Google Cloud BYOK

Integration Guide

CryptoServer HSM

4.55.0.0

utimaco®

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-05-21
Status	PUBLISHED
Document No.	IG-2026-0044

Table of Contents

1 Introduction

This guide is part of the information and support provided by Utimaco. Additional documentation produced to support your Utimaco SecurityServer product can be found in the document directory of the Utimaco SecurityServer product bundle.

All Utimaco SecurityServer product documentation is available from Utimaco's website at https://utimaco.com/.

2 About This Guide

This guide describes how to bring your own key into the Google Cloud Key Management Service with the Utimaco HSM.

2.1 Target Audience for This Guide

This guide is intended for Google Cloud administrators and HSM administrators.

2.2 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Select **Details** and click on **Properties** button
`Monospaced`	Code that is given for explanation or as an example, file paths	`certreq.exe -new request.inf IISCertRequest.csr`
Italic	References and important terms	Operating system listed in *Tested Versions*

Table 1: Document conventions

We use special icons to highlight the most important notes and information.

Here you will find important safety information that should be followed.

Here you will find additional notes or supplementary information.

This message marks the result expected after the successful execution of an instruction.

2.3 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
AES	Advanced Encryption Standard
BYOK	Bring Your Own Key
CD	Compact Disc
CLI	Command Line Interface
CNG	Cryptography API Next Generation
CXI	Cryptographic eXtended Services Interface
FIPS	Federal Information Processing Standards
GCP	Google Cloud Platform
GUI	Graphical User Interface
HSM	Hardware Security Module
JCE	Java Cryptography Extension

Abbreviation	Meaning
KMS	Key Management System
LAN	Local Area Network
P11CAT	PKCS#11 CryptoServer Administration Tool
PCIe	PCI Express Interface
PKCS#11	Public-Key Cryptography Standard #11
RSA	Rivest-Shamir-Adleman
SDK	Software Development Kit
URL	Uniform Resource Locator

Table 2: List of abbreviations

3 Overview

3.1 Key Management Service

Google Cloud Platform (GCP) is a suite of cloud computing services that run on the same infrastructure used also internally by Google for its end-user products. The Key Management Service is one of the services offered. It is a cloud-hosted KMS that lets you manage symmetric and asymmetric cryptographic keys for your cloud services in the same way you do on-premises, helping users meet the compliance, privacy, and security requirements.

3.2 Utimaco SecurityServer HSM

SecurityServer is a hardware security module developed by Utimaco IS GmbH. SecurityServer is a physically protected specialized computer unit designed to perform sensitive cryptographic tasks and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3.3 Utimaco u.trust Anchor

u.trust Anchor is the next generation hardware security module platform developed by Utimaco IS GmbH. u.trust Anchor is a physically protected, specialized computer unit designed for true multi-tenancy, and performing sensitive cryptographic tasks, and to securely manage as well as store cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

3.4 Utimaco BYOK Tool

Bring Your Own Key (BYOK) allows enterprises to encrypt their data and retain control and management of their encryption keys. Utimaco's BYOK tool enables our customers to generate cryptographic key material on the HSM, securely export it and transfer it to the cloud.

4 Integration Requirements and Prerequisites

Ensure the system environment you will be using meets the following hardware and software requirements.

4.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with Google Cloud Platform Key Management Service BYOK.

Operating System	BYOK Tool Version	Utimaco Security Server Version	Utimaco HSM
Windows Server 2019 RHEL 8	BYOK tool 1.1.0	SecurityServer V4.55.0.0	CryptoServer CSe-Series/Se-Series u.trust Anchor Se*k and u.trust Anchor CSAR

Table 3: List of tested versions

This integration is not supported with external keystore.

4.2 Software Requirements

Software	Software Requirements
BYOK tool	BYOK tool 1.1.0 developed by Utimaco
HSM Software	Utimaco SecurityServer Software 4.55.0.0
HSM Interfaces	SecurityServer PKCS#11
P11tool2	p11tool2 from product package Utimaco SecurityServer 4.55.0.0

Software	Software Requirements
Java	Version 8, Update 271 or higher

Table 4: List of software requirements

4.3 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.55.0.0 or higher u.trust Anchor Se*k and u.trust Anchor CSAR with firmware 4.55.0.0 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.55.0.0 or higher u.trust Anchor Se*k and u.trust Anchor CSAR with firmware 4.55.0.0 or higher

Table 5: List of hardware requirements

Set up an account on the Utimaco support portal and request download access at the following URL: https://support.hsm.utimaco.com/.

4.4 Prerequisites

4.4.1 GCP Key Management Service Subscription

Access to the GCP, the Key Management Service, and a billing account are required in order to create and operate with cryptographic material.

4.4.2 Google Cloud SDK

In order to send the commands through the CLI, Google's Cloud SDK needs to be installed on the workstation. It is recommended that the project, where you want the key uploaded, is set when you start using the SDK for the first time. Otherwise, you will need to add the project parameter to each command.

4.4.3 OpenSSL

OpenSSL needs to be installed on the workstation.

4.4.4 Configured Utimaco HSM

You should have your HSM configured before you proceed with the steps described in this guide. For more information about how configure your HSM, please check the documentation on the corresponding Product CD.

4.4.5 Utimaco BYOK Tool Prerequisites

To simplify the key export and import process of tenant keys, Utimaco has created an HSM Bring Your Own Key (BYOK) tool. Please, reach out to Utimaco so this tool can be provided to you.

You might need an authenticated support portal account to download the tool.

The BYOK tool supports all key types (PKCS#11, CNG, JCE, CXI). The storage of keys is still restricted to the internal storage on the Utimaco CryptoServer HSM. The BYOK tool does not support key creation, only migration. That is why it is important to have the attributes of keys you would like to migrate set to be extractable.

For more information regarding the commands and command parameters, please check the GCP documentation.

5 Implementing BYOK

This section describes the process of implementing BYOK. Each step of the implementation process is described separately for GUI users, and for CLI users.

5.1 Create Cryptographic Key on GCP KMS

5.1.1 GUI: Create Cryptographic Key on GCP KMS

First, a symmetric cryptographic key with no key material associated is created.

1. Go to the **Key Management** under **Security** page in the Cloud Console.

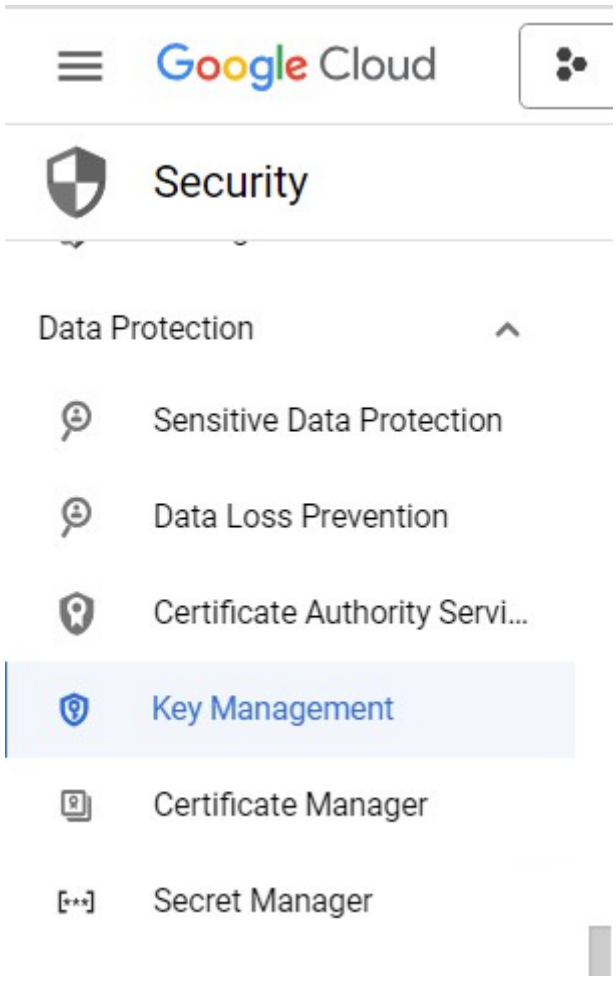

Figure 1 : Google Cloud Key Management

2. Click **Create key ring.**
3. In the **Key ring** name field, enter the name for your key ring.

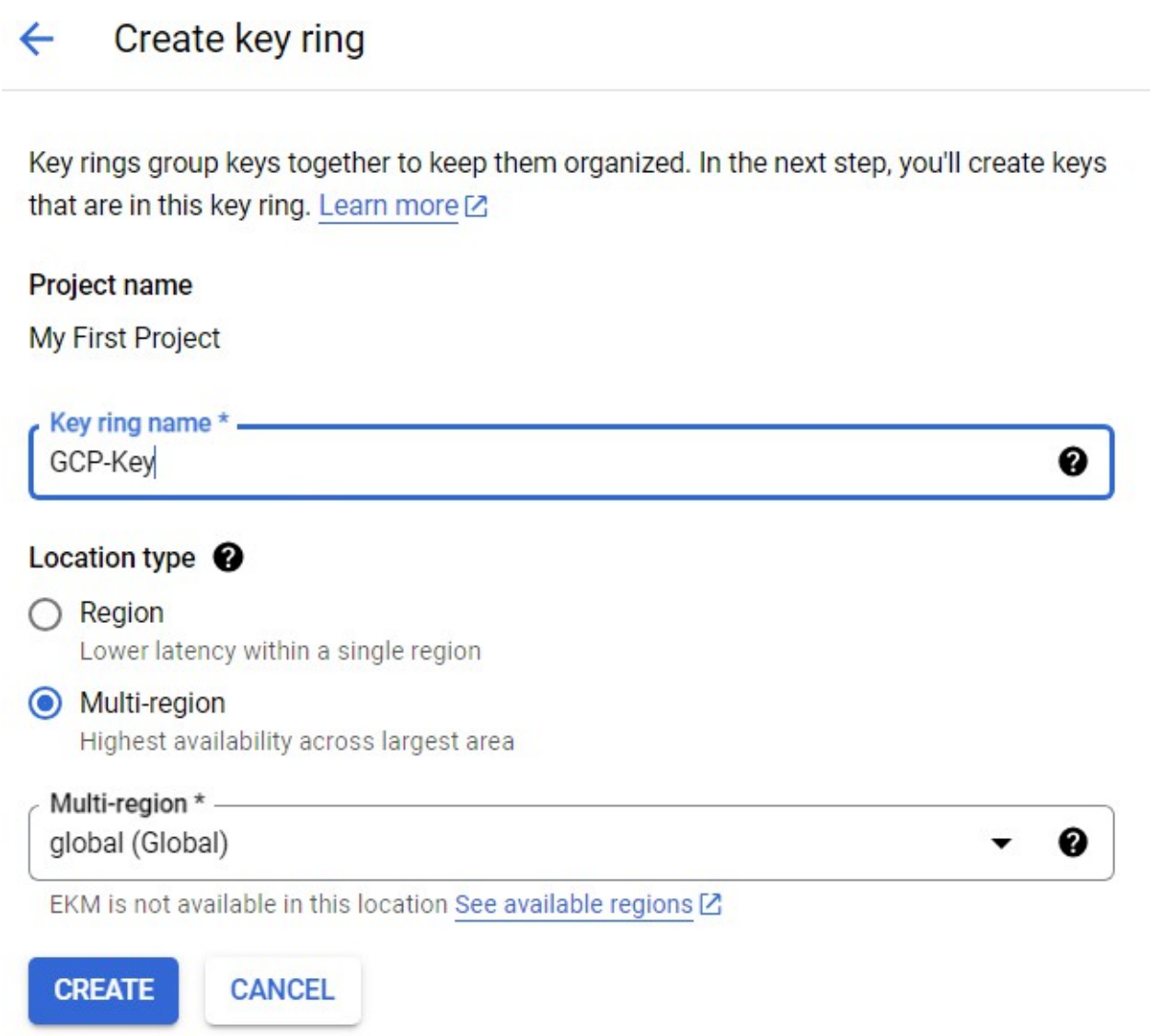

Figure 2 : Create keyring window

4. From the **Location** dropdown menu, select the location.
5. Click **Create.** The detail page for the key ring will open.
6. Click **Create key.**

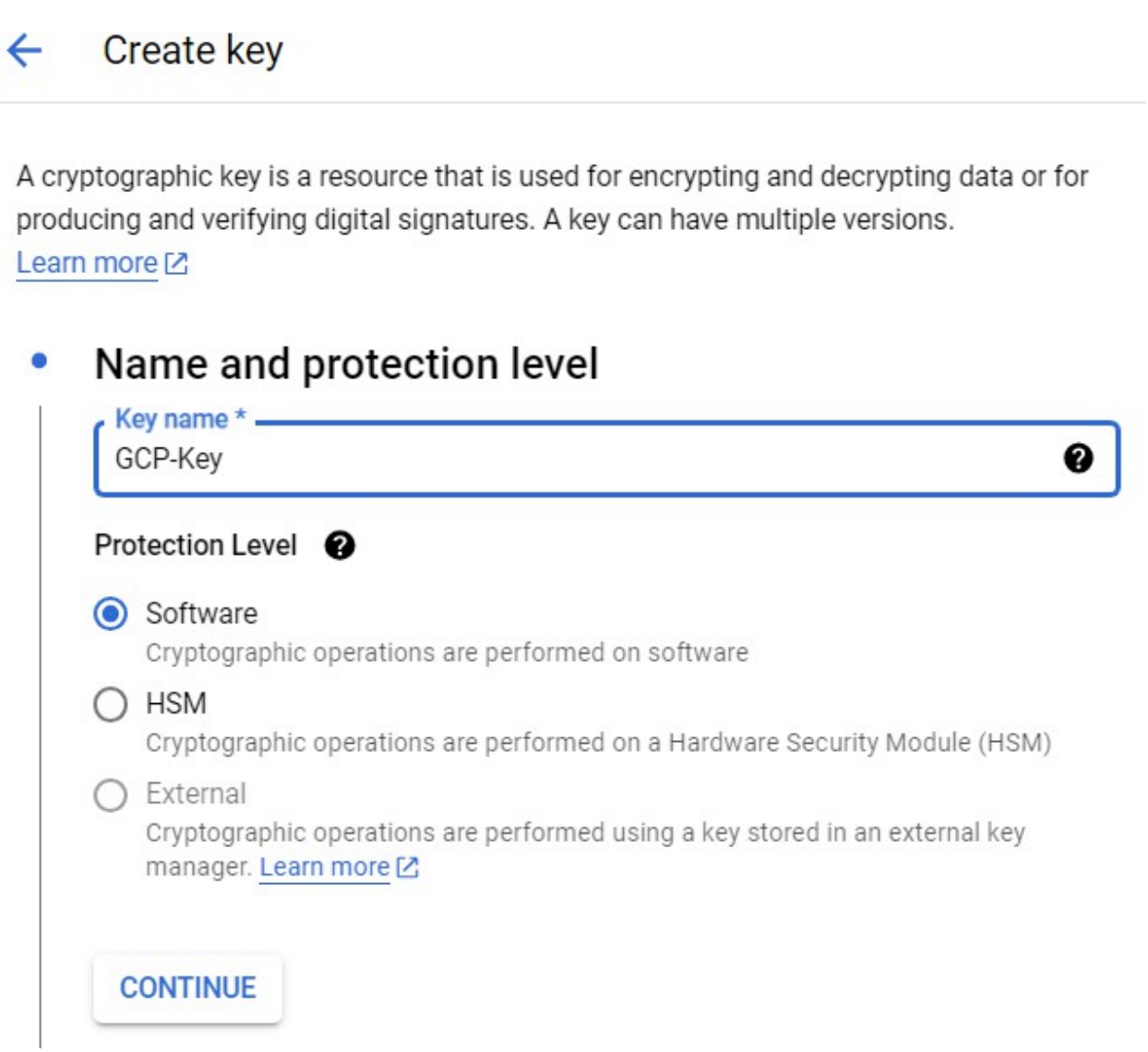

Figure 3 : Setting Key name and Protection Level

7. In the **Key name** field, enter the name for your key.
8. Set the protection level to **Software.**
9. Click **CONTINUE.**
10. Select **Imported key** in the **Key material**. This prevents an initial key version from being created.

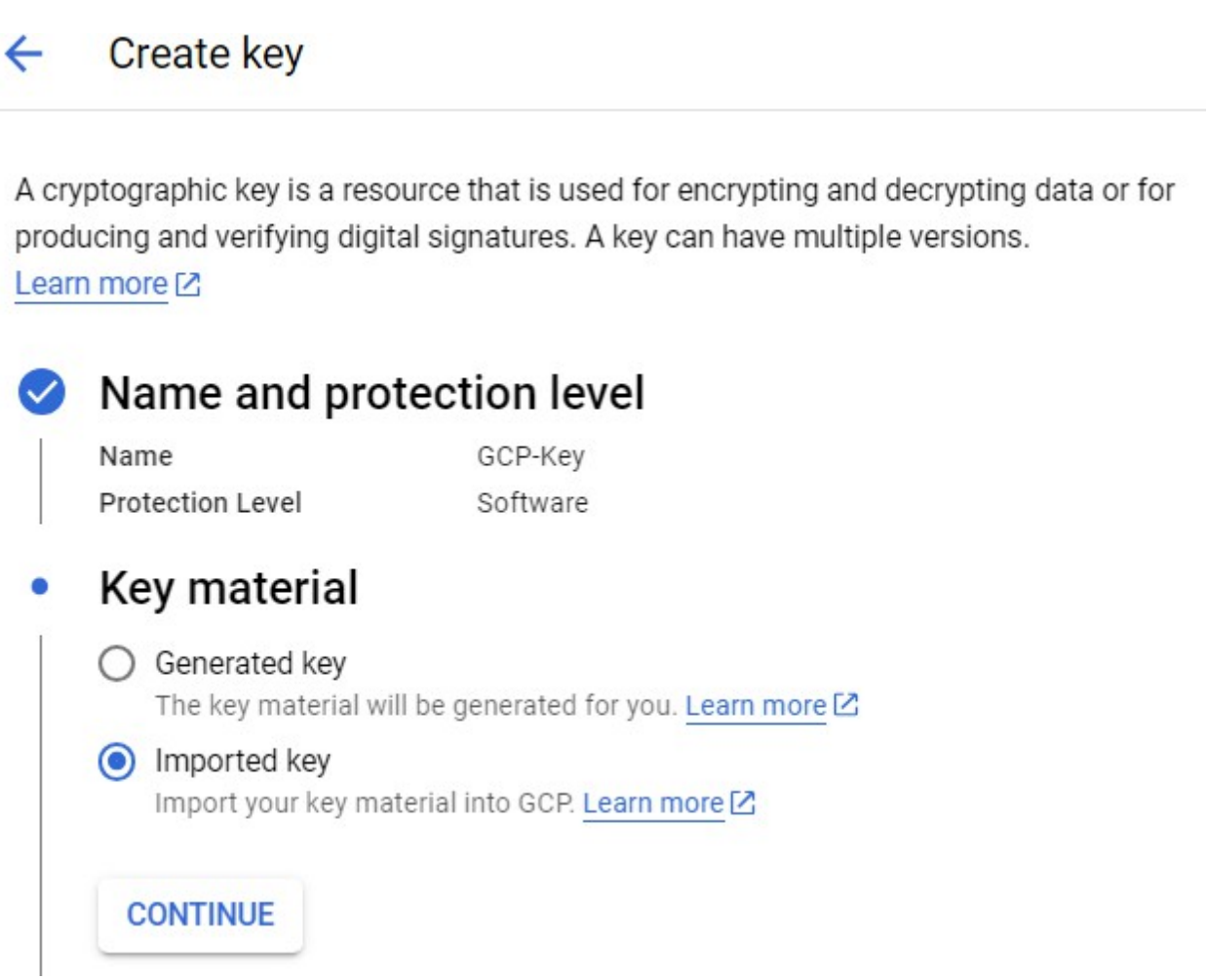

Figure 4 : Setting Key material type

11. Click **CONTINUE**.
12. Set **Purpose and algorithm** to **Symmetric encrypt/decrypt** as the key we are going to import is AES Key and its purpose will be to do symmetric encrypt/decrypt.

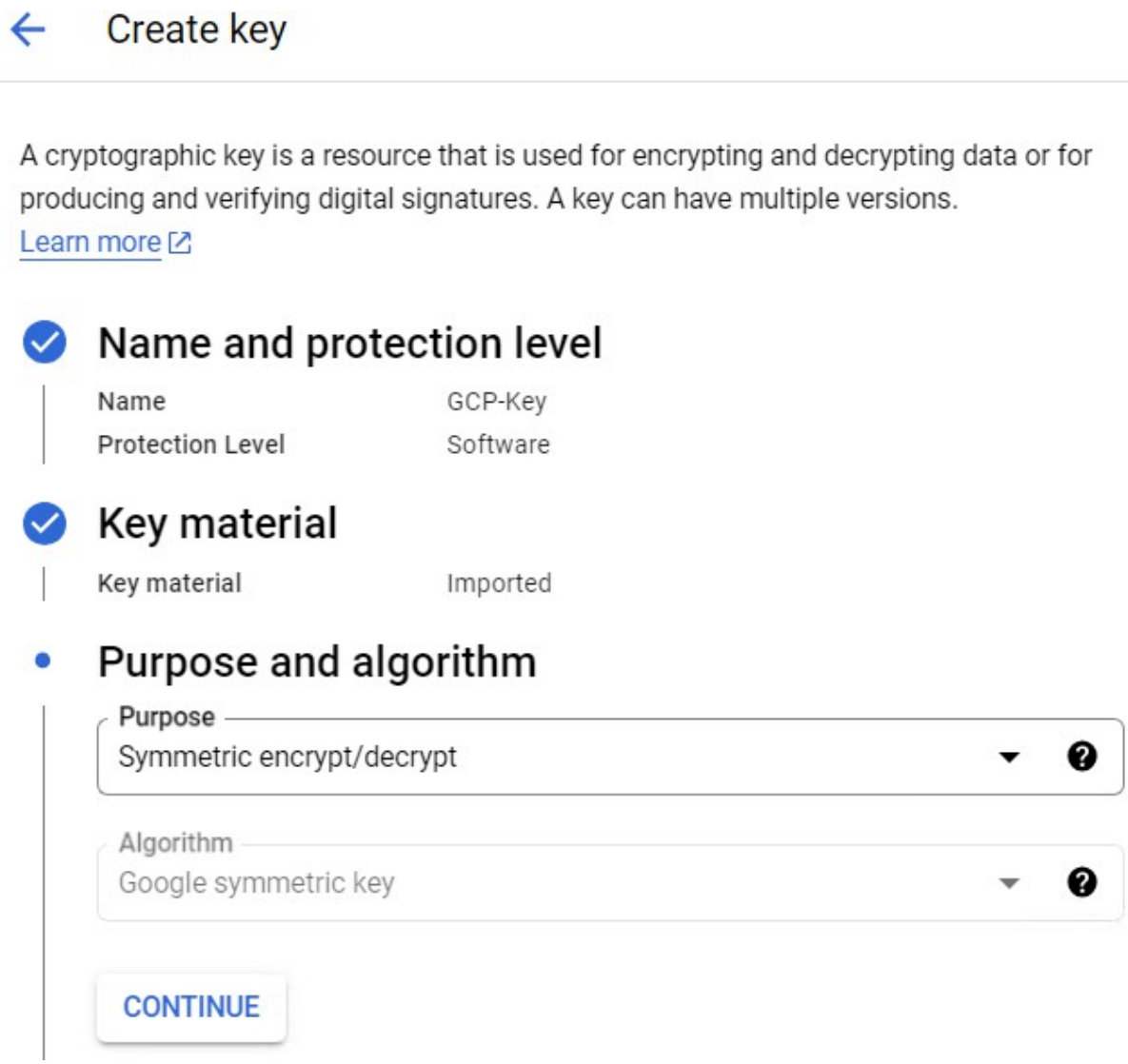

Figure 5 : Setting up Purpose and algorithm

13. Click **CONTINUE**.
14. On **Version** click **Continue** with default value.
15. Optionally, in the **Labels** field, click **Add label**, if you want to add a label to your key.

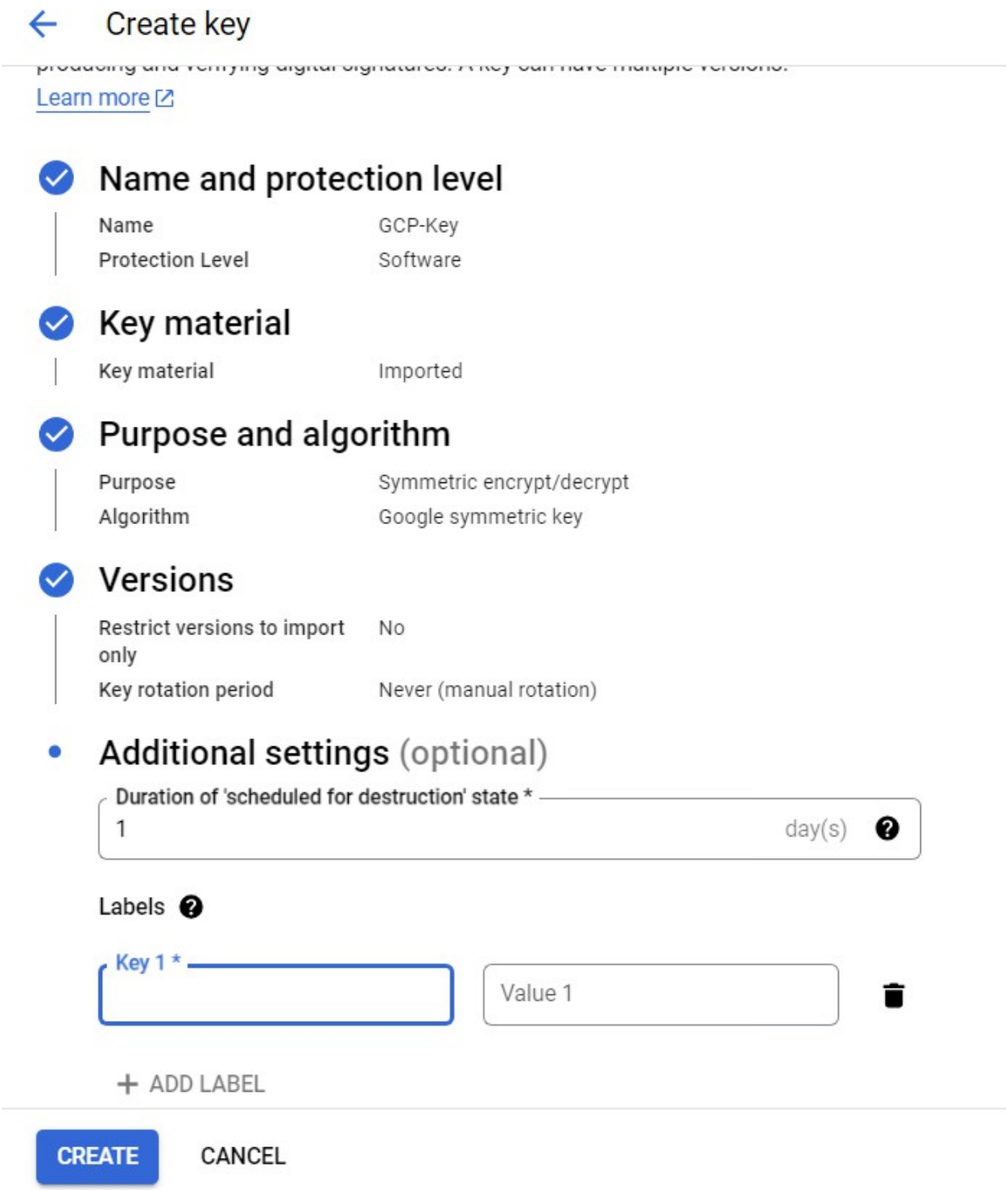

Figure 6 : Adding Labels

16. Click **Create**.

For the imported keys, automatic rotation is disabled by default. If you enable automatic rotation, new key versions will be generated in the Cloud KMS, and the imported key version will no longer be the default key version after a rotation.

5.1.2 CLI: Create Cryptographic Key on GCP KMS

1. Create the target key ring.

›_ Console

```
> gcloud kms keyrings create <key-ring-name> --location <location>
```

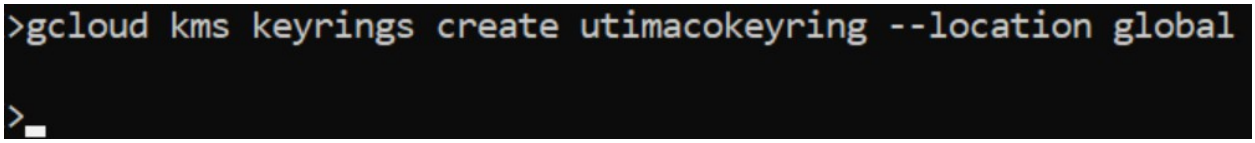

Figure 7 : Google Cloud Keyring creation

2. Create the target key.
    a. Set the key's purpose:
        i. For a symmetric key, set the purpose to "encryption".
        ii. For an asymmetric key, set the purpose to either "asymmetric-signing" or "asymmetric-encryption".
    b. Prevent an initial version from being created by using the `--skip-initial-version-creation` flag.
    c. Do not set the protection level.
    d. Do not specify an algorithm for the target key. Specify the algorithm of the imported key as a part of the import request.

›_ Console

```
> gcloud kms keys create <key-name> --location <location> --keyring <key-ring-
name> --purpose <purpose> --import-only --skip-initial-version-creation
```

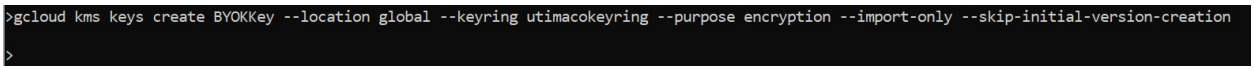

Figure 8 : Creating imported key

For the imported keys, automatic rotation is disabled by default. If you enable automatic rotation, new key versions will be generated in the Cloud KMS, and the imported key version will no longer be the default key version after a rotation.

5.2 Create Import Job and Download Corresponding Public Key

An import job defines the characteristics of the keys that it imports, including properties that cannot be changed after the key was imported.

5.2.1 GUI

1. Go to the **Key Management** page in the Cloud Console.
2. Click the name of the **Target key ring**.
3. Click **Create import job**.

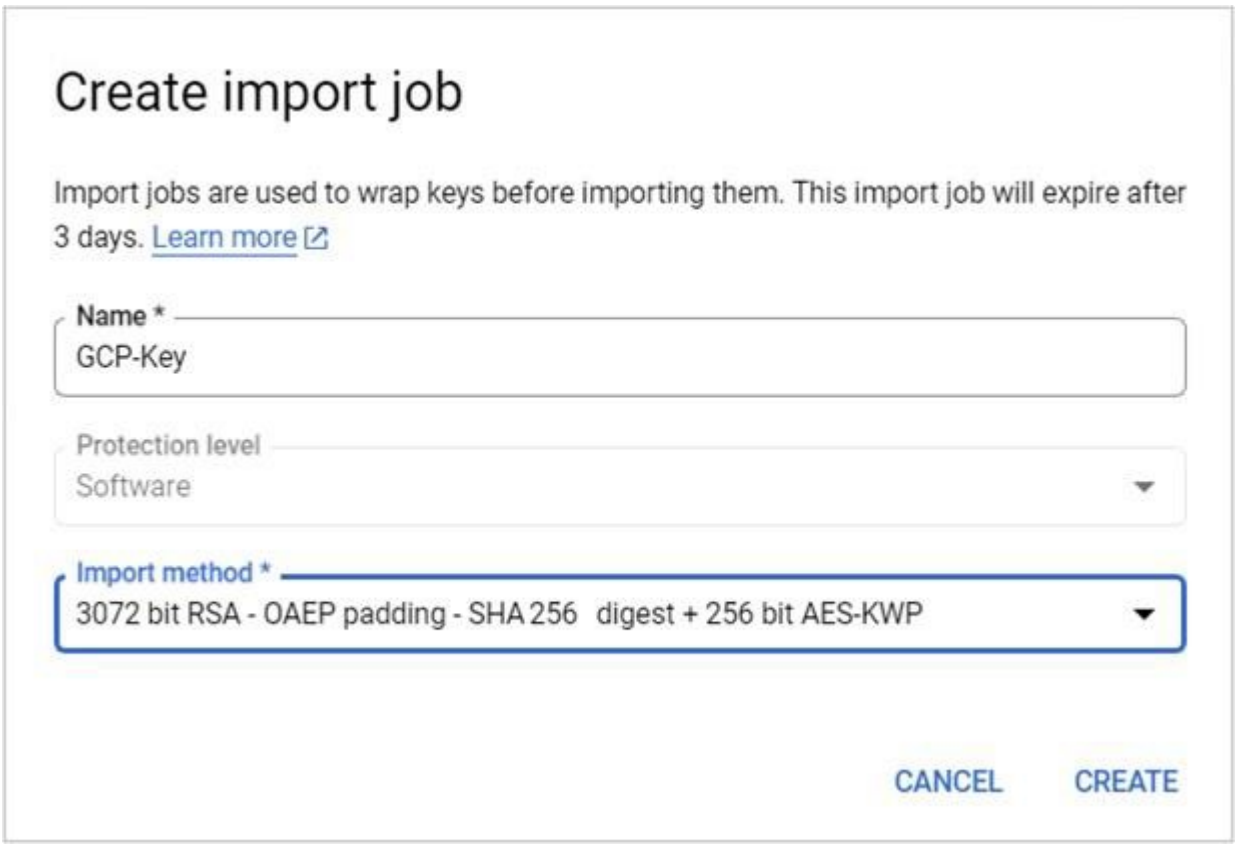

Figure 9 : Create import job window

4. In the **Name** field, enter the name for your import job.
5. From the **Import method** dropdown menu, set the import method to either **3072-bit RSA** or **4096-bit RSA -OAEP padding -SHA256 digest +256bit AES-KWP**.
6. Click **Create**.
7. Click **DOWNLOAD WRAPPING KEY.**

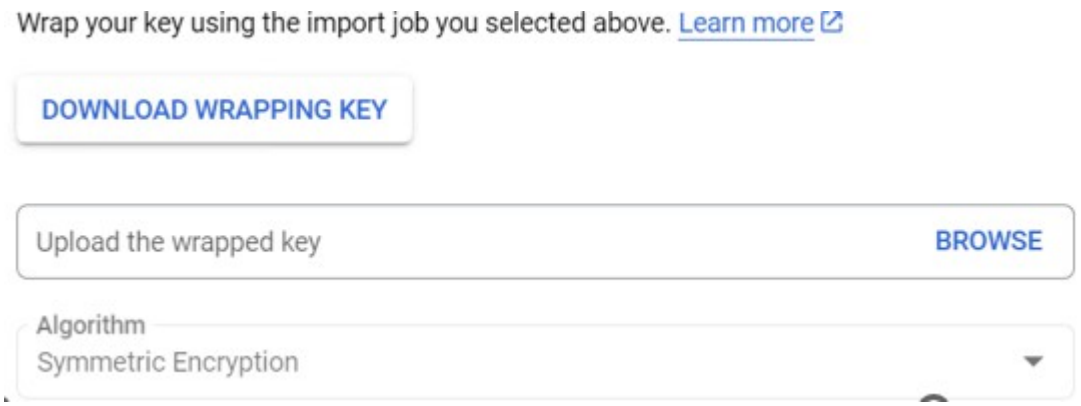

Figure 10 : Downloading wrapping key

8. Alternatively, you can click on **Import Job** tab and select the import job that you have just created and follow below steps to download wrapping key.
    a. In the **Actions** column click the three vertical dots.
    b. Click **Download wrapping key**.

The `<name_of_import job>.pem` file is automatically downloaded to your workstation.

5.2.2 CLI

1. To create an import job, follow the steps as described below:
    a. Use the same key ring and location as the target key.
    b. Set the protection level to either `software` or `hsm`.
    c. Set the import method to either `rsa-oaep-3072-sha256-aes-256` or `rsa-oaep-4096-sha256-aes-256`.

›_ Console

```
> gcloud kms import-jobs create <import-job> --location <location> --keyring
<key-ring-name> --import-method <import-method> --protection-level
<protection-level>
```

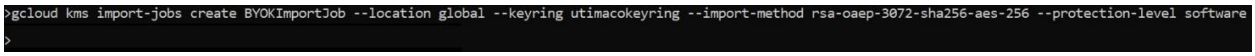

Figure 11 : Creating import job

2. To verify that the import job is active, run the following command.

›_ Console

```
> gcloud kms import-jobs describe <import-job> --location <location> --keyring

<key-ring-name> --format="value(state)"
```

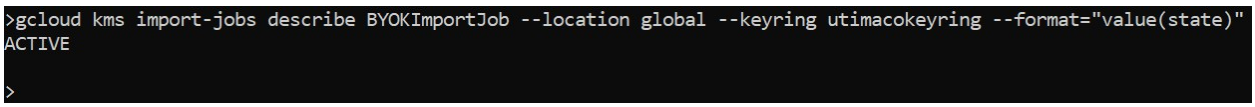

Figure 12 : Verifying import job status

3. Run the following command to save the public key of the import job.

›_ Console

```
> gcloud kms import-jobs describe --location=<location> --keyring=<keyring> --
format="value(publicKey.pem)" <import-job-name> > wrapping-key.pem
```

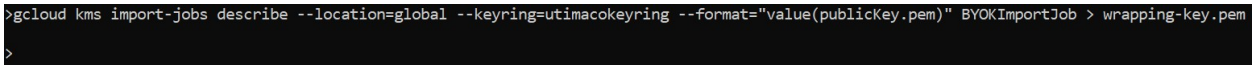

Figure 13 : Downloading wrapping key

5.3 Generating and Wrapping Your Key

Make sure that you created a user that can manage crypto operations (CryptoUser) by following the steps described in Initializing PKCS#11 on HSM.

The key will be stored to the Internal Key storage of the HSM.

5.3.1 GUI: Generating and Wrapping Your Key

1. Open the P11CAT.
2. Select the appropriate **Slot** and login as **Normal User**.
3. Click **Object Management**.
4. Click **Generate** -> **Generate Key**.
5. Chose **Mechanism**: AES.
6. In the **Create Attribute List** write:

"CKA_LABEL=<key_label>,CKA_ID=<key_ID>,CKA_EXTRACTABLE=CK_TRUE"

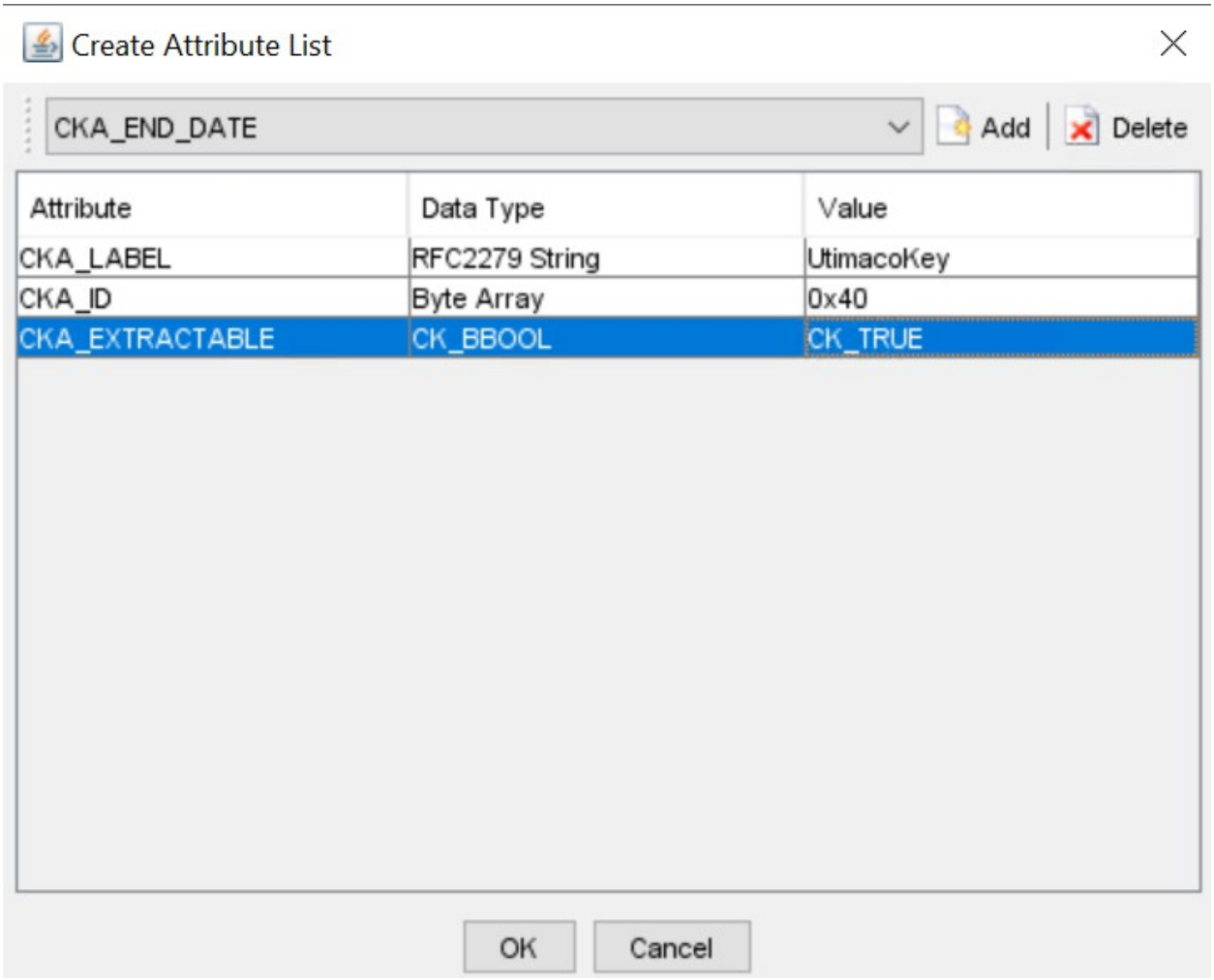

Figure 14 : Setting key parameters

7. Click **OK** and then click **Generate**.
8. The key is now generated. It still needs to be wrapped by using the Utimaco byoktool.
9. Navigate to the folder where you have the byoktool saved. Execute the following command to wrap the key by using the public key downloaded from Google Cloud KMS:

›_ Console

```
> byoktool Dev=<IP_of_UTIMACO_HSM> LogonPass=USR_0000,<user_password>
Label="<key_label>" CSP=gcp PublicKey=<Wrapping_Key_File>"
WrappedKey="<Wrapped_Key_OutputFile>"
```

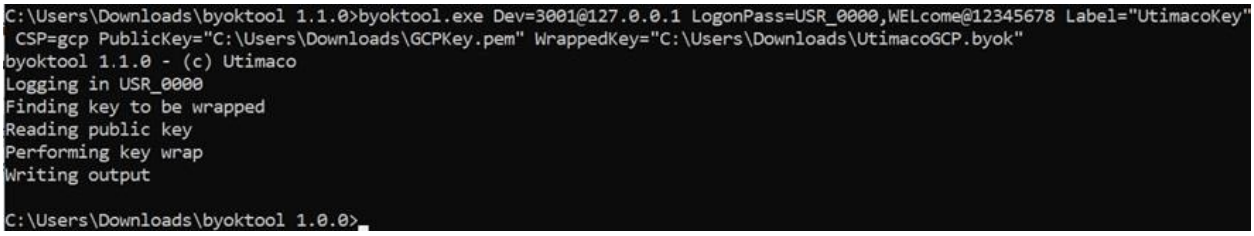

Figure 15 : Wrapping key with byoktool

5.3.2 CLI: Generating and Wrapping Your Key

1. Use the following command to generate an AES key:

›_ Console

```
> p11tool2 Slot=<slot_ID> LoginUser=ask KeyAttr=CKA_LABEL=<key_label>,CKA_ID=
<key_ID>,CKA_EXTRACTABLE=CK_TRUE GenerateKey=AES
```

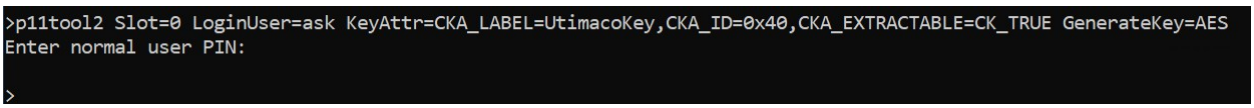

Figure 16 : Creating key with p11tool2

2. Navigate to the folder where you have the byoktool saved. Execute the following command to wrap the key by using the key, downloaded from GCP:

›_ Console

```
> byoktool Dev=<IP_of_UTIMACO_HSM> LogonPass=USR_0000,<user_password> Label="
<key_label>" CSP=gcp PublicKey=<Wrapping_Key_File>"
WrappedKey="<Wrapped_Key_OutputFile>"
```

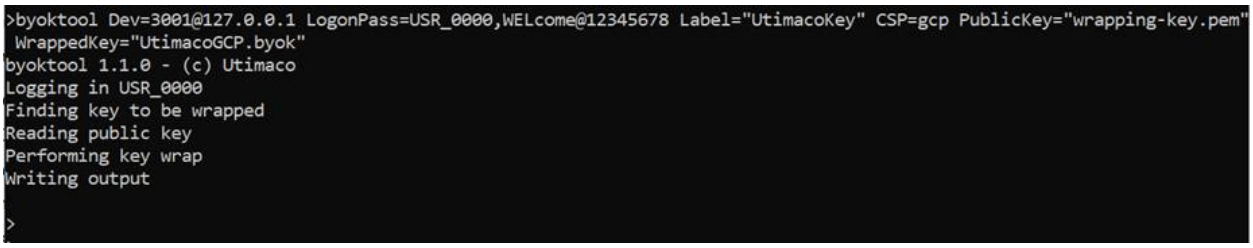

Figure 17 : Wrapping key with byoktool

5.4 Importing Wrapped Key to GCP KMS

5.4.1 GUI: Importing Wrapped Key to GCP KMS

1. Open the Cryptographic Keys page in the Cloud Console.
2. Click the name of the key ring that contains your import job. The target key is shown, along with any other keys on the key ring.

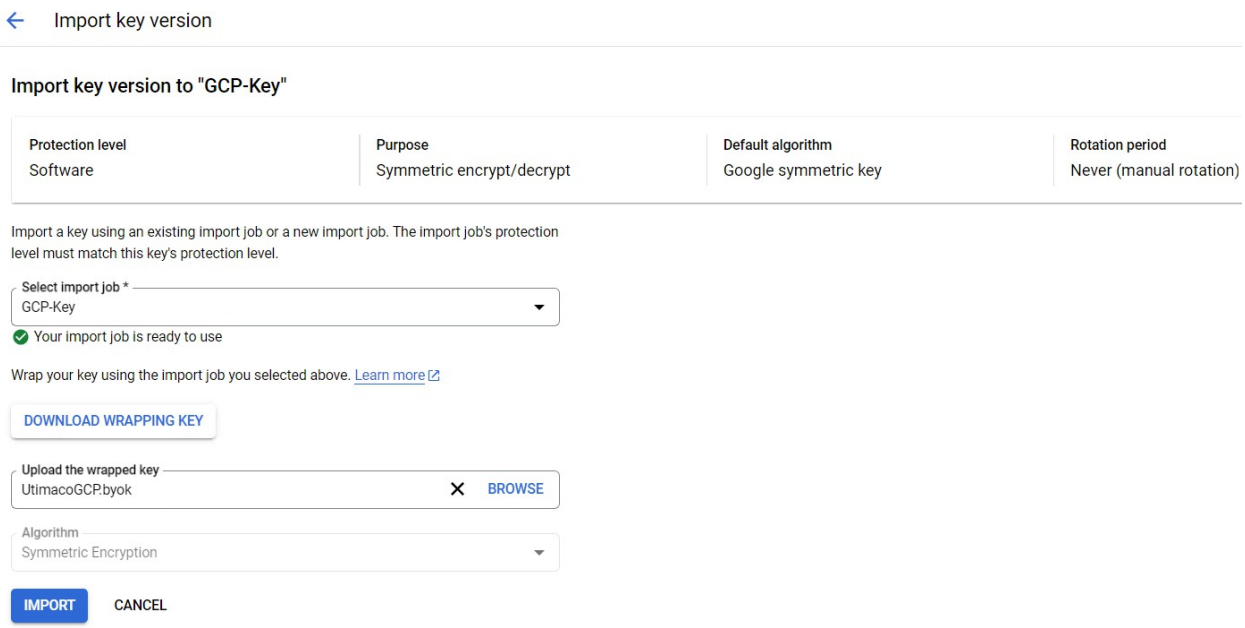

Figure 18 : Import key version window

3. Click the name of the target key, then click **Import key version**.
4. Select your import job from the **Select import job** dropdown menu.
5. In the **Upload the wrapped key** selector, select the key file that you have already wrapped.
6. Click **Import**.
7. Click on three dots under **Actions** and make this version as Primary.

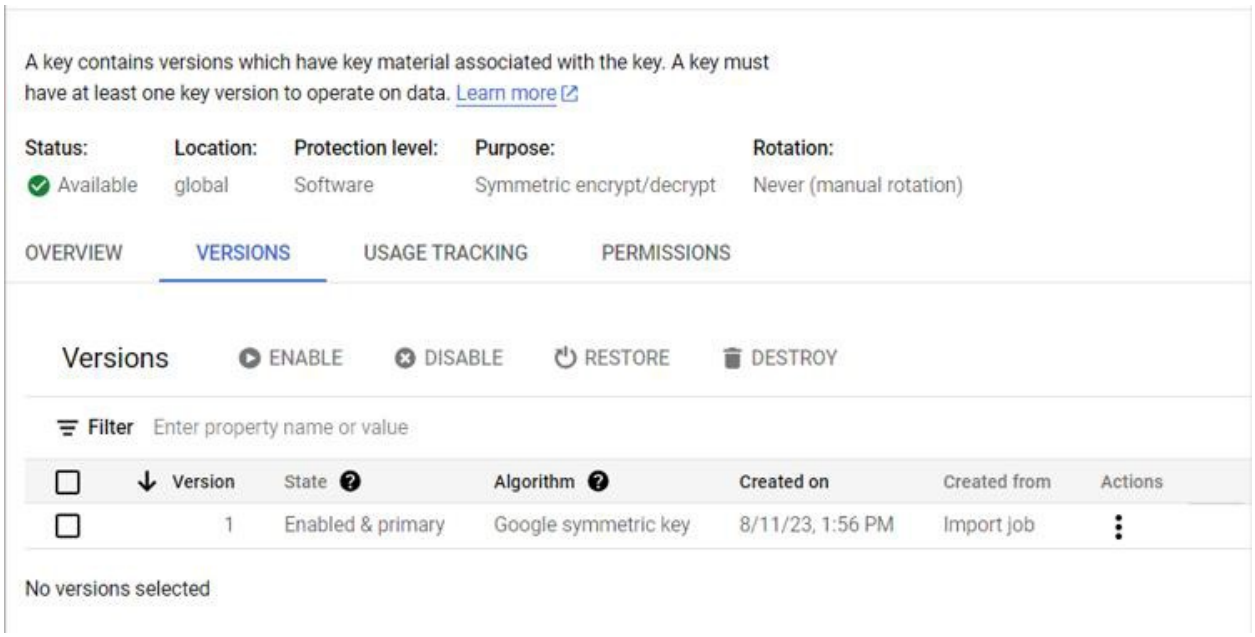

Figure 19 : Setting imported key version as primary

5.4.2 CLI: Importing Wrapped Key to GCP KMS

1. To import your WrappedKey.byok into GCP KMS, use the following command.

›_ Console

```
> gcloud kms keys versions import --import-job <import-job> --location
<location> --keyring <key-ring-name> --key <KEY_NAME> --algorithm <algorithm-
name> --wrapped-key-file <path-to- WrappedKey.byok>
```

Figure 20 : Importing wrapped key file

The **key-import** request is initiated. The initial state for an imported key is **PENDING_IMPORT**. When the state is **ENABLED**, the key has been imported successfully. If the import fails, the status is **IMPORT_FAILED**.

2. List the version of the key and verify its status.

›_ Console

```
> gcloud kms keys versions list --keyring <key-ring-name> --location
<location> --key <KEY_NAME>
```

```
>gcloud kms keys versions list --keyring utimacokeyring --location global --key BYOKKey
NAME                                                                                                STATE
projects/weighty-country-390506/locations/global/keyRings/utimacokeyring/cryptoKeys/BYOKKey/cryptoKeyVersions/1  ENABLED

>
```

Figure 21 : Verifying key version and status

3. You can set this key version as Primary by using below command.

›_ Console

```
> gcloud kms keys set-primary-version <KEY_NAME> --location=<location> --
keyring=<key-ring-name> --version=<version_number>
```

```
>gcloud kms keys set-primary-version BYOKKey --location=global --keyring=utimacokeyring --version=1
createTime: '2023-08-25T06:27:23.845536183Z'
destroyScheduledDuration: 86400s
importOnly: true
name: projects/weighty-country-390506/locations/global/keyRings/utimacokeyring/cryptoKeys/BYOKKey
primary:
  algorithm: GOOGLE_SYMMETRIC_ENCRYPTION
  createTime: '2023-08-25T07:19:11.536777088Z'
  importJob: projects/weighty-country-390506/locations/global/keyRings/utimacokeyring/importJobs/BYOKImportJob
  importTime: '2023-08-25T07:19:11.903229357Z'
  name: projects/weighty-country-390506/locations/global/keyRings/utimacokeyring/cryptoKeys/BYOKKey/cryptoKeyVersions/1
  protectionLevel: SOFTWARE
  reimportEligible: true
  state: ENABLED
purpose: ENCRYPT_DECRYPT
versionTemplate:
  algorithm: GOOGLE_SYMMETRIC_ENCRYPTION
  protectionLevel: SOFTWARE

>
```

Figure 22 : Setting imported key version as primary

5.5 FIPS Requirements

All the steps are identical to the above, when the HSM is in the FIPS 140-2 approved mode. The only difference is that the backup of the entire key database is not possible. Please refer to additional documentation on the Utimaco product CD.

6 Troubleshooting

Error	Diagnosis
LoginUser= failed: 11.08.2023 09:58:41 src/p11adm_R2.c[429] p11_login: C_Login [type=1] returned Error 0x00000032 (CKR_DEVICE_REMOVED)	Check if HSM is reachable from host machine and HSM is up and running.
The CryptoServer PKCS#11 Library R3 is not initialized. Error CKR_CRYPTOKI_NOT_INITIALIZED occurred	PKCS#11 Slot is not initialized.

Table 6: List of errors and their diagnoses

7 Further Information

This document forms a part of the information and support which is provided by the Utimaco IS GmbH. Additional documentation can be found on the product CD in the Documentation directory.

All CryptoServer product documentation is also available at the Utimaco IS GmbH website: https://utimaco.com/.

8 References

Reference	Title/Company	Document No.
[CSADMIN]	CryptoServer – csadm Manual/Utimaco IS GmbH	2009-0003
[CSTrSh]	CryptoServer Troubleshooting/Utimaco IS GmbH	M011-0008-en
[CSADMIN2]	CryptoServer_csadm_Manual_Systemadministrators.pdf	2009-0003
[CSP11Tool2]	CryptoServer_p11tool2_Manual.pdf	2012-0004
[CSPKCSM]	CryptoServer - PKCS#11 P11CAT Manual	M013-0001-en
[CSLAN5]	CryptoServerLAN_Manual_Systemadministrators.pdf	2018-0004

Table 7: References

9 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Str. 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

https://support.hsm.utimaco.com/support/rma/new

Other Support Queries

- Mail (preferred contact method)
  support@utimaco.com
  Attach the diagnostic information to your email.
- Web portal
  https://support.hsm.utimaco.com/support/cases/new/
  The diagnostic information will be requested in our response if necessary.
- By phone
  AMERICAS +1-844-UTIMACO (+1 844-884-6226)
  EMEA +49 800-627-3081
  APAC +81 800-919-1301
  The diagnostic information will be requested in our response if necessary.