Security & Identity Products (https://cloud.google.com/products/security/)
Cloud Key Management Service (https://cloud.google.com/kms/)
Documentation (https://cloud.google.com/kms/docs/) Guides

Creating asymmetric keys

This topic provides information about creating asymmetric keys. If you want to create symmetric keys, see the Creating Keys and Key Rings (https://cloud.google.com/kms/docs/creating-keys) topic.

Create a key ring

A key ring is defined by its location (https://cloud.google.com/kms/docs/object-hierarchy#location) and name.

CONSOLE COMMAND LINE API

1. Go to the **Cryptographic Keys** page in the Cloud Console.
2. Click **Create key ring**.
3. In the **Key ring name** field, enter the name for your key ring.
4. From the **Location** dropdown, select a location.
5. Click **Create**.

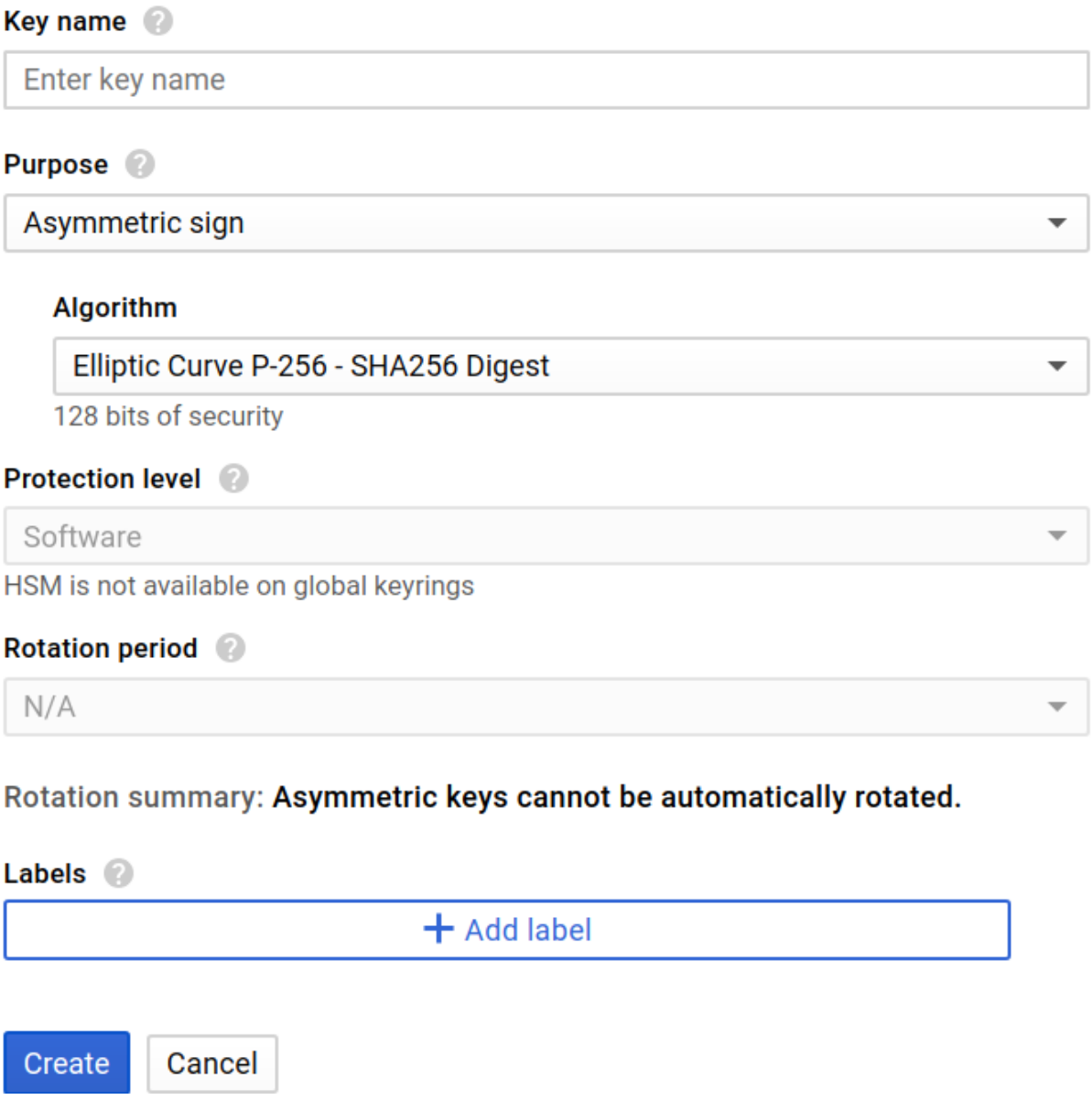
Create a key

A key must be created in a key ring.

CONSOLE COMMAND LINE API

1. Go to the **Cryptographic Keys** page in the Cloud Console.
2. Click the name of the key ring for which you will create a key.
3. Click **Create key**.
4. In the **Key name** field, enter the name for your key.

5. Click the **Purpose** dropdown. Select an asymmetric key purpose, for example **Asymmetric sign** or **Asymmetric decrypt**. To learn more about key purposes, see Key purposes (https://cloud.google.com/kms/docs/algorithms#key_purposes).
6. Click the **Algorithm** dropdown. Select the algorithm for your key. You can change this for future key versions. The choice of **Purpose** determines which algorithms are available. For example, if your key purpose is **Asymmetric sign**, one of the supported algorithms is **Elliptic Curve P-256 - SHA256 Digest**. To learn more about algorithms for an asymmetric key, see Key purposes and algorithms (https://cloud.google.com/kms/docs/algorithms).
7. For **Protection level**, select either **Software** or **HSM**. To learn more about protection levels, see Protection levels (https://cloud.google.com/kms/docs/algorithms#protection_levels).
   Your **Cryptographic Keys** page should look similar to:



8. [Optional] In the **Labels** field, click **Add label** if you want to add labels to your key (https://cloud.google.com/kms/docs/creating-managing-labels).

9. Click **Create**.

When you create an asymmetric key, the initial state for the key version is pending generation. When Cloud Key Management Service finishes generating the key version, its state automatically changes to enabled. Learn more about key version states at Key states (https://cloud.google.com/kms/docs/key-states).

If you want to retrieve the public key portion of the newly created key version, follow the instructions at Retrieving a public key (https://cloud.google.com/kms/docs/retrieve-public-key).

Access control to asymmetric keys

A signer or validator requires the appropriate permission or role on the asymmetric key.

- For a user or service that will perform signing, grant the `cloudkms.cryptoKeyVersions.useToSign` permission on the asymmetric key.
- For a user or service that will retrieve the public key, grant the `cloudkms.cryptoKeyVersions.viewPublicKey` on the asymmetric key. The public key is required for signature validation.

Learn about permissions and roles in Cloud KMS release at Permissions and Roles (https://cloud.google.com/kms/docs/reference/permissions-and-roles).

Next steps

- Learn about Creating and validating signatures (https://cloud.google.com/kms/docs/create-validate-signatures).
- Learn about Encrypting and decrypting data with an RSA key (https://cloud.google.com/kms/docs/encrypt-decrypt-rsa).
- Learn about Retrieving a public key (https://cloud.google.com/kms/docs/retrieve-public-key).

Last updated January 22, 2020.