

## Google Cloud External Key Manager and Entrust KeyControl Vault

Integration Guide

© 2025 Entrust Corporation. All rights reserved.

## Table of Contents

| 1. Introduction   | 1 |
|---|---|
| 1.1. Documents to read first  | 1 |
| 1.2. Product configurations   | 1 |
| 1.3. Features tested  | 1 |
| 1.4. Requirements   | 2 |
| 2. Install and configure KeyControl Vault   | 3 |
| 2.1. Deploy a KeyControl Vault cluster.   | 3 |
| 2.2. Create a KeyControl Cloud Key Management Vault                               | 3 |
| 3. Configure Google Cloud Platform  | 5 |
| 3.1. Required GCP permissions.  | 5 |
| 3.2. Create a service account in GCP.   | 5 |
| 3.3. Service Account Permissions  | 6 |
| 3.4. Create a key for the service account   | 7 |
| 3.5. Create a GCP key ring  | 7 |
| 4. Configure KeyControl as GCP KMS.   | 9 |
| 4.1. Create a KeyControl Vault CSP account for the GCP service account            | 9 |
| 4.2. Update the EKM, Key Access Justification Policy, and EKM Access Control List |   |
| sections  | С |
| 4.3. Create a KeySet for GCP 13   | 3 |
| 4.4. Create a CloudKey for GCP  | 4 |
| 4.5. Verify the CloudKey  | 7 |
| 5. Test integration   | 9 |
| 5.1. Check if Cloud Key is Working as expected                                    | 9 |
| 5.2. Create a Cloud Storage Bucket  | 9 |
| 5.3. Test access to an object in the bucket                                       | 1 |
| 5.4. Rotate a cloud key in KeyControl   | 3 |
| 5.5. Delete a cloud key in KeyControl   | 3 |
| 5.6. Cancel deletion of a deleted KeyControl key                                  | 4 |
| 5.7. Sign/Verify an input file with a GCP CloudKey                                | 4 |
| 5.8. Create a Cloudkey with purpose of 'Asymmetric Sign'                          | 5 |
| 5.9. Use gcloud to sign/verify a file using the cloud key                         | 7 |
| 6. Additional resources and related products                                      | 1 |
| 6.1. nShield Connect  | 1 |
| 6.2. nShield as a Service   | 1 |
| 6.3. KeyControl   | 1 |
| 6.4. KeyControl as a Service  | 1 |
| 6.5. Entrust products   | 1 |

| .6. nShield product documentation |
|-----------------------------------|
|-----------------------------------|

## Chapter 1. Introduction

This document describes the integration of Google Cloud Platform (GCP) External Key Manager (EKM), referred to as GCP EKM in this guide, with the Entrust KeyControl Vault Key Management Solution (KMS).

#### 1.1. Documents to read first

This guide describes how to configure KeyControl Vault server as a KMS in GCP. To install and configure the KeyControl Vault server see KeyControl Vault Installation and Upgrade Guide.

Also refer to the documentation and set-up process for GCP EKM in the Google Cloud External Key Manager documentation.

#### 1.2. Product configurations

Entrust has successfully tested the integration of KeyControl Vault with GCP EKM in the following configurations:

| System           | Version       |  |  |
|------------------|---------------|--|--|
| KeyControl Vault | 10.2 / 10.3.0 |  |  |

### 1.3. Features tested

Entrust has successfully tested the following features:

| Feature                   | Tested       |
|---------------------------|--------------|
| Create cloud key          | $\checkmark$ |
| Enable cloud key          | $\checkmark$ |
| Disable cloud key         | $\checkmark$ |
| Rotate cloud key          | $\checkmark$ |
| Delete a cloud key        | $\checkmark$ |
| Cancel cloud key deletion | $\checkmark$ |

| Feature  | Tested       |
|--|--------------|
| Access an object protected by cloud key in GCP | $\checkmark$ |
| Sign/Verify an input file with GCP cloud key   | $\checkmark$ |

#### 1.4. Requirements

Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

# Chapter 2. Install and configure KeyControl Vault

#### 2.1. Deploy a KeyControl Vault cluster

For this integration, KeyControl Vault was deployed as a two-node cluster.

Follow the installation and set-up instructions in KeyControl Vault Installation and Upgrade Guide.

### 2.2. Create a KeyControl Cloud Key Management Vault

- 1. Sign in to the KeyControl Vault Manager.
- 2. In the home page, select Create Vault.

| ENTRUST KeyControl<br>Vault Management                        | secroot v Switch to:<br>Applicance Management ? |
|---|---|
| Vaults<br>Each vault has unique authentication and management | Settings  |
| +   |   |
| Let's get started!  |   |
| + Create Vault  |   |

3. Select Create Vault.

The Create Vault dialog appears.

- In the Type drop-down box, select Cloud Key Management. Enter the required information.
- 5. Select Create Vault.

For example:

| Vaults<br>Each vault has unique authentication and management  |
|--|
| Create Vault<br>A vault will have unique authentication and management.  |
| Type<br>Choose the type of vault to create   |
| Cloud Key Management v   |
| Name *   |
| 6CP 0301   |
| Description  |
| Vault to test integration of Google Cloud Platform EKM Integration.  |
| Max. 300 characters  |
| Administration<br>Invite an individual to have complete access and control over this vault. They will be responsible for inviting additional members.<br>Admin Name*   |
| Administrator  |
| Admin Email *  |
| access constitution and a consti |
| Create Vault Cancel  |

6. When you receive an email with a URL and sign-in credentials to the KeyControl vault, bookmark the URL and save the credentials.

You can also copy the sign-in credentials when the vault details gets displayed and use that to sign in using the vault URL.

7. Sign in to the URL provided.

Change the initial password when prompted.

## Chapter 3. Configure Google Cloud Platform

#### 3.1. Required GCP permissions

The GCP account performing this integration had the following permissions. These were granted by the project admin. Not all these permissions are required to perform this integration.

- Cloud Build Editor
- Cloud KMS Admin
- Compute Admin
- Deployment Manager Editor
- Private Logs Viewer
- Service Account Admin
- Service Account Key Admin
- Service Account User
- Service Management Administrator
- Service Usage Admin
- Storage Admin
- Viewer

| ≡   | Google Cloud              | :• | HyTrust DataControl 👻 | Search (/) for resources, docs, pr | oducts, and mo | ore                   | Q Search |
|-----|---------------------------|----|-----------------------|------------------------------------|----------------|-----------------------|----------|
| 0   | IAM & Admin               | Ŧ  | IAM                   |                                    |                |                       |          |
| ••  | IAM                       |    | PERMISSIONS RE        | COMMENDATIONS HISTORY              |                |                       |          |
| 0   | PAM NEW                   |    |                       |                                    |                | Viewer                |          |
| ଜ   | Principal Access Boundar  |    | □ ≛                   |                                    |                | Cloud KMS Admin       |          |
| θ   | Identity & Organization   |    |                       |                                    |                | Editor                |          |
| ٩   | Policy Troubleshooter     |    |                       |                                    |                | Private Logs Viewer   |          |
| Ę   | Policy Analyzer NEW       |    |                       |                                    |                | Service Account Adn   | nin      |
|     | Organization Policies     |    |                       |                                    |                | Service Account Key   | Admin    |
| 图   | Service Accounts          |    |                       |                                    |                | Service Directory Vie | wer      |
| II. | Workload Identity Federat |    |                       |                                    |                | Storage Admin         |          |
| ≣   | Workforce Identity Federa |    |                       |                                    |                | Viewer                |          |

#### 3.2. Create a service account in GCP

A service account needs to be created in a GCP IAM. This service account will be used by

KeyControl Vault to access the GCP key rings. Once created, this service account needs permissions that have to be granted by the project admin.

- 1. Open a browser and sign in to the GCP portal https://console.cloud.google.com.
- 2. Select IAM & Admin on Google Cloud Menu.
- 3. Select Service Accounts in the left-hand pane.
- 4. Select CREATE SERVICE ACCOUNT.
- 5. Enter the Service account details.

For example:

| 0  | IAM & Admin 📮             | ← Create service account  |
|----|---------------------------|---|
| +• | IAM                       | Service account details   |
| 0  | PAM NEW                   | Service account name  |
| G  | Principal Access Boundar  | Display name for this service account                                     |
| Θ  | Identity & Organization   | Service account ID *  |
| 3  | Policy Troubleshooter     | Email address: acp-ekm-entrust-kc@htdc-project.jam.aserviceaccount.com    |
| ٦  | Policy Analyzer NEW       | Service account description   |
|    | Organization Policies     | Describe what this service account will do                                |
| 연  | Service Accounts          |   |
| æ  | Workload Identity Federat | CREATE AND CONTINUE   |
| ≡  | Workforce Identity Federa | Grant this service account access to project                              |
| ۰  | Labels                    | (optional)  |
|    | Tags                      | <ul> <li>Grant users access to this service account (optional)</li> </ul> |
| ø  | Manage Resources          | DONE CANCEL   |
|    |                           |   |

- ° Select CREATE AND CONTINUE
- ° In the Grant this service account access to project section, select Continue.
- In the Grant users access to this service account section, select DONE.

#### 3.3. Service Account Permissions

- 1. Open a browser and sign in to the GCP portal https://console.cloud.google.com.
- 2. Select IAM & Admin on Google Cloud Menu.
- 3. Select Service Accounts in the left-hand pane.
- 4. Select the service account that you have just created.
- 5. In the **DETAILS** tab.
  - a. Take note of the **Account Name**.

- b. Take note of the **Unique ID**.
- 6. The following roles were given to this service account by the system admin after it was created:
  - ° Browser
  - ° Cloud KMS Admin
  - ° Service Account Key Admin

#### 3.4. Create a key for the service account

A key needs to be created for the service account created in Create a service account in GCP. This key will be used by KeyControl Vault to access the GCP service account.

- 1. Open a browser and sign in to the GCP portal: https://console.cloud.google.com.
- 2. Select IAM & Admin on Google Cloud Menu.
- 3. Select Service Accounts in the left-hand pane.
- 4. Select the service account created in Create a service account in GCP from the list.
- 5. Select the **KEYS** tab.

For example:

- 6. Select ADD KEY and then select Create new key.
- 7. Select **JSON** from the available **Key type** options.
- 8. Select **CREATE**. A pop-up message appears indicating that the key created was downloaded to your computer.
- 9. Verify by checking your **Downloads** folder that a **.json** file was created in the Downloads folder.
- 10. Take note of the new key in the GCP console.

| ADD KEY | ( •    |                                       |               |                 |   |
|---------|--------|---------------------------------------|---------------|-----------------|---|
| Туре    | Status | Кеу                                   | Creation date | Expiration date |   |
| 0       | Active | 41417-1474618-414-04-0417125-014-47-5 | Jun 13, 2024  | Dec 31, 9999    | Î |

#### 3.5. Create a GCP key ring

This key ring will be used to store keys managed by KeyControl Vault. A new GCP key ring was created for this integration to show the entire process. You can use an existing key ring instead.

If you are using an existing GCP key ring, proceed to section Create a KeyControl Vault CSP account for the GCP service account directly, skipping this section entirely.

- 1. Open a browser and sign in to the GCP portal: https://console.cloud.google.com.
- 2. In the navigation menu select **Security** > **Key Management**.
- 3. Select + CREATE KEY RING.
- 4. Enter the Key ring name and select the Location type.

For example:

| - Create key ring   |  |
|---|--|
| (ey rings group keys together to keep them organized. In the next step, you'll create keys<br>hat are in this key ring. Learn more <ि |  |
| Project name  |  |
| tdc-project   |  |
| Key ring name *   |  |
| Location type 👔   |  |
| Cover latency within a single region  |  |
| Multi-region     Highest availability across largest area   |  |
| Multi-region *us (multiple regions in United States) v  |  |
| CREATE CANCEL   |  |

- 5. Select **CREATE** to create the key ring
- 6. Select **CANCEL** in the **Create key** pane.

## Chapter 4. Configure KeyControl as GCP KMS

## 4.1. Create a KeyControl Vault CSP account for the GCP service account

The following steps establish the connection between KeyControl Vault and GCP, making KeyControl Vault the CSP of the GCP service account. You must have created a service account in GCP and downloaded the JSON file before you can add a CSP account. For more information see GCP Service Account Requirements.

- 1. Log into the KeyControl Cloud Key Management Vault webGUI using an account with Cloud Admin privileges.
- 2. Select the **CLOUDKEYS** icon on the toolbar.
- 3. Select the CSP Accounts tab.
- 4. Select the **Action** icon and then **Add CSP Account** from the drop-down menu that appears.

The Add CSP Account dialog appears.

- 5. In the **Details** tab:
  - a. Enter the **Name** and **Description**.
  - b. From the Admin Group drop-down menu box, select Cloud Admin Group.
  - c. From the Type drop-down menu box, select GCP.
  - d. In the **Service Account Key File (.json)** field, select the file download to your computer in Create a key for the service account.

For example:

|                    | KeyControl<br>Vault for Cloud Key Management                | CLOUDKEYS SECURITY      | AUDIT LOG ALERTS | SETTINGS | GCP-EKM 🛛 🔮 Administrator 🔻 |
|--------------------|---|-------------------------|------------------|----------|-----------------------------|
| Actions - Key Sets | CloudKeys CSP Accounts                                      |                         |                  |          | Refresh 🕄                   |
| CSP Account Name   | Desc     Details Schedule     Name •                        | Add CSP Acco            | ount             | ×        | × Type × ≡                  |
|                    | GCP - CSP - Account<br>Description<br>GCP CSP Account to be | used in the GCP - EKM - | KCV Integration. |          |                             |
|                    | Admin Group •<br>Cloud Admin Group                          |                         |                  | ~        |                             |
|                    | GCP<br>There<br>Service Account Key File(<br>Cancel         | json) 😧 •<br>Clear Pre  | eview            | Continue | ions.                       |

- 6. Select Continue.
- 7. In the **Schedule** tab, select **Never**.
- 8. Select Add.

When the service account keys are rotated, the KeyControl Cloud Key Management Vault creates a new key and replaces the key that was used when you registered the CSP account. Do not delete the service account key.

## 4.2. Update the EKM, Key Access Justification Policy, and EKM Access Control List sections

Before you can use KeyControl Vault as a GCP EKM provider, you must set up the following parameters in the **CSP Account details** page.

- External Key Manager (EKM URI)
- Key Access Justification Policy (optional)
- EKM Access Control List (optional)
- 1. View the **Details** tab on the CSP account that you created.

| ENTRUST Visit for Cloud Key Management                       |  |                                     |         | OCP-EXX 🗎 🛦 Administrator = |
|--|--|-------------------------------------|---------|-----------------------------|
| Actions - Key Sets Cloudikeys CSP Accounts                   |  |                                     |         | Refresh Ø                   |
| CSP Account Name   | <ul> <li>Description</li> </ul>  | Admin Group ~                       | Key Set | Type 🗸 🗉                    |
|  |  |                                     |         |                             |
| GCP - CSP Account  | GCP Account for the intervation  | Cloud Admin Group                   |         | GCP                         |
|  |  |                                     |         |                             |
|  |  |                                     |         |                             |
|  |  |                                     |         |                             |
|  |  |                                     |         |                             |
|  |  |                                     |         |                             |
|  |  |                                     |         |                             |
|  |  |                                     |         |                             |
|  |  |                                     |         |                             |
|  |  |                                     |         |                             |
| Details External Key Manager Key Access Justification Policy |  |                                     |         |                             |
| Name:  | GCP - CSP Account  |                                     |         |                             |
| Description  | GCP Account for the inte   | agration.                           |         |                             |
| Type:  | GCP  |                                     |         |                             |
| Key Set:   | Not Available  |                                     |         |                             |
| Project ID:  | http:-project  |                                     |         |                             |
| Status:  | Network Ok, Credential   | OR .                                |         |                             |
|  | Test Connection  |                                     |         |                             |
|  | Last Checked: Jun 14, 2  | 024 11:52:23 AM                     |         |                             |
| Service Account ID:  | 11359064272090786026   | 33                                  |         |                             |
| Service Account Name:  | particiti concerna   |                                     |         |                             |
| Service Account Email ID:                                    | particle effective gen   | to project and part transmission on |         |                             |
| Rotation Schedule:   | No Scheduled Rotation  |                                     |         |                             |
|  | Flotate Now  |                                     |         |                             |
| Last Rotated   | Jun 14, 2024 11:52:12 A  | м                                   |         |                             |
| Service Account Key ID O                                     | Charlenge and a second and as second and a | Autor Contests                      |         |                             |
|  | Update Key   |                                     |         |                             |

2. Select the **External Key Manager** tab and enter the URI for the KeyControl Vault server.

Keep in mind that the EKM URI is the URI used by GCP to access the keys from KeyControl Vault. If a single KeyControl Vault is deployed, then it directly points to that vault. However if you deploy a KeyControl Vault cluster with multiple nodes, then we recommend deploying a load balancer in front of the KeyControl Vault cluster. In this case the EKM URI points to the load balancer.

| Details                             | External Key Manager  | Key Access Justification Policy   | EKM ACLs   |                               |
|-------------------------------------|---|---|--|-------------------------------|
| EKM URI<br>directly po<br>a load ba | is the URI used by GCP to<br>pints to the KeyControl. How<br>lancer in front of the KC clus | access the keys from KeyControl. If<br>vever if multi node KeyControl cluste<br>ster. In this case the EKM URI points | a single KeyControl is deplo<br>or is deployed then it is advis<br>s to the load balancer. | yed then it<br>able to deploy |
| For EKM                             | via Internet use https://exar   | nple.server.com   |  |                               |
| For EKM                             | via VPC use https:// <hostna< th=""><td>ame&gt;</td><td></td><td></td></hostna<>            | ame>  |  |                               |
| https://                            | hay y for front com   |   |  |                               |
| Save                                |   |   |  |                               |

- 3. Select Save.
- 4. Select the Key Access Justification Tab. We highly recommend that you create a Key Access Justification policy at the CSP and KeySet level that specifies access justification reasons. These apply to all the keys created in this keyset, unless the policy is specified at the key level, which overrides this policy.

|                       | alls External Key Manager                | Key Access Justification Policy         | EKM ACLs            |  |  |  |
|-----------------------|--|---|---------------------|--|--|--|
| Key A                 | Access Justification Policy              |   |                     |  |  |  |
| Status                | s:                                       |   |                     |  |  |  |
| Set th                | e permissions for this policy. This      | will be the default for all the CloudKe | eys in this CSP Acc |  |  |  |
| <b>~</b>              | Customer initiated access 🚱              |   |                     |  |  |  |
| ✓                     | Modified Customer initiated acce         | ess 🕜                                   |                     |  |  |  |
| ✓                     | Google initiated system operation        | n 😧                                     |                     |  |  |  |
| <ul><li>✓</li></ul>   | Modified Google initiated system         | operation 😧                             |                     |  |  |  |
| <                     | No justification reason expected         | 0                                       |                     |  |  |  |
| ✓                     | Customer initiated support 2             |   |                     |  |  |  |
| <ul> <li>✓</li> </ul> | Google initiated service 2               |   |                     |  |  |  |
| ✓                     | Third party data request 🚱               |   |                     |  |  |  |
| ✓                     | Google initiated review 📀                |   |                     |  |  |  |
| ✓                     | Google response to production a          | lert 🕑                                  |                     |  |  |  |
| ✓                     | No justification reason specified        | 0                                       |                     |  |  |  |
| ✓                     | Customer Authorized Workflow Servicing @ |   |                     |  |  |  |
|                       | Allow missing access justification       | 0                                       |                     |  |  |  |

- 5. Select **Save**.
- 6. (Optional)

Select the EKM ACLs tab to configure the EKM access control list.

This policy also applies to all the keys which are created in the associated KeySet (to this CSP account) unless a policy at Key level overrides it. For GCP Control plane access so-called *coordinated keys*, only the CSP level permissions apply. The EKM ACL specifies the list of GCP identities and permissions they have. The identities can be specified with their service account email, that is:

#### xxxx@htdc-project.iam.gserviceaccount.com

The supported permissions are:

- ° wгар
- ° unwrap
- asymmetricSign
- o getPublicKey

- ° checkCryptoSpacePermissions
- createKey
- destroyKey

#### 4.3. Create a KeySet for GCP

- 1. Log into the KeyControl Cloud Key Management Vault webGUI using an account with Cloud Admin privileges.
- 2. In the top menu bar, select CloudKeys.
- 3. Select the Key Sets tab.
- 4. Select Actions > Create Key Set.
- 5. Select the type of key to be contained in the Key Set: GCP Key
- 6. On the **Details** tab of the **Create Key Set** dialog box, enter the following:
  - a. **Name\*** Enter the name for the Key Set.
  - b. Description Enter the optional description for the Key Set.
  - c. Admin Group Select the Admin Group: Cloud Admin Group
- 7. Select Continue.

| Create Key Set |             |     |          |  |          |  |
|----------------|-------------|-----|----------|--|----------|--|
| Details        | CSP Account | HSM | Schedule |  |          |  |
| Name *         |             |     |          |  |          |  |
| GCP Key        | Set         |     |          |  |          |  |
| Description    |             |     |          |  |          |  |
|                |             |     |          |  |          |  |
| Admin Grou     | ıb <b>*</b> |     |          |  |          |  |
| Cloud Adr      | min Group   |     |          |  | ~        |  |
| Cancel         |             |     |          |  | Continue |  |

8. On the **CSP Account** tab, select an existing CSP Account or add a new account to use with this Key Set. Select the account you created earlier.

| Create Key Set            |                             |              |                              | ×        |
|---------------------------|-----------------------------|--------------|------------------------------|----------|
| Details                   | CSP Account                 | HSM          | Schedule                     |          |
| CSP Accour<br>Choose an e | nt *<br>existing CSP Accoun | t or add a r | new one to use with this Key | Set.     |
| GCP - CS                  | SP Account                  |              |                              | ~        |
| Cancel                    |                             |              |                              | Continue |

#### 9. Select Continue.

10. On the **HSM** tab, check the **Enable HSM** checkbox if you plan to use an HSM to create CloudKeys that can be uploaded to the cloud.

When the key material is in the KMS, the HSM is no longer required. However, if you remove the CloudKey from the cloud, you will need to use the HSM to upload the key again.

If you selected Enable HSM, select **Verify HSM** connection to test the connectivity and suitability of the configured HSM. KeyControl Vault checks if the HSM is accessible and if it supports the creation and export of relevant keys.

Some HSM servers with old version of firmware do not support key creation and wrapping. If the connection test fails, check the firmware version of the HSM server. If it is old, update it to the latest version.

- 11. Select Continue.
- 12. On the **Schedule** tab, determine the default rotation schedule for the CloudKeys created in this Key Set.

This rotation schedule is applied to all CloudKeys created in the Key Set, unless a different value is explicitly selected. If there are existing CloudKeys in the Key Set, you can update the rotation schedule of the CloudKeys to align with your selected rotation schedule by checking Apply to all CloudKeys.

13. Select Apply.

#### 4.4. Create a CloudKey for GCP

Before you can create a CloudKey, you must Create a KeySet for GCP. This procedure is for creating an External Key Manager (EKM) key.

- 1. Log into the KeyControl Cloud Key Management Vault webGUI using an account with Cloud Admin privileges.
- 2. In the top menu bar, select CloudKeys.
- 3. Select the CloudKeys tab and select the Key Set and the Key Ring.

If you do not finish the selections on the **CloudKeys** page, you will need to add them on the Details tab of the Create CloudKey dialog box.

~

- 4. Select Actions > Create CloudKey.
- 5. On the Details tab of the Create CloudKey dialog box, enter the following:
  - a. **Name**: Enter the name for the CloudKey.
  - b. Description: Enter the optional description for the CloudKey
  - c. Key Management: Select External Key Management (EKM).

|         |                   |                    | Crea            | ate CloudKe      | У                     |            |   |
|---------|-------------------|--------------------|-----------------|------------------|-----------------------|------------|---|
|         | Details           | Purpose            | Schedule        |                  |                       |            |   |
|         | Туре              | GCP                |                 |                  |                       |            |   |
|         | Key Set           | GCP Key            | Set             |                  |                       |            |   |
|         | Key Ring          | generation of      | antrust for he  | , ing (an)       |                       |            |   |
|         | Name *            |                    |                 |                  |                       |            |   |
|         | GCP-EKN           | I-CLOUDKEY         |                 |                  |                       |            |   |
|         | Description       |                    |                 |                  |                       |            |   |
|         | Optional          |                    |                 |                  |                       |            | , |
|         | Key Manage        | ement              |                 |                  |                       |            |   |
|         | O Customer        | r Managed Ke       | у               |                  |                       |            |   |
|         | A standard cu     | ustomer manag      | ed encryption k | ey. The key mate | erial will be uploade | d to gcp   |   |
|         | External I        | Key Manager        | (EKM)           |                  |                       |            |   |
|         | The key mate      | erial will remain  | in this KeyCon  | trol             |                       |            |   |
|         | Cancel            |                    |                 |                  |                       | Continue   | e |
| Seleo   | et <b>Continu</b> | e.                 |                 |                  |                       |            |   |
| . On th | ne <b>Purpose</b> | a tab, comp        | lete the foll   | owing:           |                       |            |   |
| a.      | Connectio         | <b>n Type</b> : Se | lect how the    | e external ke    | y manager will        | be reached | • |

- b. **Purpose**: This can be one of the following:
  - i. Symmetric encrypt/decrypt

- ii. Asymmetric Sign
- c. **Algorithm**: Select the algorithm that matches the purpose you selected. This can be one of the following:
  - i. For Symmetric encrypt/decrypt: External symmetric key
  - ii. For Asymmetric Sign:
    - A. Elliptic Curve P-256 SHA256 Digest
    - B. Elliptic Curve P-384 SHA384 Digest
    - C. 2048 bit RSA PKCS#1 v1.5 padding SHA256 Digest
    - D. 3072 bit RSA PKCS#1 v1.5 padding SHA256 Digest
    - E. 4096 bit RSA PKCS#1 v1.5 padding SHA256 Digest
    - F. 4096 bit RSA PKCS#1 v1.5 padding SHA512 Digest
    - G. 2048 bit RSA PSS Padding SHA256 Digest
    - H. 3072 bit RSA PSS Padding SHA256 Digest
    - I. 4096 bit RSA PSS Padding SHA256 Digest
    - J. 4096 bit RSA PSS Padding SHA512 Digest

| Create | CloudKey |
|--------|----------|
|        |          |

| Details                                  | Purpose                              | Schedule                                    |          |
|--|--------------------------------------|---|----------|
| Connection<br>O External<br>Reach your e | Type *<br>via VPC<br>external key ma | nager via a Virtual Private Cloud(VPC) netw | ork      |
| External<br>Reach your e                 | via Internet<br>external key ma      | nager via the internet                      |          |
| Choosing a                               | purpose will d                       | etermine the key type and algorithm sele    | ction    |
| Purpose *                                |                                      |   |          |
| Symmetrie                                | c encrypt/decr                       | ypt   | ~        |
| Algorithm *                              |                                      |   |          |
| External s                               | ymmetric key                         |   | ~        |
| Cancel                                   |                                      |   | Continue |
|  |                                      |   |          |

#### 8. Select Continue.

- 9. On the Schedule tab, determine the rotation schedule for the CloudKey. This can be one of the following:
  - a. Inherit from Key Set—The CloudKey will use the default schedule from the Key Set. If the Key Set schedule changes after the CloudKey is created, the CloudKey schedule will not be updated.

- b. Never The CloudKey will never be rotated.
- c. Once a year The CloudKey will be rotated once a year.
- d. Every 6 months The CloudKey will be rotated once every 6 months.
- e. Every 30 days The CloudKey will be rotated once every 30 days.
- f. Other The CloudKey will be rotated at the interval you select.
- 10. Select when the CloudKey should expire. This can be **Never**, or you can select a specific date.

|                             | ate CloudKey ×              |                |                  |
|-----------------------------|-----------------------------|----------------|------------------|
| Details                     | Purpose                     | Schedule       |                  |
| Rotation Sc<br>Define a sch | hedule *<br>edule for which | the CloudKey   | will be rotated. |
| Inherit fro                 | m keyset (Nev               | /er)           | ~                |
| Expiration *<br>Define when | the CloudKey                | should be expi | red.             |
| <ul> <li>Never</li> </ul>   | ⊖ Choose a                  | date           |                  |
| Cancel                      |                             |                | Apply            |

If you selected an expiration date, select the Expire Action to define what happens to the CloudKey when it expires.

When the CloudKey expires, the selected Expire Action is performed on the key. The KeyControl Vault handles the expiration date and expire action. The expire date is not set in the cloud service provider.

11. Select Apply.

If you get errors about not being able to validate the TLS server certificate for the key, you will need to install the SSL certificate in the KeyControl Vault node.

#### 4.5. Verify the CloudKey

You need to make sure the CloudKey status is **AVAILABLE** so it can be used in GCP.

1. Verify the Key is Available, by selecting the CloudKey and checking its status in the details tab.

| Details      | Permissions  | Labels | Versions | Key Access | Justification Policy        | EKM ACLs           | C Sync Now       |
|--------------|--------------|--------|----------|------------|-----------------------------|--------------------|------------------|
| Name:        |              |        |          |            | GCP-EKM-CLOUDK              | EY                 |                  |
| Key Id:      |              |        |          |            | property field and property | to cations to deep | ma <sup>14</sup> |
| Description  |              |        |          |            | test                        |                    |                  |
| Key Status   | 0:           |        |          |            | AVAILABLE                   |                    |                  |
| Key Source   |              |        |          |            | KEYCONTROL                  |                    |                  |
| Key Mode:    |              |        |          |            | GCP EKM                     |                    |                  |
| EKM Mana     | gement Mode: |        |          |            | Manual                      |                    |                  |
| Algorithm:   |              |        |          |            | External symmetric k        | ey                 |                  |
| Кеу Туре:    |              |        |          |            | Symmetric                   |                    |                  |
| Purpose:     |              |        |          |            | Symmetric encrypt/de        | ecrypt             |                  |
| Key Set:     |              |        |          |            | GCP-EKM-KEYSET              |                    |                  |
| Key Ring:    |              |        |          |            | pay over an the local       | 10.010             |                  |
| Rotation Sc  | hedule:      |        |          |            | Never<br>Rotate Now         |                    |                  |
| Last Rotatio | on Date:     |        |          |            | 06/17/2024                  |                    |                  |
| Expires:     |              |        |          |            | ● Never ○ Choo              | se a date          |                  |

- 2. Verify the Key status in the GCP Platform.
  - a. Open a browser and sign in to the GCP portal: https://console.cloud.google.com.
  - b. In the navigation menu select **Security** > **Key Management**.
  - c. Look for the key ring that was used in the CloudKey creation process in KCV and select on it to view its details. You should see the CloudKey you created. Its protection level should state **External Via Internet**.

| Keys                                       | for ",, i i i i i   | g" key ring  |                              |                           |                 |         |
|--|---|--|------------------------------|---------------------------|-----------------|---------|
| A cryptog<br>producin<br>the Cloud<br>T Fi | graphic key is a resource that<br>g and verifying digital signa<br>I KMS API. Learn more [2]<br>Iter Enter property name of | at is used for encrypting and decrypting<br>tures. To perform operations on data wit | data or for<br>th a key, use |                           |                 |         |
|  | Name 个  | Status 🕜   | Protection level             | Purpose 🚱                 | Next rotation 😮 | Actions |
|  | GCP-EKM-CLOUDKEY  | 🛇 Available in Google Cloud  | External via internet        | Symmetric encrypt/decrypt | Not applicable  | :       |

## Chapter 5. Test integration

### 5.1. Check if Cloud Key is Working as expected

To check if the Cloud Key created earlier is functioning as designed we will do the following:

- Create a Cloud Storage Bucket
- Test if items in the cloud storage bucket are protected by the Cloud Key

### 5.2. Create a Cloud Storage Bucket

This bucket will be used to test the Cloud Key when attempting to view an object stored in the bucket. All objects will be encrypted by the cloud key, and only visible when the cloud key is active. If the cloud key has been disabled, the object in the bucket will not be accessible.

- 1. Copy the Cloud Key name created earlier.
- 2. Open a browser and sign in to the GCP portal: https://console.cloud.google.com.
- 3. In the navigation menu select Cloud Storage > Buckets.
- 4. Select Create.
- 5. Enter the **Name** of the bucket.
- 6. Select Continue.
- 7. On the Choose Where to Store Your Data, for Location Type, select Region.
- 8. Select us-east1
- 9. Select Continue.
- 10. On the **Choose a storage class for your data**, select **Set as a default class** and select **Standard**.
- 11. Select Continue.
- 12. On the **Choose how to control your objects**, deselect **Enforce public access prevention on this bucket**.
- 13. Select Continue.
- 14. On the **Choose how to protect your data**, Expand the **Data Encryption** section and select **Cloud KMS Key**.
  - a. For Key Type, select Cloud KMS.
  - b. For Select a customer-managed key, enter the cloud key name you created.

#### 15. Select Create.

#### Possible issues while creating the bucket

If the service agent account for the Cloud Storage service does not have the appropriate roles, the creation of the bucket may fail with the following error:



Talk to your GCP administrator and ask for the role to be added to the service account.

The service account above is a default "Service Agent" of the Cloud Storage service and this Agent doesn't have access to role cloudkms.cryptoKeyEncrypterDecrypter. If you select **Settings** under **Cloud Storage**, you will be able to see the service account being used.



Once the role has been granted, you can see it.

- 1. In the navigation menu select IAM & Admin.
- 2. Make sure Include Google-provided role grants is selected.
- 3. Select the View by Roles tab.
- 4. Look for the **Cloud KMS CryptoKey Encrypter/Decrypter (x)** Role and you should be able to see the account listed under that role.

|   | <ul> <li>Cloud KMS CryptoKey Encrypter/Decrypter (3)</li> </ul> |   |   |
|---|---|---|---|
|   | 에 :   | APBYOK  | 1 |
|   | ₫<br>   | Google Storage Service Agent 🕜                        | 1 |
|   | 역 · · · · · · · · · · · · · · · · · · ·                         | Compute Engine Service Agent for Project 788120191304 | 1 |
| _ |   |   |   |

5. Now go back and attempt to create the bucket again.

You may see the message again, but this time GCP will create the bucket which will allow you to do the testing.

#### 5.3. Test access to an object in the bucket

- 1. Upload a file to the bucket. We suggest you upload an image.
- 2. Once the file has been uploaded, select on it to see its details. For example:

|          | Cloud Storage 📮  | ← Object details                        |                          |  |  |
|----------|------------------|---|--------------------------|--|--|
| •        | Buckets          | Buckets > gcp-ekm-bucket > hurricane.pr | 19 <b>6</b>              |  |  |
| <b>~</b> | Monitoring       |   |                          |  |  |
|          |                  | LIVE OBJECT VERSION HISTORY             |                          |  |  |
|          | Settings         |   |                          |  |  |
|          |                  | 🛨 DOWNLOAD 🛛 🖍 EDIT METADATA            | LE EDIT ACCESS 📋 DELETE  |  |  |
|          |                  | Overview                                |                          |  |  |
|          |                  | Туре                                    | image/png                |  |  |
|          |                  | Size                                    | 50.9 KB                  |  |  |
|          |                  | Created                                 | Jun 20, 2024, 1:59:54 PM |  |  |
|          |                  | Last modified                           | Jun 20, 2024, 1:59:54 PM |  |  |
|          |                  | Storage class                           | Standard                 |  |  |
|          |                  | Custom time                             | -                        |  |  |
|          |                  | Public URL 😧                            | Not applicable           |  |  |
|          |                  | Authenticated URL                       | /hurricane.png           |  |  |
|          |                  | gsutil URI 🕜                            | /hurricane.png           |  |  |
|          |                  | Permissions                             |                          |  |  |
|          |                  | Public access                           | Not public               |  |  |
|          |                  | Protection                              |                          |  |  |
|          |                  | Version history 🕜                       | -                        |  |  |
| •        | Manage Resources | Retention expiration time ?             | None                     |  |  |
|          |                  | Object retention retain until time      | None                     |  |  |
| )<br>Č   | Marketplace      | Bucket retention retain until time      | None                     |  |  |
|          |                  | Hold status                             | None 🧪                   |  |  |
| Ē        | Release Notes    | Encryption type                         | Customer-managed         |  |  |
| <1       |                  | Encryption key                          | ، ټ ټ ک                  |  |  |

3. Copy the **Authenticated URL** in the **Object Details** view and use it in another tab in the browser. You should be able to see the contents of the file. In this case an image:

🗧 🔶 C 😫 ff208d4d50c8fed818a101aad7aa555957b4d100a18d69f12c461d5-apidata.googleusercontent.com/download/storage/v1/b/gcp-ekm-bucket/o/hurricane.png?jk=A51gM...



- 4. Now go back to the KeyControl Vault and disable the cloudkey.
- 5. Log into the KeyControl Cloud Key Management Vault webGUI using an account with Cloud Admin privileges.
- 6. In the top menu bar, select CloudKeys.
- 7. Select the CloudKeys tab and select the Key Set.
- Select the CloudKey used in the Bucket in GCP. In the Actions menu, select Disable CloudKey.

| ENTRUST KeyControl<br>Vault for Cloud Keys |  | UBITY AUDITLOG ALERTS SETTINGS  | GCP-EKIA-INTEGRAT 🛛 🛔 Administrator 🔹 |
|--|--|---------------------------------|---------------------------------------|
|  | This vault is not connected to KeyContro | Compliance Manager. Connect Now |                                       |
| Actions - Key Sets CloudKeys CSP Accounts  |  |                                 | Refresh 🕽                             |
| Create CloudKey EYSET (GCP) V Key Ring: *  | All 🗸                                    |                                 |                                       |
| Delete CloudKey v [                        | Description ~                            | Expires ~                       | Cloud Status 0                        |
|  |  |                                 |                                       |
| GCP-EKM-CLOUDKEY 1                         | test                                     | Never                           | AVAJLABLE                             |
| GCP-EKM-CLOUDKEY-2                         |  | Never                           | AVAILABLE                             |

9. Now if you try to access the image file uploaded in the bucket earlier, you should see the following message:



The Cloud Storage service agent does not have permission to access the KMS key in Cloud EKM. Grant the appropriate permissions in your external key manager.

- 10. Go back to the KeyControl Vault and enable the cloudkey.
- 11. Select the CloudKey used in the Bucket in GCP. In the **Actions** menu, select **Enable CloudKey**.
- 12. The image file now is visible again.

#### 5.4. Rotate a cloud key in KeyControl

To rotate a cloud key in KeyControl:

- 1. Sign in to the KeyControl Vault URL bookmark from Create a KeyControl Cloud Key Management Vault.
- 2. Select the **CLOUDKEYS** icon on the toolbar.
- 3. Select the **CloudKeys** tab.
- 4. From the Key Set menu, select the Key Set created in Create a KeySet for GCP.
- 5. From the Key Ring menu, select the key ring created in Create a GCP key ring.
- 6. Select the key to rotate.
- 7. Select Rotate Now in the Details tab of the key.
- 8. Once rotated, select the **Versions** tab of the key, to see that a new version of the key has been created.
- 9. In GCP, navigate to Security > Key Management.
- 10. In the KEY RINGS tab, select the key ring created in Create a GCP key ring.
- 11. Select the key you just rotated in KeyControl.
- 12. Verify that the key has been rotated in GCP in synchronization with KeyControl.

#### 5.5. Delete a cloud key in KeyControl

A deleted cloud key in KeyControl will no longer be available for use in GCP. However, KeyControl will keep a copy of the deleted cloud key, which can be reloaded back to GCP for use.

- 1. Sign in to the KeyControl Vault URL bookmark from Create a KeyControl Cloud Key Management Vault.
- 2. Select the **CLOUDKEYS** icon on the toolbar.
- 3. Select the CloudKeys tab.
- 4. In the Key Set menu, select the Key Set created in Create a KeySet for GCP.
- 5. In the Key Ring menu, select the key ring created in Create a GCP key ring.
- 6. Select the key to the deleted.
- 7. Select Actions > Delete CloudKey.

The **Delete Cloudkey** dialog appears.

- 8. Enter the number of days when the cloud key should be permanently deleted.
- 9. Select Delete.

- 10. Verify the Key status changed in KeyControl to **PENDING DELETE**.
- 11. Verify the key is now scheduled to be deleted from GCP.

| ⊦or ex                               | ample                                       |  |                              |                        |                  |                           |         |   |
|--------------------------------------|---|--|------------------------------|------------------------|------------------|---------------------------|---------|---|
| ← Key: "                             | 07 0MM 01.01                                | " () F   | ROTATE KEY                   |                        |                  |                           |         |   |
| A key contains v<br>have at least on | ersions which have<br>e key version to oper | key material associated<br>rate on data. <u>Learn more</u> | with the key. A key must     |                        |                  |                           |         |   |
| Status:                              | Location:                                   | Protection level:  | Purpose:                     |                        |                  |                           |         |   |
| 😣 Not available                      | e 🕜 us                                      | External via internet                                      | Symmetric encrypt/decry      | rpt                    |                  |                           |         |   |
| OVERVIEW                             | VERSIONS                                    | USAGE TRACKING   | PERMISSIONS                  |                        |                  |                           |         |   |
| 🔺 To o                               | perate on data with                         | this key, restore primary                                  | version or select a new prin | ary version            |                  |                           |         |   |
| Versions                             | C ENABLE                                    | OISABLE  | 🖞 RESTORE 🏾 📋 DEST           | ROY                    |                  |                           |         |   |
| ₩ Filter E                           | nter property name (                        | or value   |                              |                        |                  |                           |         | 0 |
| □ ↓                                  | Version State                               | 0  |                              | Algorithm 👩            | Created on       | Created from              | Actions |   |
|                                      | 2 Will be                                   | destroyed in Google Clo                                    | ud on 7/21/24, 9:58 AM       | External symmetric key | 6/21/24, 9:51 AM | External key via Internet | :       |   |
|                                      | 1 Enable                                    | d in Google Cloud  |                              | External symmetric key | 6/17/24, 2:28 PM | External key via Internet | :       |   |
| No versions sele                     | ected                                       |  |                              |                        |                  |                           |         |   |

#### 5.6. Cancel deletion of a deleted KeyControl key

Follow these steps to cancel the deletion and enable back to GCP the KeyControl key deleted in Delete a cloud key in KeyControl.

- 1. Sign in to the KeyControl Vault URL bookmark from Create a KeyControl Cloud Key Management Vault.
- 2. Select the **CLOUDKEYS** icon on the toolbar.
- 3. Select the CloudKeys tab.

-

- 4. From the Key Set menu, select the Key Set created in Create a KeySet for GCP.
- 5. From the Key Ring menu, select the key ring created in Create a GCP key ring.
- 6. Select the key pending to be deleted.
- 7. Select Actions > Cancel Deletion.

The Cancel Deletion dialog appears.

- 8. Select Yes, Cancel Deletion.
- 9. Verify the status change in KeyControl to **DISABLED**.
- 10. Now enable the key so it is **Available** in GCP.
- 11. Select Actions > Enable Key.
- 12. Verify the status change in KeyControl to **AVAILABLE**.

#### 5.7. Sign/Verify an input file with a GCP CloudKey

This test case uses gcloud to sign a file with a GCP cloudkey and OpenSSL to verify the signing.

To install gcloud, we use an Ubuntu server to the installation.

1. Install needed packages.

% sudo apt-get install apt-transport-https ca-certificates gnupg

2. Add gcloud cli distribution.

echo "deb [signed-by=/usr/share/keyrings/cloud.google.gpg] https://packages.cloud.google.com/apt cloud-sdk main" | sudo tee -a /etc/apt/sources.list.d/google-cloud-sdk.list

3. Acquire the Public Key.

\$ curl https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo apt-key --keyring
/usr/share/keyrings/cloud.google.gpg add -

#### 4. Install gcloud.

\$ sudo apt-get update && sudo apt-get install google-cloud-cli

#### 5.8. Create a Cloudkey with purpose of 'Asymmetric Sign'

This procedure is for creating an cloudkey that can be used for signing.

- 1. Log into the KeyControl Cloud Key Management Vault webGUI using an account with Cloud Admin privileges.
- 2. In the top menu bar, select CloudKeys.
- 3. Select the CloudKeys tab and select the Key Set and Key Ring.

If you do not finish the selections on the CloudKeys page, you will need to add them on the Details tab of the Create CloudKey dialog box.

- 4. Select Actions > Create CloudKey.
- 5. On the **Details** tab of the **Create CloudKey** dialog box, enter the following:
  - a. **Name**: Enter the name for the CloudKey.
  - b. Description: Enter the optional description for the CloudKey
  - c. Key Management: Select External Key Management (EKM).

#### Create CloudKey

×

| Details       | Purpose               | Schedule  |          |
|---------------|-----------------------|---|----------|
| Туре          | GCP                   |   |          |
| Key Set       | GCP-EKN               | I-KEYSET  |          |
| Key Ring *    |                       |   |          |
| grap where it | a 182 keyding         | (111)   | ~        |
| Name *        |                       |   |          |
| OCF CH        | FOLOURNEY             | 0004  |          |
| Description   |                       |   |          |
| test signin   | ıg                    |   |          |
| Key Manage    | ement                 |   |          |
| ○ Custome     | r Managed Ke          | У   |          |
| A standard c  | ustomer mana <u>o</u> | ged encryption key. The key material will be uploaded | to gcp   |
| External      | Key Manager           | (EKM)   |          |
| The key mate  | erial will remain     | in this KeyControl                                    |          |
| Cancel        |                       |   | Continue |

- 6. Select Continue.
- 7. On the **Purpose** tab, complete the following:
  - a. **Connection Type**: Select how the external key manager will be reached.
  - b. Purpose: Select Asymmetric Sign
  - c. Algorithm: Select the algorithm 2048 bit RSA PKCS#1 v1.5 padding SHA256 Digest

#### Create CloudKey

×

| Details Purpose Schedule  |          |
|---|----------|
| Connection Type *<br>O External via VPC<br>Reach your external key manager via a Virtual Private Cloud(VPC) network   |          |
| <ul> <li>External via Internet</li> <li>Reach your external key manager via the internet</li> <li>Choosing a purpose will determine the key type and algorithm selection</li> </ul> |          |
| Purpose *   |          |
| Asymmetric sign   | ~        |
| Algorithm *   |          |
| 2048 bit RSA - PKCS#1 v1.5 padding - SHA256 Digest  | ~        |
| Cancel  | Continue |

- 8. Select Continue.
- 9. On the **Schedule** tab, determine the rotation schedule for the CloudKey.
- 10. Select when the CloudKey should expire. This can be Never, or you can select a specific date.
- 11. Select Apply.

#### 5.9. Use gcloud to sign/verify a file using the cloud key

1. Initialize the gcloud cli.

\$ gcloud init

You need to do this on the console of the machine that has gcloud installed. This procedure will attempt to open a browser window for you to sign in to GCP so it can authenticate gcloud. Do not ssh and attempt to do this as it will fail to open the browser window if you don't have access to the UI.

2. Set the project

\$ gcloud config set project htdc-project

- 3. Create a Key for the service account used in the guide.
  - a. Open a browser and sign in to the GCP portal: https://console.cloud.google.com.
  - b. Select IAM & Admin on Google Cloud Menu.
  - c. Select Service Accounts in the left-hand pane.
  - d. Select the service account created in Create a service account in GCP from the list.
  - e. Select the **KEYS** tab.
  - f. Select ADD KEY and then select Create new key.
  - g. Select **JSON** from the available **Key type** options.
  - h. Select CREATE.

A pop-up message appears indicating that the key created was downloaded to your computer.

- i. Transfer the json file that was downloaded to the machine you installed gcloud.
- 4. Authorize the Service account

\$ gcloud auth activate-service-account [Account] --key-file=Key\_FILE

Do this in the machine gcloud was installed.

\$ gcloud auth activate-service-account gcp-ekm-entrust-kc@htdc-project.iam.gserviceaccount.com --key
-file=htdc-project-29f147e89a52.json

- 5. Give Permission to the service account to manipulate the key.
  - a. In GCP, navigate to Security > Key Management.
  - b. In the **KEY RINGS** tab, select the key ring created earlier.
  - c. Select the key that will be used for the signing.
  - d. Select Grant Access
  - e. In the Grant Access Pane:
    - i. For the **Principal**, enter the service account.
    - ii. For the Role, select Cloud KMS Crypto Operator
    - iii. Select **Save**.

| Grant access to "  | CLOCKET BON   |                  |
|--|---|------------------|
| Grant principals access to this resou<br>principals can take. Optionally, add c<br>specific criteria is met. <u>Learn more a</u> | rce and add roles to specify what actions<br>conditions to grant access to principals or<br>bout IAM conditions [2] | the<br>Iy when a |
| Resource   |   |                  |
|  |   |                  |
| Add principals   |   |                  |
| Principals are users, groups, domain<br>in IAM [2]   | s, or service accounts. <u>Learn more about</u>   | principals       |
| New principals *   | 8   | Ø                |
| Assign roles   |   |                  |
| Roles are composed of sets of perm<br>this resource. Learn more 🗹  | issions and determine what the principal  | can do with      |
| Role * Cloud KMS CryptoKey Pu  | IAM condition (optional) ? + ADD IAM CONDITION  | Î                |
| Enables GetPublicKey<br>operations   |   |                  |
| + ADD ANOTHER ROLE   |   |                  |
| SAVE   |   |                  |
| CANCEL   |   |                  |
|  |   |                  |

6. Download the public key for the cloudkey created earlier.

Back in the terminal, use **gcloud** to download the public key for the key being used for signing.

% gcloud kms keys versions get-public-key 1 --location \$location --keyring \$keyring --key \$key --output -file \$public\_key

For example:

```
$ gcloud kms keys versions get-public-key 1 --key GCP-EKM-CLOUDKEY-SIGN --location us --keyring gcp-ekm-
kc102-keyring --output-file public.key
```

7. Create a temp file with some text in it.

% vi sign.txt

Enter some text in it, for example: I want to sign this.

8. Sign the file with gcloud cli:

```
$ gcloud kms asymmetric-sign --location $location --keyring $keyring --key $key --version 1 --input-file
inputfile.txt --signature-file $sign_file
```

For example:

```
$ gcloud kms asymmetric-sign --location us --keyring gcp-ekm-kc102-keyring --key GCP-EKM-CLOUDKEY-SIGN
--version 1 --input-file sign.txt --signature-file sign.signed
```

9. Now verify the signed file with download public key using OpenSSL.

\$ openssl dgst -sha256 -verify \$public\_key -signature \$sign\_file inputfile.tx

For example:

```
$ openssl dgst -sha256 -verify public.key -signature sign.signed sign.txr
Verified OK
```

If verification is exited with ok, then operation is complete successfully.

# Chapter 6. Additional resources and related products

- 6.1. nShield Connect
- 6.2. nShield as a Service
- 6.3. KeyControl
- 6.4. KeyControl as a Service
- 6.5. Entrust products
- 6.6. nShield product documentation