Salesforce

Shield Platform Encryption BYOK

Integration Guide

CryptoServer HSM

SecurityServer v4.55.0

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	2026-07-03
Status	PUBLISHED
Document No.	IG-2026-0048

Table of Contents

1 Introduction 5
1.1 About This Guide 5
1.1.1 Target Audience for This Guide 5
1.1.2 Document Conventions 5
1.1.3 Abbreviations 6
2 Overview 8
2.1 Salesforce 8
2.2 Utimaco SecurityServer HSM 8
2.3 Utimaco u.trust Anchor 8
2.4 Utimaco ByokTool 8
3 Integration Requirements and Prerequisites 9
3.1 Tested Versions 9
3.2 Software Requirements 9
3.3 Hardware Requirements 10
3.4 Prerequisites 10
4 Installing and Configuring Utimaco SecurityServer Software 12
4.1 On Linux 12
4.1.1 Download and Install Utimaco Software 12
4.1.2 SecurityServer PKCS#11 Configuration 13
4.1.3 Create SO User and Initialize a Slot 14
4.2 On Windows 15
4.2.1 Update cs_pkcs11_R3.cfg 15
4.2.2 Create an SO User and Initialize a Slot 16
5 Implementing BYOK 18
5.1 Salesforce Shield Platform Encryption 18
5.2 Salesforce User Permissions 18
5.3 Utimaco BYOK Tool 18
5.4 Create a Self-Signed Certificate 19
5.5 Generating and Wrapping BYOK 20
5.5.1 Generating HSM Key using GUI 20
5.5.2 Generating HSM Key using CLI 21

5.5.3 Wrapping HSM Key 21
5.6 Importing Wrapped Key to Salesforce 22
5.7 FIPS Requirements 23
6 Troubleshooting 24
7 Further Information 25
8 References 26
9 Contact and Support Information 27

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/.

1.1 About This Guide

This guide describes how to bring your own key into the Salesforce Shield Platform Encryption Bring Your Own Key service with the Utimaco HSM.

1.1.1 Target Audience for This Guide

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

1.1.2 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.

1.1.3 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
AES	Advanced Encryption Standard
BYOK	Bring Your Own Key
CA	Certificate Authority
CD	Compact Disc
CLI	Command line interface
CNG	Cryptography API Next Generation
CSADM	CryptoServer Command-line Administration Tool

Abbreviation	Meaning
CSAR	Cloud Service Architecture
CRM	Customer Relationship Management
CXI	Cryptographic eXtended Services Interface
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HSM	Hardware Security Module
ID	Identity
JCE	Java Cryptography Extension
KMS	Key Management Service
LAN	Local Area Network
PCIe	PCI Express Interface
PKCS#11	Public-Key Cryptography Standard #11
P11CAT	PKCS#11 Crypto Administration Tool

Table 2: List abbreviations

2 Overview

2.1 Salesforce

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

2.2 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.

2.3 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, performing sensitive cryptographic tasks, and securely managing, as well as storing, cryptographic keys and data. It can be used as a universal, independent security component for heterogeneous computer systems.

2.4 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 Salesforce KMS on Windows.

3 Integration Requirements and Prerequisites

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

3.1 Tested Versions

The Salesforce Shield Platform Encryption BYOK Service integrations that have been successfully tested with the Utimaco HSM.

Operating System	BYOK Tool Version	Utimaco Security Server Version	Utimaco HSM
Windows Server 2016 RHEL 8	BYOK tool 1.0.0	SecurityServer V4.55.0	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.

3.2 Software Requirements

Software	Software Requirements
BYOK tool	Byoktool 1.0.0 developed by Utimaco

Software	Software Requirements
HSM Software	Utimaco SecurityServer Software 4.55.0
HSM Interfaces	SecurityServer PKCS#11
P11tool2	p11tool2 from product package Utimaco SecurityServer 4.55.0
Java	Version 8, Update 271 or higher

Table 4: List of software requirements

3.3 Hardware Requirements

Hardware	Hardware Requirements
Utimaco LAN HSM	CryptoServer CSe-Series/Se-Series LAN with firmware SecurityServer 4.55.0 or higher u.trust Anchor Se*k and u.trust Anchor CSAR with firmware 4.55.0 or higher
Utimaco PCI-e HSM	CryptoServer CSe-Series/Se-Series PCI-e with firmware SecurityServer 4.55.0 or higher u.trust Anchor Se*k and u.trust Anchor CSAR with firmware 4.55.0 or higher

Table 5: List of hardware requirements

3.4 Prerequisites

Before you begin, please ensure:

- The SecurityServer is set up and configured. Refer to the SecurityServer documentation to set up the HSM.

- The SecurityServer Default Admin has been replaced with a new admin user.
- The MBK has been created and stored onto each HSM. Refer to the SecurityServer documentation to set up the MBK.
- The operating system used is listed in *Tested Versions*.
- The SecurityServer used is listed in *Tested Versions*.
- You familiarize yourself with Salesforce Shield Platform Encryption BYOK Service documents.

4 Installing and Configuring Utimaco SecurityServer Software

4.1 On Linux

4.1.1 Download and Install Utimaco Software

If you have not already done so, please create and request an Utimaco Support Portal Account. This will allow you to download the software components needed for this installation.

1. Copy the downloaded software at the appropriate location on the client machine where you will install the Utimaco software.
2. Create an `utimaco` folder under the `/opt` directory, and further create 2 directories; `/opt/utimaco/bin` and `/opt/utimaco/lib`.

›_ Console

```
# mkdir -p /opt/utimaco/bin

# mkdir /opt/utimaco/lib
```

3. Copy the pkcs11 library file `libcs_pkcs11_R3.so` from the Utimaco SecurityServer software to the `/opt/utimaco/lib` directory.

›_ Console

```
# cp ~/path_to_application_folder/lib/libcs_pkcs11_R3.so /opt/utimaco/lib
```

4. Copy the `csadm` and `p11tool2` files from the Utimaco SecurityServer software to the `/opt/utimaco/bin` directory, and make both the files executable.

›_ Console

```
# cd ~/path_to_application_folder

# cp csadm p11tool2 /opt/utimaco/bin

# chmod +x /opt/utimaco/bin/csadm /opt/utimaco/bin/p11tool2
```

4.1.2 SecurityServer PKCS#11 Configuration

1. Create the directory `/etc/utimaco`. Locate the Utimaco PKCS#11 configuration file in your SecurityServer directory, `Linux/x86-64/Crypto_APIS/PKCS11_R3/sample`.

Copy the Utimaco PKCS#11 configuration file `cs_pkcs11_R3.cfg` into the `/etc/utimaco` directory.

›_ Console

```
# mkdir /etc/utimaco

# cd <install directory>/Software/Linux/x86-64/Crypto_APIs/PKCS11_R3/sample # cp
cs_pkcs11_R3.cfg /etc/utimaco # cd /etc/utimaco
```

2. Edit the `cs_pkcs11_R3.cfg` file and make the appropriate changes to it.

cs_pkcs11_R3.cfg

```
[Global]
# For unix:
Logpath = /tmp
# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 1
Keepalive = true
# Set the Device to connect with
[CryptoServer]
# Device specifier
Device = <HSM_IP>
```

For more information regarding the commands and command parameters, please check the Utimaco CryptoServer documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor: Device = 288@<HSM IP address> Hardware (LAN) HSM

OR

Device = /dev/cs2.0 Hardware (PCIe) HSM

To make your testing easier, it would be good to enable the PKCS#11 log file. That can be enabled by editing the **Logging Loglevel**. Set the **LogPath** and **Logging Loglevel** to **1**. For testing you may want to increase it to **4**.

The added **LogPath** points to a writable directory, not to a file.

If you encounter problems, check the log file named `cs_pkcs11_R3.log` in the **LogPath** defined directory. When you are done testing, you should change **Logging** to **1** or **2**. This will limit the logging to only critical and important messages.

4.1.3 Create SO User and Initialize a Slot

You must initialize a slot with a custom label using p11tool2.

›_ Console

```
# p11tool2 slot=<slot_no> Label=<token_label> Login=ADMIN,ADMIN.key
InitToken=<ask>

# p11tool2 slot=<slot_no> LoginSO=<ask> InitPin=<ask>
```

First, using p11tool2 create the Security Officer (SO). Then, using the `p11tool2` command initialize the Slot that you want to use, as well as the slot user, as shown below.

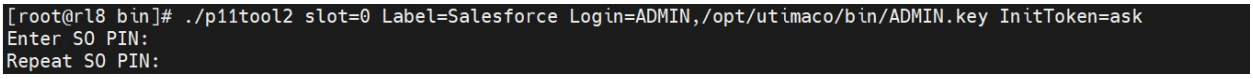

Figure 1 : Slot initialization output

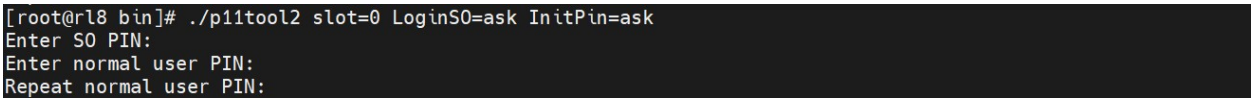

Figure 2 : Slot initialization output

4.2 On Windows

On Windows, as part of the CryptoServer software installation, `cs_pkcs11_R3.cfg` will be automatically created and will be available under the `C:\ProgramData\Utimaco\PKCS11_R3` folder.

4.2.1 Update cs_pkcs11_R3.cfg

Example Values

cs_pkcs11_R3.cfg

```
[Global]
# For windows:
Logpath = C:/ProgramData/Utimaco/PKCS11_R3
# Loglevel (0 = NONE; 1 = ERROR; 2 = WARNING; 3 = INFO; 4 = TRACE)
Logging = 1

# Prevents expiring session after inactivity of 15 minutes
KeepAlive = true

# Set the Device to connect with
[CryptoServer]
# Device specifier
Device = <HSM_IP>
```

For more information regarding the commands and command parameters please check the Utimaco CryptoServer documentation. The device may be a CryptoServer (PCIe or LAN) device. The device line will follow one of these patterns, based on the HSM form-factor:

Device = 288@<HSM IP address> Hardware (LAN) HSM

OR

Device = /dev/cs2.0 Hardware (PCIe) HSM

To make your testing easier, it would be good to enable the PKCS#11 log file. That can be enabled by editing the **Logging Loglevel**. Set the **LogPath** and **Logging Loglevel** to **1**. For testing you may want to increase it to **4**.

The added **LogPath** points to a writable directory, not to a file.

If you encounter problems, check the log file named `cs_pkcs11_R3.log` in the LogPath defined directory. When you are done testing, you should change **Logging** to **1** or **2**. This will limit the logging to only critical and important messages.

4.2.2 Create an SO User and Initialize a Slot

You must initialize a slot with a custom label using p11tool2 .

First, using p11tool2 create the Security Officer (SO). Then, using the `p11tool2` command initialize the Slot that you want to use, as well as the slot user.

Alternatively, you can use the p11CAT tool to initialize a token and create an SO user. After that, you can set the normal user PIN.

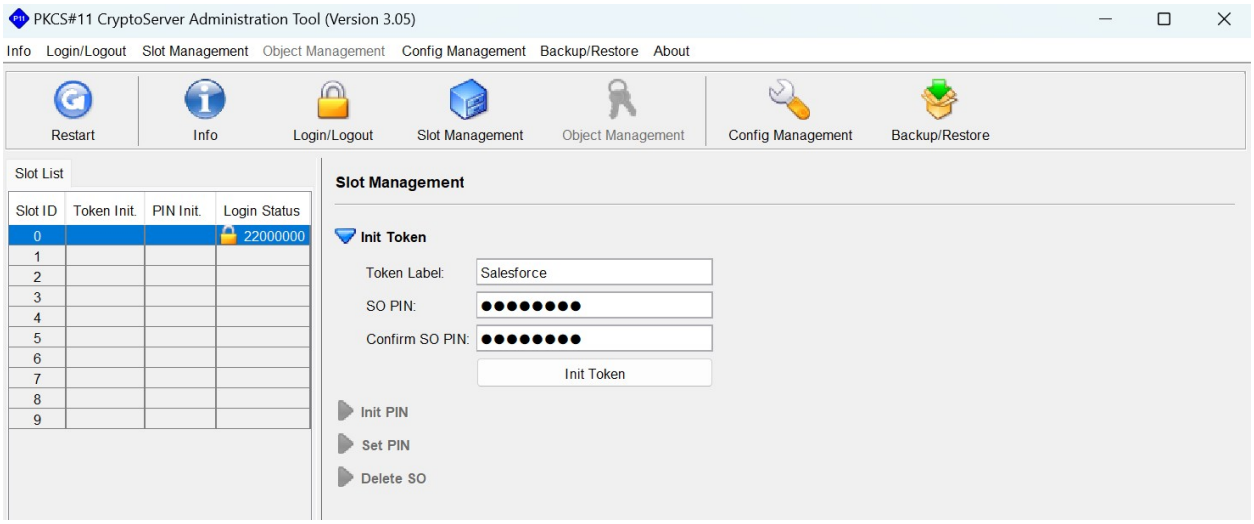

Figure 3 : Slot initialization console

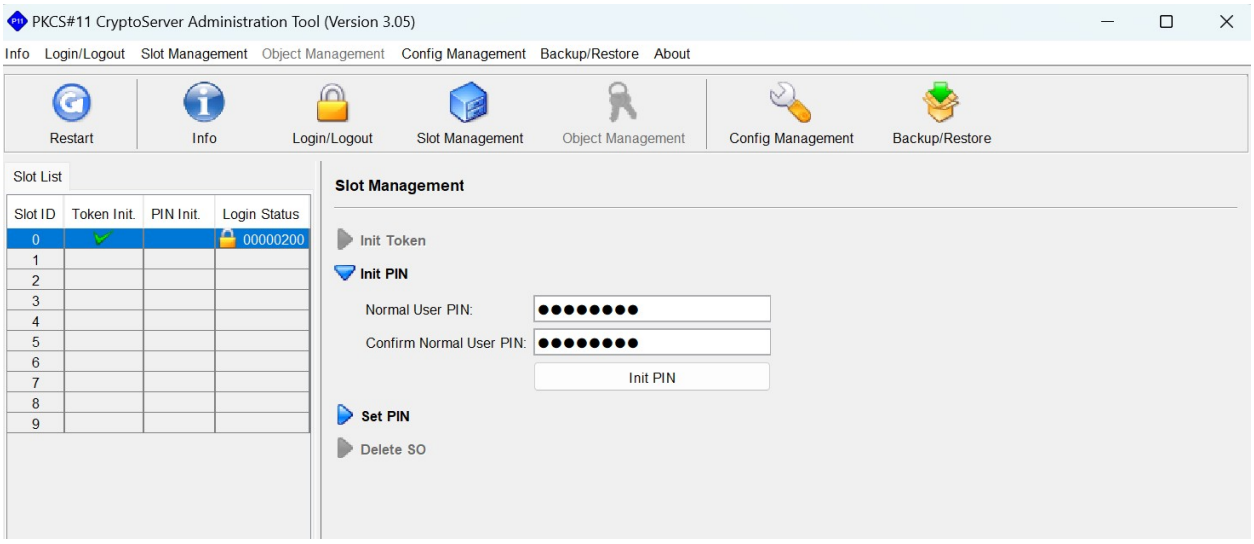

Figure 4 : Normal user PIN initialization

5 Implementing BYOK

5.1 Salesforce Shield Platform Encryption

Salesforce Bring Your Own Key (BYOK) is available as an add-on subscription in: Enterprise, Performance, and Unlimited Editions. It requires purchasing the 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.

5.2 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.

5.3 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.

5.4 Create a Self-Signed Certificate

To create a self-signed certificate in Salesforce classic, please follow the 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.

Figure 5 : Creating a self-signed certificate

6. 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.

5.5 Generating and Wrapping BYOK

Make sure that you created a user that can manage crypto operations (CryptoUser) by following the steps, described in Create SO User and Initialize a Slot section. The key will be stored to the Internal Key storage of the HSM.

5.5.1 Generating HSM Key using GUI

1. Open the P11CAT.
2. Select the appropriate **Slot** and log in 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**.

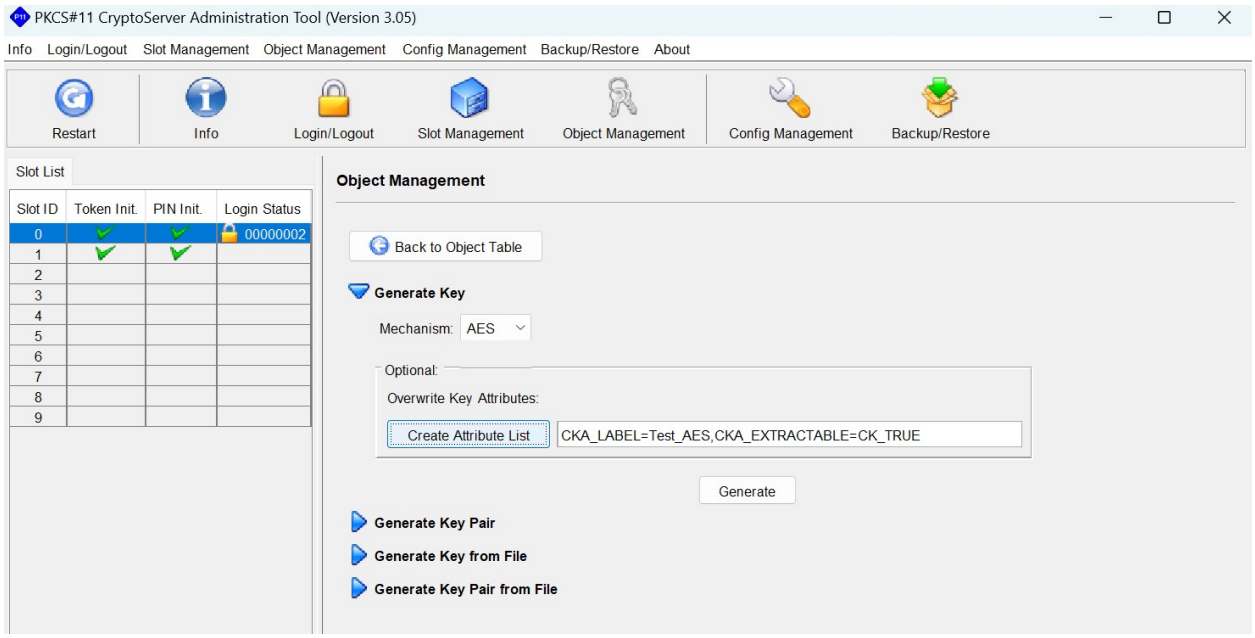

Figure 6 : Generating key using p11CAT tool

5.5.2 Generating HSM Key using CLI

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
```

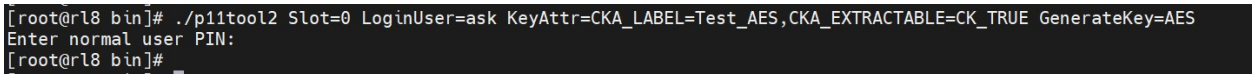

Figure 7 : Generating key using p11tool2

5.5.3 Wrapping HSM Key

1. Convert the public key downloaded from Salesforce to `der` format with the help of the `openssl` command.

›_ Console

```
> openssl rsa -in public.key -pubin -out public.der -outform der
```

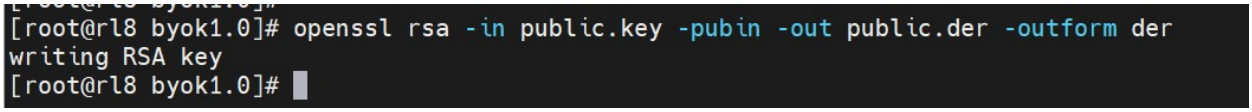

Figure 8 : Converting public key to der format

2. Navigate to the folder where you have the `byoktool` saved. Execute the following command to wrap the key material by using the public key in `der` :

›_ 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
```

```
[root@rl8 byok1.0]#  ./byoktool Dev=3001@localhost LogonPass=USR_0000,12345678 Label="Test_AES" csp=salesforce publickey=public.der wrappedkey=WrappedKe
y.dat hash=Hash_of_wrapped_key.hash
byoktool 1.0.0 - (c) Utimaco
Logging in USR_0000
Finding key to be wrapped
Reading public key
Performing key wrap
Writing output
[root@rl8 byok1.0]#
[root@rl8 byok1.0]#
```

Figure 9 : Wrapping HSM key using byoktool

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

5.6 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**.

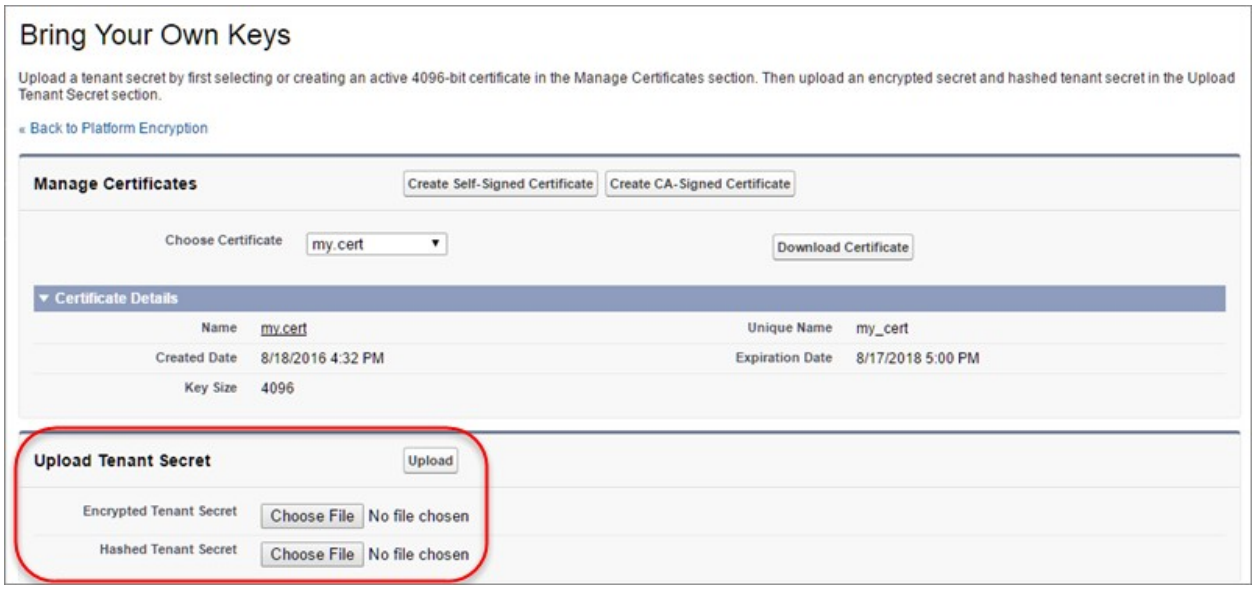

Figure 10 : Uploading encrypted tenant secret and hashed tenant secret to Salesforce

5.7 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
[root@rl8 byok1.0]# ./byoktool Dev=3001@localhost LogonPass=USR_0000,12345678 Label="Test_AES" csp=salesforce publickey=public.key wrappedkey=WrappedKey.dat hash=Hash_of_wrapped_key.hash byoktool 1.0.0 - (c) Utimaco Logging in USR_0000 Finding key to be wrapped Reading public key ERROR: ASN.1 unknown field	You need to convert the public key downloaded from Salesforce to `der` format with the help of the `openssl` command.

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 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

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.