JBoss

Enterprise Application Platform

7.4.0

Integration Guide

CryptoServer JCE Provider

SecurityServer 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	2026-07-21
Status	PUBLISHED
Document No.	IG-2026-0080

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/*.

1.1 About This Guide

This guide provides an integration guide explaining how to integrate an Utimaco CryptoServer Hardware Security Module (HSM) with JBoss EAP. Utimaco securely generates and stores the private keys of SSL certificate used by JBoss EAP.

1.2 Target Audience for This Guide

This guide is intended for administrators of JBoss Administrator and of Utimaco HSMs.

1.3 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.

1.4 Abbreviations

The following abbreviations are used in this guide:

Abbreviation	Meaning
CA	Certificate Authority
CSADM	CryptoServer Command-line Administration Tool
CSAR	Certificate Signing Request
CSR	Certificate Signing Request
CXI	Cryptographic eXtended Interface
EAP	Enterprise Application Platform
EC	Elliptic Curve

Abbreviation	Meaning
EE	Enterprise Edition
GUI	Graphical User Interface
HSM	Hardware Security Module
IP	Internet Protocol
JBoss	JavaBeans Open-Source Software
JCE	Java Cryptography Extension
JDK	Java Development Kit
LAN	Local Area Network
MBK	Master Backup Key
PCIe	PCI Express Interface
PIN	Personal Identification number
PKCS#11	Public-Key Cryptography Standard #11
P11CAT	PKCS#11 CryptoServer Administration Tool
RSA	Rivest, Shamir, Adleman (cryptosystem)
SSL	Secure Socket Layer

Abbreviation	Meaning
URL	Uniform Resource Locator

Table 2: List of abbreviations

2 Overview

2.1 JBoss EAP

JBoss EAP is an open-source platform for highly transactional, web-scale Java applications. JBoss EAP combines the familiar and popular Jakarta EE specifications with the latest technologies, like Eclipse MicroProfile, to modernize your applications from traditional Java EE into the new world of DevOps, cloud, containers, and microservices.

JBoss EAP includes everything needed to build, run, deploy, and manage enterprise Java applications in a variety of environments, including on-premises, virtual environments, and in private, public, and hybrid clouds. JBoss EAP is based upon the popular open-source project WildFly.

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 and 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 Integration Requirements and Prerequisites

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

3.1 Tested Versions

The integrations that have been successfully tested with the Utimaco HSM with JBoss.

Operating System	JBoss EAP Version	Utimaco Security Server Version	Utimaco HSM
Rhel 8	7.4.0	SecurityServer 4.55.0.0	CryptoServer CSe-Series/Se-Series u.trust Anchor Se*k and u.trust Anchor CSAR

Table 3: List of tested versions

3.2 Software Requirements

Software	Software Requirements
HSM Utility	csadm, cxitool
HSM Interfaces	CryptoServer JCE Provider
JBoss EAP	7.4.0
JAVA	OpenJDK 8u202

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 4.55.0.0 or higher u.trust Anchor Se*k and CSAR Series LAN 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 CSAR Series PCI-e 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/.

3.4 Prerequisites

Before you begin, please ensure that:

- The Utimaco CryptoServer HSM is set up and configured. Refer to the CryptoServer documentation to set up the HSM.
- The MBK has been created and stored onto each HSM. Refer to the CryptoServer documentation to set up the MBK.
- The CryptoServer Default Admin has been replaced with a new admin user.
- You have installed/set up an operating system listed in *Tested Versions*.
- You have installed/set up a SecurityServer listed in *Tested Versions*.
- There is a user with root privilege as it is required to install the packages.
- You allow port 8080, 8443 through firewall.

4 Installing and Configuring Utimaco SecurityServer Software

4.1 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 JBoss server.
2. Create utimaco folder under /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 jce library file `CryptoServerJCE.jar` from Utimaco SecurityServer software to the `/opt/utimaco/lib` directory.

›_ Console

```
# cp ~/path_to_application_folder/lib/ CryptoServerJCE.jar /opt/utimaco/lib
```

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

›_ Console

```
# cd ~/path_to_application_folder

# cp csadm ADMIN.key cxitool /opt/utimaco/bin

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

4.2 SecurityServer JCE Configuration

1. Locate the Utimaco JCE configuration file in your SecurityServer directory, `Linux/x86-64/Crypto_APIs/JCE/sample/CryptoServer.cfg`.
2. Create a user for JBoss EAP.

›_ Console

```
# useradd jboss
```

3. Log in to jboss user and copy the Utimaco JCE configuration file `CryptoServer.cfg` into jboss's home directory.

›_ Console

```
# cd <installation_directory>/Software/Linux/x86-

64/Crypto_APIs/JCE/sample/CryptoServer.cfg # cp CryptoServer.cfg $home
```

4. Open `/home/jboss/.bash_profile` and add the following line.

.bash_profile

```
export CRYPTOSERVER_JCE_CONFIG=/home/jboss/CryptoServer.cfg
```

5. Create one Cryptographic user with CXI group.

›_ Console

```
# csadm Dev=<HSM_IP> LogonSign=ADMIN,/opt/utimaco/bin/ADMIN.key AddUser=<

Cryptographic_user_name>,00000002{CXI_GROUP=<cxi_group_name>},hmacpwd,<PIN>
```

Figure 1 : User creation with csadm

6. Edit the `$home/CryptoServer.cfg` file and make the appropriate changes to the file.

CryptoServer.cfg

```
LogFile = /tmp/CryptoServerJCE.log
LogLevel = 1
LogSize = 10000
Device = <HSM_IP>
ConnectionTimeout = 3000
Timeout = 30000
KeepSessionAlive = 1
DefaultUser = <Cryptographic_User_Name>
KeyGroup = <CXI_Group_Name>
StoreKeysExternal = false
```

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 Cryptoserver JCE log file. That can be enabled by editing the **Logging Loglevel**. Set the **LogFile** and **Logging Loglevel** to 1. For testing you may want to increase it to 4. The added **LogFile** points to a file. If you encounter problems, check the log file named `CryptoServerJCE.log` in the **LogFile** defined file. When you are done testing, you should change **Logging** to 1 or 2. This will limit the logging to only critical and important messages.

5 JAVA Installation and Configuration

5.1 Installing JAVA

1. (Optional) It is recommended to update the system with latest security patch.

›_ Console

```
# dnf -y update
```

2. Download and extract Oracle OpenJDK 8.

›_ Console

```
# cd /opt

# tar -xvf jdk-8u202-linux-x64.tar.gz
```

5.2 Update java.security file to use Utimaco HSM

1. Copy the file CryptoServerJCE.jar for JAVA 8 from `/opt/utimaco/lib/` to `<javahome>/lib/ext`.

›_ Console

```
# cp /opt/utimaco/lib/CryptoServerJCE.jar /opt/jdk1.8.0_202/jre/lib/ext/
```

2. Go to the `<JDK_Installation_directory>/jre/lib/security` directory.

›_ Console

```
# cd /opt/jdk1.8.0_202/jre/lib/security/
```

3. Edit the `java.security` configuration file to add provider as highlighted below.

java.security

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=sun.security.ec.SunEC

security.provider.4=com.sun.net.ssl.internal.ssl.Provider
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=sun.security.jgss.SunProvider
security.provider.7=com.sun.security.sasl.Provider
security.provider.8=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.9=sun.security.smartcardio.SunPCSC

security.provider.10=CryptoServerJCE.CryptoServerProvider /home/ jboss /
CryptoServer.cfg
```

Specify correct provider number and path for CryptoServerJCE Provider.

6 Integrating JBoss EAP with Utimaco HSM

6.1 Installing JBoss EAP

1. Log in to the *Red Hat Customer Portal* and download Red Hat JBoss Enterprise Application Platform 7.4.0 Installer.
2. Open a terminal and navigate to the directory containing the downloaded JBoss EAP installer.
3. Run the text-based installer using the following command:

›_ Console

```
# java -jar jboss-eap-7.4.0-installer.jar
```

```
[root@JBoss opt]# java -jar jboss-eap-7.4.0-installer.jar
Select your language below :
0: English
1: 中文
2: Deutsch
3: français
4: 日本語
5: português
6: español
Please choose [0] :
0
```

Figure 2 : JBoss installation

```
Configure Runtime Environment
There are several additional options for configuring Red Hat JBoss Enterprise Application Platform now that the server has bee
n installed. Each option can be individually chosen, and will be configured in the order displayed upon pressing "Next". What
would you like to do now?
0  [x] Perform default configuration
1  [ ] Perform advanced configuration
Input Selection:
0

press 1 to continue, 2 to quit, 3 to redisplay.
1

[ Starting processing ]
Starting process Logging installation information (1/3)
IzPack variable state written to /opt/EAP-7.4.0/installation/InstallationLog.txt
Starting process Adding admin user (2/3)
Starting process Cleanup extraneous folders and tepmorary files (3/3)
Installation has completed successfully.
Application installed on /opt/EAP-7.4.0

Would you like to generate an automatic installation script and properties file? (y/n) [n]:
y
Select path for the automatic installation script: [/opt/EAP-7.4.0/auto.xml]

XML written successfully.
[ Console installation done ]
[root@JBoss opt]#
```

Figure 3 : JBoss installation

4. Change the owner & group of the JBoss EAP folder.

›_ Console

```
# chown -R jboss:jboss /opt/EAP-7.4.0/
```

5. Edit JBoss EAP configuration file `/opt/EAP-7.4.0/bin/init.d/jboss-eap.conf` with below entries.

jboss-eap.conf

```
JAVA_HOME=/opt/jdk1.8.0_202

JBOSS_HOME=/opt/EAP-7.4.0

JBOSS_USER=jboss
```

You need to modify the above values according to your environment. After adding the above lines, save the file.

6. Now edit the `/etc/profile` file to add the below lines.

profile

```
export JAVA_HOME=/opt/jdk1.8.0_202 export JBOSS_HOME=/opt/EAP-7.4.0

export PATH=$PATH:$JAVA_HOME/bin:$JBOSS_HOME/bin
```

7. Run the command below to reload the profile.

›_ Console

```
# source /etc/profile
```

8. Verify java home and jboss home path.

›_ Console

```
# echo $JAVA_HOME

# echo $JBOSS_HOME
```

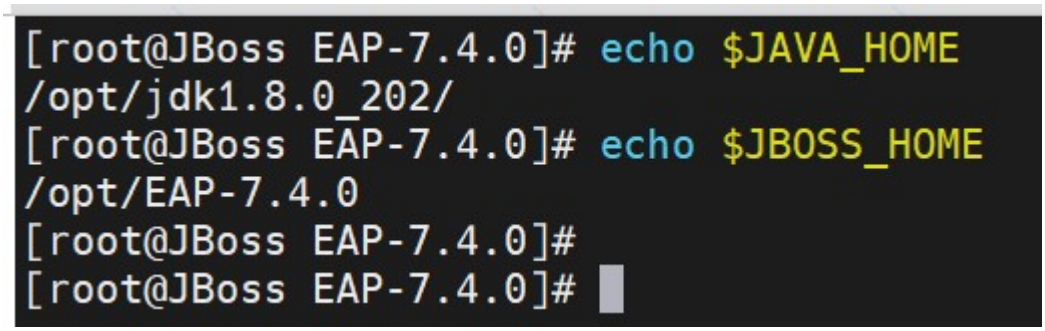

Figure 4 : Verify Java and JBoss home PATH

9. Copy the below two files.

›_ Console

```
# cp /opt/EAP-7.4.0/bin/init.d/jboss-eap.conf /etc/default

# cp /opt/EAP-7.4.0/bin/init.d/jboss-eap-rhel.sh /etc/init.d/
```

```
[root@JBoss ~]# cp /opt/EAP-7.4.0/bin/init.d/jboss-eap.conf /etc/default
[root@JBoss ~]#
[root@JBoss ~]# cp /opt/EAP-7.4.0/bin/init.d/jboss-eap-rhel.sh /etc/init.d
[root@JBoss ~]#
```

Figure 5 : Copy JBoss service files

10. Run below two commands to reset the security context.

›_ Console

```
# restorecon /etc/init.d/jboss-eap-rhel.sh

# chkconfig --add jboss-eap-rhel.sh
```

11. Start JBoss EAP service.

›_ Console

```
# systemctl enable jboss-eap-rhel

# systemctl start jboss-eap-rhel
```

12. Check the status of JBoss EAP service.

›_ Console

```
# systemctl status jboss-eap-rhel
```

```
[root@JBoss EAP-7.4.0]# systemctl status jboss-eap-rhel
● jboss-eap-rhel.service - SYSV: JBoss EAP startup script
   Loaded: loaded (/etc/rc.d/init.d/jboss-eap-rhel.sh; generated)
   Active: active (running) since Wed 2023-11-01 15:05:42 UTC; 1min 12s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 25701 ExecStart=/etc/rc.d/init.d/jboss-eap-rhel.sh start (code=exited, status=0/SUCCESS)
 Main PID: 25802 (java)
    Tasks: 43 (limit: 49124)
   Memory: 585.9M
   CGroup: /system.slice/jboss-eap-rhel.service
           ├─25720 /bin/sh /opt/EAP-7.4.0/bin/standalone.sh -c standalone.xml
           └─25802 /opt/jdk1.8.0_202/bin/java -D[Standalone] -server -verbose:gc -Xloggc:/opt/EAP-7.4.0/standalone/log/gc.log>

Nov 01 15:05:37 JBoss systemd[1]: Starting SYSV: JBoss EAP startup script...
Nov 01 15:05:37 JBoss runuser[25718]: pam_unix(runuser:session): session opened for user jboss by (uid=0)
Nov 01 15:05:37 JBoss runuser[25718]: pam_unix(runuser:session): session closed for user jboss
Nov 01 15:05:37 JBoss jboss-eap-rhel.sh[25701]: Starting jboss-eap: /
Nov 01 15:05:42 JBoss jboss-eap-rhel.sh[25701]: [  OK  ]
Nov 01 15:05:42 JBoss systemd[1]: jboss-eap-rhel.service: Supervising process 25802 which is not our child. We'll most likely>
Nov 01 15:05:42 JBoss systemd[1]: Started SYSV: JBoss EAP startup script.
lines 1-19/19 (END)
```

Figure 6 : JBoss service status

6.2 Generating SSL Key and Certificate for JBoss Server on Utimaco HSM

6.2.1 For RSA Key

1. Log in as root user and generate a keypair on Utimaco HSM.

›_ Console

```
# keytool -genkey -keyalg RSA -keysize 2048 -keystore NONE -storetype

CryptoServer -storepass 12345678 -providername CryptoServer -alias jbossrsa
```

Provide information when prompted. Here:

- RSA is the key algorithm.
- 2048 is the key size.
- NONE is the keystore for HSM.
- CryptoServer is the storetype.

- 12345678 is the slot PIN.
- CryptoServer is the provider name.

```
[root@JBoss bin]# keytool -genkey -keyalg RSA -keysize 2048 -keystore NONE -storetype CryptoServer -storepass 12345678 -provid
ername CryptoServer -alias jbossrsa
What is your first and last name?
  [Unknown]:  Jboss
What is the name of your organizational unit?
  [Unknown]:  Utimaco
What is the name of your organization?
  [Unknown]:  Utimaco
What is the name of your City or Locality?
  [Unknown]:  Campbel
What is the name of your State or Province?
  [Unknown]:  DE
What is the two-letter country code for this unit?
  [Unknown]:  CN
Is CN=Jboss, OU=Utimaco, O=Utimaco, L=Campbel, ST=DE, C=CN correct?
  [no]:  yes

Enter key password for <jbossrsa>
        (RETURN if same as keystore password):
Re-enter new password:
[root@JBoss bin]#
```

Figure 7 : Key generation using the keytool command

2. Verify that the keys have been generated using the keytool command.

›_ Console

```
# keytool -list -keystore NONE -storetype CryptoServer -providername

CryptoServer -storepass 12345678 -v
```

Here:

- NONE is the keystore for HSM.
- CryptoServer is the storetype.
- 12345678 is the slot PIN.
- CryptoServer is the provider's name.

```
[root@JBoss bin]# keytool -list -keystore NONE -storetype CryptoServer -providername CryptoServer -storepass 12345678 -v
Keystore type: CRYPTOSERVER
Keystore provider: CryptoServer

Your keystore contains 1 entry

Alias name: jbossrsa
Creation date: Nov 2, 2023
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Jboss, OU=Utimaco, O=Utimaco, L=Campbel, ST=DE, C=CN
Issuer: CN=Jboss, OU=Utimaco, O=Utimaco, L=Campbel, ST=DE, C=CN
Serial number: 644e0f4c
Valid from: Thu Nov 02 05:38:02 UTC 2023 until: Wed Jan 31 05:38:02 UTC 2024
Certificate fingerprints:
         MD5:  29:69:00:69:86:0D:74:8B:BC:AA:92:62:BF:93:AA:BB
         SHA1: B8:1A:BB:6F:81:20:59:71:C9:F1:20:98:00:78:4F:2B:C8:A0:F1:82
         SHA256: DC:2B:58:C1:9F:01:0A:25:74:36:08:EE:7B:FD:D3:D0:2C:57:43:EA:E6:E4:14:74:01:FE:37:81:50:E5:58:34
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: EB 32 31 A9 A0 5B E6 4F   B2 67 13 19 F6 09 8B 5A  .21..[.O.g.....Z
0010: FF 72 2A 0B                                        .r*.
]
]



*******************************************
*******************************************
```

Figure 8 : List keystore entries

3. List the keys using cxitool.

›_ Console

```
# cxitool Dev=<HSM_IP> Logonpass=<user_name>,<PIN> Group=<cxi_group_name>}
Listkeys
```

```
[root@JBoss ~]# /opt/utimaco/bin/cxitool Dev=288@10.44.223.141 Logonpass=jboss-user,12345678 Group=Cryptoserver Listkeys

idx algo  size type     group                  name                           spec
-------------------------------------------------------------------------------
5   RSA   2048 pub+prv  Cryptoserver           jbossrsa

[root@JBoss ~]#
```

Figure 9 : List keys output using cxitool

4. Generate a CSR using Keytool command.

›_ Console

```
# keytool -certreq -alias jbossrsa -file rsa.csr -storetype CryptoServer
keystore NONE -v
```

```
[root@JBoss bin]# keytool -certreq -alias jbossrsa -file rsa.csr -storetype CryptoServer -keystore NONE -v
Enter keystore password:
Certification request stored in file <rsa.csr>
Submit this to your CA
[root@JBoss bin]#
[root@JBoss bin]# ls -la | grep rsa.csr
-rw-r--r--. 1 root root   1081 Nov  2 07:11 rsa.csr
[root@JBoss bin]#
```

Figure 10 : CSR generation

Provide the keystore password when prompted. Here:

- NONE is the keystore for HSM.
- CryptoServer is the storetype.
- CryptoServer is the provider name.
- jbossrsa is the key name.
- rsa.csr is the CSR file name that will be generated.

5. Get this CSR signed by CA.
6. Copy the signed certificate along with Root CA certificate on the JBoss server.
7. Import the Root certificate into the HSM keystore. Type yes when prompted.

›_ Console

```
# keytool -importcert -alias RootCA -file /opt/TestCA-Root.crt -storetype

CryptoServer -keystore NONE -providername CryptoServer -storepass 12345678
```

```
[root@JBoss bin]# keytool -importcert -alias RootCA -file /opt/TestCA-Root.crt -storetype CryptoServer -keystore NONE -provide
rname CryptoServer -storepass 12345678
Owner: CN=TestCA-Root, OU=Utimaco, O=Utimaco, L=Campbell, ST=CA, C=US
Issuer: CN=TestCA-Root, OU=Utimaco, O=Utimaco, L=Campbell, ST=CA, C=US
Serial number: 572b22a8b2e2e2f4
Valid from: Wed Nov 30 06:28:00 UTC 2022 until: Tue Nov 30 06:28:00 UTC 2032
Certificate fingerprints:
         MD5:  96:B7:1B:41:D9:C3:75:9D:4E:F2:04:EA:22:B0:8C:18
         SHA1: 38:F3:13:04:4E:F7:B9:37:1C:69:06:59:DE:3B:FC:60:9D:A4:9B:87
         SHA256: 5B:90:A1:00:DD:7A:9A:A5:7B:32:ED:E4:0E:37:BB:9D:DE:9A:79:73:9F:0A:CD:92:1B:6B:04:C0:17:AD:96:11
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 0E 55 74 69 6D 61 63   6F 20 54 65 73 74 43 41  ..Utimaco TestCA


#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL CA
   S/MIME CA
   Object Signing CA]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 1A BD 88 8B 07 06 9A 02   13 CB F6 8E 94 04 8E A6  ................
0010: EC 49 5E 36                                        .I^6
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[root@JBoss bin]#
```

Figure 11 : Import root CA certificate into keystore

8. Import the signed certificate using the command below.

›_ Console

```
# keytool -importcert -alias jbossrsa -file /opt/Jboss.pem -storetype

CryptoServer -keystore NONE -providername CryptoServer -storepass 12345678
```

```
[root@JBoss bin]# keytool -importcert -alias jbossrsa -file /opt/Jboss.pem -storetype CryptoServer -keystore NONE -providername CryptoServer -storepass 12345678
Certificate reply was installed in keystore
[root@JBoss bin]#
```

Figure 12 : Import signed certificate into keystore

9. List the keystore entries.

›_ Console

```
# keytool -list -keystore NONE -storetype CryptoServer -providername

CryptoServer -storepass 12345678 -v
```

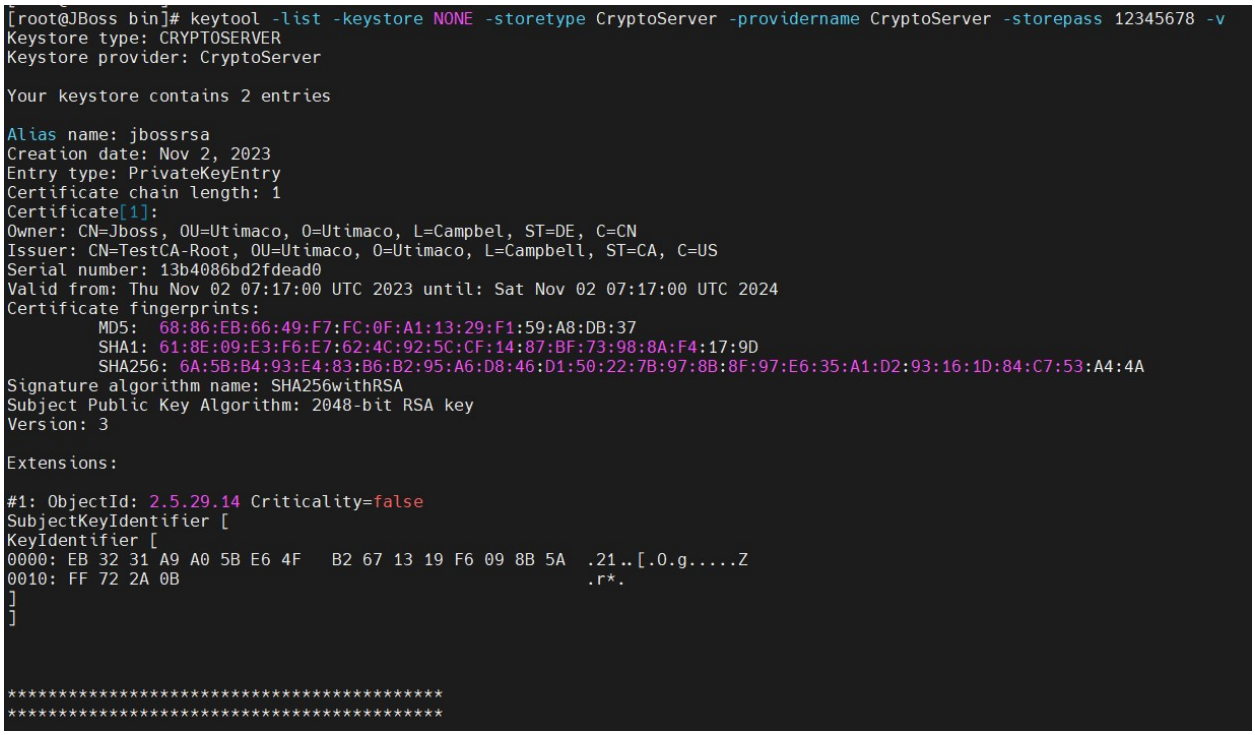

Figure 13 : Keytool list output

```
Alias name: RootCA
Creation date: Nov 2, 2023
Entry type: trustedCertEntry

Owner: CN=TestCA-Root, OU=Utimaco, O=Utimaco, L=Campbell, ST=CA, C=US
Issuer: CN=TestCA-Root, OU=Utimaco, O=Utimaco, L=Campbell, ST=CA, C=US
Serial number: 572b22a8b2e2e2f4
Valid from: Wed Nov 30 06:28:00 UTC 2022 until: Tue Nov 30 06:28:00 UTC 2032
Certificate fingerprints:
         MD5:  96:B7:1B:41:D9:C3:75:9D:4E:F2:04:EA:22:B0:8C:18
         SHA1: 38:F3:13:04:4E:F7:B9:37:1C:69:06:59:DE:3B:FC:60:9D:A4:9B:87
         SHA256: 5B:90:A1:00:DD:7A:9A:A5:7B:32:ED:E4:0E:37:BB:9D:DE:9A:79:73:9F:0A:CD:92:1B:6B:04:C0:17:AD:96:11
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 0E 55 74 69 6D 61 63   6F 20 54 65 73 74 43 41  ..Utimaco TestCA


#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL CA
   S/MIME CA
   Object Signing CA]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 1A BD 88 8B 07 06 9A 02   13 CB F6 8E 94 04 8E A6  ................
0010: EC 49 5E 36                                        .I^6
]
]



*******************************************
*******************************************


[root@JBoss bin]#
```

Figure 14 : Keytool list output

6.2.2 For EC Key

1. Generate an EC keypair on Utimaco HSM.

›_ Console

```
# keytool -genkey -keyalg EC -keystore NONE -storetype CryptoServer -storepass

12345678 -providername CryptoServer -alias jbosseckey
```

Provide information when prompted. Here:

- EC is the key algorithm.
- NONE is the keystore for HSM.
- CryptoServer is the storetype.
- 12345678 is the slot PIN.
- CryptoServer is the provider name.
- jbosseckey is the key name that will be generated on Utimaco HSM.

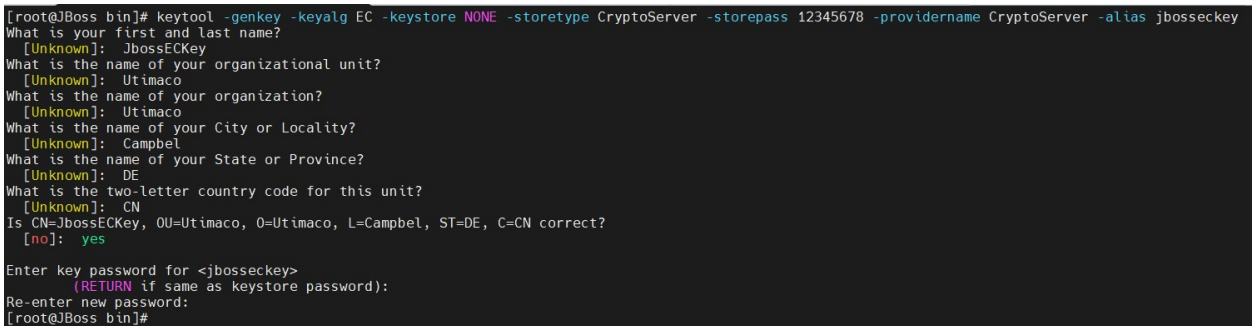

Figure 15 : Key generation using keytool command

2. Verify that the keys have been generated.

›_ Console

```
# keytool -list -keystore NONE -storetype CryptoServer -providername

CryptoServer -storepass 12345678 -v
```

Here:

- NONE is the keystore for HSM.
- CryptoServer is the storetype.
- 12345678 is the slot PIN.
- CryptoServer is the provider's name.

```
[root@JBoss bin]# keytool -list -keystore NONE -storetype CryptoServer -providername CryptoServer -storepass 12345678 -v
Keystore type: CRYPTOSERVER
Keystore provider: CryptoServer

Your keystore contains 3 entries
```

Figure 16 : List keystore entries

```
Alias name: jbosseckey
Creation date: Nov 2, 2023
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=JbossECKey, OU=Utimaco, O=Utimaco, L=Campbel, ST=DE, C=CN
Issuer: CN=JbossECKey, OU=Utimaco, O=Utimaco, L=Campbel, ST=DE, C=CN
Serial number: 3bd5b96f
Valid from: Thu Nov 02 08:09:18 UTC 2023 until: Wed Jan 31 08:09:18 UTC 2024
Certificate fingerprints:
         MD5:  B0:6C:BD:81:7C:8F:F0:68:50:52:E8:6B:AE:27:34:73
         SHA1: 27:8C:1C:66:99:72:54:DD:04:66:15:C9:51:21:45:AD:DC:BE:D2:09
         SHA256: E1:B2:F7:EE:B8:D9:E2:FD:1D:60:98:E4:63:98:DE:24:BC:AF:48:8F:67:FB:B8:61:9F:1A:37:51:50:C9:32:14
Signature algorithm name: SHA256withECDSA
Subject Public Key Algorithm: 256-bit EC key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 33 BC 9C 6D B7 92 A5 DE   AA 97 40 AD C2 BD 09 F9  3..m......@.....
0010: BE DA E2 DD                                        ....
]
]



*******************************************
*******************************************
```

Figure 17 : List keystore entries

3. List the keys using cxitool.

›_ Console

```
# cxitool Dev=<HSM_IP> Logonpass=<user_name>,<PIN> Group=<cxi_group_name>}
Listkeys
```

```
[root@JBoss bin]# /opt/utimaco/bin/cxitool Dev=288@10.44.223.141 Logonpass=jboss-user,12345678 Group=Cryptoserver Listkeys

idx algo  size type     group                   name                            spec
-------------------------------------------------------------------------------------
5   ECDSA 256  pub+prv  Cryptoserver            jbosseckey

[root@JBoss bin]#
```

Figure 18 : List keys output using cxitool

4. Generate a CSR using the Keytool command.

›_ Console

```
# keytool -certreq -alias jbosseckey -file jbosseckey.csr -storetype

CryptoServer -keystore NONE -v
```

```
[root@JBoss bin]# keytool -certreq -alias jbosseckey -file jbosseckey.csr -storetype CryptoServer -keystore NONE -v
Enter keystore password:
Certification request stored in file <jbosseckey.csr>
Submit this to your CA
[root@JBoss bin]#
```

Figure 19 : CSR generation

Provide the keystore password when prompted. Here:

- NONE is the keystore for HSM.
- CryptoServer is the storetype.
- CryptoServer is the provider name.
- jbosseckey is the key name.
- jbosseckey.csr is the CSR file name that will be generated.

5. Get this CSR signed by CA.
6. Copy the signed certificate along with Root CA certificate on the JBoss server.
7. Import the Root certificate into the HSM keystore. Type yes when prompted.

›_ Console

```
# keytool -importcert -alias RootCA -file /opt/rootca.crt -storetype

CryptoServer -keystore NONE -providername CryptoServer -storepass 12345678
```

```
[root@JBoss bin]# keytool -importcert -alias RootCA -file /opt/TestCA-Root.crt -storetype CryptoServer -keystore NONE -provide
rname CryptoServer -storepass 12345678
Owner: CN=TestCA-Root, OU=Utimaco, O=Utimaco, L=Campbell, ST=CA, C=US
Issuer: CN=TestCA-Root, OU=Utimaco, O=Utimaco, L=Campbell, ST=CA, C=US
Serial number: 572b22a8b2e2e2f4
Valid from: Wed Nov 30 06:28:00 UTC 2022 until: Tue Nov 30 06:28:00 UTC 2032
Certificate fingerprints:
         MD5:  96:B7:1B:41:D9:C3:75:9D:4E:F2:04:EA:22:B0:8C:18
         SHA1: 38:F3:13:04:4E:F7:B9:37:1C:69:06:59:DE:3B:FC:60:9D:A4:9B:87
         SHA256: 5B:90:A1:00:DD:7A:9A:A5:7B:32:ED:E4:0E:37:BB:9D:DE:9A:79:73:9F:0A:CD:92:1B:6B:04:C0:17:AD:96:11
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 0E 55 74 69 6D 61 63   6F 20 54 65 73 74 43 41  ..Utimaco TestCA


#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL CA
   S/MIME CA
   Object Signing CA]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 1A BD 88 8B 07 06 9A 02   13 CB F6 8E 94 04 8E A6  ................
0010: EC 49 5E 36                                        .I^6
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[root@JBoss bin]#
```

Figure 20 : Importing root CA certificate into keystore

8. Import the signed certificate using the command below.

›_ Console

```
# keytool -importcert -alias jbosseckey -file /opt/JbossECKey.pem -storetype

CryptoServer -keystore NONE -providername CryptoServer -storepass 12345678
```

```
[root@JBoss bin]# keytool -importcert -alias jbosseckey -file /opt/JbossECKey.pem -storetype CryptoServer -keystore NONE -prov
idername CryptoServer -storepass 12345678
Certificate reply was installed in keystore
[root@JBoss bin]#
```

Figure 21 : Import signed certificate into keystore

9. List the keystore entries.

›_ Console

```
# keytool -list -keystore NONE -storetype CryptoServer -providername

CryptoServer -storepass 12345678 -v
```

Here:

- NONE is the keystore for HSM.
- CryptoServer is the storetype.
- 12345678 is the slot PIN.
- CryptoServer is the provider's name.

```
[root@JBoss bin]# keytool -list -keystore NONE -storetype CryptoServer -providername CryptoServer -storepass 12345678 -v
Keystore type: CRYPTOSERVER
Keystore provider: CryptoServer

Your keystore contains 3 entries
```

Figure 22 : keytool list output

```
Alias name: jbosseckey
Creation date: Nov 2, 2023
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=JbossECKey, OU=Utimaco, O=Utimaco, L=Campbel, ST=DE, C=CN
Issuer: CN=TestCA-Root, OU=Utimaco, O=Utimaco, L=Campbell, ST=CA, C=US
Serial number: 17207d0e1408e866
Valid from: Thu Nov 02 08:29:00 UTC 2023 until: Sat Nov 02 08:29:00 UTC 2024
Certificate fingerprints:
         MD5:  B9:A5:7F:D7:D8:98:B3:3F:78:02:6B:B2:0E:74:5A:50
         SHA1: 5C:9C:39:60:5A:28:7F:02:B2:6A:44:96:3E:F5:21:57:A1:03:F1:F6
         SHA256: 72:6C:D0:09:F6:8E:B1:B8:B7:31:04:1B:80:EB:0E:A7:E5:0E:3C:45:19:03:A5:B9:15:21:B7:E7:5A:43:77:DB
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 256-bit EC key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 33 BC 9C 6D B7 92 A5 DE   AA 97 40 AD C2 BD 09 F9  3..m......@.....
0010: BE DA E2 DD                                        ....
]
]



*******************************************
*******************************************
```

Figure 23 : keytool list output

6.3 Configuring JBoss to use SSL Key and Certificate Present on Utimaco HSM

1. Copy the `CryptoServer.cfg` file under Jboss configuration directory.

›_ Console

```
# cp /home/jboss/CryptoServer.cfg /opt/EAP-

7.4.0/standalone/configuration/CryptoServer
```

2. Open the `$JBOSS_HOME/standalone/configuration/standalone.xml` file.
3. Edit the `<ssl>` configuration under the `<management> <security-realms>` section, as indicated below:

standalone.xml

```
<security-realm name="ApplicationRealm">

<server-identities>

<ssl>

<keystore path="CryptoServer" provider="CryptoServer"
relativeto="jboss.server.config.dir"

keystore-password="12345678" alias="jbossrsa" />

</ssl>

</server-identities>
```

Update alias name and keystore password according to your setup.

4. Restart the jboss service.

›_ Console

```
# systemctl restart jboss-eap-rhel
```

5. Open any browser and access the URL https://< jboss_ip_address>:8443.
6. After the page is loaded, verify the SSL certificate details.

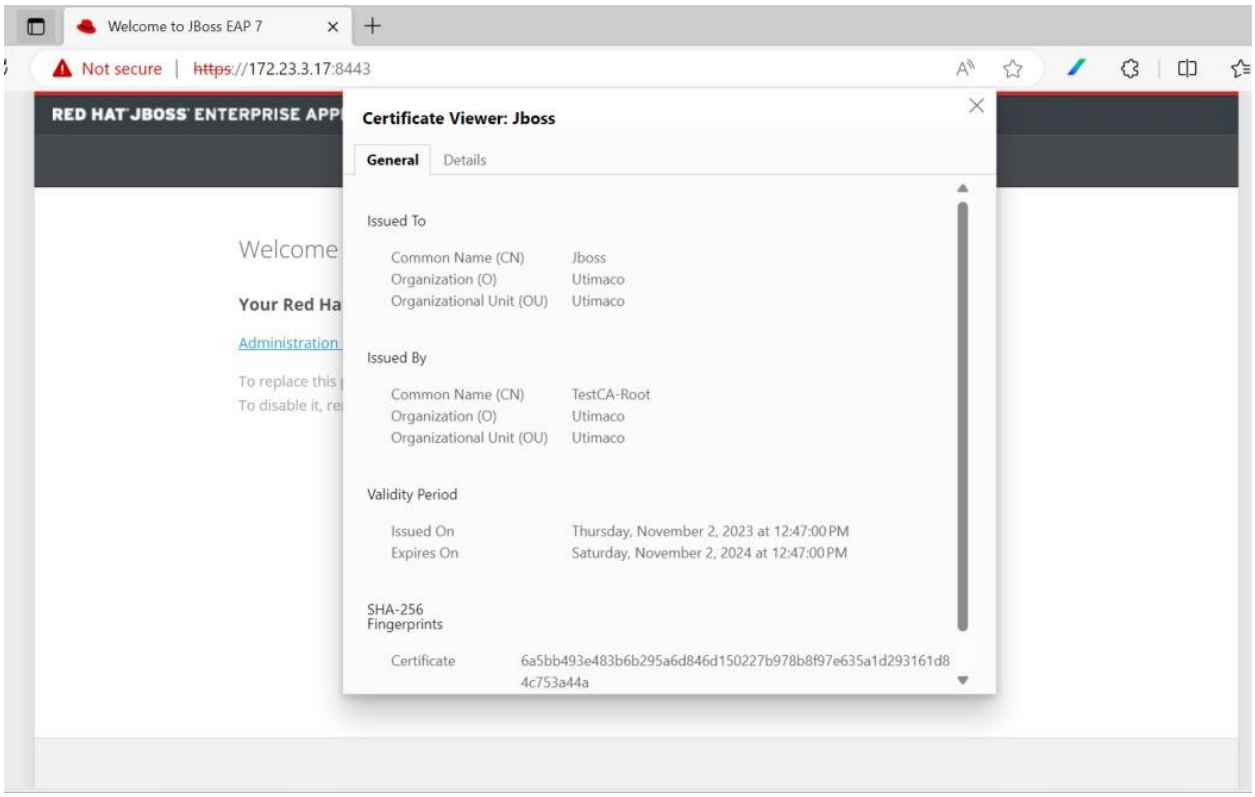

Figure 24 : Loading page over HTTPS

This completes the integration of JBoss Enterprise Application Platform with Utimaco SecurityServer using CryptoServer JCE.

7 Troubleshooting

Error	Diagnosis
JBoss HTTPS Page is not loading with IP address	Change public interface in /opt/EAP- 7.4.0/standalone/configuration/standalone.xml file as below: <interface name="public"> <inet-address value="${jboss.bind.address:0.0.0.0}"/> </interface

Table 6: List of errors and their diagnoses

8 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/*.

9 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

10 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.