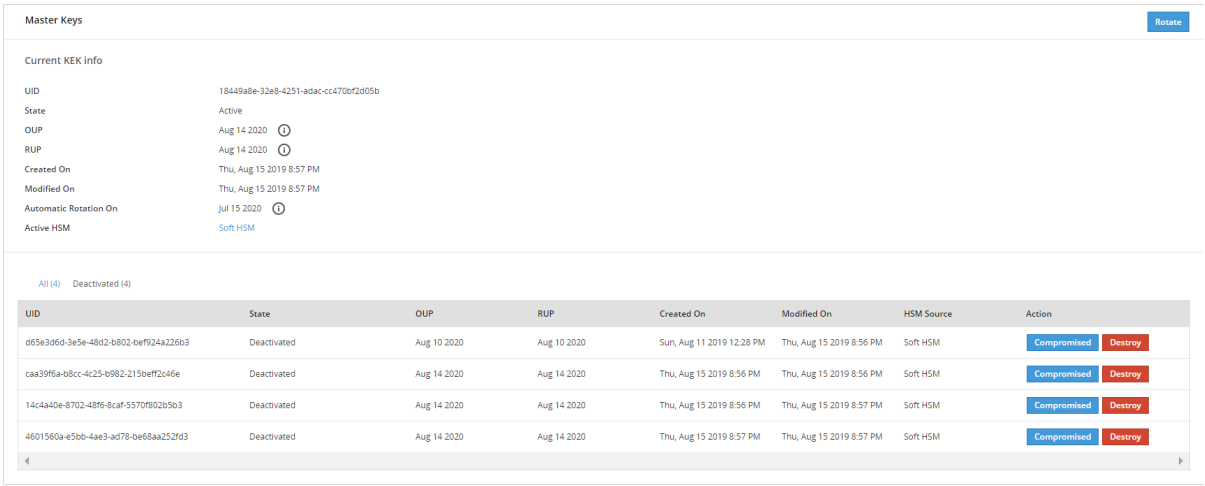


Figure 4-1: Protegrity Key Management Workflow – Master Keys

4.3 Repository Keys Web UI

Information related to Repository keys such as state, timestamps for key creation and modification, and so on is available on the Repository Keys Web UI.

The following image shows the Repository Keys UI.

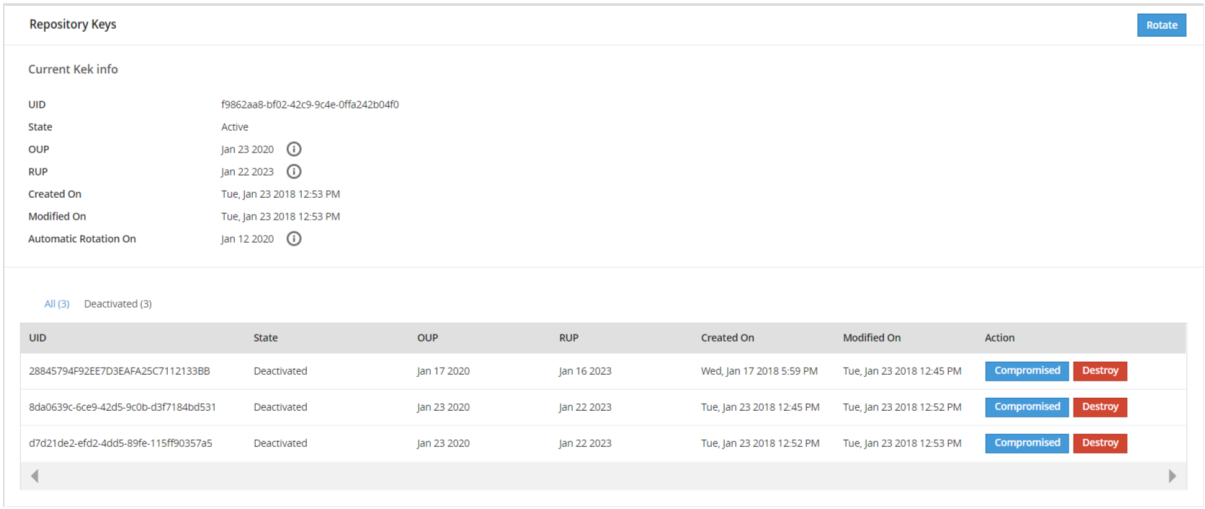


Figure 4-2: Protegrity Key Management Workflow – Repository Keys

4.4 Data Store Keys Web UI

Information related to DSKs such as state, timestamps for key creation and modification, and so on is available on the Data Store Keys Web UI.

The following image shows the Data Store Keys UI.

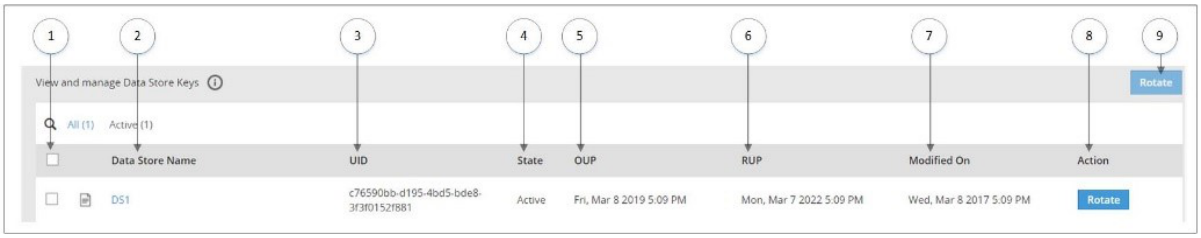


Figure 4-3: Figure 2: Protegrity Key Management Workflow – DSKs

The options available as part of the UI are explained in the following table.

Table 4-1: Data Store Key Web UI Options

No	Option		Description
1	Select multiple Data Store		Select the check box to rotate multiple Data Stores at the same time.
2	Data Store Name		Click to view information related to Active DSK and older keys.
3	UID		Unique identifier of the key.
4	State		Current State of the DSK linked to the Data Store.
5	OUP		The period of time in the cryptoperiod of a symmetric key during which cryptographic protection may be applied to data.
6	RUP		The period of time during the cryptoperiod of a symmetric key during which the protected information is processed.
7	Modified On		Time stamp when DSK was last modified.
8	Action		
		Rotate	Click to rotate the DSK for a Data Store.
9	Rotate		

If you click the Data Store name, for example DS1, you can view detailed information about the Active key and older keys.

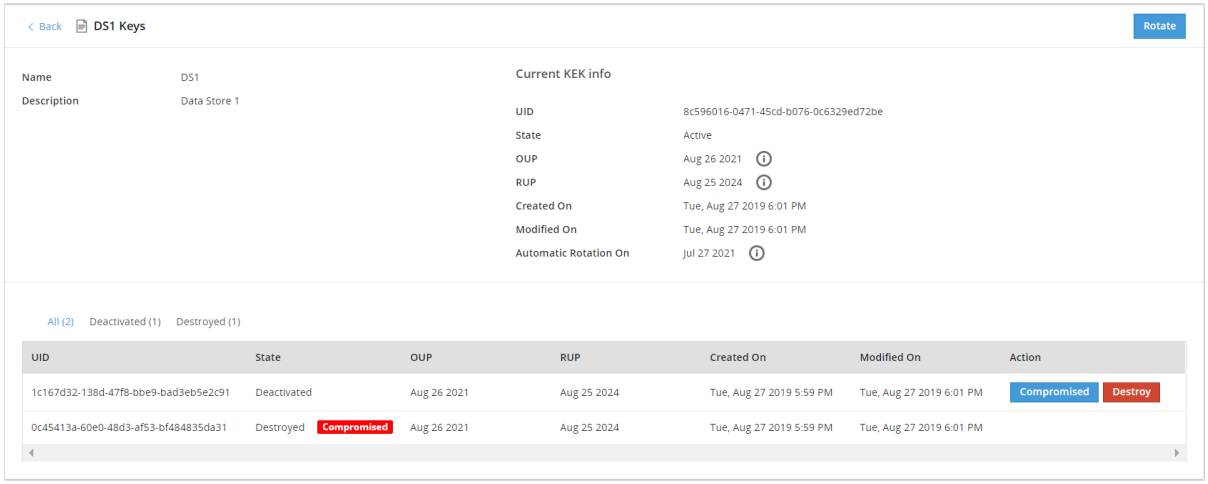


Figure 4-4: Data Store Key Detailed Information

The **Action** column provides an option to change the state of a key to *Destroyed* or mark the key as *Compromised*. For more information about the options available for DSK states, refer to *Changing Key States*.

4.5 Signing Key

Starting from the 8.1.0.0 release, a Signing Key is used to add a signature to the log records generated for each data protection operation, which are then sent from the Protector to the ESA.

When the ESA v8.1.0.0 is installed and key management is initialized, a Signing Key is created, which is encrypted by the Master Key. All the data stores are linked with the Signing Key. It includes any new data stores that are created or existing data stores linked to protectors with version 8.1.0.0 and higher. In case of data store deployment to protectors with version lower than 8.1.0.0, the Signing Key is not applicable. In this case, the DSK is applicable to protect the audit log information and to support compatibility with protectors prior to version 8.1.0.0.

The protector uses the Signing Key to sign the audit logs for each data protection operation. The signed audit log records are then sent to the ESA, which authenticates and displays the signature details received for the log records. The Signing Key helps to identify if the log records are not tempered and are received from the required protection endpoint or Protector.

For more information about the signature details for the log records, refer to the *Protegrity Log Forwarding Guide 9.1.0.5*.

A single Signing Key is linked and deployed with all the data stores. At a time, only one Signing Key can be in the *Active* state.

Chapter 5

Working with Keys

This section provides information about viewing active MK, RK, and DSK information and key rotation for MK, RK, and DSK.

5.1 Viewing the Master Key Information

You can view the Master key-related information such as state, OUP, RUP, and other details using the Web UI.

➤ To view information about the Master key:

1. On the ESA Web UI, click **Key Management** > **Master Keys**.
2. In the **Current KEK info** area, view the current Master Key information.
3. In the <Master_key_table> table, view the information related to the older Master Key.

5.1.1 Rotating the Master Key

The Master key can be rotated from the ESA Web UI. When the Master key is rotated, the old key state changes from *Active* to *Deactivated*, while the new key becomes *Active*. In this release, MK is governed by two states, namely *Active* and *Deactivated*.

Before you begin

Note:

- Starting from version 7.1, the rotation for the RK, MK, and DSK requires the user to be assigned with the *KeyManager* role.
- It is recommended that the RK, MK, and DSK are not rotated simultaneously. Also, ensure that all keys are in *Active* state before performing key rotation.

➤ To rotate the Master key:

1. On the ESA Web UI, click **Key Management** > **Master Keys**.

The current KEK information appears.

2. Click **Rotate**.
   A confirmation message appears for rotation of the Master Key.
3. Click **Ok**.
   A message *Key has been rotated successfully* appears.

   The MK is set for automatic rotation ten days prior to the *Originator Usage Period (OUP)* expiration date by default. In the ESA Web UI, navigate to **Key Management** > **Master Keys** to check the automatic rotation date.

5.1.2 Changing MK States

You can assign key states to the MK using the ESA Web UI.

➤ To change MK state:

1. Rotate the MK.
   For more information about rotating a MK, refer to the section *Rotating the Master Key*.
2. In the MK table, click the states available under the *Action* column to change the state for an MK.
   The following table provides information about the possible key states for MK that you can change based on their current state.

Current Key State	*Can change state to…*		*State Change*
	State	*Reason*	
Active	Deactivated	• Key Rotation • OUP expiration	Auto
Deactivated	Compromised **Note:** You can click **Compromised** to mark the key as *Compromised*. This displays a *Compromised* label next to the state.	Key is compromised.	Manual
	Note: You can click **Destroy** to mark the key as *Destroyed*. This displays a *Destroyed* label next to the state.	Organization requirement	Manual

5.2 Viewing Repository Key Information

You can view the repository key-related information such as state, OUP, RUP, and other details using the Web UI.

➤ To view information about the Repository Key:

1. On the ESA Web UI, click **Key Management** > **Repository Keys**.
2. In the **Current KEK info** area, view the current Repository Key information.
3. In the Repository Key table, view the information related to the older Repository Key.

5.2.1 Rotating the Repository Key

The Repository Key (RK) can be rotated manually on expiry of the OUP using the ESA Web UI.

Before you begin

> **Note:**
> - Starting from version 7.1, the rotation for the RK, MK, and DSK requires the user to be assigned with the *KeyManager* role.
> - It is recommended that the RK, MK, and DSK are not rotated simultaneously. Also, ensure that all keys are in *Active* state before performing key rotation.

To rotate the RK:

1. On the ESA Web UI, click **Key Management** > **Repository Keys**.
   The screen displays the current KEK information with the list of any older keys.
2. Click **Rotate**.
   A confirmation message appears.
3. Click **OK**.
   A message *Key has been rotated successfully* appears.

The RK is set for automatic rotation ten days prior to the *Originator Usage Period (OUP)* expiration date by default. In the ESA Web UI, navigate to **Key Management** > **Repository Keys** to check the automatic rotation date.

5.2.2 Changing RK States

You can assign key states to the RK using the ESA Web UI.

To change RK state:

1. Rotate the RK.
   For more information about rotating a RK, refer to the section *Rotating the RK*.
2. In the RK table, click the states available under the Action column to change the state for an RK.
   The following table provides information about the possible key states for RK that you can change based on their current state.

Current Key State	*Can change state to…*		*State Change*
	State	*Reason*	
Active	Deactivated	• Key Rotation • OUP expired	Auto
Deactivated	Compromised	Key is compromised.	Manual

Current Key State	*Can change state to…*		*State Change*
	State	*Reason*	
	Note: You can click **Compromised** to mark the key as *Compromised*. This displays a *Compromised* label next to the state.		
	Note: You can click **Destroy** to mark the key as *Destroyed*. This displays a *Destroyed* label next to the state.	Organization Requirement	Manual

> **Note:** It is advised to not create token elements when RK is in the Deactivated state.

5.3 Viewing Data Store Key (DSK) Information

A DSK is unique and linked to a Data Store. Along with changing the state of a key, you can also view the older keys and the related information.

Before you begin

Before you can view information related to a DSK, ensure that the following prerequisites are completed.

- Create a policy with all the elements. For more information about creating a policy, refer to the *Policy Management Guide*.
- As part of creating a policy, create a Data Store, for example DS1. When this Data Store is created, a unique DSK for the Data Store is generated and can be seen in the Key Management UI.

➤ To view DSK information:

1. On the ESA Web UI, click **Key Management** > **Data Store Keys**.
   A list of data stores appears.
2. Click a Data Store name, for example **DS1**.
3. In the **Current KEK info** area, view the current DSK information.
4. In the <DSK_table> table, view the information related to the older DSKs.

5.3.1 Rotating a DSK

A DSK can be rotated manually on expiry of the OUP using the ESA Web UI.

Before you begin

> **Note:**
> - Starting from version 7.1, the rotation for the RK, MK, and DSK requires the user to be assigned with the *KeyManager* role.
> - It is recommended that the RK, MK, and DSK are not rotated simultaneously. Also, ensure that all keys are in *Active* state before performing key rotation.

➤ To rotate a DSK manually:

1. On the ESA Web UI, click **Key Management** > **Data Store Keys**.
   A list of data stores appears.
2. Select the Data Store for which you want to rotate the key, and then click **Rotate**.

   Warning: You can select multiple Data Stores linked to keys at the same time and perform key rotation.

3. Click **Rotate**.
4. Click the Data Store name to view the older key information.

5.3.2 Changing DSK States

The key states are supported for the DSK. You can assign states for the DSK using the ESA Web UI.

To change DSK state:

1. Rotate the DSK.
   For more information about rotating a DSK, refer to *Rotating a Data Store Key (DSK)*.
2. Click the Data Store name to view the older key information.
3. In the <DSK_table> table, click the states available under the Action column to change the state for a DSK.

   Note: The DSKs are identified using the UID column that displays the Key Id.

   The following table provides information about the possible key states that you can change based on their current state.

Table 5-1: Key States

Current Key State	Can change state to…		State Change
	State	Reason	
Preactive	Active	When a Data Store is deployed	Automatic
	Destroyed	Key Rotation	Manual
Active	Deactivated	• Key Rotation • OUP expired	Automatic
	Destroyed	Key Rotation	Manual
Deactivated	Compromised **Note:** You can click **Compromised** to mark the key as *Compromised*. This displays a *Compromised* label next to the state.	Key Rotation	Manual
	Destroyed **Note:**	Organization Requirement	Manual

Current Key State	Can change state to…		State Change
	State	Reason	
	You can click **Destroy** to mark the key as *Destroyed*. This displays a *Destroyed* label next to the state.		

5.4 Viewing Signing Keys Information

You can view the Signing Key-related information, such as, state, OUP, RUP, and other details using the ESA Web UI.

➤ To view information about the Signing Key:

1. On the ESA Web UI, click **Key Management** > **Signing Keys**.
2. In the **Current KEK info** area, view the current Signing Key information.
3. In the *Signing Keys* table, view the information related to the older Signing Keys.

5.4.1 Rotating the Signing Key

➤ To rotate the Signing Key:

1. On the ESA Web UI, click **Key Management** > **Signing Keys**.
   The screen displays the current KEK information with the list of any older keys.
2. Click **Rotate**.
   A confirmation message appears.
3. Click **OK**.
   A message *Key has been rotated successfully* appears.

The Signing Key is set for automatic rotation ten days prior to the *Originator Usage Period (OUP)* expiration date by default. On the ESA Web UI, navigate to **Key Management** > **Signing Keys** to check the automatic rotation date.

5.4.2 Changing Signing Key States

You can assign key states to the Signing Key using the ESA Web UI.

➤ To change the Signing Key state:

1. Rotate the Signing Key.
   For more information about rotating a Signing Key, refer to the section *Rotating the Signing Key*.
2. In the *Signing Key* table, click the states available under the *Action* column to change the state for a Signing Key.
   The following table provides information about the possible key states for the Signing Key that you can change based on their current state.

Current Key State	*Can change state to…*		*State Change*
	State	***Reason***	
Active	Deactivated	• Key Rotation • OUP expired	Auto
Deactivated	Compromised **Note:** You can click **Compromised** to mark the key as *Compromised*. This displays a *Compromised* label next to the state.	Key is compromised	Manual
	Note: You can click **Destroy** to mark the key as *Destroyed*. This displays a *Destroyed* label next to the state.	Organizational Requirement	Manual

Appendix A

Appendix A: Best Practices for Key Management

Best practices can be followed to leverage the best out of the Protegrity Key Management functionality.

- Starting from version 7.1, the rotation of the Repository Key (RK), Master Key (MK), and Data Store Key (DSK) requires the user to be assigned with the *KeyManager* role.
- The rotation of the Signing Key, which is applicable from version 8.0, requires the user to be assigned with the *KeyManager* role.
- It is recommended that the Signing Key, RK, MK, and DSK are not rotated simultaneously.
- Key Rotation must be performed only after reviewing existing policies or regulatory compliances followed by your organization.
- It is essential that a Corporate Incident Response Plan is drafted to:
  - Understand the security risks of key rotation
  - Handle situations where keys might be compromised
- Consult security professionals, such as, Protegrity, to understand how to enable key rotation with minimal impact on business processes that are affected by the keys.

Appendix B

Appendix B: Keys-Related Terminology

The following table provides an introduction to terminology related to keys that can help you understand Protegrity Key Management.

Table B-1: Keys Terminology

Term	***Definition***
Master Key (MK)	The Master Key is generated in the configured HSM or Key Store when the ESA is installed and the key management is initialized. It resides in the configured HSM or Key Store permanently. Master key protects the **Policy-Key repository, which stores the internal MK properties, RK, and DSK.**
Repository Key (RK)	**The Repository Key (RK)** is generated in the configured HSM or Key Store when the ESA is installed and the key management is initialized. It is protected by the Master key. It protects the **Policy** Repository in ESA.
Data Store Key (DSK)	The Data Store Key (DSK) is generated in the configured HSM or Key Store when a Data Store is created. It is protected by the Master key. It protects the audit logs and policy information at the protection endpoint, which is the Protector.
Signing Key	The Signing Key is created when the ESA v8.0 is installed and key management is initialized. It is protected by the Master Key. It is used by the Protector to add a signature to the log records generated for each data protection operation, which are then sent from the Protector to the ESA. The Signing Key helps to identify if the log records are not tempered and are received from the required protection endpoint or Protector.
Key Encryption Keys (KEK)	The keys that protect other keys. In Protegrity Data Security Platform, the MK and RK are KEKs.
Data Encryption Key	The Data Encryption Key is generated when a data element is created. This key protects actual sensitive data.
Protegrity Soft HSM	The Protegrity Soft HSM is internally housed in the ESA. It is a **FIPS 140-2 Level 1** non-certified module. It is used to generate keys and stores the Master key.
Key Store or External HSM	An external **FIPS 140-2 Level 2 compliant** module for storing keys.

Term	*Definition*
NIST 800-57	NIST Special Publication 800-57 defines best practices and recommendations for Key Management.
FIPS 140-2 Level 1 and Level 2	Federal information process standard (FIPS) used to accredit cryptographic modules.
PKCS#11 Interface	Standard API for key management.
Key States	The state of a key during the key life cycle.
Cryptoperiods	The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect.
Originator Usage Period (OUP)	The period of time in the cryptoperiod of a symmetric key during which cryptographic protection may be applied to data
Recipient Usage Period (RUP)	The period of time during the cryptoperiod of a symmetric key during which the protected information is processed.
Endpoint	Endpoint is the protection endpoint. In most cases, it is the Protector.
Policy-Key Repository	**Internal storage in ESA,** which stores the internal MK properties, RK, and DSK**.**