IBM WebSphere MQ

Integration Guide

gemalto
security to be free

Document Part Number: 007-011561-001, Rev. D

Release Date: March 2016

Contents

Preface

This document is intended to guide administrators through the steps for IBM WebSphere MQ and SafeNet Luna HSM integration, and also covers the necessary information to install, configure, and integrate IBM WebSphere MQ with SafeNet Luna HSM.

Scope

This technical information guide provides instructions for setting up a small test lab with IBM WebSphere MQ running with SafeNet Luna HSM for securing the private keys, public keys, and certificates. It explains how to install and configure software that is required for setting up an IBM WebSphere MQ while storing keys and certificates on SafeNet Luna HSM.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type **dir /p**.) • Button names (Click **Save As**.) • Check box and radio button names (Select the **Print Duplex** check box.) • Window titles (On the **Protect Document** window, click **Yes**.) • Field names (**User Name:** Enter the name of the user.) • Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) • User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

Overview

This document covers the necessary information to install, configure, and integrate IBM WebSphere MQ with SafeNet Luna HSM.

Understanding the IBM WebSphere MQ

IBM WebSphere MQ is a family of network software products launched by IBM in March 1992. It was previously known as MQSeries. It allows independent and potentially non-concurrent applications on a distributed system to communicate with each other. SafeNet Luna HSM provides Key Management security for certificates and certificate-based authentication, including import of trusted CA certificates from software based keystore to hardware based keystores, generation of self-signed certificates and personal certificate requests via the IBM Key Management Utility. It can be configured to use SafeNet Luna HSM for SSL connectivity. IBM WebSphere MQ utilizes the PKCS #11 APIs.

The SafeNet Luna HSM solution for IBM WebSphere MQ provides secure key management as well as secure SSL Acceleration.

3rd Party Application Details

- IBM WebSphere MQ

Supported Platforms

IBM WebSphere	Platforms Tested	SafeNet Network HSM Software version / f/w version	Luna Client Software version
IBM WebSphere MQ V 7.5.0.5	Windows Server 2008 R2	6.2.0-15 f/w 6.10.9	6.x 6.2.0-15
IBM WebSphere MQ V 7.5.0.5	Windows Server 2008 R2	6.2.0-15 f/w 6.24.0	6.x 6.2.0-15

IBM WebSphere	Platforms Tested	SafeNet Network HSM Software version / f/w version	Luna Client Software version
IBM WebSphere MQ V7.5	AIX 7.1 (64-bit)	5.4 f/w 6.21.0	5.x (v 5.2.1, 5.3)
IBM WebSphere MQ V7.5 & Patch “7.5-WS-MQ-Windows-GSKit8.0.14.28”	Windows Server 2008 R2	5.4 f/w 6.21.0	5.x (v 5.2.1, 5.3)
IBM WebSphere MQ V7.0.1.3	AIX 6.1, 64-bit	5.2.1 f/w 6.10.1	5.x (v 5.2.1)

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for the installation steps and details regarding configuring and setting up the box on Windows/Linux systems. Before you get started, ensure the following:

- SafeNet Network HSM appliance and a secure admin password.
- SafeNet Network HSM, and a hostname, suitable for your network.
- SafeNet Network HSM, network parameters are set to work with your network.
- Initialize the HSM on the SafeNet Network HSM appliance.
- Create and exchange certificates between the SafeNet Network HSM and Client system.

- Create a partition on the HSM, remember the partition password that will be later used by IBM WebSphere MQ. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from SafeNet Network HSM.
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to SafeNet Network HSM with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

NOTE: There is a known issue with 64-bit libshim.so library. IBM Key Management Utility does not accept it. You need to install 32-bit SafeNet Luna HSM client first and configure IBM Key Management Utility using 32-bit libshim.so to create key repository. Once this is done, you need to replace it with 64-bit SafeNet Luna HSM client. This is discussed in detail in Chapter 2.

NOTE: Ensure that SafeNet Network HSM partition label is in lowercase letters (as required by Websphere MQ), e.g. ‘part1’. Also, partition password should not contain any special characters and this should also be in lowercase letters, e.g. ‘temp1234’.

IBM WebSphere MQ Setup

IBM WebSphere MQ must be installed on the target machine to carry on with the integration process. It does not have a GUI for AIX. You can install IBM WebSphere MQ explorer for a Windows or Linux machine. This graphical tool enables you to explore and configure all WebSphere MQ objects and resources and can remotely connect to queue managers on any supported platform. You also need to create the required user ID and group ID before you install WebSphere MQ. Both user ID and group ID must be set to ‘mqm’. For a detailed installation procedure, refer to the WebSphere MQ documentation.

2

Integrate IBM WebSphere MQ with SafeNet Luna HSM

Create queue managers and connect to MQ explorer:

To set up SafeNet Network HSM for IBM WebSphere MQ, perform the following steps:

1. Log in as a user in the **mqm** group.
2. Create two queue managers called queuemanager1 and queuemanager2 by entering the below commands:

   ```
   crtmqm –q queuemanager1
   crtmqm –q queuemanager2
   ```

3. To start the queue managers, execute the below commands:

   ```
   strmqm queuemanager1
   strmqm queuemanager2
   ```

4. Enable MQSC commands for queuemanager1 by executing the below command:

   ```
   runmqsc queuemanager1
   ```

5. Create a connection channel and a listener using following command:

   ```
   DEFINE CHANNEL (SN1.CHANNEL) CHLTYPE(SVRCONN)
   MCAUSER('mqm')
   DEFINE LISTENER(SN1.LISTENER) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)
   ```

   NOTE: If channel named SYSTEM.ADMIN.SVRCONN does not exist in your queue manager, create one in order for it to be accessible from MQ Browser.

   ```
   DEFINE CHANNEL(SYSTEM.ADMIN.SVRCONN) CHLTYPE(SVRCONN)
   ```

6. Start channel and listener created above using following command:

   ```
   START CHL(SN1.CHANNEL)
   START LSTR(SN1.LISTENER)
   START CHL(SYSTEM.ADMIN.SVRCONN)
   ```

7. Close MQSC session using following command :

   ```
   END
   ```

8. Enable MQSC commands for queuemanager2 using following command :

   ```
   runmqsc queuemanager2
   ```

9. Create a connection channel and a listener using following command:

```
DEF CHANNEL (SN2.CHANNEL) CHLTYPE(SVRCONN)
MCAUSER('mqm')
DEFINE LISTENER(SN2.LISTENER) TRPTYPE(TCP) PORT(1415) CONTROL(QMGR)
```

> **NOTE:** If channel named SYSTEM.ADMIN.SVRCONN does not already exist in your queue manager, create one in order for it to be accessible from MQ Browser.

```
DEFINE CHANNEL(SYSTEM.ADMIN.SVRCONN) CHLTYPE(SVRCONN)
```

10. Start channel and listener created above and close MQSC session using following command:

```
START CHL(SN2.CHANNEL)
START LSTR(SN2.LISTENER)
START CHL(SYSTEM.ADMIN.SVRCONN)
```

11. Close MQSC session using following command:

```
END
```

12. For Aix connect both queue managers to MQ explorer from **Add remote queue manager** option by specifying queue manager name, IP address of AIX machine where these queue managers are running, port number and connection channel name. Refer to the IBM documentation for details.

Configure IBM Key Management Utility to Recognize SafeNet Network HSM Cryptographic Device

- Verify the existence of respective library on the following machine:
  a. For Safenet Network HSM 4.4.1 on Aix ensure that the file libshim.so is in the directory:

     ```
     <Luna Client installation path>/lib
     ```

  b. For Safenet Network HSM 5.2.1 on Windows 2008 R2 verifies if cryptoki.dll is present in below directory:

     ```
     <Luna Client installation path>\win32
     ```

  c. For Safenet Network HSM 5.3 on Aix ensure that the file libCryptoki2_64.so is in the directory:

     ```
     <Luna Client installation path>/lib
     ```

> **NOTE:** Ensure that currently 32-bit SafeNet Network HSM client is installed.

For AIX:

- Perform the below steps:
  a. Traverse to the directory:

     `/usr/opt/ibm/gsksa/classes/`

  b. Rename ikmuser.sample to ikmuser.properties.
  c. Uncomment and edit the following setting to use the cryptographic shim (libshim):

     `DEFAULT_CRYPTOGRAPHIC_MODULE=/usr/lunasa/lib/libshim.so`

  d. Add following to the Safenet Network HSM configuration file (`/etc/Chrystoki.conf`) file for **Shim Support**:

```
Misc = {
ApplicationInstance=HTTP_SERVER;
AppIdMajor=1;
AppIdMinor=1;
}
```

For IBM MQ 7.5:

- Perform the below steps:
  a. Modify the java.security file located in the directory /usr/mqm/java/jre64/jre/lib/security:

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.4=com.ibm.security.cmskeystore.CMSProvider
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl <Path to the
configuration file>
security.provider.8=com.ibm.security.sasl.IBMSASL
security.provider.9=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.10=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.11=org.apache.harmony.security.provider.PolicyProvider
security.provider.12=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

Creating configuration file

The required entries in the luna.cfg configuration file are:

```
description = Luna config
slotListIndex = 0
disabledMechanisms = {
CKM_DH_PKCS_KEY_PAIR_GEN
CKM_DH_PKCS_PARAMETER_GEN
CKM_DH_PKCS_DERIVE
}
attributes (*, CKO_PRIVATE_KEY, *) = {
CKA_SENSITIVE = true
CKA_SIGN=true
CKA_DECRYPT=true
}
attributes (*, CKO_PUBLIC_KEY, *) = {
```

```
CKA_VERIFY=true
CKA_ENCRYPT=true
}
attributes (*, CKO_SECRET_KEY, *) = {
CKA_SENSITIVE = true
CKA_ENCRYPT=true
CKA_DECRYPT=true
CKA_SIGN=true
CKA_VERIFY=true
}
```

Verifying Chrystoki.conf

For AIX:

Use the below entry in the Chrystoki.conf file under the "`/etc`" directory:

Cryptoki with Logging

```
Chrystoki2 = {
LibUNIX=/usr/lunasa/lib/libcklog2.so;
}
Cklog2 = {
LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
NewFormat=1;
Enabled=1;
Error=/tmp/ErrorLunaSA2.txt;
File=/tmp/LogLunaSA2.txt;
}
```

Cryptoki without Logging

```
Chrystoki2 = {
LibUNIX=/usr/lunasa/lib/libCryptoki2.so;
}
```

For Windows:

Use the below entry in the Chrystoki.conf file under the "`C:\Program Files\SafeNet\LunaClient`" directory:

Cryptoki with Logging

```
[Chrystoki2]
LibNT=C:\Program Files\SafeNet\LunaClient\win32\cklog201.dll
[CkLog2]
LibNT=C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll
Enabled=1
NewFormat=1
File=C:\ LogLunaSA2.txt
Error=C:\ ErrorLunaSA2
```

Cryptoki without Logging

```
[Chrystoki2]
LibNT=C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll
```

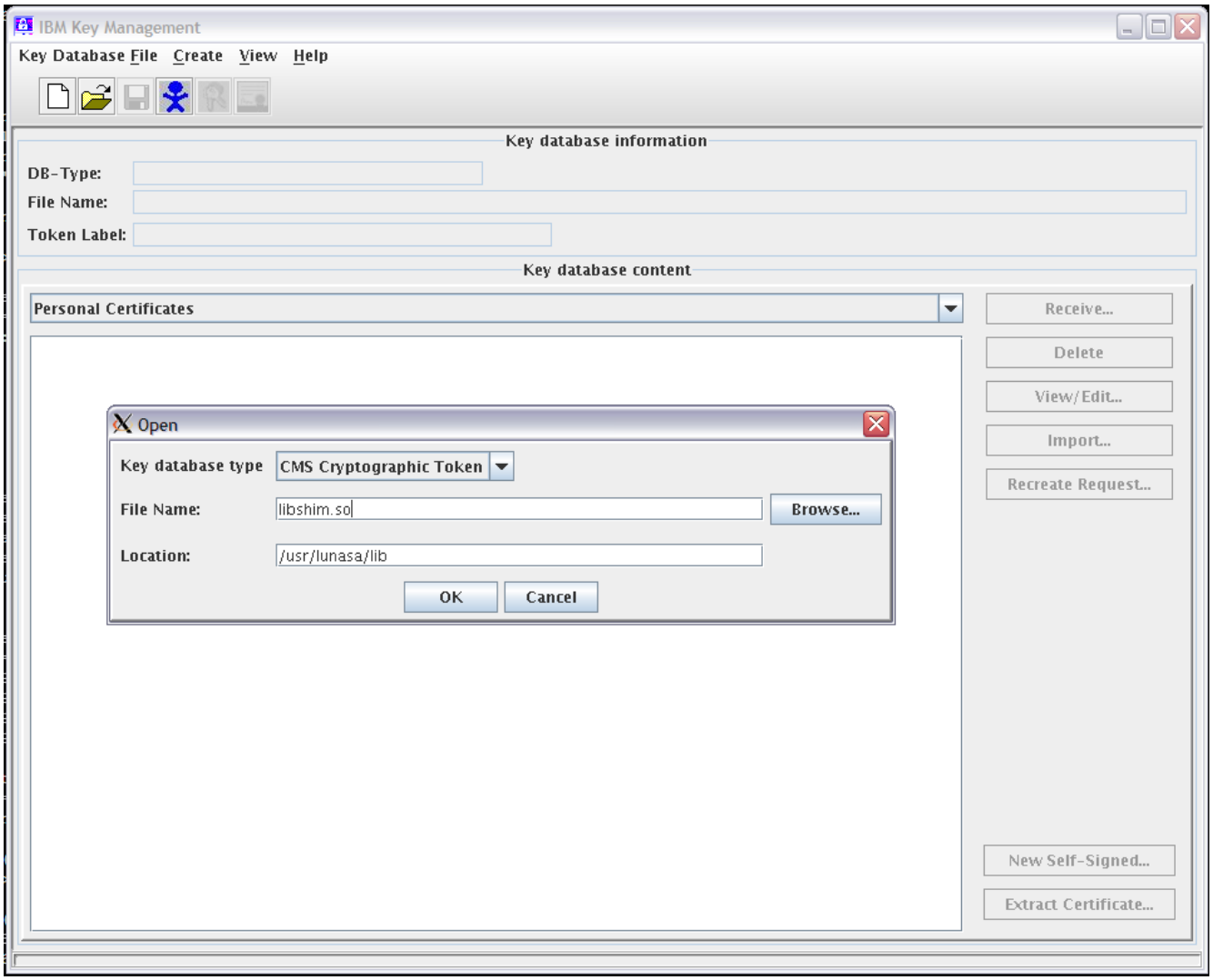
Open IBM Key Management Utility

For AIX:

- Traverse to the directory "`/usr/opt/ibm/gsksa/bin/`" and execute `gsk7ikm_64`.

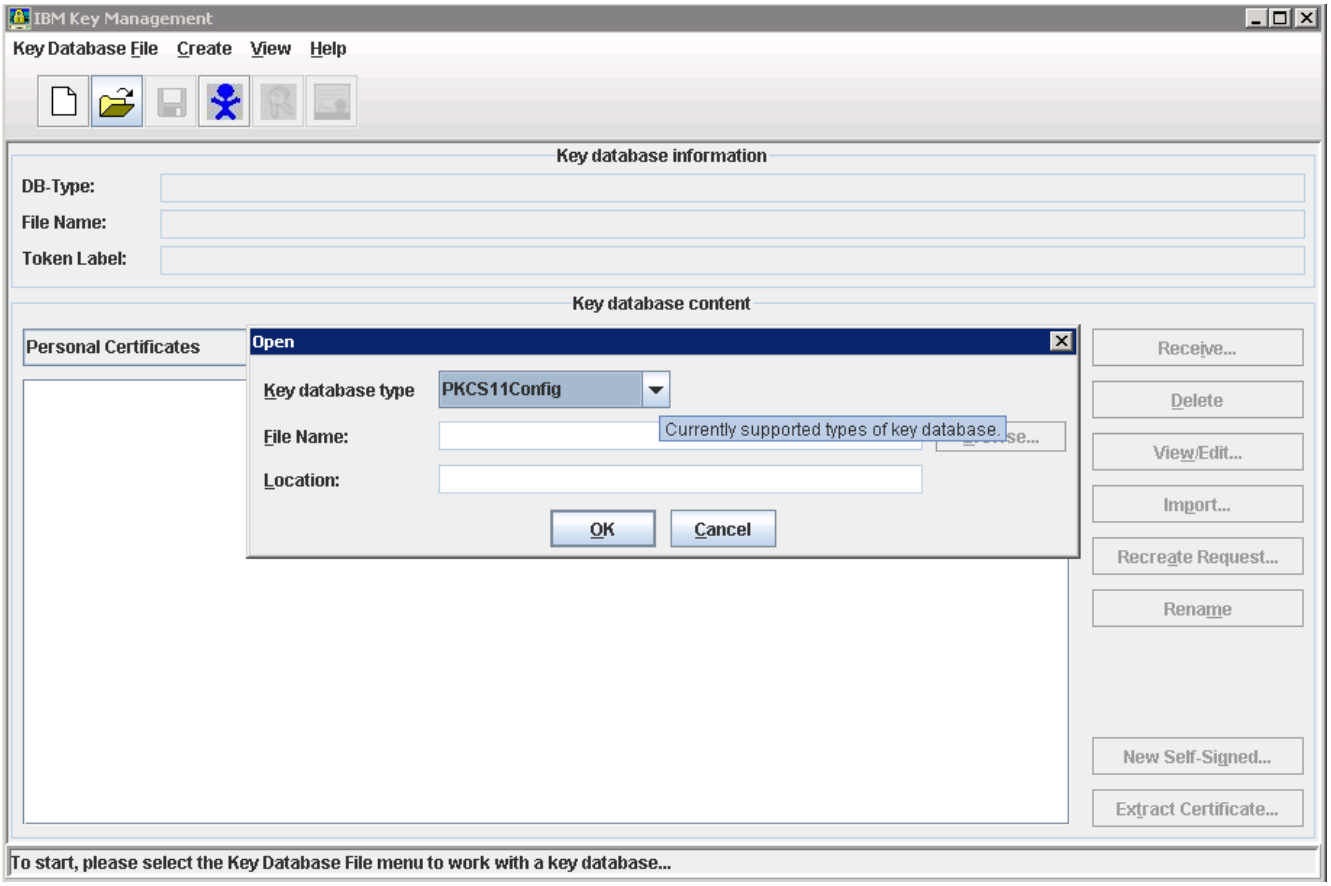
  The **Cryptographic Token** menu option appears.

- Select **Open** option from the **Key Database File** menu. Specify **Key Database Type** as **CMS Cryptographic Token**, **File Name** as **libshim.so** and **Location** as `<Luna Client installation path>/lib`. Click **OK**.



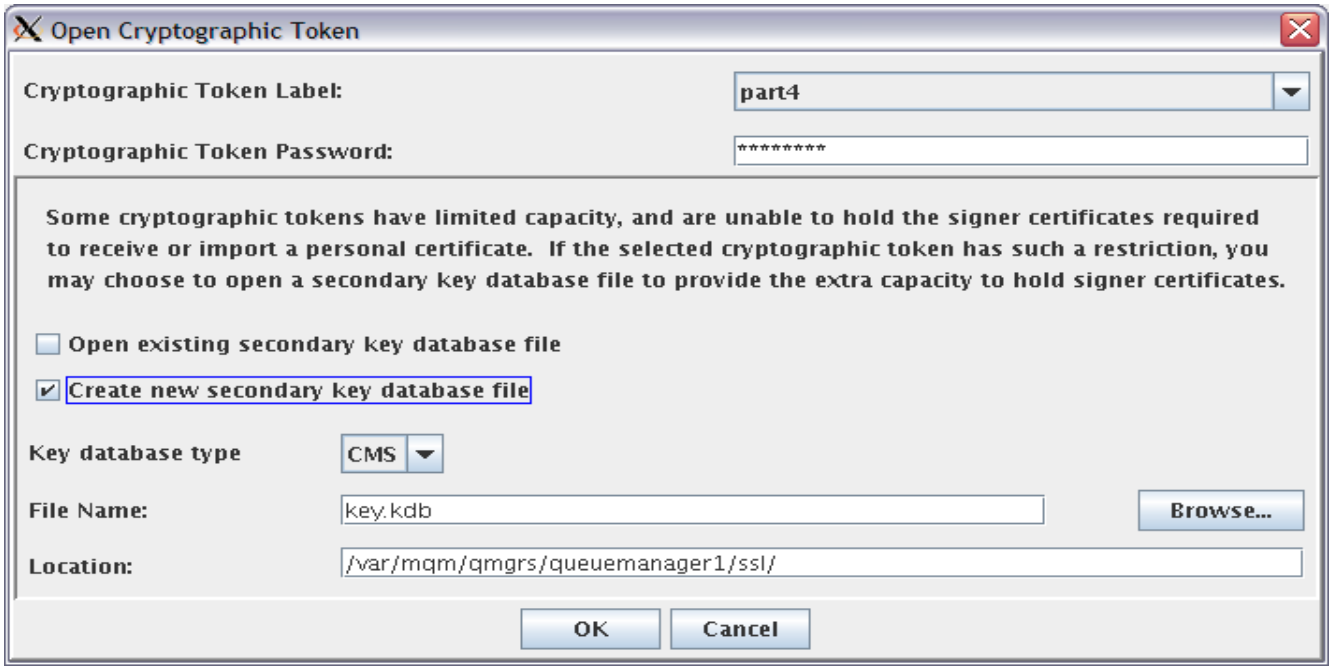
For Windows:

- From **Start** menu, open **IBM WebSphere MQ** > **IBM Key Management**
- Select **Open** option from the **Key Database File** menu. Specify **Key Database Type** as **PKCS11Config** and click **OK**.



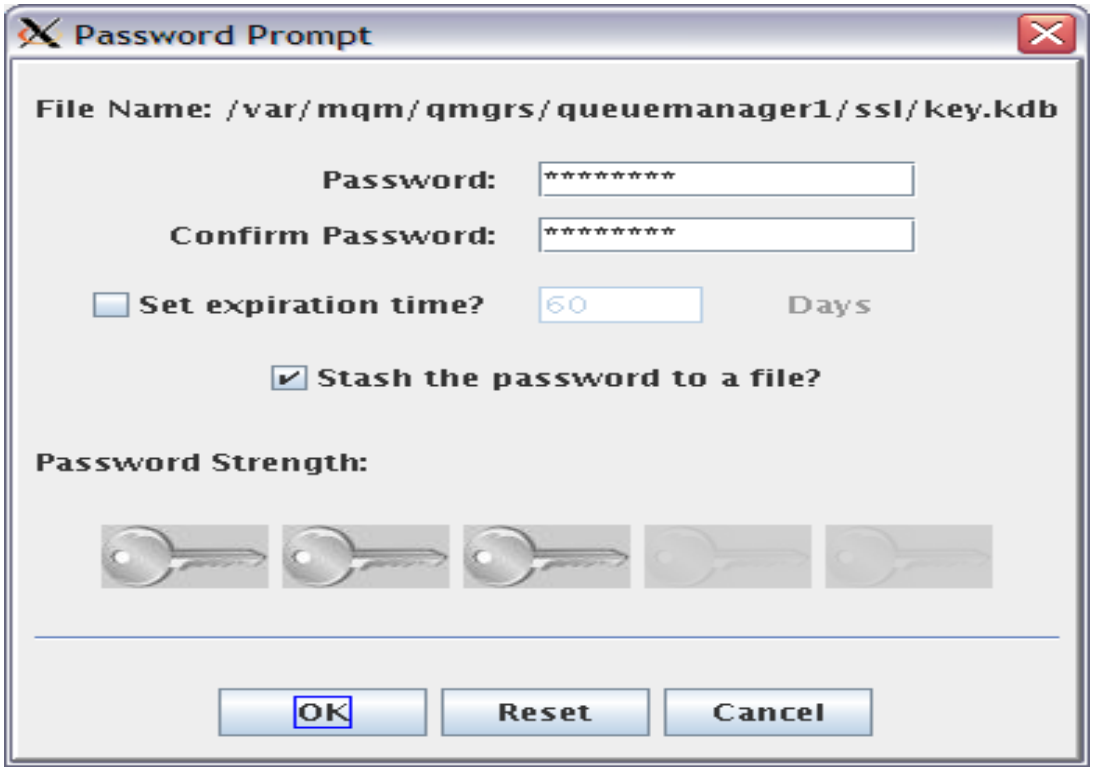
- **Open Cryptographic Token** window displays where **Cryptographic Token Label** represents the partition in which objects will be created. Specify the **SafeNet Luna HSM Partition password** for **Cryptographic Token Password**. You should check on PED device if password/Key is required to be entered.

  AIX Example:



  Windows Example:

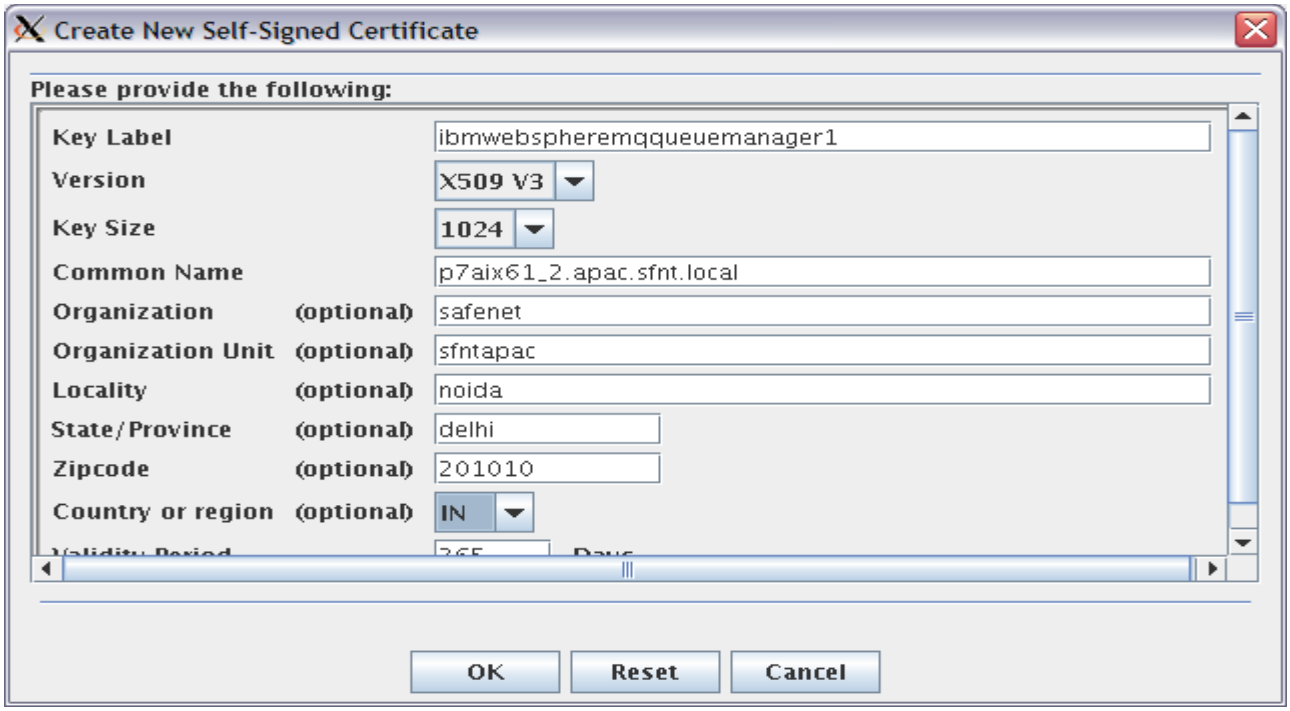
- Select the **Create new secondary key database file** check box to create the CMS Key Database key.kdb in location `/var/mqm/qmgrs/queuemanager1/ssl` on AIX and `C:\Program Files (x86)\IBM\WebSphereMQ\Qmgrs\QM1\ssl` on Windows. You are prompted to create a password to access this file, use **partition password** here. In addition, select the **Stash the password to a file** check box.



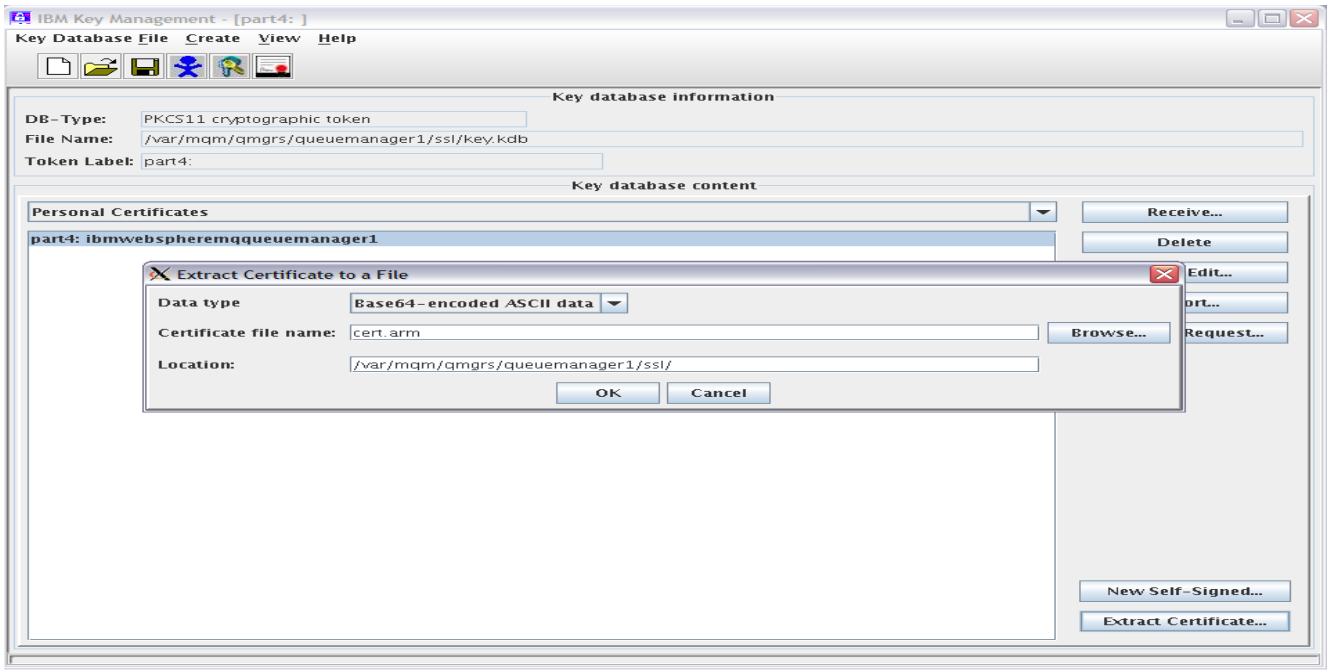
- Select the **Create New Self-Signed Certificate** option from Create menu. Type **key Label** which must be in the format “ibmwebspheremq*xx*” where “xx” is the name of the queue manager.

  For example: ibmwebspheremqqueuemanager1.

  Provide other required information. Click **OK.** RSA Public and Private Keys as well as Self-Signed Certificate now exist on the SafeNet Network HSM Partition. Self-Signed Certificate also displays in the form *<token label>:<key label>*.



- Select the certificate that you have created. Click **Extract Certificate.** The extracted certificate is located at ***/var/mqm/qmgrs/queuemanager1/ssl*** and **`C:\Program Files(x86)\IBM\WebSphereMQ\Qmgrs\QM1\ssl`** directory for AIX and Windows respectively. Click **OK**.



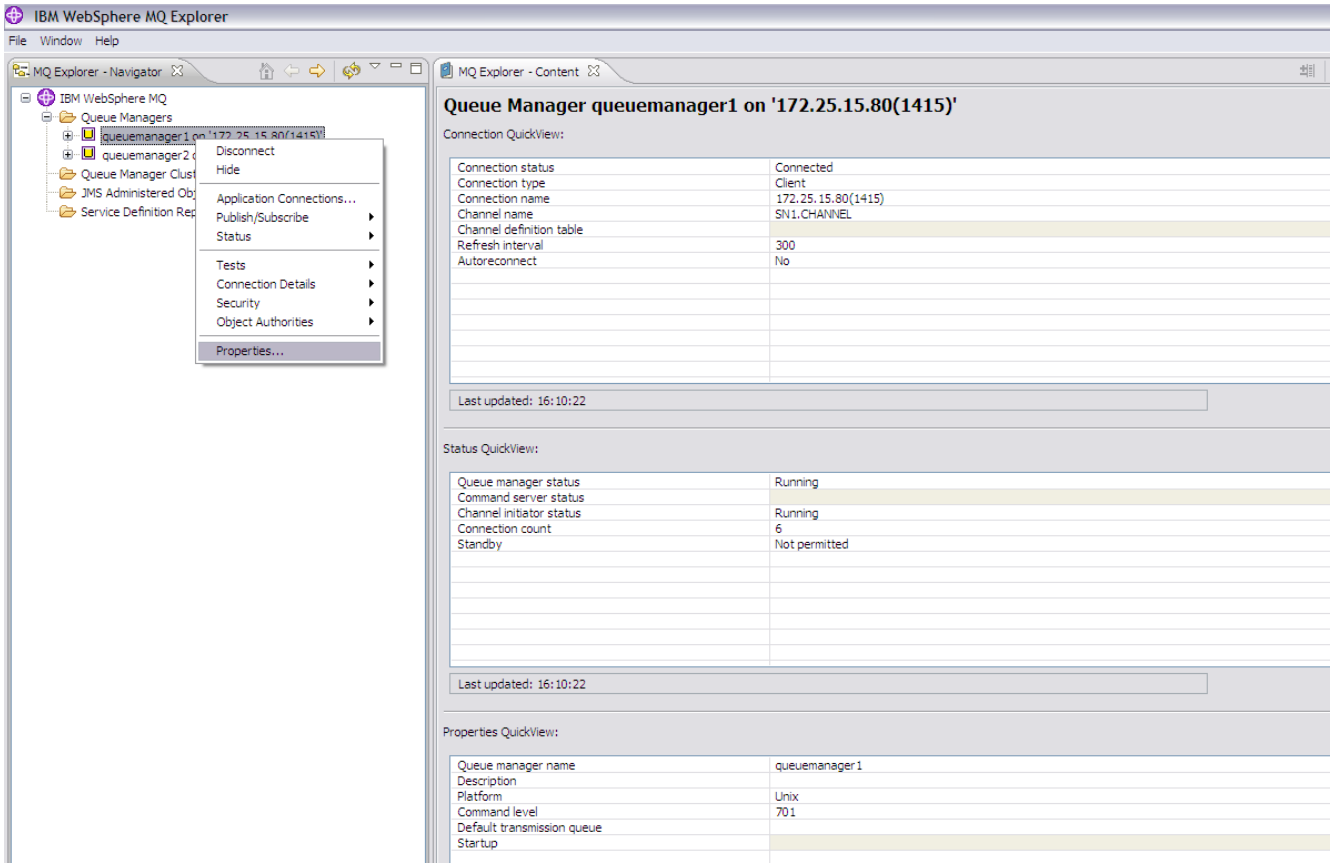
- Select **Key Database File** and click **Exit**.
- Repeat the same steps to create a key repository for **queuemanager2.**

Configure the queue manager to use SSL

For AIX:

- Now uninstall the 32-bit SafeNet Luna HSM client. Go to the directory <Luna Client installation path>/bin and execute the **./uninstall.sh** command.
- Install 64-bit SafeNet Luna HSM client. Go to the `/aix/64` directory of installation media and execute the **sh install.sh** command.

1. Open **IBM WebSphere MQ explorer**, right-click on **queuemanager1**, and click **Properties**.



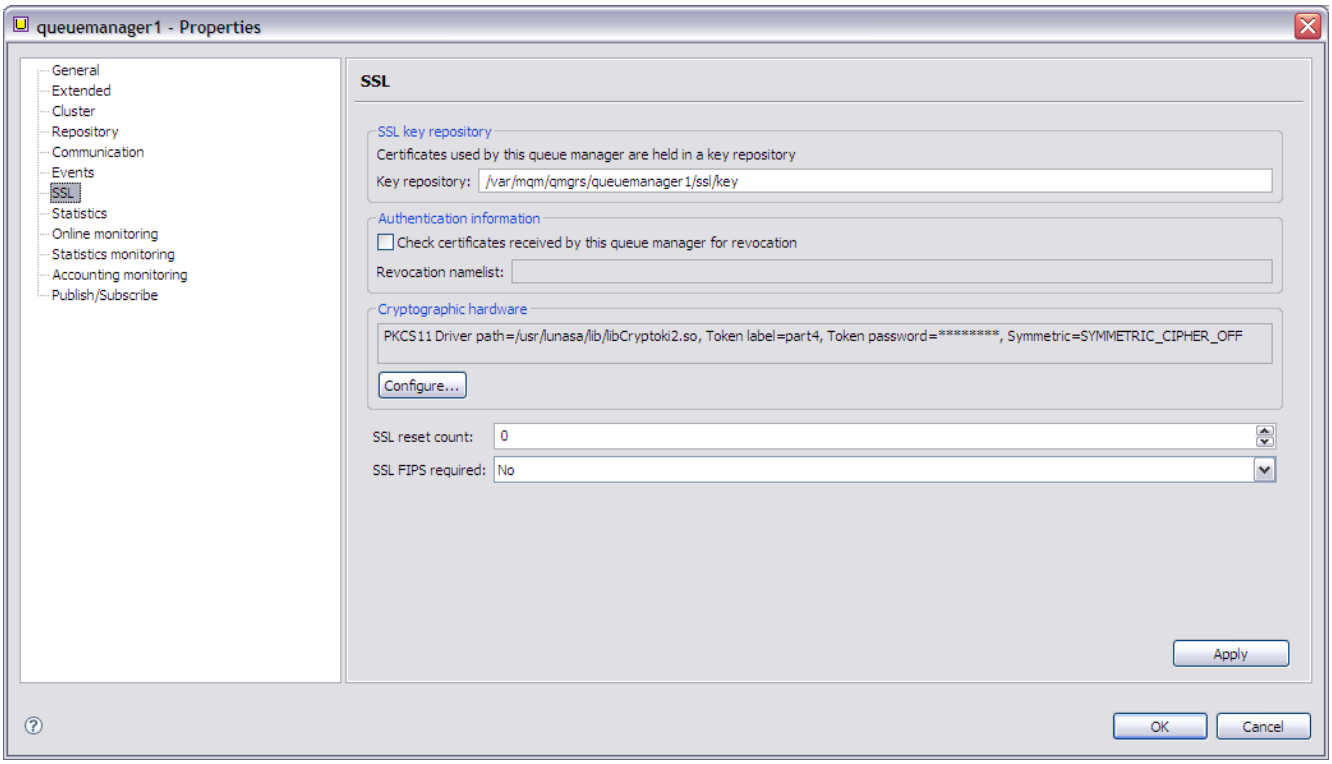
2. In the **Properties** window, select **SSL** and update the **Key repository** field.

For AIX:

```
/var/mqm/qmgrs/queuemanager1/ssl/key
```

For Windows:

```
C:\Program Files (x86)\IBM\WebSphere MQ\Qmgrs\QM1\ssl\key
```



3. Click **Configure**, Select the **other (PKCS11)** check box and update the **Driver path** field.

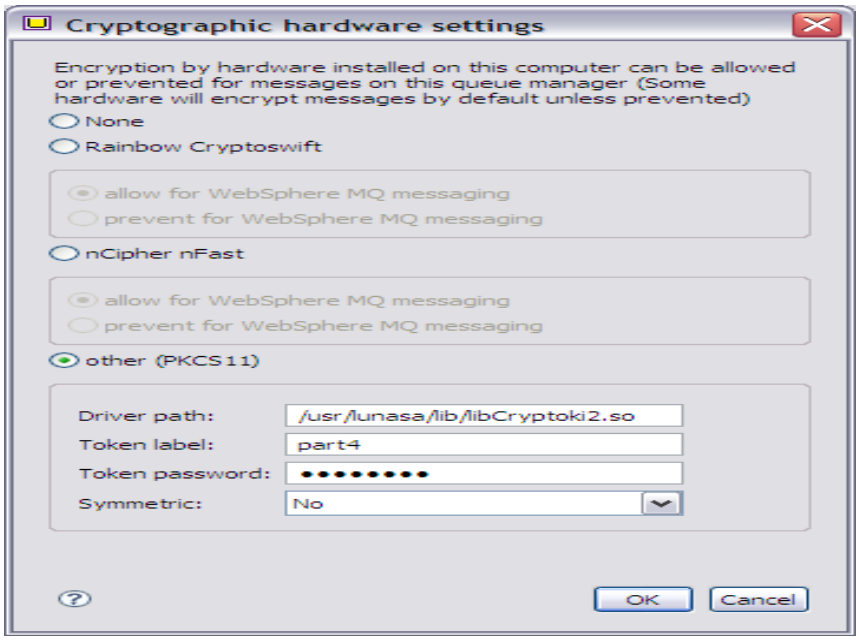
For AIX:

```
<Luna Client installation path>/lib/libCryptoki2.so
```

For Windows:

```
<Luna Client installation path>\win32\cryptoki.dll
```

Provide **Token label** and **Token password**. Click **OK**.



4. Click **Apply** and then **OK**.
5. Right-click on **queuemanager1**, select **Security** and click **Refresh SSL**.
6. Repeat steps one to five for **queuemanager2**.
7. Open MQSC session for queuemanager1 and check properties. Type:

   ```
   runmqsc queuemanager1
   DISPLAY QMGR
   ```

8. Verify the following:

For AIX:

```
SSLCRYP(GSK_PKCS11=/usr/lunasa/lib/libCryptoki2.so;part4;********;SYMMETRIC_CIPHER
_OFF;)
SSLEV(DISABLED) SSLFIPS(NO)
SSLKEYR(/var/mqm/qmgrs/queuemanager1/ssl/key)
```

For Windows:

```
SSLCRYP(GSK_PKCS11=C:\Program Files\SafeNet\LunaClient\win32\cryptoki.dll;par
t1;********;SYMMETRIC_CIPHER_OFF;)
```

9. Repeat steps seven and eight for **queuemanager2**.

Creating sender and receiver channels in both queue managers and testing the connection

1. Open MQSC session for queuemanager2 and define a local queue called QM2.XMITQ using following command:

   ```
   runmqsc queuemanager2
   ```

   ```
   DEFINE QLOCAL(QM2.XMITQ) USAGE(XMITQ)
   ```

2. Define a sender channel called QM1.TO.QM2 using following command:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) CONNAME(<provide full DN here>) XMITQ(QM2.XMITQ)
   SSLCIPH(NULL_MD5) SSLPEER('CN=<provide full DN here>')
   ```

   For example:

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(SDR) CONNAME(p7aix61_2.apac.sfnt.local) XMITQ(QM2.xmitq)
   SSLCIPH(NULL_MD5) SSLPEER('CN=p7aix61_2.apac.sfnt.local')
   ```

3. Start channel using following command:

   ```
   START CHL(QM1.TO.QM2)
   ```

4. Close MQSC session using following command:

   ```
   END
   ```

5. Open MQSC session for queuemanager1 and define a receiver channel

   ```
   runmqsc queuemanager1
   ```

   ```
   DEFINE CHANNEL(QM1.TO.QM2) CHLTYPE(RCVR) TRPTYPE(TCP) SSLCIPH(NULL_MD5) SSLCAUTH(REQUIRED)
   ```

6. Start channel using following command:

   ```
   START CHL(QM1.TO.QM2)
   ```

7. Close MQSC session using following command:

   ```
   END
   ```

8. Open MQSC session for queuemanager2 and ping the channel using following command:

   ```
   runmqsc queuemanager2
   ```

   ```
   PING CHL(QM1.TO.QM2)
   ```

   You should see below mentioned response.

   ```
   Channel 'QM2.TO.QM1' is in use.
          or
   Channel 'QM2.TO.QM1' is in use, now we are getting “AMQ9202: Remote host
   'P7AIX61_2.APAC.SFNT.LOCAL' not available, retry later.”
          or
   AMQ9202: Remote host 'P7AIX61_2.APAC.SFNT.LOCAL' not available, retry later.
   ```

9. Run the below command:

   ```
   DISPLAY CHL(*) ALL
   ```

3
Troubleshooting

Troubleshooting

Problem – 1

Channel cannot be started successfully.

Solution

After configuring SSL on Windows, if you are not able to start sender receiver channel, first verify that all steps are followed correctly. If you are still facing this issue consider changing the HSM password. Sometimes encrypted password contains null characters and IBM MQ is unable to access the HSM.

Problem – 2

Certificate request "xxxxxx" could not be created. The request could not be signed.

Solution

On Windows there is a known problem with IKEYMAN provided with IBM MQ 7.5. CSR cannot be generated using SHA2WithRSA as Signing Algorithm, contact IBM for IKEYMAN fix.

Problem – 3

AMQ8242: SSLCIPH definition wrong. (Window Server 2012R2).

Solution

- Navigate to “`C:\ProgramData\IBM\MQ\Qmgrs\QM1`” and “`C:\ProgramData\IBM\MQ\Qmgrs\QM2`”.
- Open “qm.ini” file in the respective QM.
- Re-enable the SSL V3.0 protocol:

```
SSL:
AllowSSLV3=Y
```

Or

Set the `AMQ_SSL_V3_ENABLE=1` environment variable.