GOOGLE CLOUD EKM (EXTERNAL KEY MANAGER)

Integration Guide

Applicable Services:
VirtuCrypt Enterprise Key Management

TABLE OF CONTENTS

[1] OVERVIEW OF THE GOOGLE CLOUD EKM / VIRTUCRYPT 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., VirtuCrypt Enterprise Key Management service) 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 / VirtuCrypt 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 VirtuCrypt 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 in VirtuCrypt, and is never sent to Google.

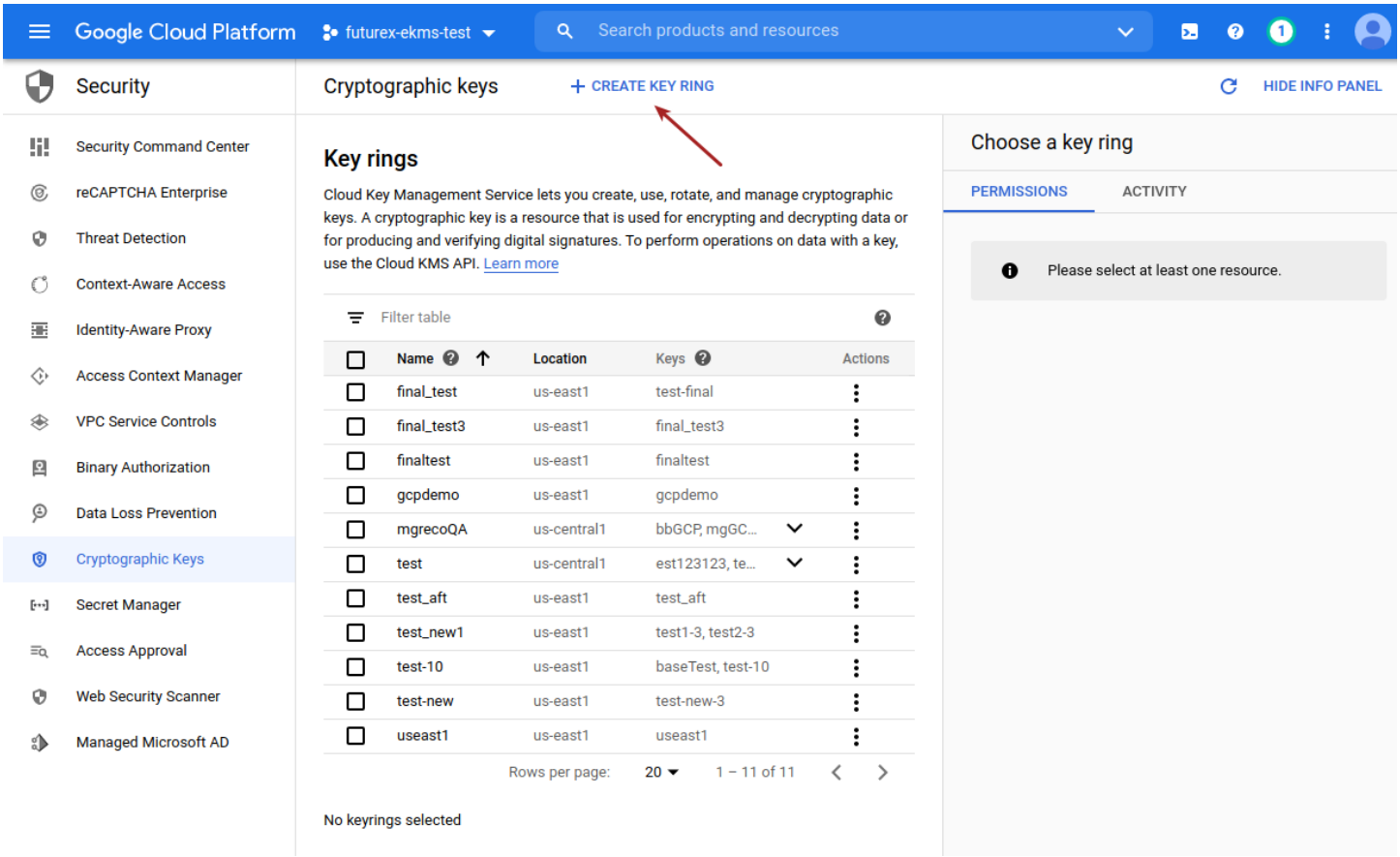
[2] INITIAL SETUP IN THE GOOGLE KMS DASHBOARD

[2.1] NAVIGATE TO THE CLOUD KMS DASHBOARD

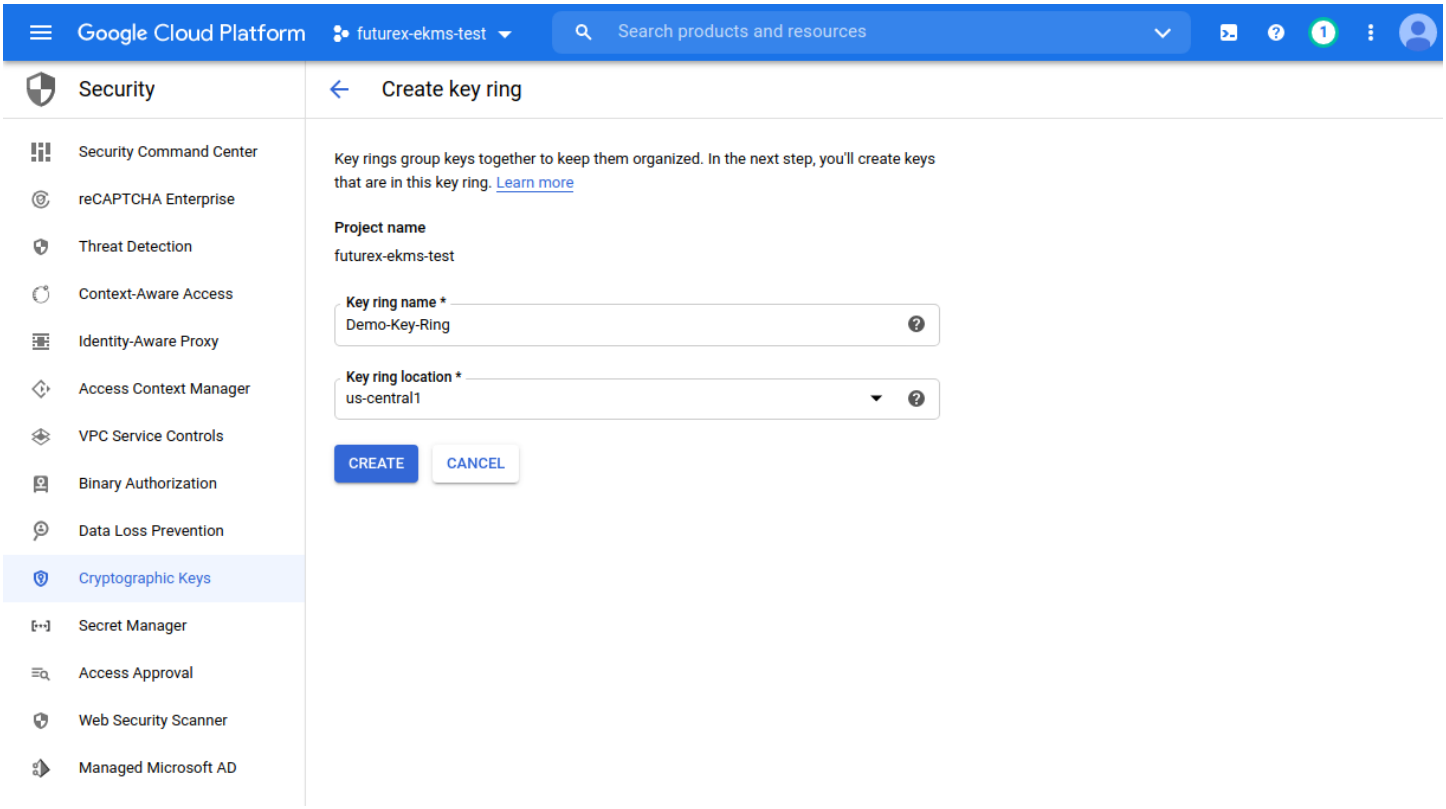
From the main GCP dashboard, type "Key Management Service", into the search bar at the top of the page. Then, click on "Cryptographic Keys".

[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).

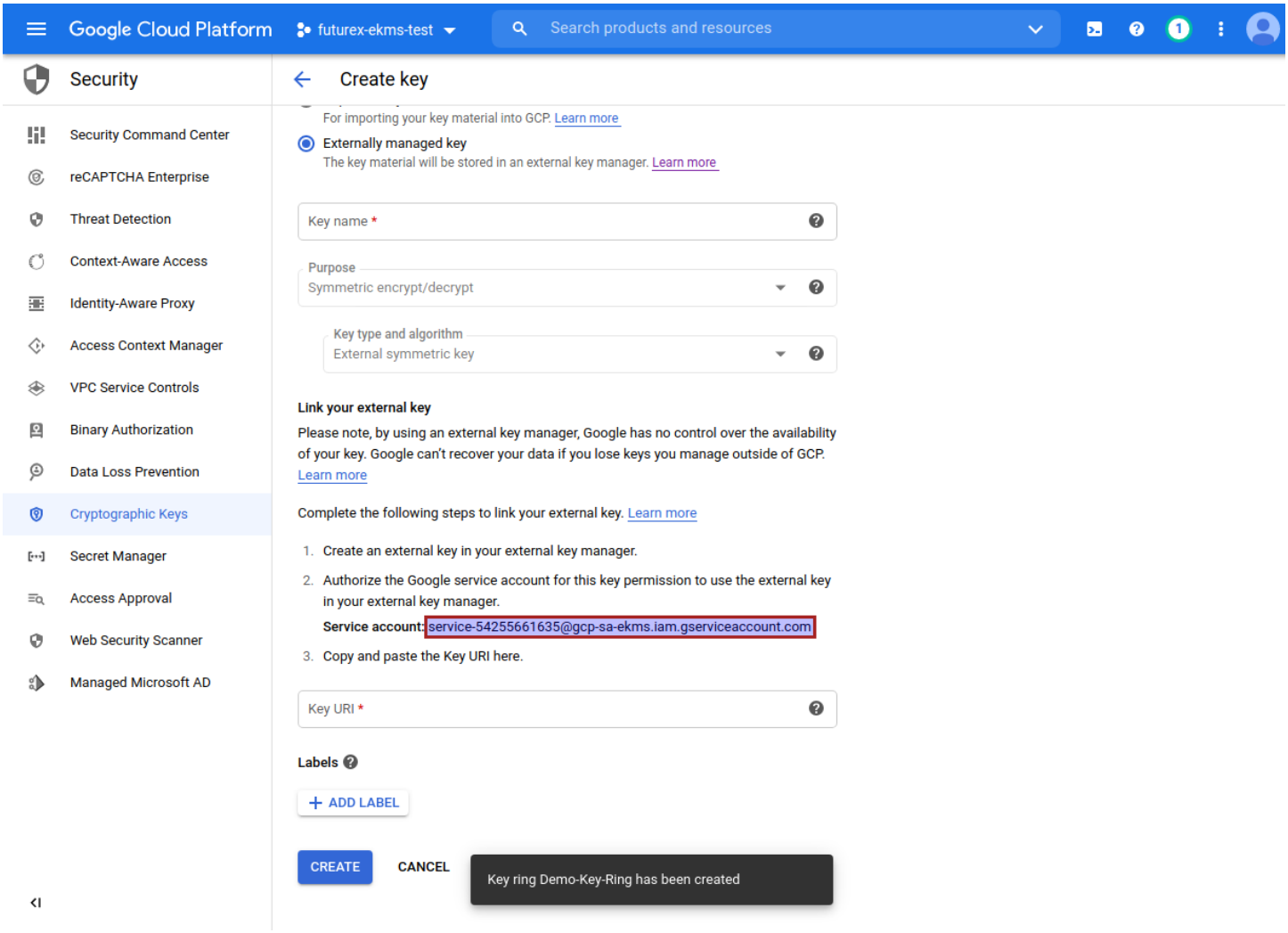
Select the key ring location.

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 VirtuCrypt region where the key resides.
- 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.



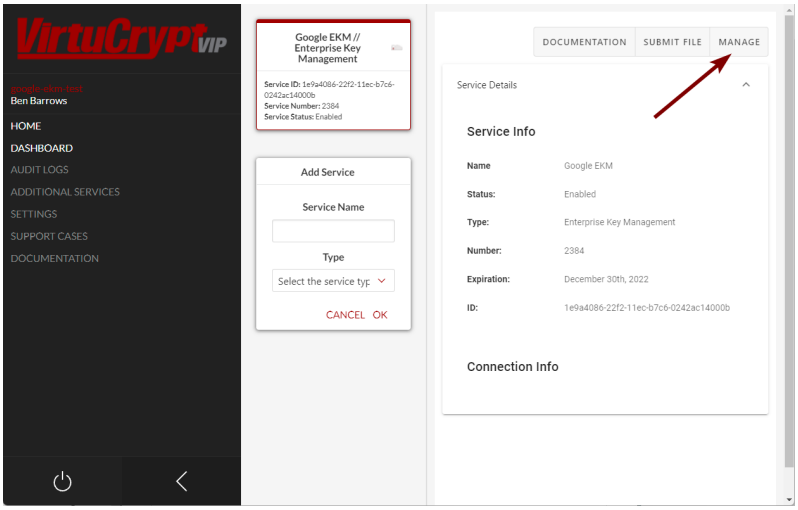
Note the service account email address, because it will be used in the next section that covers various configurations that need to be made in the VirtuCrypt Intelligence Portal (VIP).

[3] CONFIGURATION IN THE VIRTUCRYPT INTELLIGENCE PORTAL (VIP)

NOTE: Before proceeding with the steps in this section, a new VIP user needs to be created inside your VirtuCrypt account. The name of this user must match the service account email that Google EKM provided in the previous section (e.g., service-54255661635@gcp-sa-ekms.iam.gserviceaccount.com). Please reach out to the Futurex Xceptional support team to request that this user be added to your account.

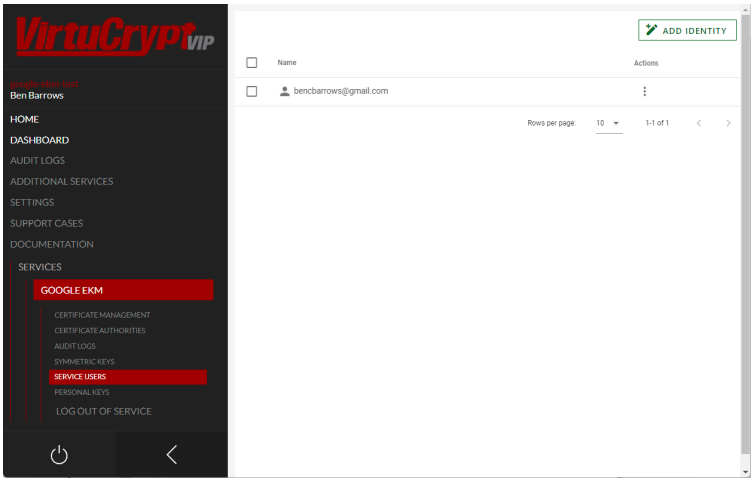
[3.1] LOG IN TO THE GOOGLE EKM VIRTUCRYPT SERVICE

1. Log in at https://vip.virtucrypt.com/login with an account identity that is authorized to access the Enterprise Key Management service created for integration with Google EKM.
2. Once logged in to the VIP, select the Google EKM service, then click the **Manage** button in the top right-hand corner of the page.



[3.2] CREATE A NEW IDENTITY AND ASSIGN IT THE "GOOGLE KEY MANAGEMENT" ROLE

1. Once logged in to the Google EKM service, navigate to the *Service Users* page in the left menu.



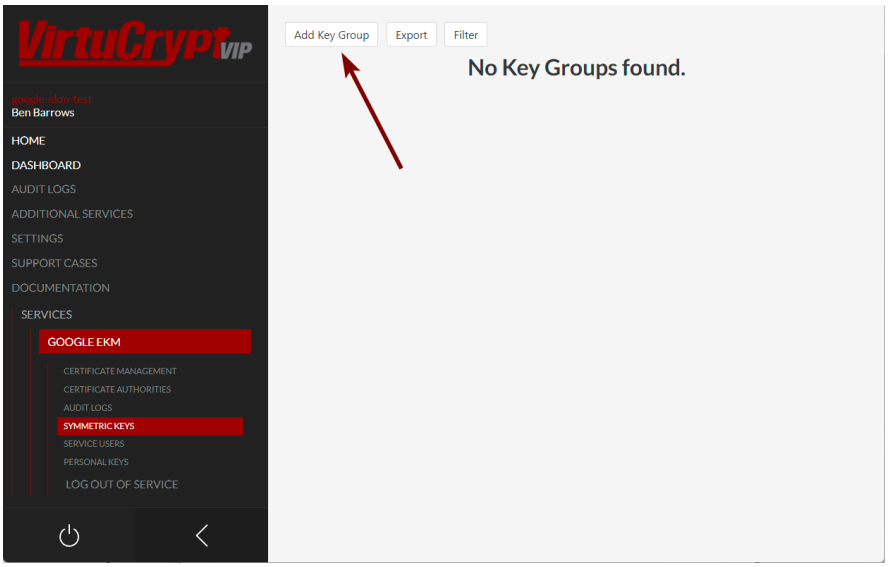
2. Click the **Add Identity** button in the top-right corner of the page.

3. In the VIP User field, select the VIP user that was added to your VirtuCrypt account at the beginning of this section (e.g., service-54255661635@gcp-sa-ekms.iam.gserviceaccount.com).
4. In the Roles field, select the **Google Key Management** role. Click the **Submit** button to save the changes.

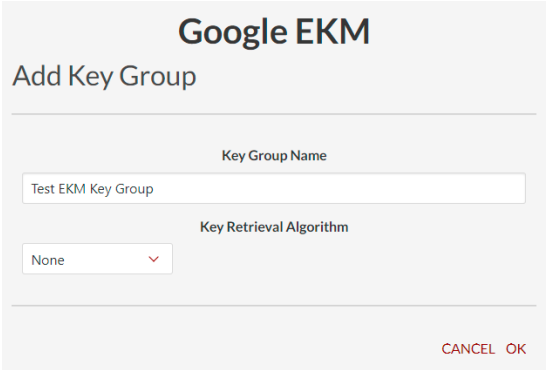
[3.3] CREATE A NEW SYMMETRIC KEY

Add a new Key Group

1. Navigate to the *Symmetric Keys* page in the left menu, then click the **Add Key Group** button at the top of the page.



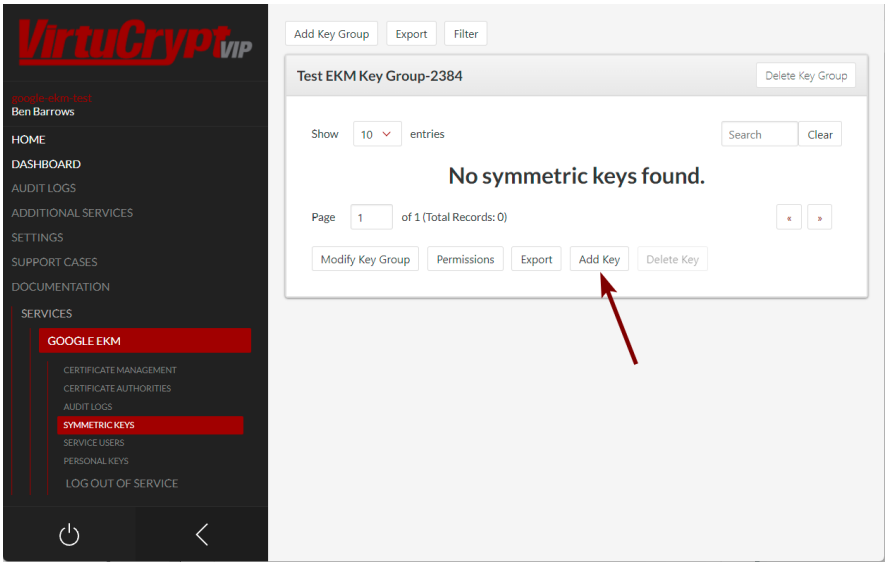
2. Specify a key group name and the key retrieval algorithm to use.



3. Click **OK** to save. A message should appear at the top of the screen stating that the key group was created successfully.

Create a new symmetric key

1. Select the key group that was just created, then click the **Add Key** button.



2. In the *General* tab, select **Random** as the encryption mode, **Data Encryption Key** as the key type, and choose one of the **AES** algorithms. The name of the key can be anything.

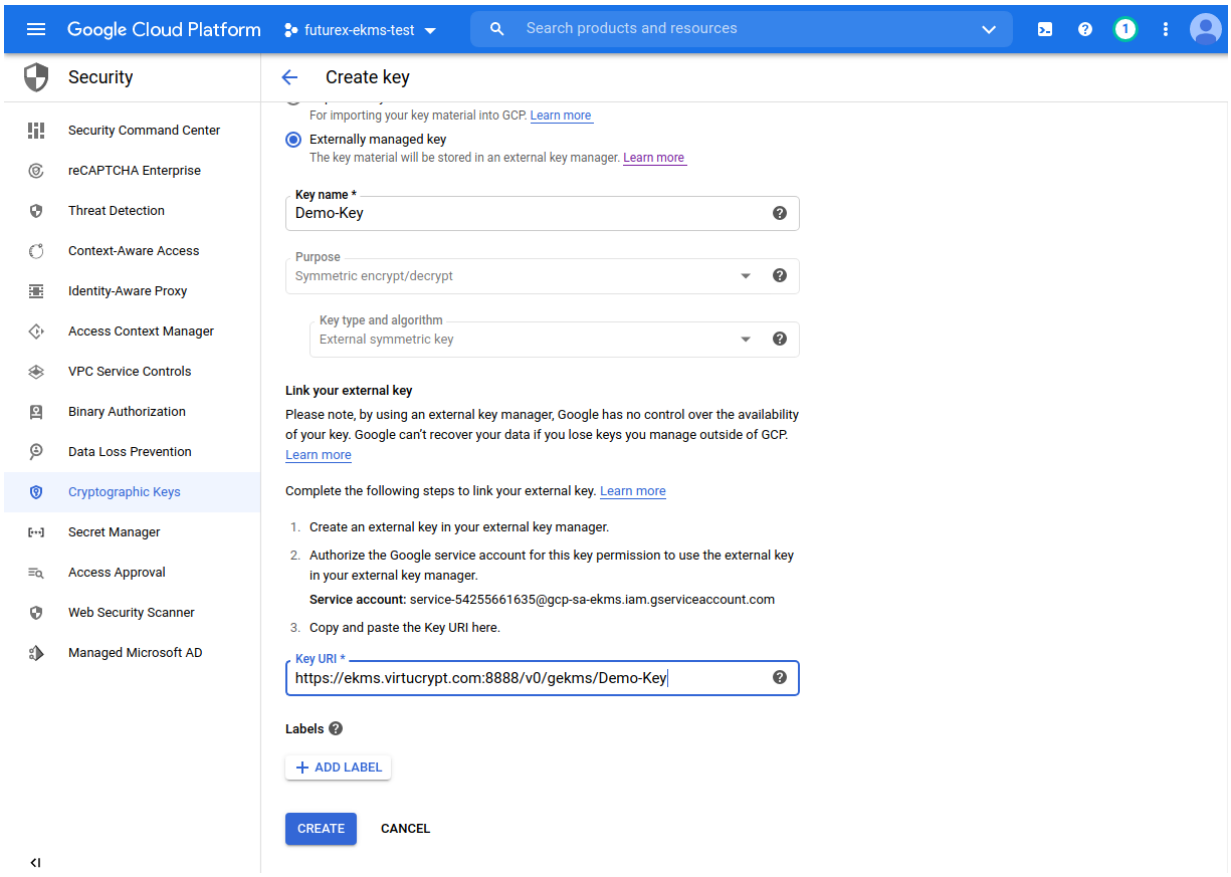
   NOTE: Using the AES algorithm allows the key that is being created to have key usages set. The key usages set for Data Encryption Keys in VirtuCrypt are "Encrypt/Decrypt"; therefore, Google EKM can use the same key for encryption and decryption.

3. In the *Validity* tab, set the desired validity start and end dates.

4. Click **OK** to save. A message should appear at the top of the screen stating that the key was created successfully.

[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 was created in the VirtuCrypt Enterprise Key Management service.

In the *Key URI* field, the unique identifying string for the external key that was created in the VirtuCrypt Enterprise Key Management service must be specified.

Format: https://[domain name]:[port]/v0/gekms/[key name]
Example: https://ekms.virtucrypt.com:8888/v0/gekms/Demo-Key

The [key name] is simply the name of the key that was created in the VirtuCrypt Enterprise Key Management service.

The [domain name] and [port] will always be "ekms.virtucrypt.com" and "8888", respectively, for the Google EKM / VirtuCrypt integration.

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