

IBM WebSphere MQ

INTEGRATION GUIDE

SAFENET LUNA HSM



Document Information

Document Part Number	007-011561-001
Release Date	12 December 2019

Revision History

Revision	Date	Reason
F	12 December 2019	Update

Trademarks, Copyrights, and Third-Party Software

© 2019 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Disclaimer

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- > The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- > This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages

resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

CONTENTS

PREFACE	5
Audience	5
Document Conventions	5
Notifications	5
Command Syntax and Typeface Conventions	6
Support Contacts	6
Customer Support Portal	7
Telephone Support	7
Email Support	7
CHAPTER 1: Introduction	8
About IBM WebSphere MQ	8
Third Party Application Details	8
Supported Platforms	8
Prerequisites	9
Configuring the SafeNet Luna HSM	9
Using SafeNet Luna HSM in FIPS Mode	10
Setting up IBM Websphere MQ	10
CHAPTER 2: Integrating IBM Websphere MQ with SafeNet Luna HSM	11
Configuring SSL/TLS for IBM Websphere MQ using SafeNet Luna HSM	11
Starting the Queue Manager	11
Creating TLS certificates for MQ Server and MQ Client using SafeNet Luna HSM	12
Configuring Queue Manager on MQ Server to use SSL/TLS	17
Configuring MQ Client to use SSL/TLS	20
Verifying SSL/TLS connectivity between MQ Server and MQ Client	21

PREFACE

This guide is intended to provide instructions for setting up a small test lab that has IBM WebSphere MQ running with SafeNet Luna HSM to secure the private keys, public keys, and certificates. The guide explains how to install and configure software required for setting up an IBM WebSphere MQ while storing keys and certificates on SafeNet Luna HSM.

Audience

This document is intended to guide administrators through the steps of supporting IBM WebSphere MQ with SafeNet HSMs, including installation, configuration, and integration.

All products manufactured and distributed by Gemalto, Inc. are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

Document Conventions

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

Notifications

This template uses notes, cautions, and warnings to alert you to important information that may help you to complete your task, or prevent personal injury, damage to the equipment, or data loss.

Notes

Notes are used to alert you to important or helpful information.

NOTE: Notes contain important or helpful information.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury.

****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	<p>The bold attribute is used to indicate the following:</p> <ul style="list-style-type: none"> > 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.)
<i>Italic</i>	The italic attribute is used for emphasis or to indicate a related document. (See the <i>Installation Guide</i> for more information.)
Double quote marks	Double quote marks enclose references to other sections within the document.
<variable>	In command descriptions, angle brackets represent variables. You must substitute a value for command line arguments that are enclosed in angle brackets.
[optional] [<optional>]	Square brackets enclose optional keywords or <variables> in a command line description. Optionally enter the keyword or <variable> that is enclosed in square brackets, if it is necessary or desirable to complete the task.
[a b c] [<a> <c>]	Square brackets enclose optional alternate keywords or variables in a command line description. Choose one command line argument enclosed within the braces, if desired. Choices are separated by vertical (OR) bars.
{ a b c } { <a> <c> }	Braces enclose required alternate keywords or <variables> in a command line description. You must choose one command line argument enclosed within the braces. Choices are separated by vertical (OR) bars.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to 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.

Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is a repository where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Gemalto Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@gemalto.com.

CHAPTER 1: Introduction

This document provides the necessary information to install, configure, and integrate IBM WebSphere MQ with SafeNet HSMs. The integration between SafeNet HSMs and IBM WebSphere MQ uses the IBM Java interface to generate the keys and certificates on SafeNet HSMs. SafeNet HSMs integrate with IBM WebSphere MQ to generate 2048 bit RSA key pairs for SSL and provide security by protecting the private keys within a FIPS 140-2 certified hardware security module.

The benefits of using SafeNet HSMs to generate the SSL keys for IBM WebSphere MQ include the following:

- > Secure generation, storage, and protection of the SSL keys on FIPS 140-2 level 3 validated hardware.
- > Full life cycle management of the keys.
- > HSM audit trail.
- > Significant performance improvements by off-loading cryptographic operations from servers.

About IBM WebSphere MQ

IBM MQ supports the exchange of information between applications, systems, services and files by sending and receiving message data via messaging queues. This simplifies the creation and maintenance of business applications. Secure communications that use the TLS cryptographic security protocols involve setting up the communication channels and managing the digital certificates that you will use for authentication.

IBM WebSphere MQ is a family of network software products launched by IBM in March 1992. It was previously known as MQ Series. It allows independent and potentially non-concurrent applications on a distributed system to communicate with each other.

SafeNet HSMs provides key management security for certificates and certificate-based authentication, including import of trusted CA certificates from software based keystore to hardware based keystore, and generation of self-signed certificates and personal certificate requests via the IBM Key Management Utility.

IBM WebSphere MQ can be configured to use SafeNet HSMs for SSL connectivity that utilizes the PKCS #11 APIs through IBM Java.

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

Third Party Application Details

This integration uses the following third party applications:

- > IBM WebSphere MQ

Supported Platforms

List of the platforms which are tested with the following HSMs:

SafeNet Luna HSM: SafeNet Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government

organizations. SafeNet Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing.

The SafeNet Luna HSM on premise offerings include the SafeNet Luna Network HSM, SafeNet PCIe HSM, and SafeNet Luna USB HSMs. SafeNet Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

The following platforms are supported for IBM WebSphere MQ:

IBM WebSphere MQ	Platforms Tested
IBM WebSphere MQ v9.1.0 FP2 with IT15253 (Patch 9.1.0.2-IBM-MQ-Win64-TF55486)	Windows Server 2016

The Patch 9.1.0.2-IBM-MQ-Win64-TF55486 can be obtained from IBM Support which fixes the HSM Password issue “AMQ9671E: The PKCS #11 token password specified is invalid.” at MQ Client end when communicating to HSM using password provided in MQClient.ini file. The APAR for this fix is IT30722 which can be downloaded from IBM ecurep on request.

NOTE: If you are using older versions of IBM Websphere MQ, please refer the earlier Safenet Luna HSM integration guide “*IBM_WebSphere_MQ_Integration_Guide_RevE*”

Prerequisites

Before you proceed with the integration, complete the following processes:

Configuring the SafeNet Luna HSM

SafeNet Luna HSMs provide strong physical protection of secure assets, including keys, and should be considered a best practice when building systems based on IBM Websphere MQ.

To configure the SafeNet Luna HSM

1. Ensure that the HSM is set up, initialized, provisioned and ready for deployment. Refer to the HSM product documentation for help.
2. Create a partition that will be later used by IBM Websphere MQ. It is recommended to use separate partition for MQ Client and MQ Server.
3. Register clients for the MQ Client and MQ Server hosts and assign each client to its corresponding partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partitions.
4. Ensure that the partitions are successfully registered and configured. The command to see the registered partitions is:

```
C:\>"C:\Program Files\SafeNet\LunaClient\lunacm.exe"
```

```
lunacm.exe (64-bit) v7.3.0-165. Copyright (c) 2018 SafeNet. All rights reserved.
```

```
Available HSMs:
```

```
Slot Id -> 0
```

```
Label -> ibmmq
```

```

Serial Number ->      1280780175928
Model ->              LunaSA 7.3.0
Firmware Version ->   7.3.0
Configuration ->      Luna User Partition With SO (PW) Key Export With
Cloning Mode
Slot Description ->    Net Token Slot
Current Slot Id: 0

```

5. For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

NOTE: Follow the SafeNet Network Luna HSM documentation for detailed steps for creating NTLS connection, initializing the partitions, and various user roles.

Ensure that the SafeNet Luna HSM partition label is in lowercase letters (as required by IBM Websphere MQ), for example 'ibmmq'. Also, the partition password must be in lowercase and not contain any special characters, for example "temp1234".

Using SafeNet Luna HSM in FIPS Mode

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using the SafeNet Luna HSM in FIPS mode, you have to make the following change in configuration file:

```

[Misc]
RSAKeyGenMechRemap = 1

```

The above setting redirects the older calling mechanism to a new approved mechanism when SafeNet Luna HSM is in FIPS mode.

Setting up IBM Websphere MQ

IBM WebSphere MQ (Server or Client) must be installed on the target machines to carry on with the integration process. You can install IBM WebSphere MQ explorer for a Windows or Linux system. 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. For a detailed installation procedure, refer to the IBM WebSphere MQ documentation.

https://www.ibm.com/support/knowledgecenter/en/SSFKSJ/com.ibm.mq.helphome.doc/product_welcome_wmq.htm

CHAPTER 2: Integrating IBM Websphere MQ with SafeNet Luna HSM

Integration of IBM Websphere MQ with SafeNet Luna HSM involves two stages:

- > Configuring SSL/TLS for IBM Websphere MQ using SafeNet Luna HSM
- > Verifying SSL/TLS connectivity between MQ Server and MQ Client

Configuring SSL/TLS for IBM Websphere MQ using SafeNet Luna HSM

To set up your SSL/TLS installation, you must start the queue manager, obtain and manage your digital certificates, and define your channels to use TLS. On a test system, you can use self-signed certificates or certificates issued by a local certificate authority (CA). On a production system, use certificates issued by a trusted CA.

Starting the Queue Manager

Before you can use messages and queues, you must create and start at least one queue manager and its associated objects.

To create and start the Queue Manager

1. Log on to the IBM MQ Server as Administrator and create a queue manager, if not created already.
2. To create the queue manager, open the command prompt from the <IBM MQ Installation Directory>/bin folder and then run the following command:

```
C:\Program Files\IBM\MQ\bin>crtmqm.exe QM1
```

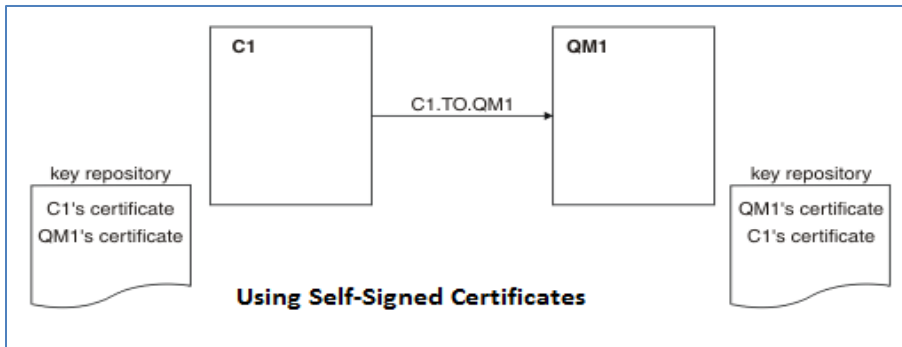
Where **QM1** is queue manager name.

3. After creating the queue manager, start the queue manager using the following command:

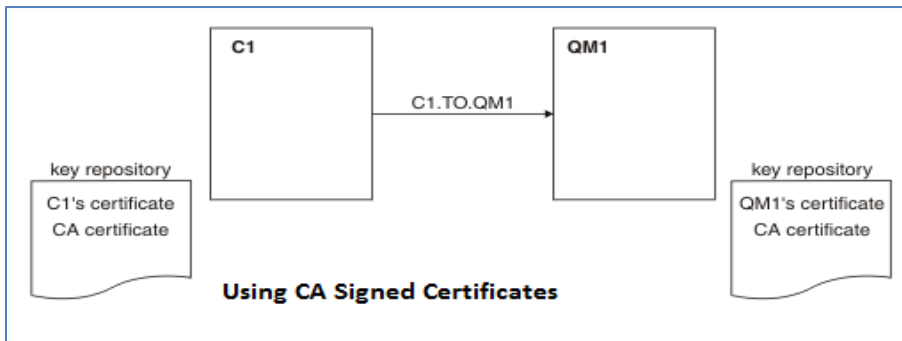
```
C:\Program Files\IBM\MQ\bin>strmqm.exe QM1
```

Creating TLS certificates for MQ Server and MQ Client using SafeNet Luna HSM

You can use a self-signed certificate or CA signed certificate as per your requirement. The steps provided here depict how to use a self-signed certificate. To use a CA signed certificate, you need to obtain the CA signed certificate and import both the CA certificate and the signed certificate into the key database.



In the above figure, the key repository for QM1 contains the certificate for QM1 and the public certificate from C1. The key repository for C1 contains the certificate for C1 and the public certificate from QM1.



In the above figure, the key repository for C1 contains certificate for C1 and the CA certificate. The key repository for QM1 contains the certificate for QM1 and the CA certificate.

To create the SSL/TLS certificate/key on SafeNet Luna HSM,

NOTE: These steps configure both MQ Server and MQ Client.

1. Log on to the IBM MQ Server using the Administrator account or user added in the MQM group.
2. Create the **luna.cfg** file with the following contents and save the file at any location.

```
-----
name = LUNA
library = C:\Program Files\SafeNet\LunaClient\cryptoki.dll
description = Luna config
slotListIndex = 0
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
}

```

3. Open <IBM MQ installation directory>\java\jre\lib\security\java.security file and edit IBMPKCS11 provider with the path to luna.cfg as follows:

```

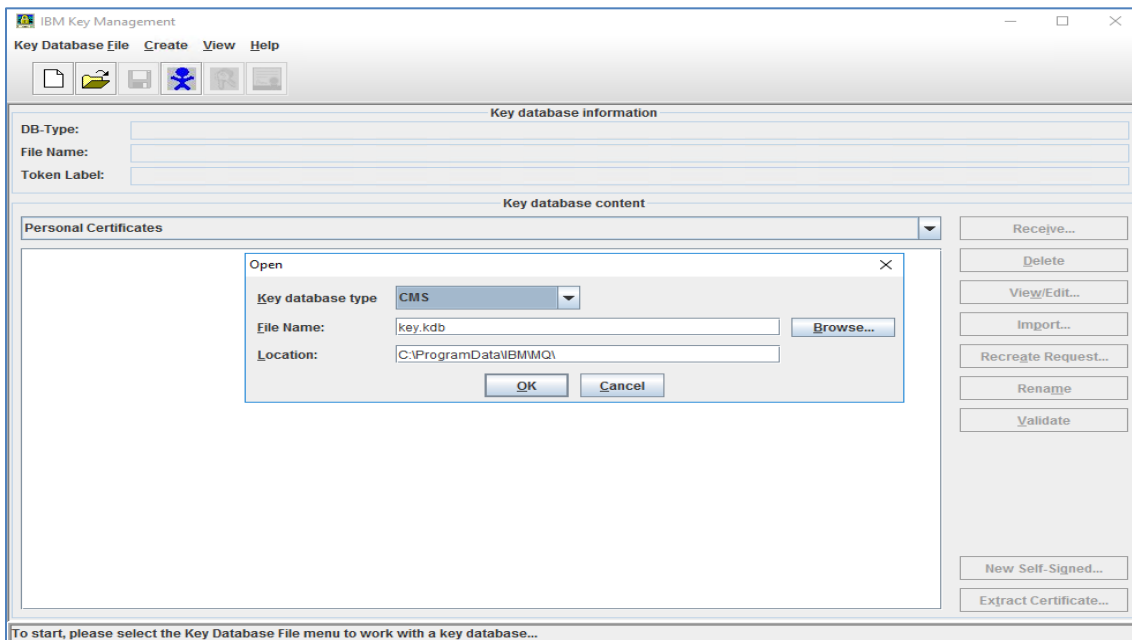
-----
security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPSProvider
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.crypto.provider.IBMJCE
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
c:\\luna.cfg
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=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.12=sun.security.provider.Sun
security.provider.13=com.ibm.security.cmskeystore.CMSProvider
-----

```

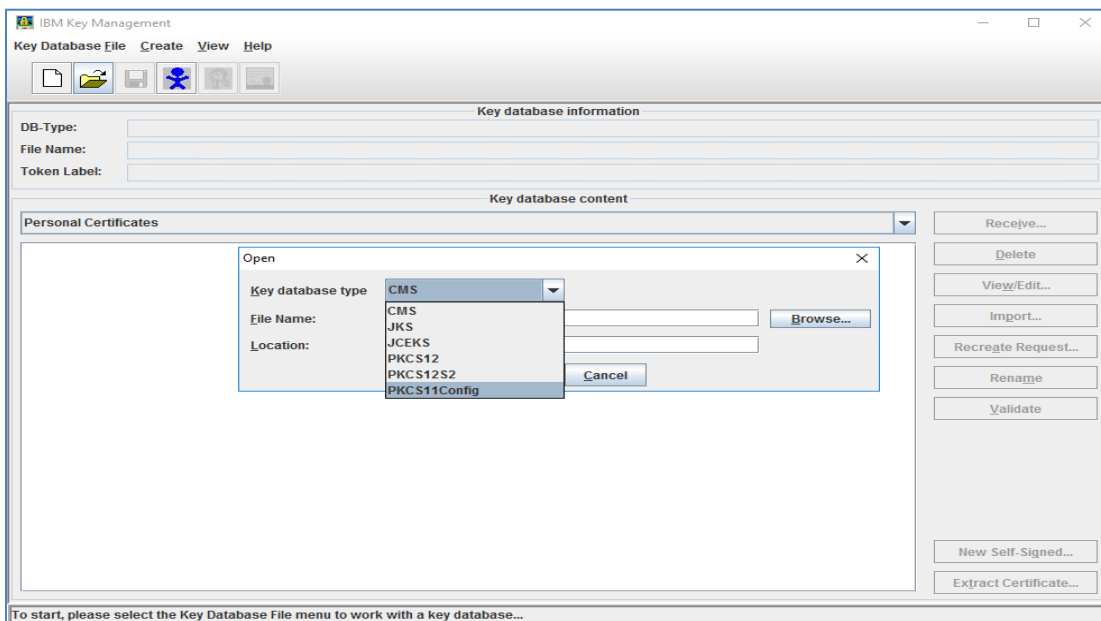
4. Run the **strmqikm.exe** from the <IBM MQ installation directory>/bin directory.

```
C:\Program Files\IBM\MQ\bin>strmqikm.exe
```

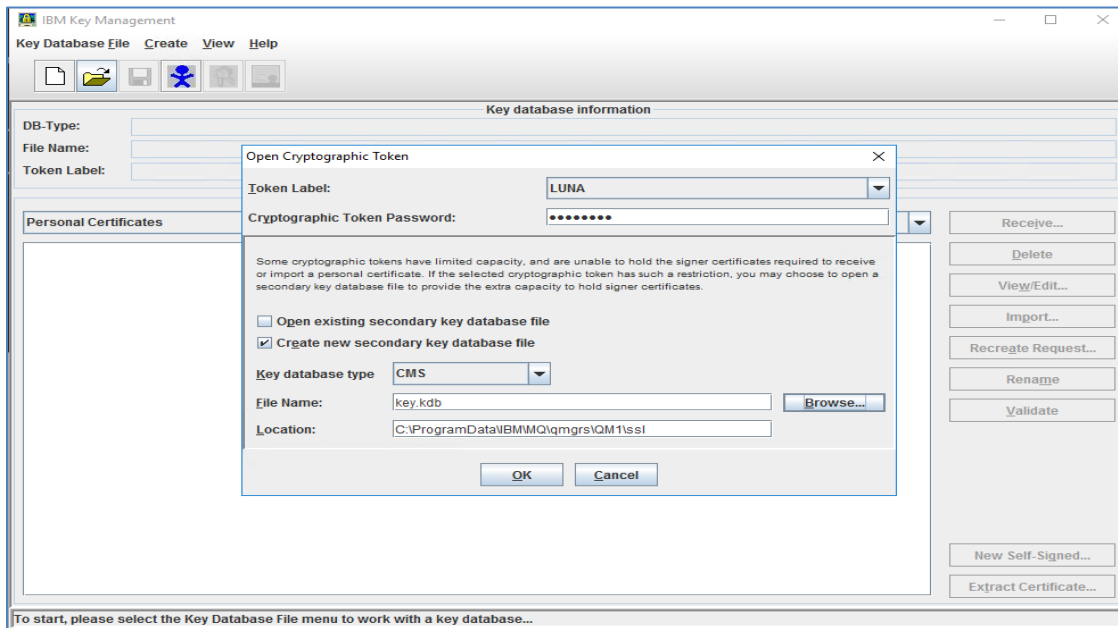
5. When **IBM Key Management** windows pops up, click **Key Database File > Open**.



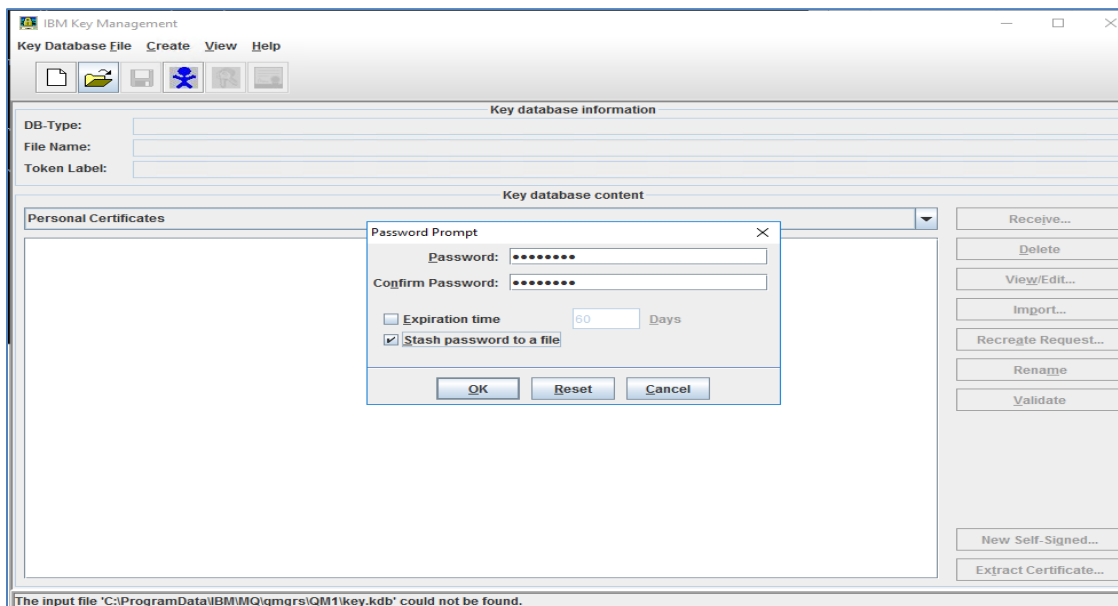
6. Select **PKCS11Config** from **Key database type** drop-down and click **OK**.



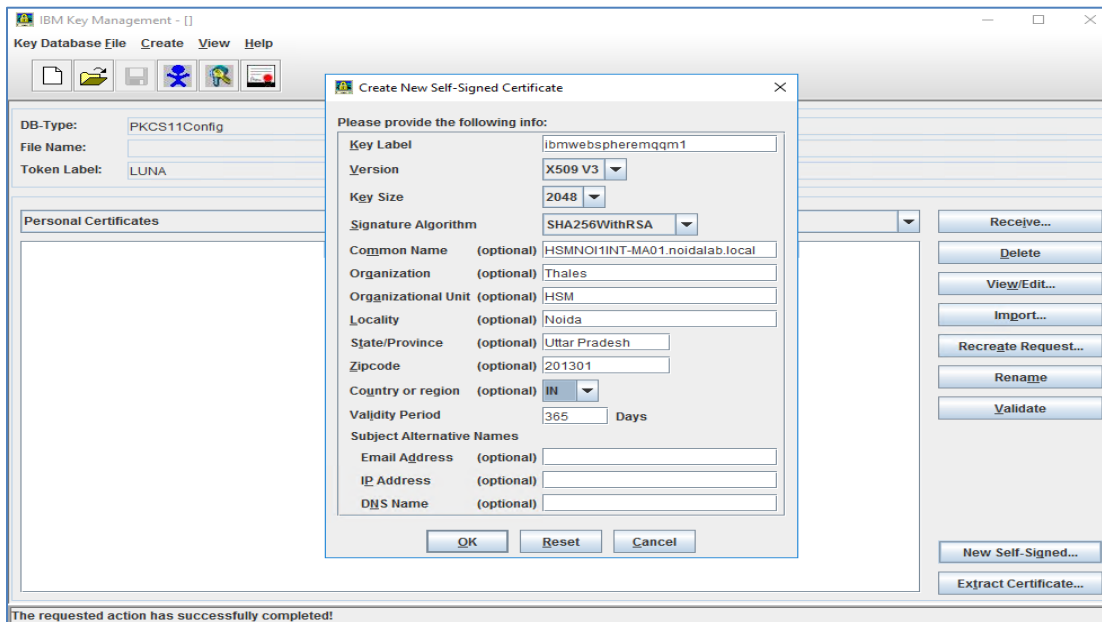
7. Enter partition password in **Cryptographic Token Password**, select **Create new secondary key database file**, and then click **Browse...** to select the **key.kdb** file location. Click **OK** after selecting the file location.



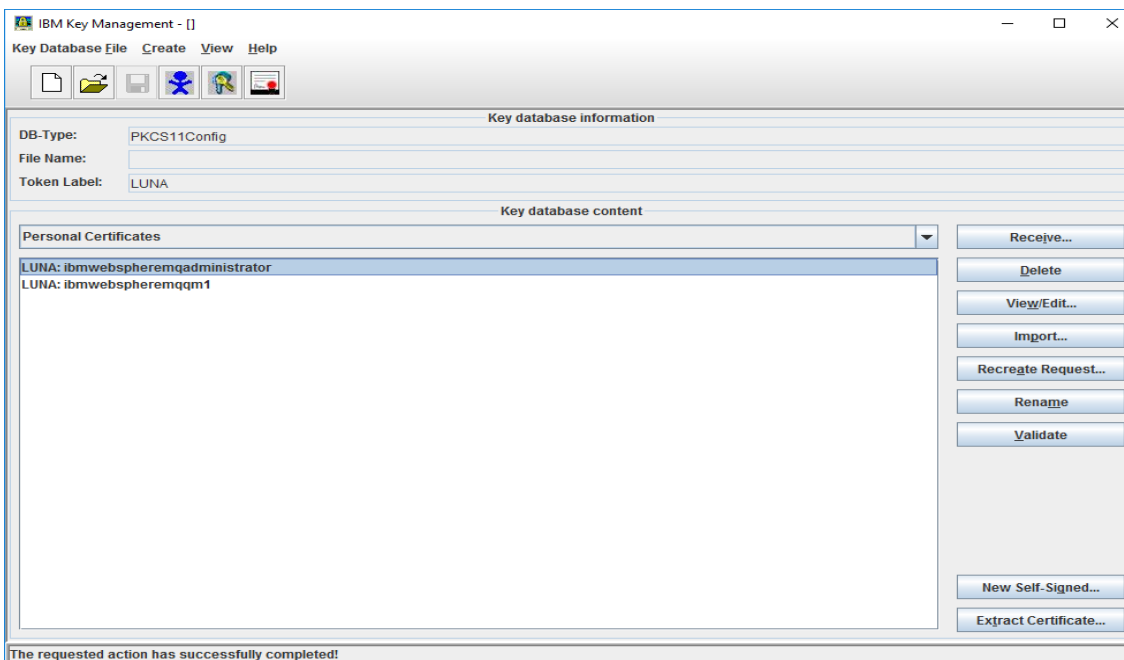
8. A password prompt window will pop up. Create a password for **key.kdb** file, select the **Stash password to a file**, and then click **OK**.



9. Click **Create > New Self-Signed Certificate**. Enter the **Key Label** in lowercase letters in the specific format “**ibmwebspheremq+queue name**”, where queue name is the name of the queue manager. Enter all other details for the certificate and then click **OK**.



10. Log on to the IBM MQ Client using the administrator or user account added in the MQM group.
11. Repeat steps 1-9 for MQ Client to generate the IBM MQ Client certificate, while ensuring that IBM MQ Client Key Label also has the specific format “**ibmwebspheremq+<logged_in_user>**” with lowercase letters. Both MQ Server and Client Certificates are generated on the SafeNet Luna HSM partition and are visible under Personal Certificates.



NOTE: For demonstration purpose in this guide, the same partition and self-signed certificate is used for both MQ Server and Client, but it is recommended to use separate partition and CA signed certificates for MQ Server and Client.

12. Export the Server Certificate. To export the MQ Server certificate, select the certificate under **Personal Certificate** and click **Extract Certificate...**, save the certificate file and transfer the file to the MQ Client.
13. To import the Server Certificate on MQ Client, select **Signer Certificate** from **Key database content** drop-down and click **Add...** browse the server certificate you transferred, and click **OK** to add the Server certificate. Provide a label for the certificate and click **OK**.
14. Repeat steps 12-13 to export the Client certificate and add it to the Server certificate database.

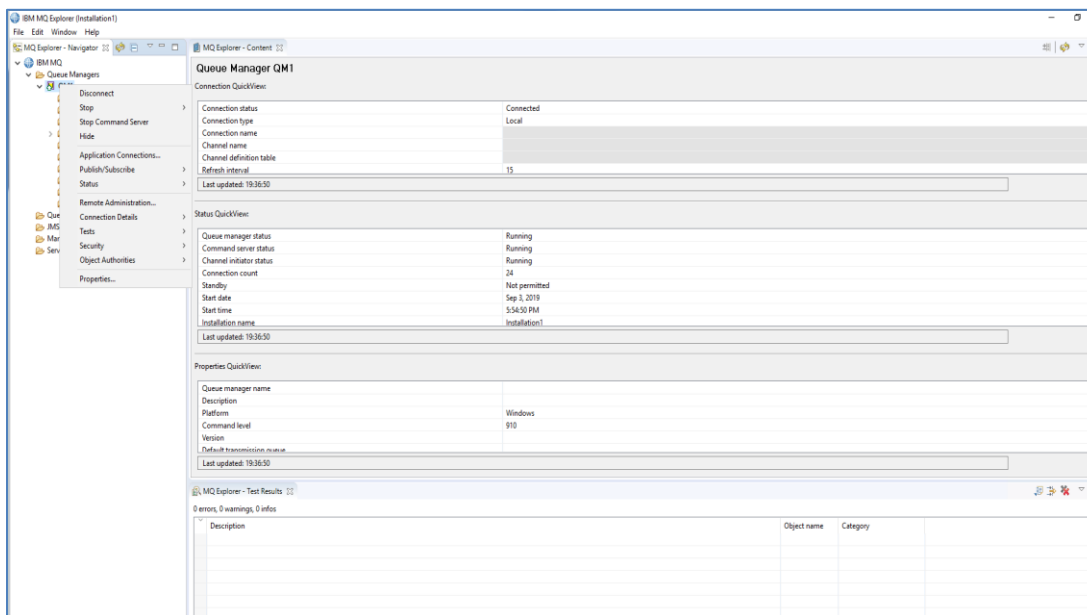
NOTE: If you are using a CA signed certificate, you are required to add the CA public certificate of MQ Server and MQ Client in certificate database of MQ Client and MQ Server, respectively.

Configuring Queue Manager on MQ Server to use SSL/TLS

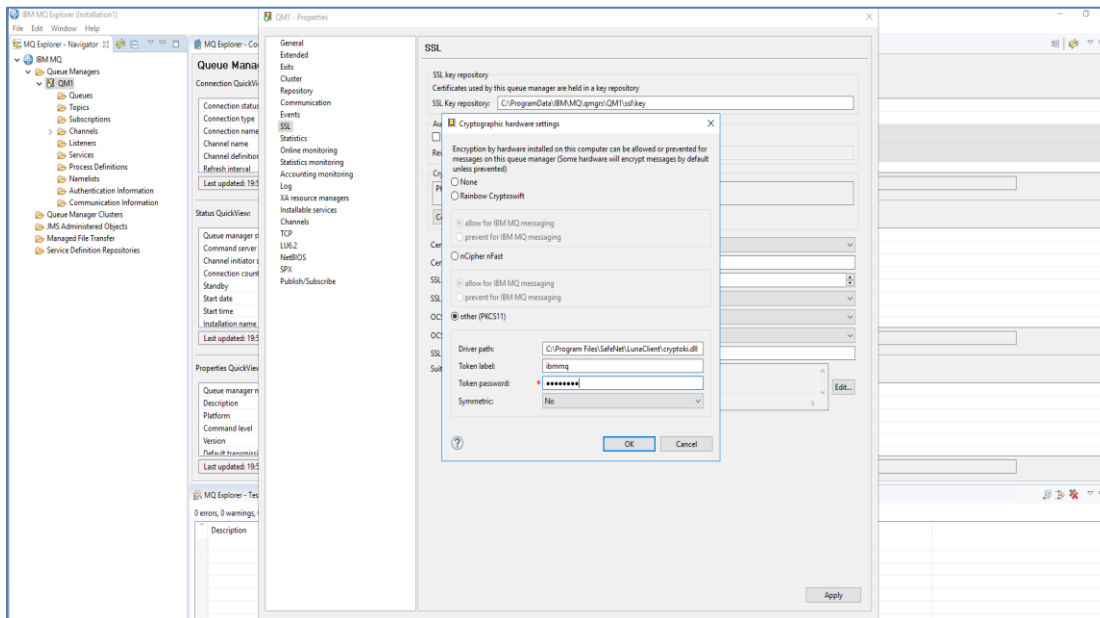
IBM MQ Server must be configured to use the SafeNet Luna HSM for certificate and keys used to create the SSL/TLS connection with client.

To configure the IBM MQ Server

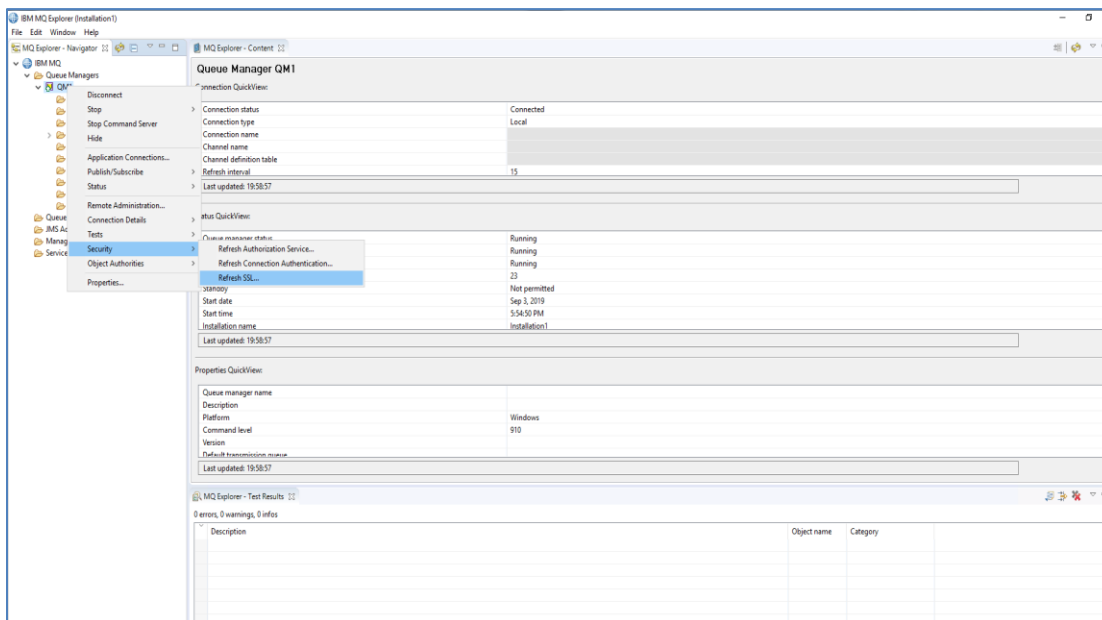
1. Log on to the IBM MQ Server using Administrator or user added in the MQM group.
2. Run the **MQExplorer.exe** from the <IBM MQ installation directory>/bin directory.
`C:\Program Files\IBM\MQ\bin>MQExplorer.exe`
3. In MQ Explorer–Navigator pane, expand **IBM MQ > Queue Managers**, right-click on queue manager you have created, and then click **Properties...**



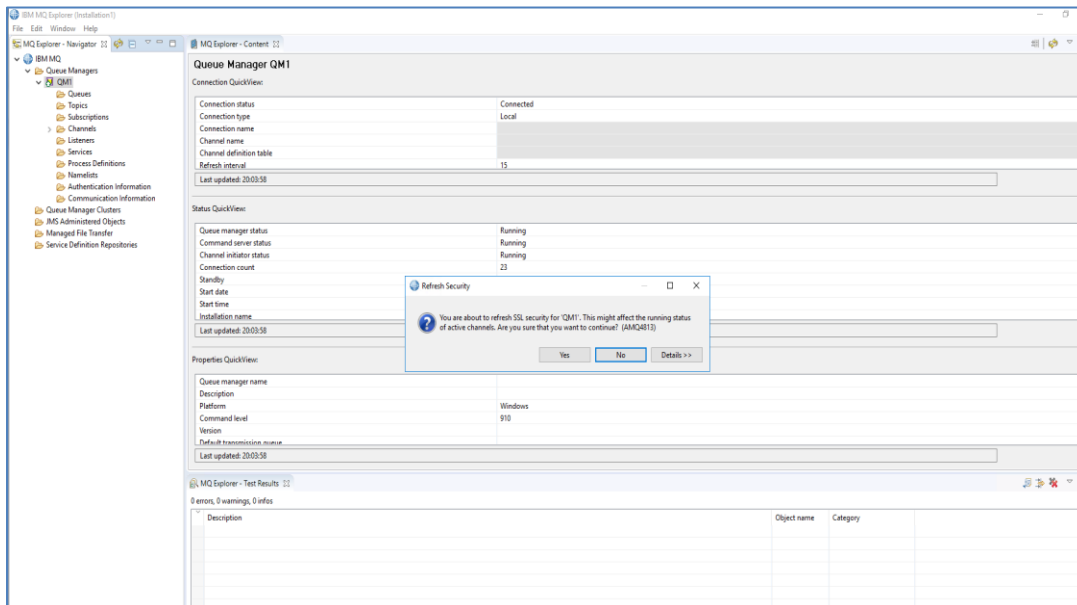
4. In Queue Manager-Properties window, click **SSL** from the menu on the right side and then **Configure...** under the **Cryptographic hardware** section. Select **other (PKCS11)** and enter the **Driver path** (**C:\Program Files\SafeNet\LunaClient\cryptoki.dll**), **Token label** and **Token password**. Click **OK**.



5. Click **Apply** and then **OK** to close the Properties window.
6. Right Click on Queue Manager and click **Security > Refresh SSL...**



7. A message will pop up to ensure that you are refreshing the SSL security. Click **Yes** to refresh the SSL settings.



8. Enable MQSC commands for queue manager.

```
C:\Program Files\IBM\MQ\bin>runmqsc.exe QM1
```

9. Verify the **SSLCRYP** and **SSLKEYR** value.

```
DISPLAY QMGR
```

```
SSLCRYP(GSK_PKCS11=C:\Program  
Files\SafeNet\LunaClient\cryptoki.dll;ibmmq;*****;)
```

```
SSLKEYR(C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl\key)
```

10. On QM1, create a listener for the connection channel.

```
DEFINE LISTENER(QM1.TCP) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)
```

Where **LISTENER** is the user-defined name, such as **QM1.TCP**.

11. Start the listener.

```
START LISTENER(QM1.TCP)
```

12. Check the status of listener.

```
DISPLAY LSSTATUS(QM1.TCP)
```

13. Create server connection channel.

```
DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) MCAUSER('MUSR_MQADMIN')  
SSLCAUTH(REQUIRED) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) DESCR('Server  
channel using SSL from C1 to QM1')
```

Where:

- **CHANNEL** is the user-defined channel name.
- **MCAUSER** is the user added in the MQM group.

14. Start the channel.

```
START CHANNEL(C1.TO.QM1)
```

15. Create a client connection channel.

```
DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(CLNTCONN) TRPTYPE(TCP) CONNAME('HSMNOI1INT-
MA01.noidalab.local') QMNAME(QM1) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256)
DESCR('Client channel using SSL from C1 to QM1')
```

Where **CONNAME** is the hostname or IP of the MQ Server.

NOTE: Ensure that channel name and SSL cipher for client connection channel match the server connection channel.

16. Create channel authentication record to authorize the client when it connects to MQ Server.

```
SET CHLAUTH(C1.TO.QM1) TYPE(ADDRESSMAP) ADDRESS('HSMNOI1INT-
MA02.noidalab.local') MCAUSER('MUSR_MQADMIN')
```

Where:

- **ADDRESS** is the hostname or IP of the MQ Client.
- **MCAUSER** is the user authorized to use channel.

NOTE: For channel authentication type other than ADDRESSMAP, refer the IBM MQ Documentation.

17. Create a local queue on QM1.

```
DEFINE QLOCAL(QM1.LQ)
```

Where **QLOCAL** is the user defined local queue.

18. To close MQSC, type **END** and then press **Enter**.

19. Restart the queue manager to apply all the changes. To restart, run the following commands:

```
C:\Program Files\IBM\MQ\bin>endmqm.exe QM1
C:\Program Files\IBM\MQ\bin>strmqm.exe QM1
```

Configuring MQ Client to use SSL/TLS

MQ Client SSL keys and certificate are already generated on the SafeNet Luna HSM. Now you need to configure the MQ Client to use these keys and certificate while establishing the SSL connection with MQ Server. To configure the client, perform the following steps:

1. Log on to the IBM MQ Client using the Administrator account.
2. To configure Hardware Cryptographic Token, add the SSL stanza in the **mqclient.ini** file available at the **C:\ProgramData\IBM\MQ** directory.

SSL:

```
SSLCryptoHardware=GSK_PKCS11=C:\Program
Files\SafeNet\LunaClient\cryptoki.dll;ibmmq;userpin1;SYMMETRIC_CIPHER_OFF
SSLKeyRepository=C:\ProgramData\IBM\MQ\key
```

Where:

- **SSLCryptoHardware** is a string in the format: GSK_PKCS11 = driver path and filename;token label;token password;symmetric cipher setting and

- **SSLKeyRepository** is the location of key repository that holds the user's digital certificate in stem format. That is, it includes the full path and the file name without an extension.
3. Copy the Client Channel Definition Table (**AMQCLCHL.TAB**) from MQ Server to MQ Client.

The Client Channel Definition Table is located at the following location on the MQ server:

`C:\ProgramData\IBM\MQ\qmgrs\QM1\@ipcc\`

Copy the **AMQCLCHL.TAB** file to MQ Client at `"C:\ProgramData\IBM\MQ"`.

Verifying SSL/TLS connectivity between MQ Server and MQ Client

The TLS (Transport Layer Security) protocol enables queue managers to communicate securely with other queue managers or clients. When a queue manager connects to another queue manager or client, the two carry out a standard TLS exchange of certificates and validation checks. If the validation is successful, the connection is established. To achieve this, queue managers and client, as well as the channels that they use, must be configured with the appropriate certificate settings.

When messages are sent from one queue manager to another queue manager or client along a channel, the data is generally encrypted using a session key that has been established during the certificate exchange. To achieve this, you must configure the channels that you use with appropriate cipher specs.

You have already generated the certificates on SafeNet Luna HSM and have configured both queue manager and clients to use the TLS connection through the channel created and authenticated using Channel Authentication Record. To verify SSL/TLS connectivity between MQ server and MQ client:

1. Log on to the IBM MQ Client through the Administrator account.
2. Open the command prompt and set the following environment variables:

```
set MQCHLLIB=C:\ProgramData\IBM\MQ
```

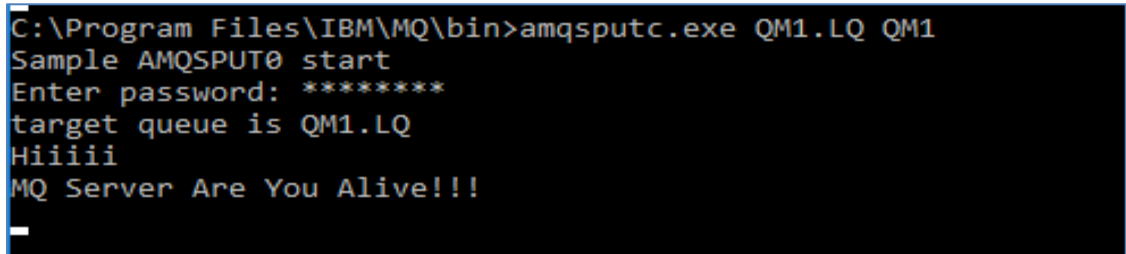
```
set MQCHLTAB=AMQCLCHL.TAB
```

```
set MQSAMP_USER_ID=MUSR_MQADMIN
```

Where:

- **MQCHLLIB** is the location of the Client Channel Definition Table.
 - **MQCHLTAB** is the Client Channel Definition Table copied from the MQ Server.
 - **MQSAMP_USER_ID** is the user authorized in MQ Server channel authentication record.
3. Now run the following command to create the SSL connection from client to server and put messages in the MQ Server queue.

```
C:\Program Files\IBM\MQ\bin>amqsputc.exe QM1.LQ QM1
```

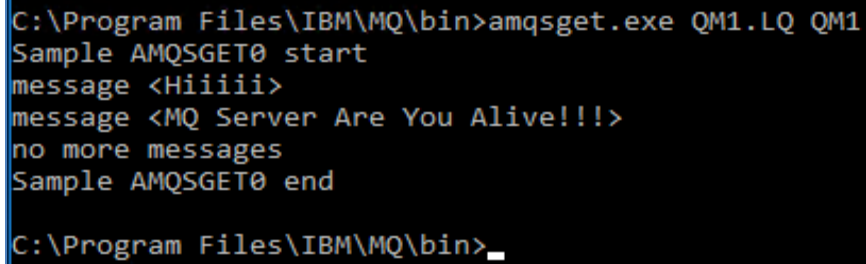


```
C:\Program Files\IBM\MQ\bin>amqsputc.exe QM1.LQ QM1
Sample AMQSPUT0 start
Enter password: *****
target queue is QM1.LQ
Hiiii
MQ Server Are You Alive!!!
```

The messages you type are delivered to MQ Server securely using the established SSL/TLS connection. MQ Server can see the messages received from MQ Client.

4. Log on to IBM MQ Server using the Administrator account.
5. Open the command prompt and run the following command to get the message sent by client:

```
C:\Program Files\IBM\MQ\bin>amqsget.exe QM1.LQ QM1
```



```
C:\Program Files\IBM\MQ\bin>amqsget.exe QM1.LQ QM1
Sample AMQSGET0 start
message <Hiiii>
message <MQ Server Are You Alive!!!>
no more messages
Sample AMQSGET0 end

C:\Program Files\IBM\MQ\bin>
```

This completes the integration of IBM Websphere MQ with SafeNet Luna HSM by securing the SSL/TLS authentication certificates/keys on SafeNet Luna HSM.