GOOGLE CLOUD EKM (EXTERNAL KEY MANAGER)

Integration Guide

Applicable Devices:
KMES Series 3
Applicable Versions:
6.3.1.x

TABLE OF CONTENTS

[1] OVERVIEW OF THE GOOGLE CLOUD EKM / KMES SERIES 3 INTEGRATION

[1.1] ABOUT GOOGLE CLOUD EKM

Within Google Cloud KMS (Key Management Service), there are several different sub offerings, and Google Cloud EKM (External Key Manager) is one of them. With Google Cloud EKM, you can use keys that you manage within a supported external key management partner (i.e., KMES Series 3) to protect data within Google Cloud. You can protect data at rest in Google's BigQuery or Compute Engine persistent storage services, or by calling the Cloud Key Management Service API directly.

[1.2] KEY BENEFITS OF THE INTEGRATION

The Google Cloud EKM / KMES Series 3 integration provides several benefits:

- **Key provenance:** You control the location and distribution of your externally-managed keys. Externally-managed keys are never cached or stored within Google Cloud. Instead, Cloud EKM communicates directly with the KMES Series 3 for each request.
- **Access control:** You manage access to your externally-managed keys. Before you can use an externally-managed key to encrypt or decrypt data in Google Cloud, you must grant the Google Cloud project access to use the key. You can revoke this access at any time.
- **Centralized key management:** You can manage your keys and access policies from a single location and user interface, whether the data they protect resides in the cloud or on your premises.

In all cases, the key resides on the KMES Series 3, and is never sent to Google.
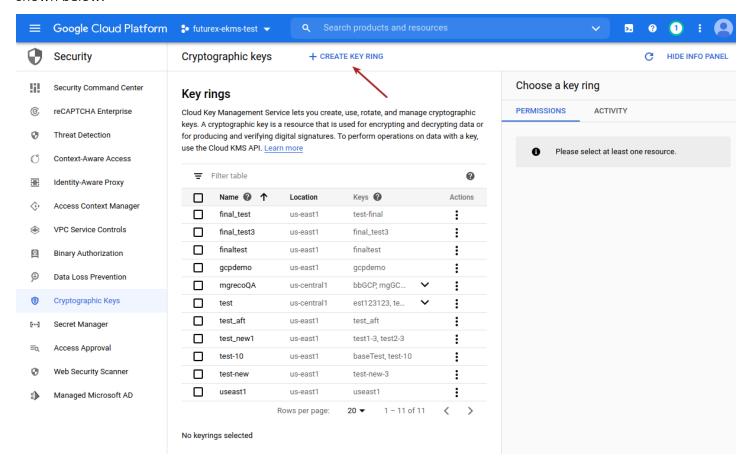
[2] INITIAL SETUP IN THE GOOGLE KMS DASHBOARD

[2.1] NAVIGATE TO THE CLOUD KMS DASHBOARD

From the main GCP dashboard, type "Key Management Service", into the search bar at the top of the page. Then, click on "Cryptographic Keys".

[2.2] CREATE A NEW KEY RING

From the "Cryptographic Keys" dashboard, click on the "Create Key Ring" button at the top of the page, as shown below.

This will pull up the "Create key ring" wizard.

Set the desired name for the key ring (NOTE: Key ring names can contain letters, numbers, underscores (_), and hyphens (-). Key rings can't be renamed or deleted).

Select the key ring location.

Note the following regarding the key ring location:

- Cloud EKM needs to be able to reach your keys quickly to avoid an error. When creating a Cloud EKM key, choose a Google Cloud location that is geographically near the location of the KMES Series 3 key.

- You can use Cloud EKM in any Google Cloud location supported for Cloud KMS, except for **global**.

[2.3] NOTE THE SERVICE ACCOUNT EMAIL FOR THE EXTERNALLY MANAGED KEY

After the Key Ring is created, the browser redirects to the key creation wizard. Select the "Externally managed key" option and scroll down to the bottom of the page.

Note the service account email address, because it will be used in the next section that covers various configurations that need to be made on the KMES Series 3.

[3] CONFIGURATION ON THE KMES SERIES 3

The instructions in this section will cover the configurations that must be made on the KMES Series 3 for Google EKMS to access externally managed keys.
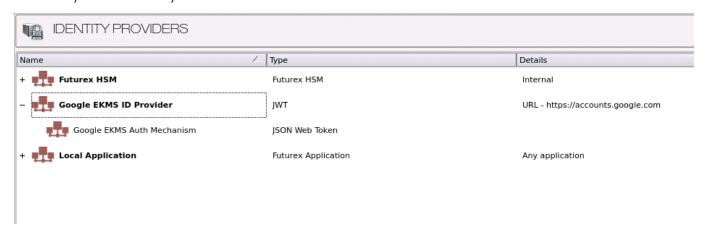
For all of the following sections, you need to be logged in to the KMES application interface with the default Admin identities.

[3.1] ADD JWT IDENTITY PROVIDER

A JSON Web Token (JWT) must be configured to allow Google to authenticate against the KMES using Google's generated JWT.

1. Navigate to *Identity Management -> Identity Providers*, then right-click and select **Add** -> **Provider** -> **JSON Web Token**. This will open the *Identity Provider Editor* dialog.

2. Under the *Info* tab, specify a name for the Identity Provider and de-select **Enforce Dual Factor**.

3. Under the *JWT Options* tab, specify "https://accounts.google.com" as the issuer. Set leeway and max validity according to your requirements.

4. Under the *JWT Key* tab, select **JWKS** and then specify "https://www.googleapis.com/oauth2/v3/certs" in the JWKS URL field. Leave the TLS PKI field blank and click **OK** to save.

5. Right-click on the Identity Provider that was just created and select **Add** -> **Mechanism** - > **JSON Web Token**.

6. In the *Info* tab, specify a name for the authentication mechanism.

7. In the *Identifiers* tab, specify "email" as the Login field and **Username** as the User ID type. Leave Role field blank and click **OK** to save.

   The newly added Identity Provider and authentication mechanism will be listed.

[3.2] CREATE AN IDENTITY FOR THE GOOGLE SERVICE ACCOUNT AND GRANT IT THE REQUIRED PERMISSIONS

Create a new role

1. Navigate to the *Identity Management -> Roles* menu and add a new role. This will open the *Role Editor* dialog.

2. Name the role "Google Key Management" and change the number of login required to 1. Leave all other fields set as the default values under the *Info* tab.

3. Under the *Permissions* tab, select the **Wrap** and **Unwrap** Cryptographic Operations permissions.

4. Click **OK** to save.

Create a new identity and assign it the Google Key Management role

1. Navigate to the *Identity Management -> Identities* menu. Right-click and select *Add -> Client Application* to add a new identity. This will open the *Identity Editor* dialog.

2. In the Name field, paste in the service account email address that Google EKM provided in the key creation wizard in the previous section.

3. Under the *Assigned Roles* tab, select the **Google Key Management** role.

4. Under the *Authentication* tab, click the **Add** button to add a new credential. In the *Configure Credential* dialog, select **JSON Web Token** as the credential type, and then select the provider and mechanism that was configured in the previous section and click **OK**.

5. Remove the default API Key mechanism, leaving only the JSON Web Token credential, and click **OK** to save.

[3.3] CREATE A NEW SYMMETRIC KEY

Create a new Key Group

1. Navigate to the *Key Management -> Keys* menu. In the key groups section, click the **Create** button.

2. For the key type, select **Symmetric**, and for the storage location, choose **HSM Trusted**, then click **OK**.

3. In the *Key Group Editor* dialog, specify a name for the key group. Then click the **Permissions** button, select "Show all roles and permissions", and set the **Use** permission for the **Google Key Management** role. Click **OK**.

4. Click **OK** to finish creating the key group.

Create a new symmetric key

1. Navigate to the *Key Management -> Keys* menu. Under the newly created key group, create a random symmetric Data Encryption or Data Decryption Key.

NOTE: Because we're setting the Key Usage to "Encrypt/Decrypt", Google EKM can use the same key for both encryption and decryption, therefore it does not matter if the key is created specifically as a Data Encryption or Data Decryption Key.
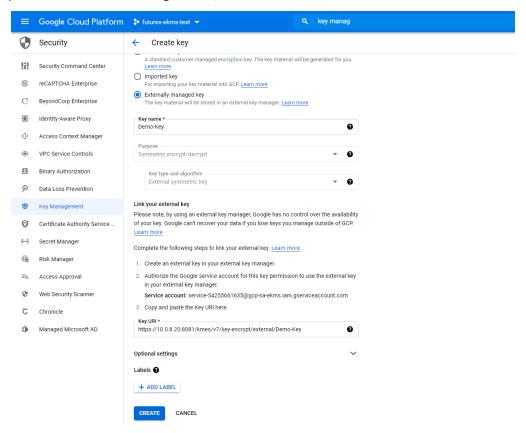
NOTE: The PMK must be used as the "Encrypting Key" or the Key Usage setting will not be available.

2. Click the **Next** button twice, which will bring you to a page confirming that the key has been created.

3. Click **Finish** to exit the key creation dialog.

[4] CREATING THE EXTERNALLY MANAGED KEY IN GOOGLE KMS

Return to the key creation wizard in Google KMS, where we left off at the end of section 2.

Select the "Externally managed key" option, and then specify a name for the key.

NOTE: The key name that is specified here does *not* have to match the name of the key that is created on the KMES Series 3.

In the *Key URI* field, the unique identifying string for the external key that was created on the KMES Series 3 needs to be specified.

Format: `https://<server ip>:<port>/kmes/v7/key-encrypt/external/<key name>`
Example: `https://10.0.8.20:8081/kmes/v7/key-encrypt/external/Demo-Key`

The two fields that need to be configured specifically to your use case are the `<server ip>` and `<key name>` fields.

In the `<key name>` field, the name of the key that was created on the KMES needs to be specified.

In the `<server ip>` field, the IP address of the KMES Series 3 device needs to be specified.

The `<port>` field needs to be set to the RA Web port on the KMES. By default, the RA Web port is 8081.

IMPORTANT: In addition to the steps above, Google must whitelist the domain specified in the *Key URI* field for your specific GCP account.

Click "CREATE" to create the externally managed key.

[5] TESTING ENCRYPTION AND DECRYPTION WITH EXTERNALLY MANAGED KEY

[5.1] DOWNLOAD AND INSTALL GOOGLE CLOUD SDK

Please follow the instructions here to download, install, and configure Google Cloud SDK:

https://cloud.google.com/sdk/docs/install

[5.2] ENCRYPT A TEST FILE USING THE EXTERNALLY MANAGED KEY

NOTE: Before proceeding with next two steps, ensure the GCP user that is calling the encrypt and decrypt methods has the **cloudkms.cryptoKeyVersions.useToEncrypt** and **cloudkms.cryptoKeyVersions.useToDecrypt** permissions on the key used to encrypt or decrypt. One way to permit a user to encrypt or decrypt is to add the user to the **roles/cloudkms.cryptoKeyEncrypter, roles/cloudkms.cryptoKeyDecrypter**, or **roles/cloudkms.cryptoKeyEncrypterDecrypter** IAM roles for that key. For more information, see Permissions and Roles.

Run the following **gcloud kms** command to encrypt a test file using the externally managed key.

```
gcloud kms encrypt \
    --key [key] \
    --keyring [key-ring] \
    --location [location]  \
    --plaintext-file [file-with-data-to-encrypt] \
    --ciphertext-file [file-to-store-encrypted-data]
```

Replace *[key]* with the name of the key to use for encryption. Replace *[key-ring]* with the name of the key ring where the key is located. Replace *[location]* with the Cloud KMS location for the key ring. Replace *[file-with-data-to-encrypt]* and *[file-to-store-encrypted-data]* with the local file paths for reading the plaintext data and saving the encrypted output.

If the command is successful it will return no output.

[5.3] DECRYPT A TEST FILE USING THE EXTERNALLY MANAGED KEY

Run the following **gcloud kms** command to decrypt the file that was encrypted in the previous step, using the externally managed key.

```
gcloud kms decrypt \
    --key [key] \
    --keyring [key-ring] \
    --location [location]  \
    --ciphertext-file [file-path-with-encrypted-data] \
    --plaintext-file [file-path-to-store-plaintext]
```

Replace *[key]* with the name of the key to use for decryption. Replace *[key-ring]* with the name of the key ring where the key is located. Replace *[location]* with the Cloud KMS location for the key ring. Replace *[file-path-with-encrypted-data]* and *[file-path-to-store-plaintext]* with the local file paths for reading the encrypted data and saving the decrypted output.

If the command is successful it will return no output.

View the contents of the plaintext file that was output from this decryption command and confirm that it is identical to the original file that was encrypted. If the two files are identical then it confirms that the externally managed key is successfully performing encryption and decryption operations.

APPENDIX A: XCEPTIONAL SUPPORT

In today's high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team does whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that you cannot find anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

ENGINEERING CAMPUS

864 Old Boerne Road

Bulverde, Texas, USA 78163

Phone: +1 830-980-9782

+1 830-438-8782

E-mail: info@futurex.com

XCEPTIONAL SUPPORT

24x7x365

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com