Using CertAgent with an Engage BlackVault Hardware Security Module (HSM)

Version 1.0.0

Sep. 28, 2018

Disclaimer

Neither Information Security Corporation (ISC), nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. ISC shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. ISC further reserves the right to make changes to the specifications of the software and contents of this guide without obligation to notify any person or organization of such changes. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation of their use. ISC assumes no responsibility with regard to the performance or use of these third-party products.

Every effort has been made to ensure that the information in this document is accurate. ISC is not responsible for printing or clerical errors.

Using CertAgent with an Engage BlackVault HSM, Version 1.0.0 (September 2018).

Information Security Corporation
1011 W. Lake St., Suite 425
Oak Park, IL 60301

Phone: +1 847 405-0500
Fax: +1 708 445-9705
E-mail: tech@infoseccorp.com
Website: www.infoseccorp.com

Table of Contents

1 Introduction 4

2 Prerequisite 4

2.1 Configuring the BlackVault HSM 4

2.2 Installing the BlackVault HSM Client Software 4

2.2.1 Windows 4

2.2.2 CentOS 4

2.3 Configuring pkcs.dat 5

2.4 Setting System Environment Variables 5

2.4.1 Windows 5

2.4.2 CentOS 6

3 Installing CertAgent 7

3.1 Updating the startup script (CentOS only) 7

4 Entering the System PIN 7

5 Configuring CertAgent 8

1 Introduction

This document describes the installation and configuration of CertAgent for use with an Engage BlackVault HSM. The provided instructions are for CertAgent 7 and Engage BlackVault HSM client software version 7.0.21.3 on Windows 2012 and CentOS 7. Instructions for different versions/platforms may differ.

2 Prerequisite

2.1 Configuring the BlackVault HSM

Follow the instructions in the BlackVault HSM User Guide provided by Engage Black to initialize and configure your HSM. In particular, you must perform the following tasks:

- ☐ initialize the HSM with FIPS mode and 1 of M setup
- ☐ create the Crypto Office Operator and User Operator cards
- ☐ configure the network setting (IP address and TLS port)

To locate the HSM's IP address and TLS port configuration:

1. Login to the HSM as a crypto officer.
2. Select Information and then Network Information.

2.2 Installing the BlackVault HSM Client Software

Follow the instructions in the BlackVault HSM User Guide provided by Engage Black to install the client software as appropriate for your system.

2.2.1 Windows

3. Run '`bv-setup.exe`' to install the BlackVault HSM client software.
4. When the prompt "Would you like to configure the BlackVault for Java?" appears, click **No**.
5. Enter the IP address and port number as appropriate for your HSM network configuration, then click **Next**.
6. In the Select Components page, select "Engage BlackVault cryptography provider", then click **Next**.

2.2.2 CentOS

Run '`rpm -i bvhsm-7.0.21.3-1.x86_64.rpm`' to install the BlackVault HSM client software. If the following failed dependencies error returned, run '`yum install libc.so.6`' to install the required libraries and run the `rpm` command again.

```
[root@localhost Desktop]# rpm -i bvhsm-7.0.21.3-1.x86_64.rpm
error: Failed dependencies:
     ld-linux.so.2 is needed by bvhsm-7.0.21.3-1.x86_64
     ld-linux.so.2(GLIBC_2.3) is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6 is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6(GLIBC_2.0) is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6(GLIBC_2.1) is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6(GLIBC_2.1.3) is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6(GLIBC_2.2) is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6(GLIBC_2.2.4) is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6(GLIBC_2.3) is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6(GLIBC_2.3.2) is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6(GLIBC_2.3.4) is needed by bvhsm-7.0.21.3-1.x86_64
     libc.so.6(GLIBC_2.4) is needed by bvhsm-7.0.21.3-1.x86_64
```

The BlackVault software will be installed in the `/usr/local/BlackVault` directory.

2.3 Configuring pkcs.dat

The HSM's IP address and TLS port configuration are stored in the pkcs.dat file with the following format:

```
<IP address> <port>
```

For example:

```
192.168.0.235 5002
```

On Windows, the `pkcs.dat` file will be automatically created and configured during the HSM client software installation and is located in the `C:\Program Files\Engage BlackVault\Configuration` directory. On CentOS, this file needs to be created manually (e.g., `/usr/local/BlackVault/Configuration/pkcs.dat`)

2.4 Setting System Environment Variables

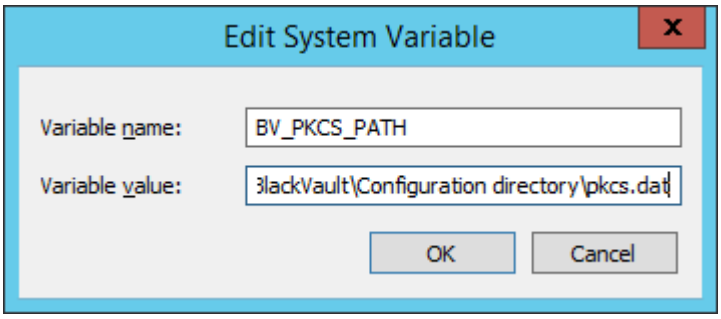
The location of the pkcs.dat file and the library containing the HSM library must be specified in the system environment variables.

BV_PKCS_PATH	Location of the HSM configuration file pkcs.dat
PATH	(Windows) Append the directory containing the 64-bit HSM library
LD_LIBRARY_PATH	(CentOS) Append the directory containing the 64-bit HSM library

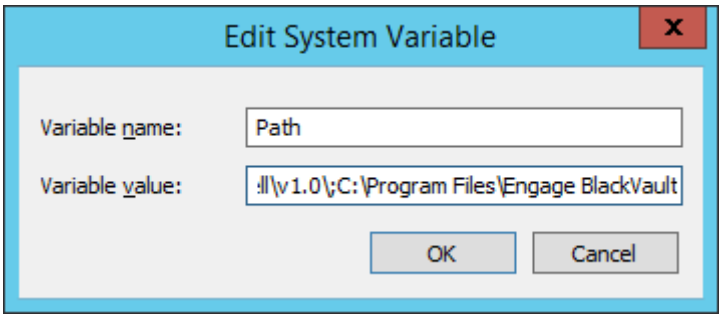
2.4.1 Windows

1. Login as administrator.
2. Open Control Panel.

3. Click System, and Advanced system settings.
4. In the Advanced tab, click Environment Variables…
5. In the System variables section, click **New** and set the name to `BV_PKCS_PATH` and its value to `C:\Program Files\Engage BlackVault\Configuration\pkcs.dat`:



6. Click **OK**.
7. Locate the `Path` variable from the System variables, and click **Edit**.



8. Append "`;C:\Program Files\Engage BlackVault\Libraries`" to the existing value.
9. Reboot your system.

2.4.2 CentOS

1. Login as root.
2. Create the configuration file in `/usr/local/BlackVault/Configuration/pkcs.dat` containing the HSM's IP address and TLS port.
3. Open a new terminal and run the following commands to set the variables:

```
export BV_PKCS_PATH=/usr/local/BlackVault/Configuration/pkcs.dat
export LD_LIBRARY_PATH=/usr/local/BlackVault/Libraries
```

4. Use this terminal to run the installation script.

3 Installing CertAgent

Follow the installation instructions as described in the *CertAgent Installation Guide*. When asked to specify the 64-bit HSM library, enter the following value as appropriate for your system:

```
C:\Program Files\Engage BlackVault\Libraries\bvpkcs64.dll              (Windows)
/usr/local/BlackVault/Libraries/libbvpkcs64.so                          (CentOS)
```

The HSM label and slot number will automatically be populated (e.g., `Label: BlackVault User; Slot: 1`). Confirm these values and enter the HSM PIN. Complete the rest of the installation, making sure to record the URLs and other information provided. CertAgent will start automatically upon installation.

3.1 Updating the startup script (CentOS only)

1. On CentOS, open the certagent script:

   `/usr/local/certagent7/certagent.sh`

   Add a new variable "`BV_PKCS_PATH=/usr/local/BlackVault/Configuration/pkcs.dat; export BV_PKCS_PATH`" and insert the directory containing the HSM library (`/usr/local/BlackVault/Libraries`) to the existing LD_LIBRARY_PATH as indicated below.

```
BV_PKCS_PATH=/usr/local/BlackVault/Configuration/pkcs.dat; export
BV_PKCS_PATH
LD_LIBRARY_PATH=$CA_HOME/bin:/usr/local/BlackVault/Libraries:$LD_LIBRARY_P
ATH; export LD_LIBRARY_PATH
```

2. Save the changes.

3. Stop and restart CertAgent:

```
/usr/local/certagent7/certagent.stop
/usr/local/certagent7/certagent.start
```

4 Entering the System PIN

Sensitive data are encrypted with the system certificate and stored in the database and configuration file. An administrator must enter the PIN of the HSM where the system credential resides each time the system is booted. Run the following command to enter the system PIN:

```
C:\Program Files\CertAgent7\certagent.bat setpin                    (Windows)
/usr/local/certagent7/certagent.sh setpin                            (CentOS)
```

5 Configuring CertAgent

Follow the instructions as described in the *CertAgent Installation Guide, Administrator Guide,* and *Certificate Authority Guide* to access the CertAgent sites and configure CertAgent. When creating new System or CA credentials on the HSM, simply select the '`Use default`' HSM setting. CertAgent will use the same HSM access info as is used by the current system credentials.