Salesforce
Key Management Service BYOK

Integration Guide

u.trust GP HSM

utimaco®

Imprint

Copyright 2025	Utimaco IS GmbH
	Germanusstr. 4
	D-52080 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	2025-09-23
Status	PUBLISHED
Document No.	IG-2025-0009

Table of Contents

1 IG-2025-0009 Introduction

Thank you for purchasing our CryptoServer security system. We hope you are satisfied with our product. Please do not hesitate to contact us if you have any complaints or comments.

1.1 IG-2025-0009 About this Guide

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

1.1.1 IG-2025-0009 Target Audience for this Guide

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

1.1.2 IG-2025-0009 Document Conventions

We use the following document conventions:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Press **OK**
`Monospaced`	Code that is given for explanation or as an example, file paths	`chsm-create`
Italic	References and important terms	See *Sample Chapter* in the *CryptoServer - Sample Manual*

Table 1: Document conventions

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

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

Here, you find additional notes or supplementary information.

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

Certifications

Chapters with certification-specific content are marked accordingly at the beginning of the chapter, e.g. FIPS 140-3.

1.1.3 IG-2025-0009 Abbreviations

We use the following abbreviations in this guide:

Abbreviation	Meaning
HSM	Hardware Security Module
BYOK	Bring Your Own Key
PKCS#11	Public-Key Cryptography Standard #11
P11CAT	PKCS#11 Crypto Administration Tool
CLI	Command line interface
MBK	Master Backup Key
GUI	Graphical user interface

Table 2: List of Abbreviations

2 IG-2025-0009 Overview

2.1 IG-2025-0009 Salesforce

Salesforce is a customer relationship management solution that brings companies and customers together. It's one integrated CRM platform that gives all your departments — including marketing, sales, commerce, and service — a single, shared view of every customer.

2.2 IG-2025-0009 Utimaco CryptoServer HSM

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

2.3 IG-2025-0009 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.

2.4 IG-2025-0009 Utimaco ByokTool

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.

This Integration guide will focus on integrating with GCP KMS on Windows.

3 IG-2025-0009 Prerequisites and Requirements

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

3.1 IG-2025-0009 Software Requirements

Software	Software Requirements
Operating system	Windows, 64-bit, Linux, 64-bit
BYOK tool	byoktool, developed by Utimaco
Java	Version 8, Update 271 or higher

Table 3: List of Software Requirements

3.2 IG-2025-0009 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.30.0 or higher u.trust Anchor CSAR Series LAN with firmware 4.30.0 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.30.0 or higher u.trust Anchor CSAR Series PCIe with firmware 4.30.0 or higher

Table 4: List of Hardware Requirements

4 IG-2025-0009 Implementing BYOK

4.1 IG-2025-0009 Prerequisites

Each step of the implementation process is described separately for Graphical user interface (GUI), and for command line interface (CLI).

4.1.1 IG-2025-0009 Salesforce Shield Platform Encryption

Salesforce Bring Your Own Key (BYOK) is available as an add-on subscription in: Enterprise, Performance, and Unlimited Editions. Requires purchasing Salesforce Shield. Salesforce BYOK is also available in Salesforce Developer Edition at no charge for orgs created in Summer '15 and later.

Available in both Salesforce Classic and Lightning Experience.

4.1.2 IG-2025-0009 Salesforce CLI

In order to send the commands through the CLI, Salesforce CLI needs to be installed on the workstation.

4.1.3 IG-2025-0009 Salesforce user permissions

To generate, destroy, export, import, and upload tenant secrets and customer-supplied key material user permission for Manage Encryption Keys is needed.

To edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service the following user permissions are needed:

Manage Encryption Keys, Manage Certificates and Customize Application.

4.1.4 IG-2025-0009 Configured 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.

User permission levels of CryptoUser (00000002) will be needed.

4.1.5 IG-2025-0009 Utimaco BYOK Tool

To simplify the key export and import process of tenant keys, Utimaco has created an HSM Bring Your Own Key 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 Salesforce documentation.

4.2 IG-2025-0009 Create a Self-signed Certificate

To create a self-signed certificate in Salesforce classic please follow these next steps:

1. From **Setup**, in the **Quick Find box**, enter "Platform Encryption"
2. Select **Key Management**.
3. Click **Bring Your Own Key**.
4. Click **Create Self-Signed Certificate**.
5. Enter a unique name for your certificate in the Label field. The **Exportable Private Key, Key Size**, and **Use Platform Encryption** settings are pre-set and should be kept as such to ensure that your self-signed certificate is compatible with Salesforce Shield Platform Encryption.

When the **Certificate and Key Detail** page appears, click **Download Certificate**.

If you are not sure whether a self-signed or CA-signed certificate is right for you, consult your organization's security policy. See Certificates and Keys in Salesforce Help for more about what each option implies.

4.3 IG-2025-0009 Generating and Wrapping BYOK

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.

4.3.1 IG-2025-0009 GUI

1. Open the P11CAT.
2. Select the appropriate **Slot** and login as **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`
7. 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 Execute the following command to wrap the key material by using the certifcate downloaded from Salesforce:

   ›_ Console

   ```
   > byoktool dev=<Utimaco_CryptoServer_HSM_IP>
   LogonPass=<user>,<user_password> Label="<key_label>" csp=salesforce
   publickey=<downloaded_salesforce _certificate> wrappedkey=WrappedKey.dat
   hash=Hash_of_wrapped_key.hash
   ```

4.3.2 IG-2025-0009 CLI

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

   ›_ Console

   ```
   > p11tool2 Slot=<slot_ID> LoginUser=<user_password>
   KeyAttr=CKA_LABEL=<key_label>,CKA_ID=<key_ID>,CKA_EXTRACTABLE=CK_TRUE
   GenerateKey=AES
   ```
2. Navigate to the folder where you have the byoktool Execute the following command to wrap the key by using the key, downloaded from GCP:

›_ Console

```
> byoktool.exe Dev=<IP_of_UTIMACO_HSM> LogonPass=USR_0000,<user_password>
Label="<key_label>" CSP=gcp PublicKey=" C:\wrappingKey.der" WrappedKey="C:
\WrappedKey.byok"
```

Make sure to have appropriate permissions to be able to generate keys on the HSM as well as to write files in the directory.

4.4 IG-2025-0009 Importing Wrapped Key to Salesforce

1. From **Setup**, in the **Quick Find box**, enter "Platform Encryption"
2. Select **Key Management**.
3. Click **Bring Your Own Key**.
4. In the **Upload Tenant Secret** section, attach both the encrypted key material and the hashed plaintext key material and click **Upload**.

4.5 IG-2025-0009 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.

5 IG-2025-0009 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:

http://hsm.utimaco.com

6 IG-2025-0009 Contact 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
Germanusstr. 4
52080 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.