Black•Vault HSM

EJBCA

Integration Guide

© Engage Black
9565 Soquel Drive
Aptos, CA 95003
Phone +1 831.688.1021
1 877.ENGAGE4 (364.2434)
sales@engageblack.com

February 28, 2021

Disclaimer and Warranty

Engage Black is a business unit of Engage Communication.

Engage Communication makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability of fitness for any particular purpose. Information in this document is subject to change without notice and does not represent a commitment on the part of Engage Communication, Inc. Product specifications are subject to change without notice. Engage Communication assumes no responsibility for any inaccuracies in this document or for any obligation to update the information in this document.

Engage Communications, Inc.9565 Soquel Drive Aptos, CA 95003

Phone +1 (831) 688-1021

http://www.engageblack.com/

http://www.engageinc.com/

Table of Contents

1. Introduction 4

2. Prerequisites 4

2.1. Install and Setup Required Resources 4

3. Generate EJBCA Keys 5

1. Introduction

EJBCA is an open-source public key infrastructure (PKI) certificate authority software package maintained by PrimeKey. EJBCA's time-proven robustness and reliability makes it the perfect certificate authority integration candidate for the BlackVault HSM.

This guide will explain how to complete a general set up of EJBCA with the BlackVault HSM.

2. Prerequisites

To proceed, the following is needed:

- BlackVault HSM, initialized and configured properly (see the BlackVault HSM User Guide for more information)
- BlackVault Card Set
- BlackVault HSM Setup CD
- A client computer that has a supported Operating System installed.

Additionally, your client computer must have Java 8 installed and configured properly with your BlackVault HSM. Please see the BlackVault HSM Java Configuration Guide and follow the Java 8 installation instructions for your client's operating system.

2.1. Install and Setup Required Resources

To successfully run the EJBCA system, in addition to Java 8, you must also install the following software packages:

- EJBCA (download here)
- Apache Ant (download here)

Next, complete the following setup steps:

1) Untar or unzip the EJBCA, JBoss Server, and Apache Ant files in the /opt/ directory:
    a) Unzip:

```
$ unzip /home/$USER/apache-ant-1.9.6-bin.zip -d /opt/
$ unzip /home/$USER/ejbca_ce_6_3_1_1.zip -d /opt/
```

    b) Untar:

```
$ tar xf /home/$USER/apache-ant-1.9.6-bin.tar.gz -C /opt/
$ tar xf /home/$USER/ejbca_ce_6_3_1_1.tar.gz -C /opt/
```

2) (Optional) We recommend changing the directory names to something more convenient. For example:

```
$ mv /opt/apache-ant-1.9.6 /opt/apache-ant
$ mv /opt/ejbca_ce_6_3_1_1 -d /opt/ejbca
```

3) Set the following system environmental variables:

```
$ export JAVA_HOME=<Path to Java JDK>
$ export PATH=$JAVA_HOME/bin:$PATH
$ export CLASSPATH=$JAVA_HOME/jre/lib/ext:$CLASSPATH
$ export ANT_HOME=/opt/apache-ant
$ export PATH=$ANT_HOME/bin:$PATH
$ export EJBCA_HOME=/opt/ejbca
```

4) If you have not already, set the BV_PKCS_PATH environmental variable:

```
$ export BV_PKCS_PATH=/home/$USER/BlackVaultSetupCD/Configuration/pkcs.dat
```

3. Generate EJBCA Keys

This section will explain how to generate the necessary EJBCA keys. To administer and generate tools, use `$EJBCA_HOME/dist/clientToolBox/ejbcaClientToolBox.sh PKCS11HSMKeyTool`

To see the `PKCS11HSMKeyTool` functionality, run it with no parameters:

```
$EJBCA_HOME/dist/clientToolBox/ejbcaClientToolBox.sh
```

You should see the following menu:

```
Use one of following commands:
  PKCS11HSMKeyTool generate
  PKCS11HSMKeyTool batchgenerate
  PKCS11HSMKeyTool certreq
  PKCS11HSMKeyTool installcert
  PKCS11HSMKeyTool delete
  PKCS11HSMKeyTool test
  PKCS11HSMKeyTool rename
  PKCS11HSMKeyTool encrypt
  PKCS11HSMKeyTool decrypt
  PKCS11HSMKeyTool sign
  PKCS11HSMKeyTool verify
  PKCS11HSMKeyTool move
  PKCS11HSMKeyTool linkcert
The optional -password <password> switch can be specified as a last argument
for scripting any of these commands.
```

When generating keys, you will need to specify the BlackVault HSM PKCS11 cryptographic library (/usr/lib/libbvpkcs.so) and the HSM slot number (1). Generate the necessary keys by completing the following steps:

1) Build the client tool box with ant:

```
$ cd $EJBCA_HOME
$ ant clientToolBox
```

2) Generate Keys:

```
$ dist/clientToolBox/ejbcaClientToolBox.sh PKCS11HSMKeyTool generate
/usr/lib/libbvpkcs.so 2048 signKey 1
$ dist/clientToolBox/ejbcaClientToolBox.sh PKCS11HSMKeyTool generate
/usr/lib/libbvpkcs.so 2048 defaultKey 1
$ dist/clientToolBox/ejbcaClientToolBox.sh PKCS11HSMKeyTool generate
usr/lib/libbvpkcs.so 2048 myKey 1
```

Note: When generating keys, when prompted to enter the `PKCS11 Token [SunPKCS11-libbvpkcs.so-slot 1]` **password, enter the BlackVault HSM user password.**

3) (Optional) To test the keys generated with EJBCA that reside on the HSM, enter the following command:

4)

```
$ dist/clientToolBox/ejbcaClientToolBox.sh PKCS11HSMKeyTool test
/usr/lib/libbvpkcs.so 1
```

Note: In the output, you should see: `Signature test of key <key name>: signature length <>; first byte <>; verifying true`

5) You can also verify the keys are on the BlackVault HSM with bvtool:

```
$ bvtool list –a
```