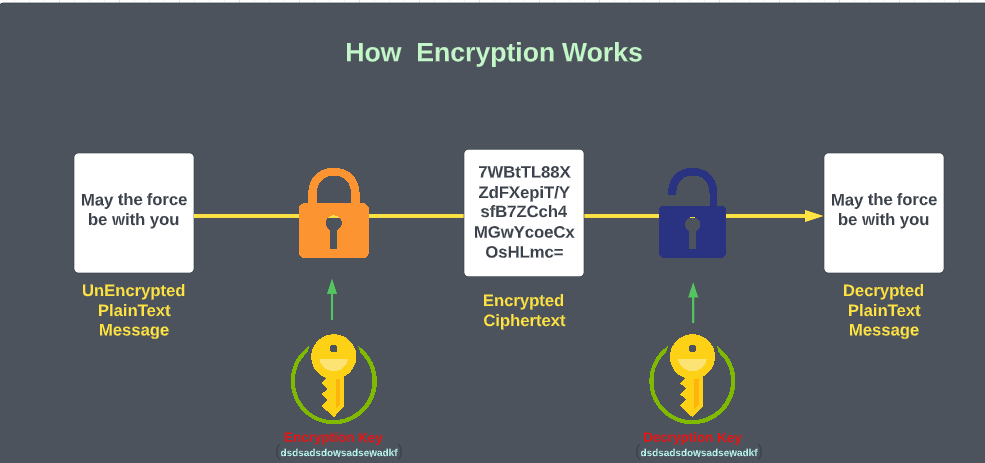
**Encryption on Google Cloud Platform**

**Introduction**

Google Cloud KMS is a managed service that allows users to create and manage encryption keys to be used to encrypt data managed by Google Cloud services at REST. There are a few core concepts that you need to be familiar with before starting using Cloud KMS. These concepts are:

**What is Encryption?**

Encryption is a process that takes legible data, referred to as plain text, as input and transforms it into illegible data, referred to as cipher text, as an output. This Transformation makes the data unreadable, revealing little to no information about the plaintext. Encryption uses an algorithm to transform this data and a key for the receiving party to decrypt that information. Many algorithms involve different ways of scrambling and then decrypting that information.



**Key Ring**

As the name suggests, a key ring is a place where you can store your keys. Its responsibility is to keep your encryption keys and to let you organize them. Key Rings are very useful when you need to handle lots of encryption keys and you want to keep them organized. When you create a Key Ring, you are required to select a location. Google supports loads of different locations and regions for creating a Key Ring. If you prefer to distribute the keys globally, you can do it by choosing global.

**Symmetric Key:**

A symmetric key is an encryption key that is shared between who needs to encrypt the data and who needs to decrypt the data. By using a symmetric Key, you only need to create a single encryption key and share it with those who will encrypt and decrypt data.

**Asymmetric Key (An asymmetric Key is a set of two encryption keys):**

A private key and a public key. The public encryption key is used to encrypt data. The private encryption key is used to decrypt data. As the name suggests, the public key is public, so anyone can encrypt data by using the public key. The secret key, instead, is private and it should be owned only by those parties who want to be able to decrypt the data. Asymmetric encryption is more secure, but it's also more complex and slow.

**Key Rotation:**

Because of security purposes, the more secure way to handle encryption keys is to periodically rotate them. This means that every week, month or so, you should create a new version of the encryption key. Rotating a key means disabling the old version of an encryption key and creating a new one.

**Enabling Cloud KMS API**

1. Once you first log in, your screen should look similar to this.



1. Click on the project selector drop-down menu at the top of the screen.



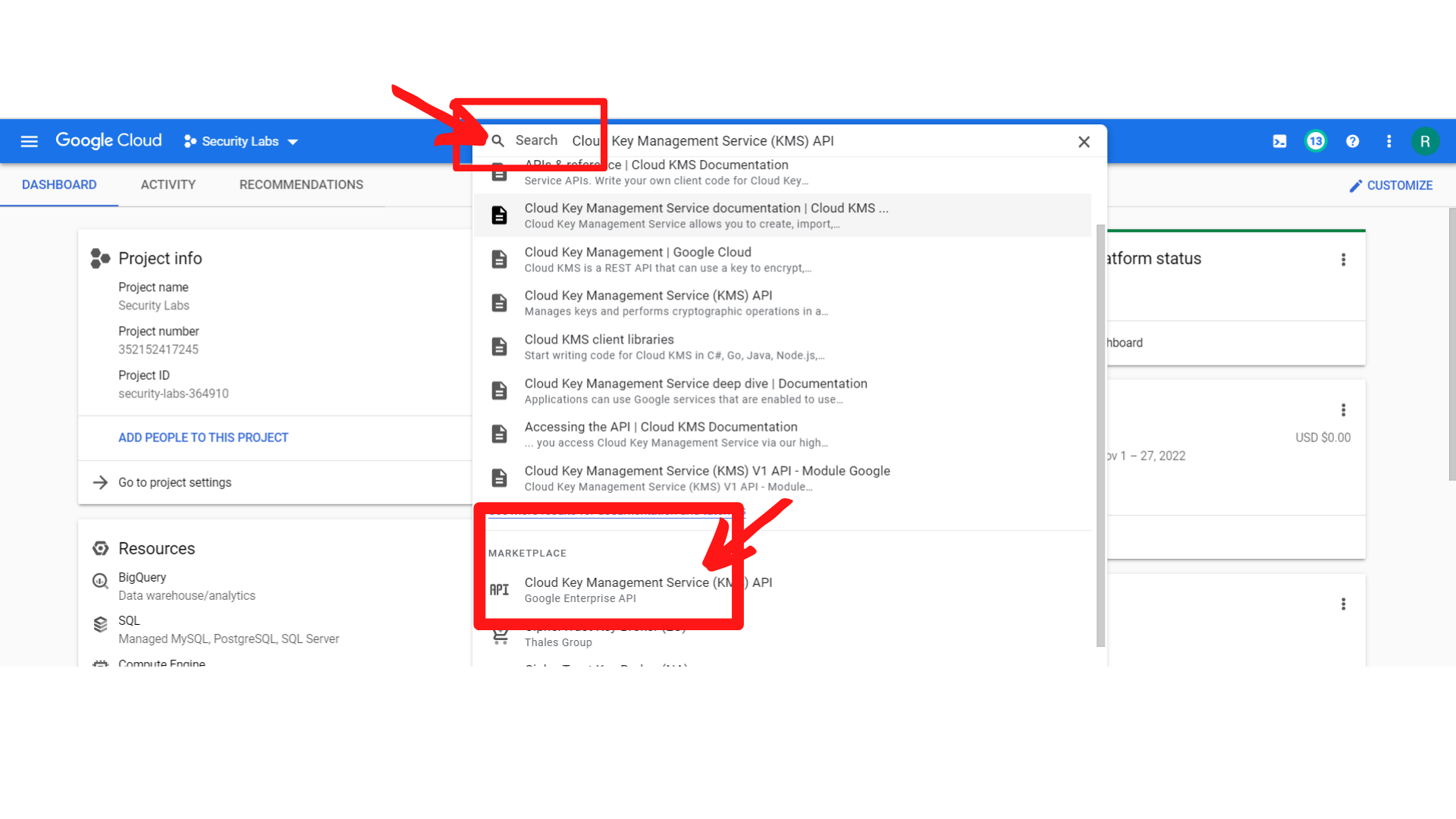
1. Since, we are doing labs on a Security Labs project, Click on *“Security Labs”*.



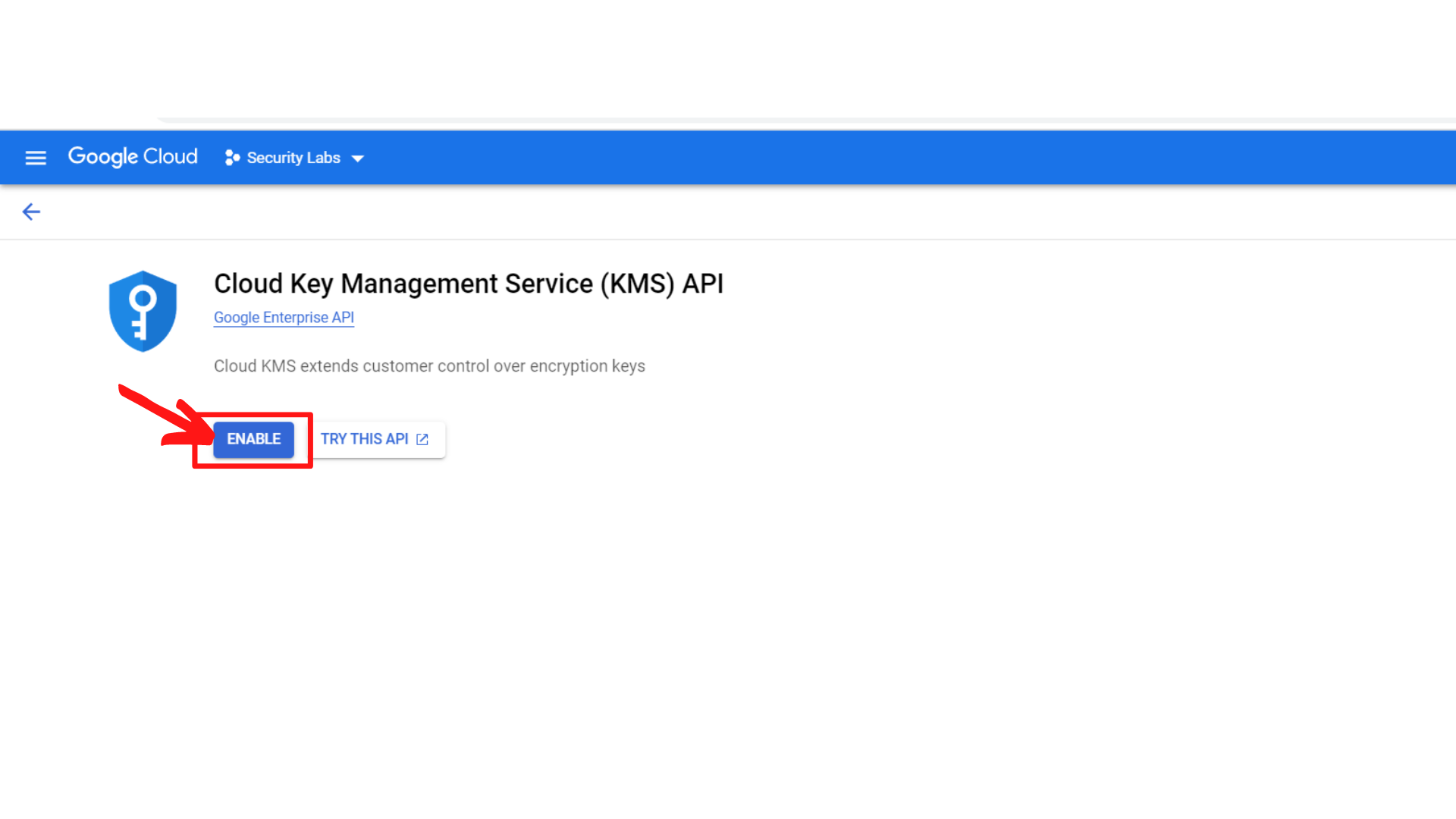
1. Your screen should look similar to this with project info changed to “*Security Labs”* project.



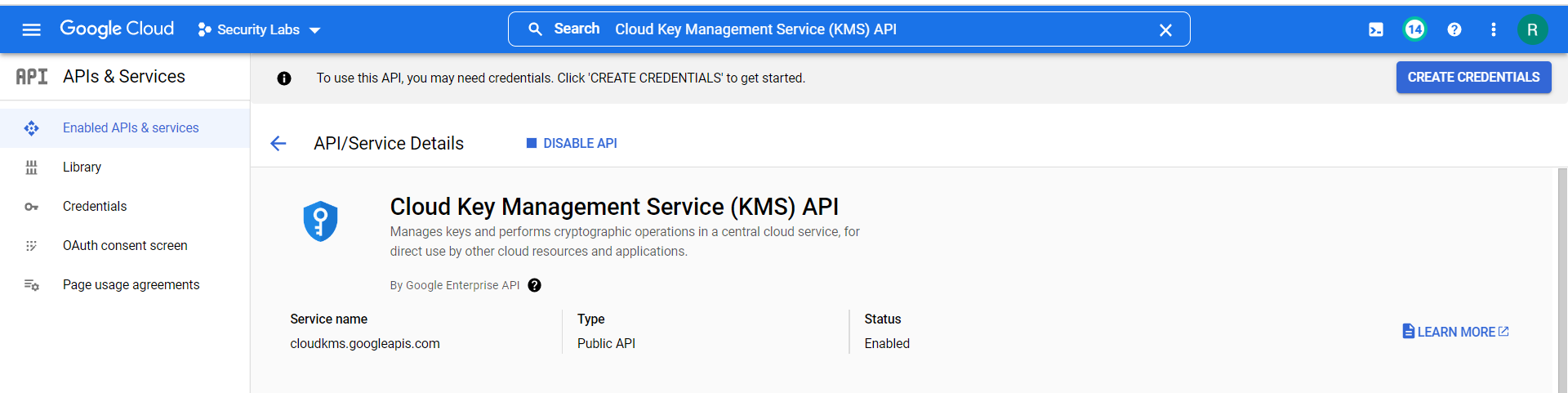
1. Now in the search bar type ***“Cloud Key Management Service (KMS) API” and select it.***



1. Your screen should look similar to this and ***“Click → Enable”***



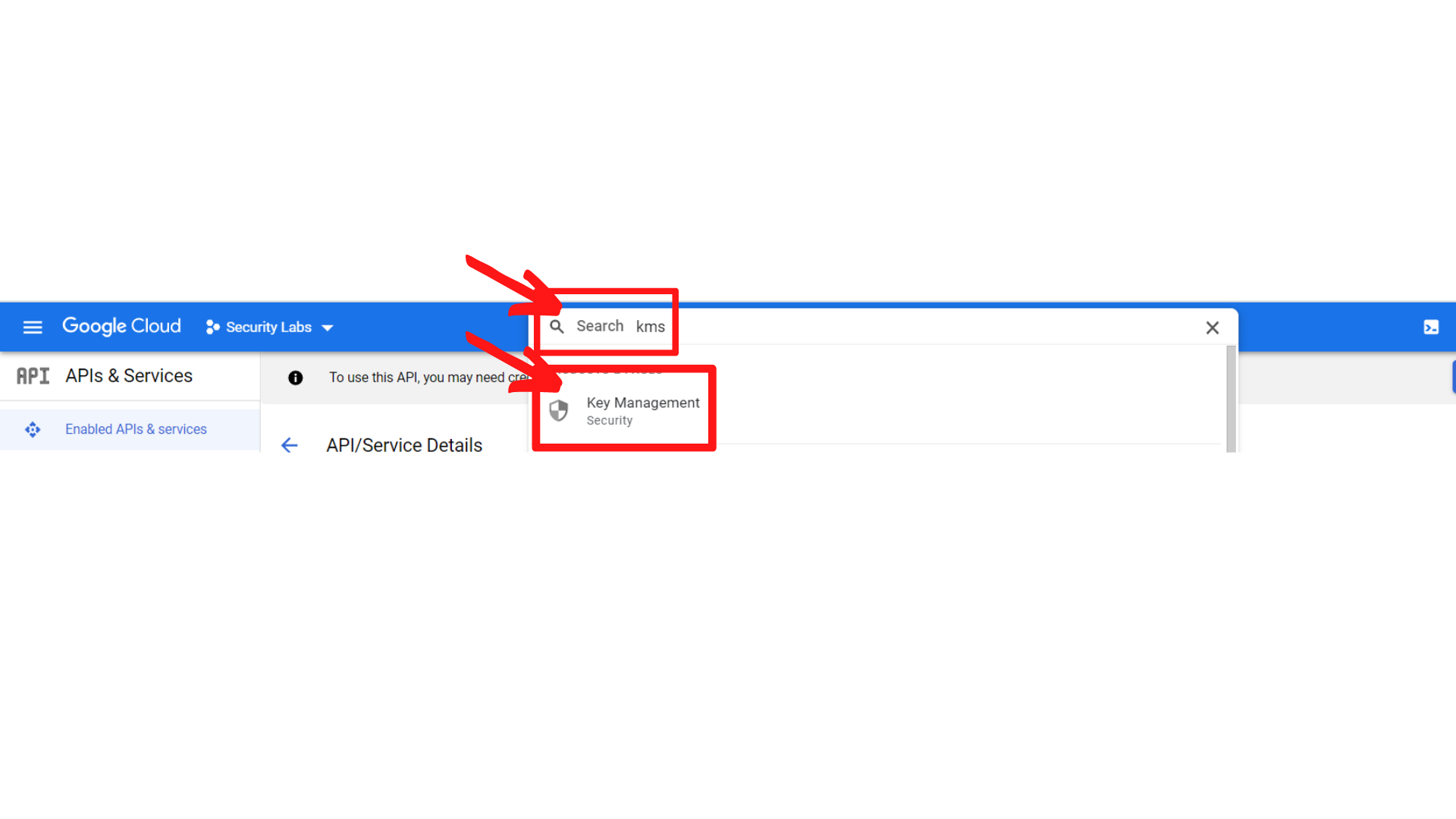
1. Your screen should look similar to this after enabling the API.



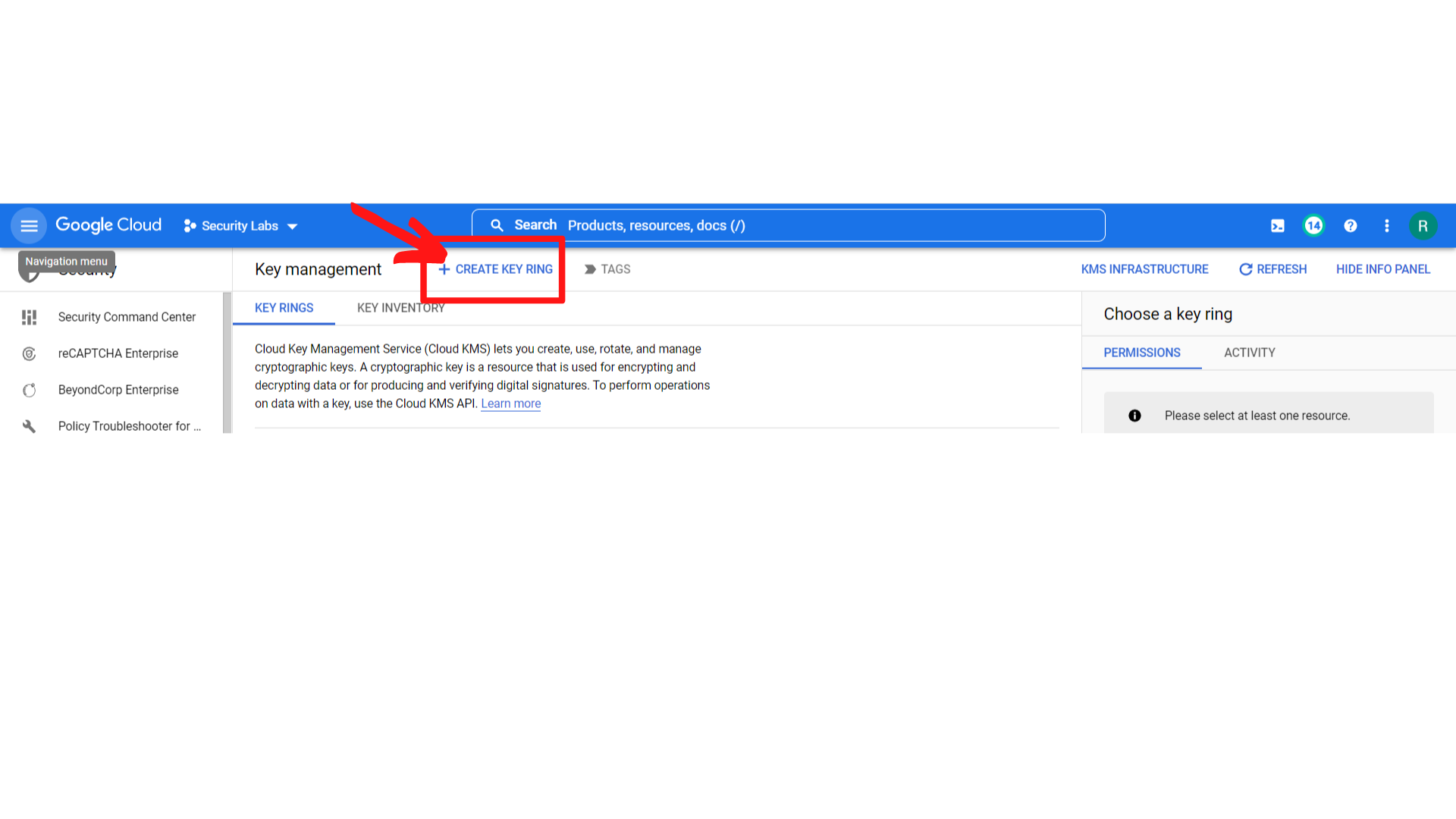
That’s it you have enable the Cloud Key Management Service (KMS) API

**Creating a Cloud KMS Key Ring**

1. Look at the upper part of the GCP console to reach the search bar. **“Enter *kms* and click on Key Management.”**



1. Your screen should look similar to this and ***“click → Create Key Ring”***

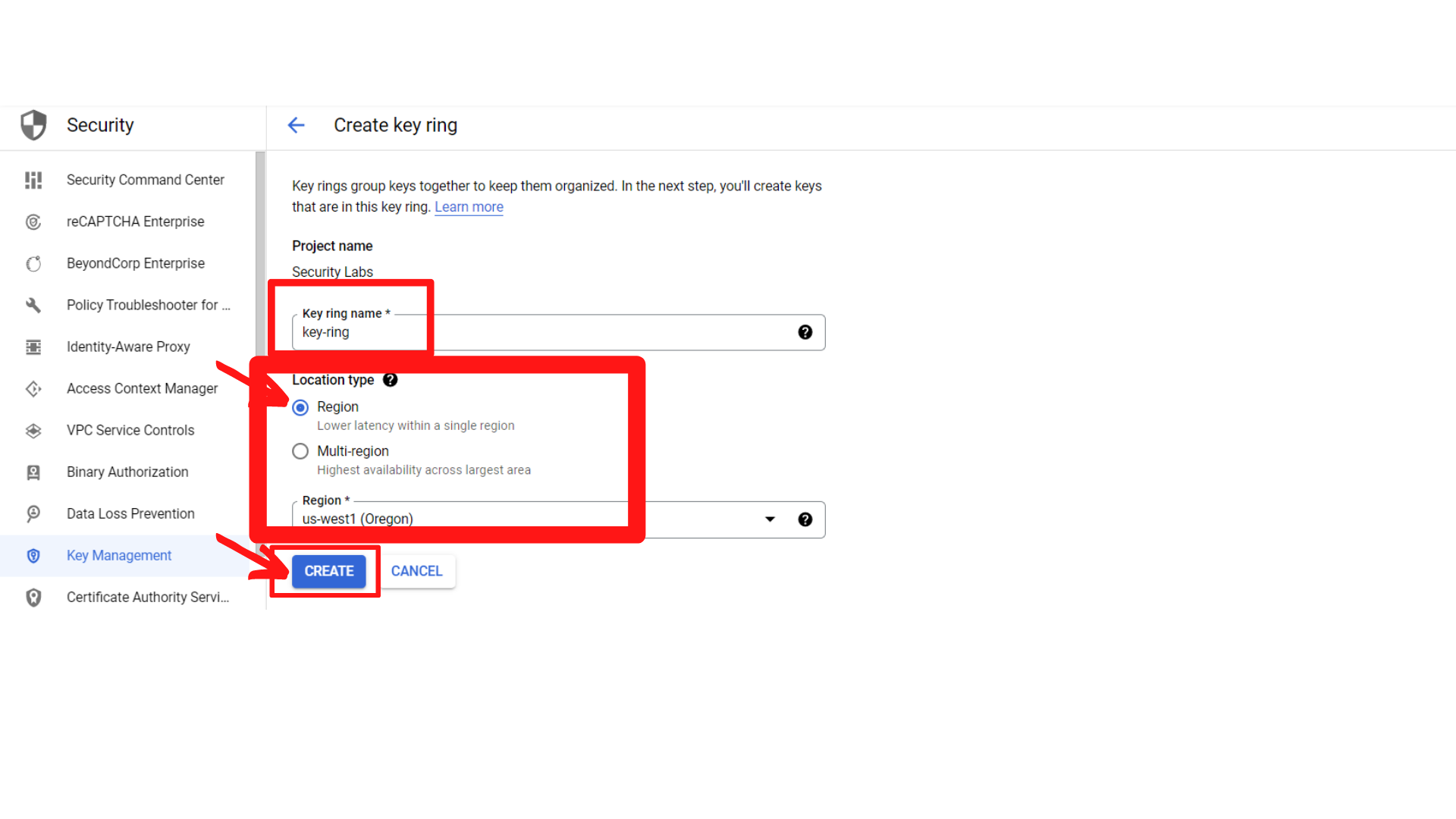


1. Fill the creation form as described below:

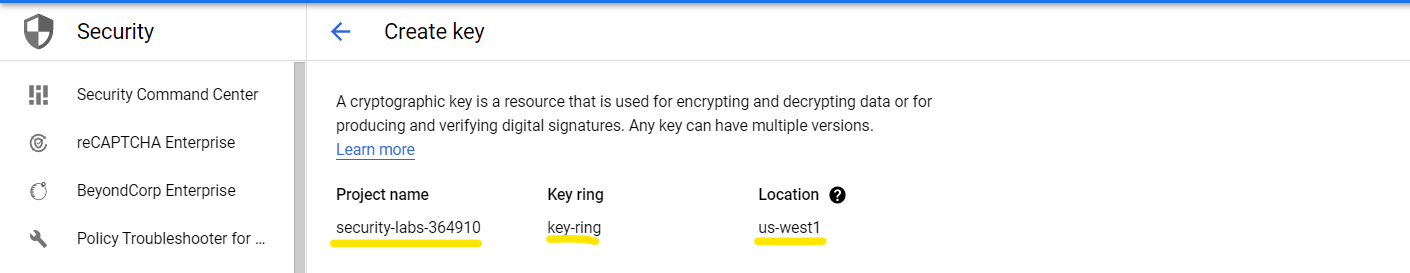
**Key ring name:** **key-ring**

**Location type:** Select Region and choose **“us-west1”** from the drop-down menu

Then **“Click → Create”**



1. You can see that the encryption key will be created in your project and in the same location you defined the key ring:



1. Now scroll down,you will see a creation form will be displayed.

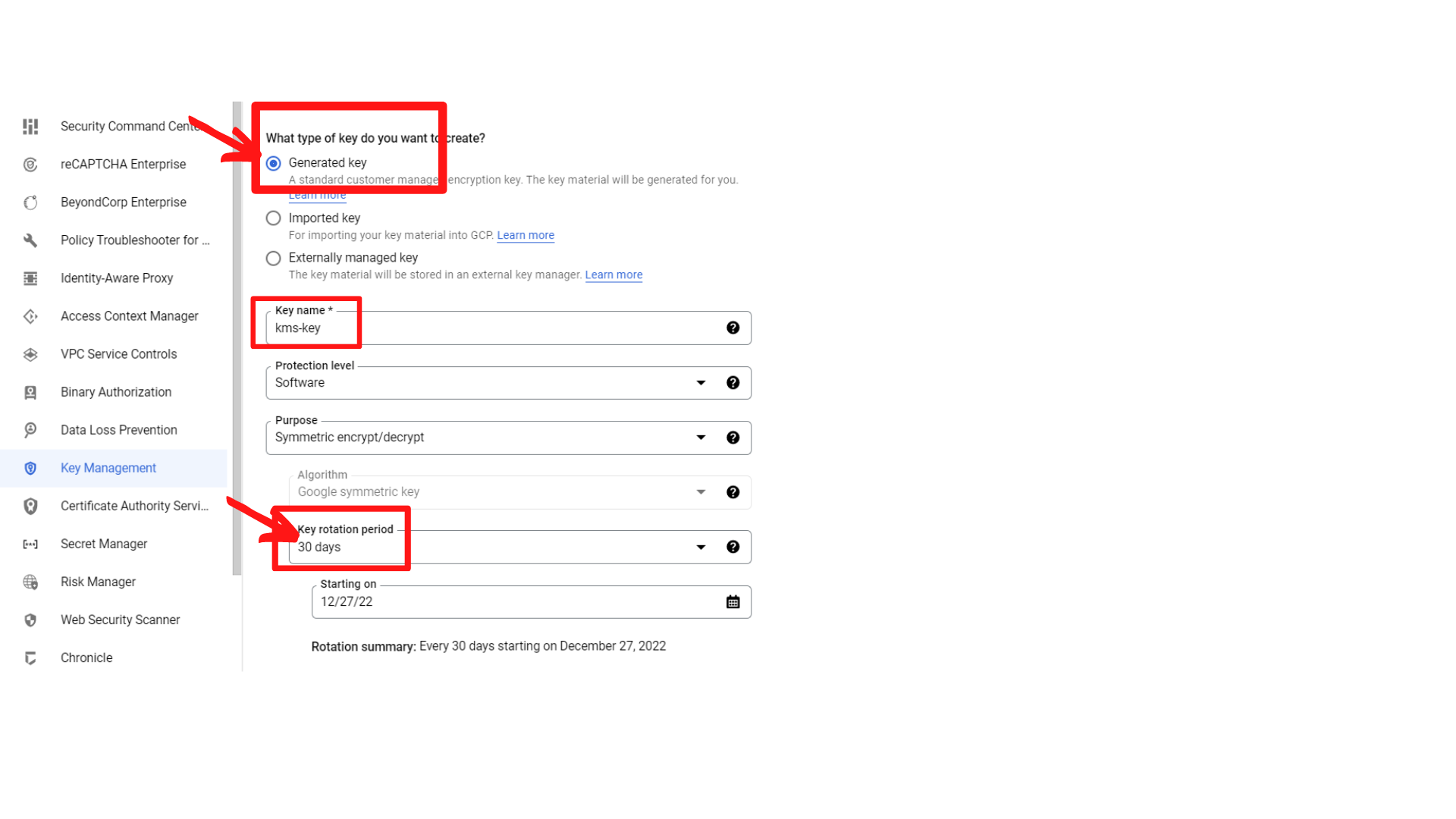
Enter the following information.

**What type of key do you want to create?** : Select **“Generated key”**

**Key name:** **kms-key**

**Rotation period:** **30 days**

**Leave all fields as default.**

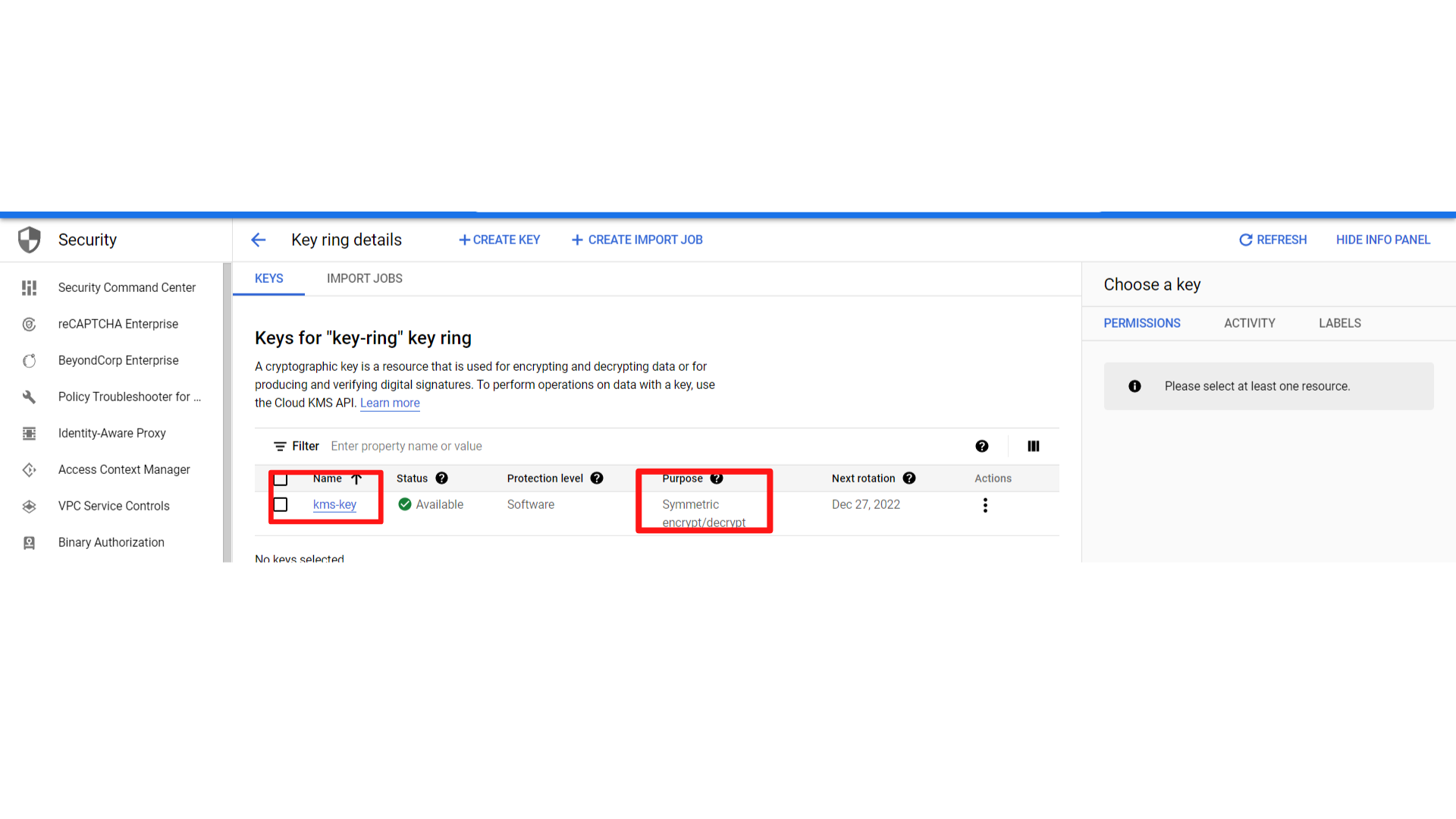


**Note: You can see that the key type is set on the Generated key. It means that the key is generated and managed by Google.**

1. Now scroll down and ***“click → Create”***



1. Now your screen should look similar to this which means a new key ring has been created.



**Note: Take a look at the Next rotation column. This indicates the date of the next rotation. When the next rotation will be performed, a new encryption key version will be created. All services that use the encryption key will automatically use the newly created version.**