IBM Software Group

SSL and TLS in WebSphere MQ Open Mic

29 April 2010

WebSphere® Support Technical Exchange

Agenda

- Introduce the panel of experts
- Introduce SSL and TLS in WebSphere MQ
- Answer questions submitted by email
- Open telephone lines for questions
- Summarize highlights

Panel of Experts

Panelist	Role at IBM®
Alex Fehners	WebSphere MQ New Market Reach Development
Andrew Akehurst	WebSphere MQ Distributed L3 Support
Calista Stevens	WebSphere MQ System i Level 2 Support
Jonathan Rumsey	WebSphere MQ Lead System i Software Developer
Mike Horan	WebSphere MQ Distributed Software Developer
Rhys Francis	WebSphere MQ z/OS Level 3 Support
Tameka Woody	WebSphere MQ Windows® Level 2 Support
Mark Womack	WebSphere MQ z/OS Level 2 - TSANet PgmMgr
Tiffanie Pearson	WebSphere MQ Unix® Level 2 Support

Introduction

- Overview of terminology (certificate types, key files and other SSL/TLS system files)
- Common certificate administration tasks (GSKit, Java™, RACF and DCM)
- How to configure SSL/TLS
- Timeline of MQ SSL/TLS features
- Feature differences between platforms

Introduction [continued]

- Security is increasingly a concern for MQ users and SSL/TLS is an important tool to help secure your queue managers.
- Many users have a basic familiarity with SSL/TLS, but find some tasks difficult. For example:
  - Connecting a new queue manager into an existing MQ SSL/TLS network
  - Replacing an expired certificate
  - Setting up SSL/TLS for client applications
- This session will explain more about MQ SSL/TLS and will answer your questions.

Question 1

- What are CA certificates, signer certificates, personal certificates, client certificates and server certificates?

Answer to Question 1 - Windows/UNIX

- **CA certificate –** A certificate that is issued by a Certificate Authority such as VeriSign and is stored in your key repository.
- **Signer certificates** – A certificate that is trusted and has been signed by a CA.
- **Personal certificate** – A certificate that is assigned to a specific entity (e.g. a queue manager) by a Certificate Authority. Each queue manager can have only one personal certificate.

Answer to Question 1 - IBM i

- **CA certificate** is a Certificate Authority certificate. On IBM i, you can create local CA certificates to use for signing certificates.
- **Server certificates** are used to authenticate the client(SDR) to the server(RCVR) and the server (RCVR) to the client(SDR)

Answer to Question 1 - z/OS terminology

- **Certificate** types (personal, CA, signer etc.) are the same as on other platforms
- A **Keyring** is the key repository used on z/OS.
  - Certificates stored in the RACF database are ‘connected’ to the keyring(s) requiring those certificates.
- **Certificate Name Filters (CNF)** are used to associate received certificates with users defined to RACF, without requiring the certificate to be added to the RACF database.

Question 2

- What is a certificate chain and how do I view it?

Answer to Question 2 - Windows

- The certificate chain, also known as the *certification path*, is a list of certificates used to authenticate an entity. The chain, or path, begins with the certificate of that entity, and each certificate in the chain is signed by the entity identified by the next certificate in the chain. The chain terminates with a root CA certificate. The root CA certificate is always signed by the CA itself. The signatures of all certificates in the chain must be verified until the root CA certificate is reached.

  More information can be found on the following link with the title “How Certificate Chains Work:

- WebSphere MQ V6

  http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp?topic=/com.ibm.mq.csqzas.doc/sy10600_.htm
- WebSphere MQ V7

  http://publib.boulder.ibm.com/infocenter/wmqv7/v7r0/index.jsp?topic=/com.ibm.mq.csqzas.doc/sy10600_.htm

Answer to Question 2 - Windows

1. Windows Explorer to view certification paths:
   - Open Windows Explorer (Start -> Programs -> Accessories -> Command Prompt)
   - Select the directory where the certificate is located
   - Ensure the certificate has .cer extension.
   - Double-click on the certificate. The certificate panel should open.
   - Select the 'Certification Path' tab for details
2. IBM Key Management Tool to view certification paths:
   - Start IBM Key Management tool
   - Open the key database
   - Select 'Personal certificates' from the drop-down
   - Double-click on the personal certificate. Take note of the value of the 'cn' under the 'Issued by:" heading. If this is a self-signed certificate the 'cn' value will be the same as the 'cn' under the 'Issued to:' heading.
   - Select 'Signer certificates' from the drop-down
   - Double-click the signer certificate which was noted in the 'Issued by" for the personal certificate in step d above. If this is the Root CA, then the 'Issued by:' value for cn will be the same as the 'Issued to:' value for cn. If the 'Issued by:' value for cn is different than the 'Issued to:' value for cn, then this is an intermediate certificate. Please take note of the value of cn for 'Issued by:'. Repeat this step until you have reached the Root CA.

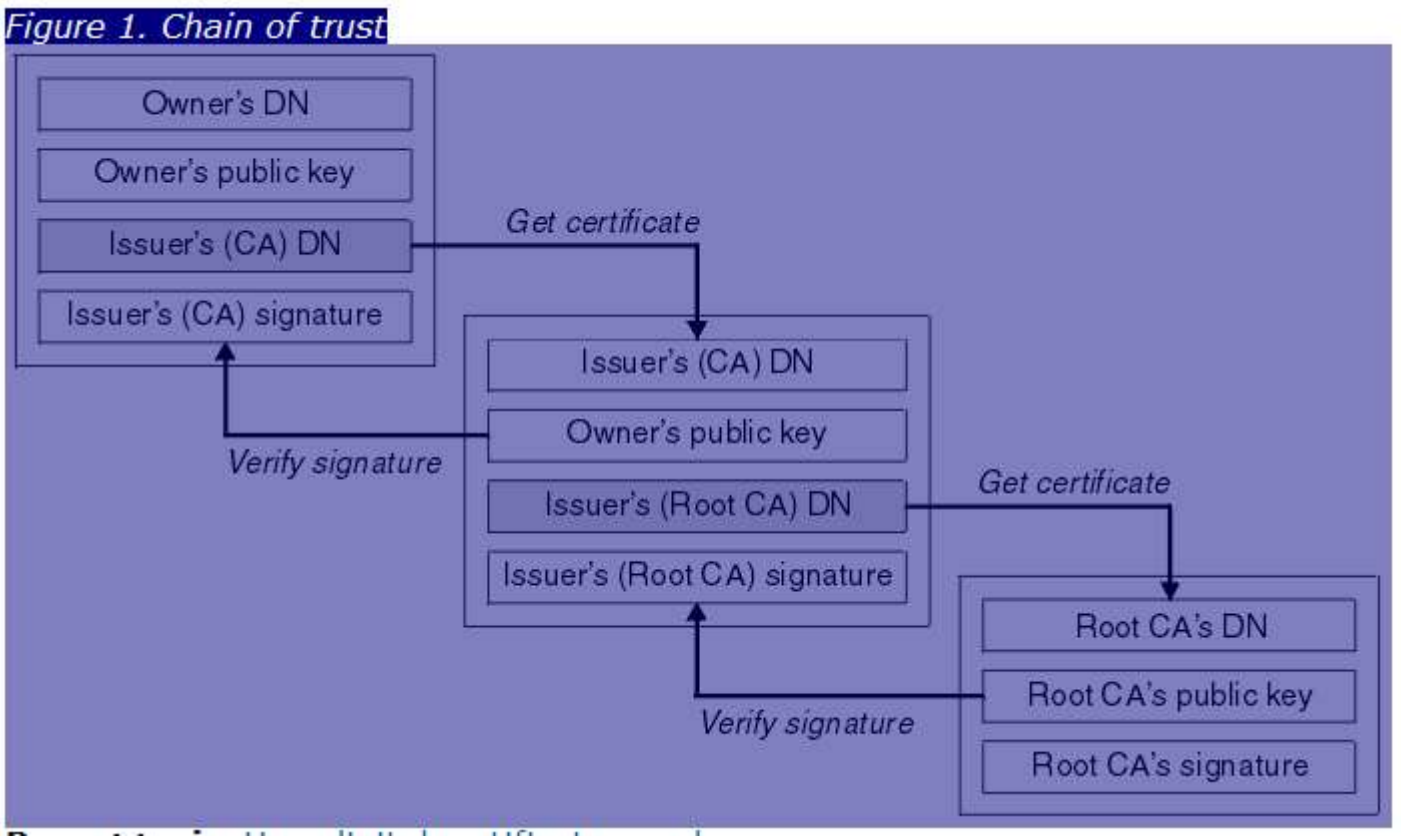
Answer to Question 2 - UNIX

1. To view the certificate chain on UNIX, use the following GSKit command:
   - gsk7cmd -cert -details -db key.kdb -pw passw0rd -label cert_label
2. Note the “Issued by” and “Issued to” fields and ensure that they show the same value.
3. Scroll through the contents of the display and verify that all certs match thru the root certificate.

Answer to Question 2 - IBM i

- Manually view each certificate and its parent issuer through DCM, repeat for each issuer until find the root, or
- Export server certificate to a PKCS#12 file through DCM
  - Manage Certificates -> Export Certificate -> File (Filename must be suffixed .p12)
  - keytool -list –v -keystore cert.p12 -storetype pkcs12
  - All certificates in the chain will be listed

Answer to Question 2 - z/OS



Question 3

- How do I renew an expired certificate?

Answer to Question 3 - Windows & UNIX

- **To renew an expired certificate:**
  - Generate a new certificate request based on the existing certificate using the GSKit -certreq -recreate command (specify the label of the expiring certificate to be replaced).
  - Send the request to be signed.
  - Receive the replacement certificate the key repository.
  - Issue a “REFRESH SECURITY TYPE(SSL)” command

Answer to Question 3 - IBM i

1. Create a new temporary certificate store.
2. Create a new Server certificate in the temporary certificate store with the label name 'ibmwebspheremq<qmgr>'. If not using a local CA signer, follow all instructions on the final panel instructing you to copy and save the text and send to the Certificate Authority.
3. Delete the old WebSphere MQ certificate from the current certificate store.
4. Export the new WebSphere MQ certificate from the temporary certificate store to the current certificate store.
5. Refresh SSL Key Repository cache.
6. Delete the temporary certificate store.

Answer to Question 3 - IBM i

- If *SYSTEM store is being used then certificate does not need to use 'ibmwebspheremq<qmgrname>' label
- Renewing expired certificates is simplified
  - Any certificate may be associated with the queue manager application
  - Reduces the steps required when changing a certificate/renewing an expired certificate
    - Import new certificate
    - Use DCM to assign new certificate to queue manager, optionally remove old certificate
    - Refresh SSL environment - RFRMQMAUT TYPE(*SSL)

Answer to Question 3 - z/OS

1. Create new cert with a different label
2. Create a REQUEST for this cert in RACF
3. Add the signed cert to RACF with the same name
4. Connect the signed cert to the keyring
5. Rename the expiring cert so it's no longer referenced
6. Rename the new cert to the previous name that expiring cert held
7. Refresh the SSL key repository with the REFRESH SECURITY TYPE(SSL)

Question 4

- How do I make sure that SSL/TLS is set up correctly?

Answer to Question 4 - Windows

1. Determine if you have one-way or two-way authentication. Review the receiver channel for the sender/receiver channel pair, or the server connection channel; if SSLCAUTH is set to REQUIRED, then there must be two personal certificates involved (one for server queue manager, one for client system). Otherwise, the personal certificate on the client system is optional, but if it is present it is authenticated.
2. Verify the SSLCIPH parameter on the sender/receiver channel pair or the client conn/server conn connection pair.
3. Verify the SSL Key Repository (SSLKEYR) parameter on the server queue manager properties and on the client queue manager, if available.
4. On the server queue manager, use the IBM Key Management tool to ensure the personal certificate named 'ibmwebspheremqXXXX' where XXXXX is the queue manager named in lower case, is available.
5. Extract the CA certificate and transfer to the client queue manager. It may require the extract of multiple signer certificates if intermediate and root certificates are involved. Please check the certificate chain to determine what's needed.
6. Open the IBM Key Management tool on the client system. If this is a client application using JAVA, ensure the type of key database is a *.jks. All other client systems (queue manager, C, C++, .NET, etc) use CMS key database types of *.kdb and *.sth.
7. Add the certificate(s), to the Signer certificates view.
8. If this is an client application connection other than JAVA/JMS applications, ensure the MQSSLKEYR, MQCHLLIB, and MQCHLTAB environment variables are set.
9. If this is two-way authentication, extract the CA certificate(s) on the client system and transfer it to the server queue manager system.
10. Add the CA certificate to the key database on the server queue manager system.

Answer to Question 4 - UNIX

- **Check the WMQ error logs for the system and for the queue manager:** WMQ records the reason for SSL/TLS errors in its error logs. If the logs from one side of the connection do not explain the cause, check the error logs from the remote system.
- **Make sure that ".kdb" is NOT included at the end of the queue manager SSLKEYR attribute:** WMQ will automatically add that extension when it is instructing GSKit to load the key repository.
- **The SSLKEYR attribute points at a different set of files from those which were configured by the user:** Make sure that SSLKEYR refers to the correct location of the key database.

Answer to Question 4 - UNIX

- **Using the wrong type of key database for the scenario:**
  The solution is to use the correct type of key database:
  - Java applications (including the WMQ V6 Explorer GUI) use JKS (or JKCES) jks files
  - C/C++/.NET Unmanaged WMQ applications (including Java applications in bindings mode) use CMS kdb files
  - MQIPT (SupportPac MS81) uses PKCS12 p12 files

Answer to Question 4 - UNIX

- **Transferring binary certificate files or key database files across an ASCII-mode FTP connection:** Transferring a binary file (e.g. a kdb file) in ASCII mode
- will corrupt the contents. The GSKit tools will report that the key database is corrupted when trying to open or view it. The solution is to transfer the files again in binary FTP mode and use one of the GSKit tools to ensure that the contents can be viewed successfully.
- **No password stash file:** (key.sth). WMQ queue managers need to have a stashed copy of the password in a file so that it can open the key database. The solution is to create a password stash file for a .kdb which does not have one, use the appropriate command below:
  - WMQ 6 and 7 (Unix)
  - gsk7cmd -keydb -stashpw -db key.kdb –pw password

Answer to Question 4 - UNIX

- **File permissions on the key repository files are set such that the key repository is not readable by the application (or channel) process**: On a queue manager, the key repository and its directory must have operating system permissions so that they can be read by members of the mqm group. On a client, the key repository must be readable by the user ID under which the application is running. The solution is to change the file permissions (and possibly the file ownership). Here are some examples:
  - Unix queue manager (assuming default SSLKEYR key repository location):
  - chown mqm:mqm /var/mqm/qmgrs/QMGR/ssl/* chmod 440 /var/mqm/qmgrs/QMGR/ssl/*
    Unix client application running as user fred (files in current working directory)
  - chown fred key.* chmod 400 key.*

Answer to Question 4 - UNIX

- **A queue manager certificate does not have the correct label.** On distributed platforms, the label of the queue manager's personal certificate must be ibmwebspheremqqmgr, where qmgr is the name of the queue manager folded to lower case.

- **The responding side of the channel has SSLCAUTH(REQUIRED) but the client has no personal certificate**. This will cause error AMQ9637. The solution is either to set SSLCAUTH(OPTIONAL) or to create a personal certificate for the client. The client's personal certificate must either conform to the ibmwebspheremqusername convention, or it must be the default certificate in the key repository. See APAR IC50156 for details of WMQ default certificate support.

Answer to Question 4 - UNIX

- **One of the certificates has expired.** In addition to checking the personal certificate of each queue manager or client, one of the CA certificates required to validate a personal certificate may be expired. The entire certificate chain should be checked. You can usually find the signer of a personal certificate by finding the certificates whose Subject Distinguished Name (DN) is the same as the Issuer DN of that personal certificate. To get a list of all certificate labels in a key database, use the appropriate command:
  - WMQ 6 and 7 (Unix)
    - gsk7cmd -cert -list -db key.kdb -pw password

      or
    - gsk7cmd -cert -details -db key.kdb -pw password -label cert_label

Answer to Question 4 - UNIX

- **One or more certificates have been changed, but cached copies of the certificates are still held in memory:**. Each WMQ channel process caches the key repository the first time it runs an SSL channel thread. If changes have been made, the REFRESH SECURITY TYPE(SSL) MQSC command (or PCF equivalent) must be used to clear the SSL cache in all channel processes. Note that a common error is to omit TYPE(SSL) from the command; if this is omitted then the command will have no effect on the SSL cache.

Answer to Question 4 - IBM i

1. Verify the key store location is correctly specified for the queue manager.
2. Verify the key store password has been specified for the queue manager.
3. Verify QMQM has *RW authority to the key store and stash files.
4. Verify QMQM has *RWX authority to the key store directory.
5. Verify CA and server certificates have been placed in correct key store and the label name for server certificate is “ibmwebspheremq<qmgr>”.
6. Verify that the SDR and RCVR channels SSLCIPH attributes are the same.
7. Verify that the RCVR channel SSLCAUTH attribute is correct for the intended type of authentication.
8. When using private key stores, verify that the server(RCVR) and the client(SDR) have exchanged CAs and that both the server and the client have server certificates.
9. When using the *SYSTEM key store, verify that the server certificate has been assigned to the application(Queue Manager).
10. When making certificate updates, verify the channels are stopped and the SSL Key Repository cache is refreshed.

Answer to Question 4 - z/OS

SSLTASKS

- Set using ALTER QMGR SSLTASKS(n)
- Must be set to at least 2 when using SSL

SSLKEYR

- Set using ALTER QMGR SSLKEYR(xxxxxxx)
- This names the keyring that the queue manager should use. The keyring should be defined in RACF, and should have the necessary personal and CA certificates connected to it

Answer to Question 4 - z/OS

Certificate label

- **Certificates for queue managers on the z/os platform must be of the form ibmWebSphereMQxxxx**
  - xxxx is either the name of the queue manager, or of the queue sharing group the queue manager belongs to (if the channel is shared)
  - Note that the capitalisation is different on z/os

CHL userid

- The userid associated with a certificate received over an SSL/TLS channel is used when checking authority to access WMQ resources for channels with PUTAUT(DEF) or PUTAUT(CTX)
  - If the received certificate exists in the RACF database, and is associated with a userid, that userid will be used
  - If the received certificate does not exist in the RACF database, the certificate subject and/or issuer DN may be mapped to a userid using a CNF
  - If no userid is associated with the certificate, the channel initiator userid is used
- Depending on the RESLEVEL authority of the channel initiator, the MCA user may be checked in addition to the channel userid.

Question 5

- What has changed in MQ SSL/TLS since version 5.3?

Answer to Question 5 - All platforms

- SSL support introduced in V5.3
- Cross-platform enhancements at V6:
  - Secret key reset
  - REFRESH SECURITY TYPE(SSL)
  - TLS CipherSpecs function properly
  - Certificate issuer's name available
    - In channel status
    - To security exits
  - Separate configuration of SSL Events
- Currency as move up releases:
  - support stronger CipherSpecs
  - support more advanced cryptographic cards

Answer to Question 5 - Windows

- At V5.3 used Microsoft® SSL
  - Windows-style key management
    - different from UNIX/Linux® configuration
  - Problem diagnosis different
  - No cryptographic hardware support
- From V6 moved to using GSKit
  - GSKit is also used by UNIX and Linux
- Key repository migration aids
  - Command-line, Install GUI
- Reverse multiple OU ordering on SSLPEER

Answer to Question 5 - Windows,UNIX

- At V7.0.1, OCSP support

Answer to Question 5 - Windows, UNIX, Java/JMS client

- From V6, support for FIPS-only operation

Answer to Question 5 - IBM i

- Support system certificate store (V6)
  - Works just like any other IBM i server enabled for SSL
  - Restrictions on certificate labelling and setting key repository passwords lifted

Answer to Question 5 - z/OS

- From V5.3, on z, a userid could be automatically associated with the DN in the received certificate
  - This functionality still only applies on z
- At V6 this userid was made available:
  - In channel status
  - To security exits

Question 6

- Must the environment variable MQSSLKEYR always be defined? Does it apply to all WMQ versions and platforms?

Answer to Question 6

- No, the MQSSLKEYR environment variable is not always defined. It should be defined when using WebSphere MQ client applications (except Java/Jms applications) to connect to a WebSphere MQ queue manager.
- The MQSSLKEYR environment variable is applicable on WebSphere MQ V6 and WebSphere MQ V7 for the following platforms:
  - AIX
  - HP-UX
  - Linux
  - Solaris
  - Windows

Open Lines for Questions

We Want to Hear From You!

Tell us about what you want to learn

Suggestions for future topics
Improvements and comments about our webcasts
We want to hear everything you have to say!

Please send your suggestions and comments to:
wsehelp@us.ibm.com

Summary

References and Useful Links

- Performing SSL/TLS secret key reset from a Java/JMS client application:
  http://www.ibm.com/support/docview.wss?uid=swg21384105
- WebSphere MQ Explorer Tests (see SSL tests section):
  http://publib.boulder.ibm.com/infocenter/wmqv7/v7r0/index.jsp?topic=/com.ibm.mq.explorer.doc/t_testsoverview.htm
- WebSphere MQ SSL Wizard: SupportPac MQ04:
  http://www-01.ibm.com/support/docview.wss?rs=171&uid=swg24010367
- Windows and UNIX SSLCHECK Tool verifies SSL configurations for MQ:
  http://www-01.ibm.com/support/docview.wss?uid=swg21282078
- z/OS Digital Certificate Commands for External Security Managers:
  http://www-01.ibm.com/support/docview.wss?uid=swg21205523

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at:
  http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at:
  http://www.ibm.com/developerworks/websphere/community/
- Join the Global WebSphere User Group Community:
  http://www.websphere.org
- Access key product show-me demos and tutorials by visiting IBM Education Assistant:
  http://www.ibm.com/software/info/education/assistant
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically:
  http://www.ibm.com/software/websphere/support/d2w.html
- Sign up to receive weekly technical My Notifications emails:
  http://www.ibm.com/software/support/einfo.html