z/TPF V1.1

TPF Users Group Fall 2008
WebSphere MQ

Support for SSL PJ34481

John Muller
Distributed Subcommittee

AIM Enterprise Platform Software
IBM z/Transaction Processing Facility Enterprise Edition 1.1.0

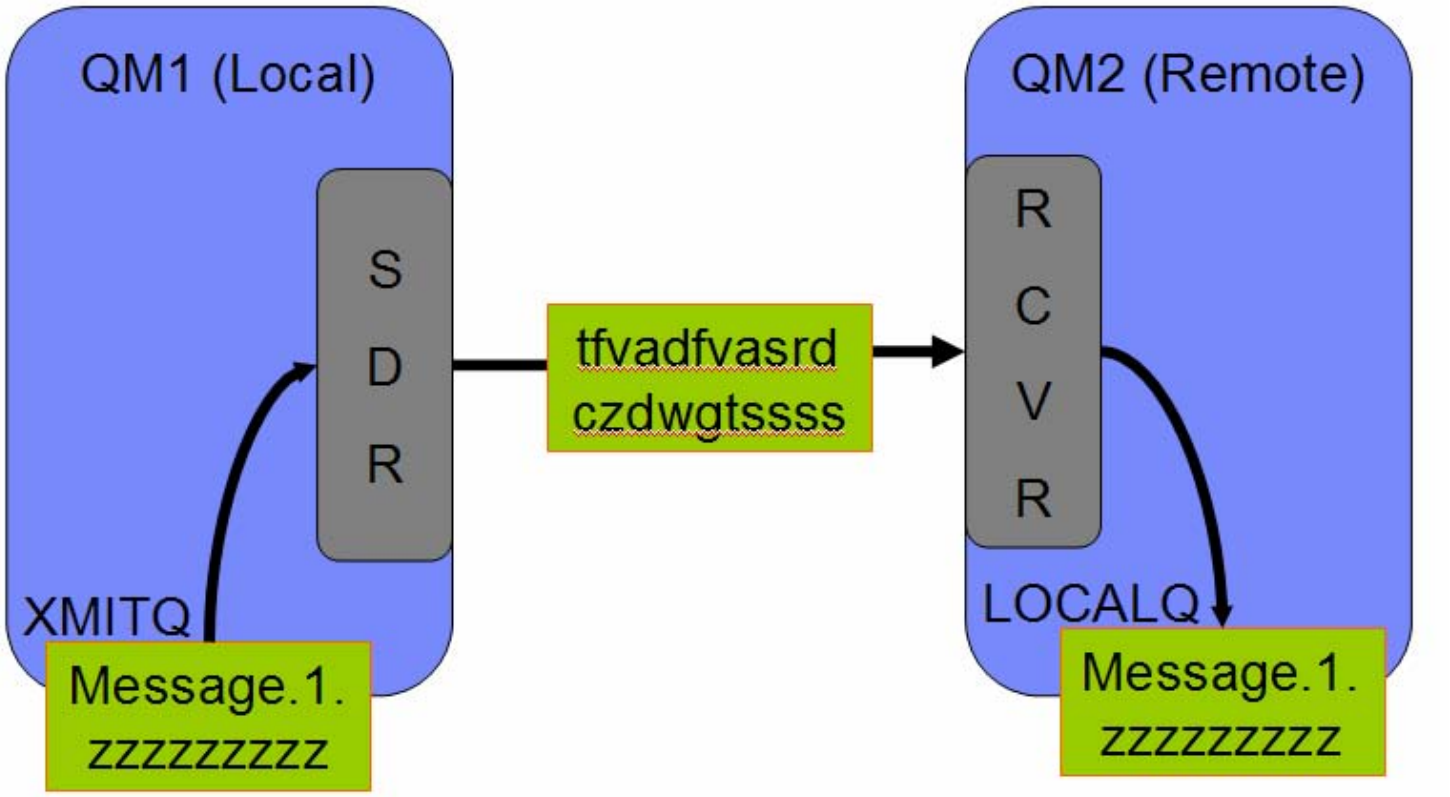
Overview z/TPF WebSphere MQ support for SSL

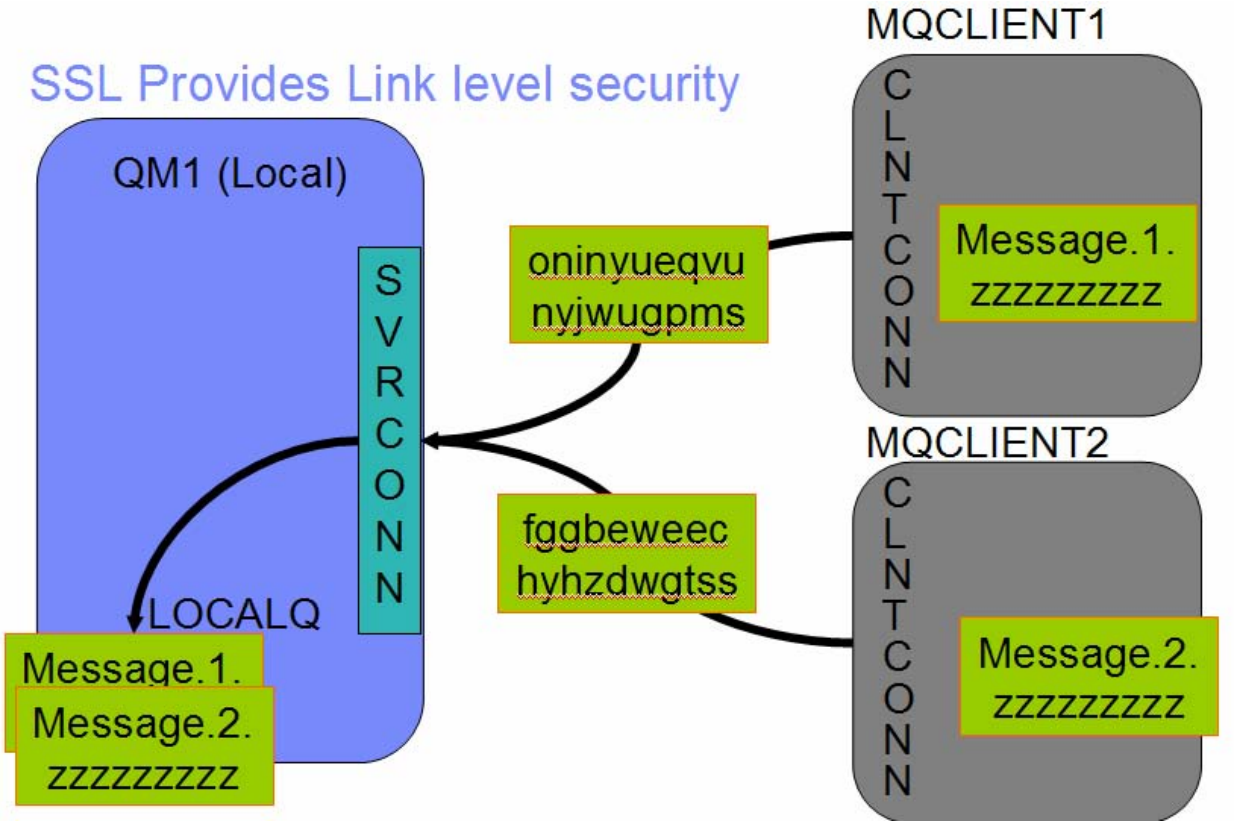
- Provide Link level security between WebSphere MQ and z/TPF WebSphere MQ
  - **SSL QMGR to QMGR, (RCVR/SDR Channels)**
    - **z/TPF to z/TPF**
    - **z/TPF to any other SSL enabled WebSphere MQ Platform**
  - **SSL Server support (SVRCONN Channels**
  - **z/TPF MQ Client not supported (ZMQID)**
- Requirement MQ04006, SSL Channels
- Makes use of z/TPF Shared SSL support
- Uses z/TPF Application configuration files for SSL
  - Used by middleware such as FTPC and HTTP
- PJ34481 has not been released yet and is subject to change.

Benefits of z/TPF WebSphere MQ SSL

- **Message Encryption during transport**
  - Supports a range of cryptographic algorithms
- **Message Integrity Checking**
- **Authentication**
  - Uses Public/Private Keys
  - Allows the checking of the Distinguished Name (DN) (SSLPEER)
  - Optional client authentication (SSLCAUTH)

SSL Provides Link level security





Channel Attributes

- **SSL (YES/NO/FILE)**
  - Whether the channel should use SSL (YES/NO) or the value contained in the application configuration file for SSL (FILE)
- **SSLCONF (*filename*.conf)**
  - Override the default Application configuration file for SSL
- **SSLCAUTH (REQUIRED/OPTIONAL)**
  - RCVR/SVRCONN channels only
  - Whether the SSL server requires the SSL client to send its digital certificate for authentication.

Queue Manager Attributes

- **SSLRKEYC (default “0” no renegotiation)**
  - The total number of unencrypted bytes that are sent and received within an SSL conversation before the secret key is renegotiated. The number of bytes includes control information.
- **SSLEVENT (ENABLED/DISABLED)**
  - Allows SSLEVENTS to be written to the SYSTEM.ADMIN.CHANNEL.EVENT queue if defined.

Application configuration files for z/TPF WebSphere MQ SSL

- Config files TPF unique way to save application OpenSSL values
- CIPHER, CAINFO, CAPATH, CERTIFICATE, CERTTYPE, KEY, KEYTYPE
  - Same as other middleware (FTPC/HTTP)
- USESSL=**YES/NO**
  - **TRY** not supported with z/TPF WebSphere MQ SSL support
- VERSION=**SSLV2/SSLV3/TLSV1**
  - **SSLV23** not supported with z/TPF WebSphere MQ SSL support
- VERIFYPEER=**YES/NO**
  - Changed from **0/1/2** with z/TPF WebSphere MQ SSL support
  - FTPC and HTTP will be changed to support this
- APPLDATA=
  - New for z/TPF WebSphere MQ SSL support for **SSLPEER**

Application configuration files for z/TPF WebSphere MQ SSL (cont'd)

- SSLPEER (appldata=*SSLPEER-*)
  - The Distinguished Name pattern that WebSphere MQ uses to decide the entities from which messages are accepted. The SSLPEER pattern filters the Distinguished Names of the entities.
  - Example:

    appldata=SSLPEER-CN=jfmuller,O=TPF,C=US

Example application configuration file for SSL

/etc/ssl/mq/mq.conf

```
# z/TPF WebSphere MQ for SSL example
usessl=yes
version=sslv3
cipher=NULL-MD5
verifypeer=yes
cainfo=/certs/cacert.pem
certificate=/certs/cert.pem
certtype=pem
key=/certs/key.pem
keytype=pem
appldata=SSLPEER-CN=jfmuller,O=TPF,C=US
```

Channel usage of Application configuration file

- **SDR channels**
  - default is /etc/ssl/mq/mq.conf
  - Override with the SSLCONF channel parameter
  - For example SSLCONF-"ch1" results in /etc/ssl/mq/ch1.conf
    - Use " " if lowercase is needed.
- **RCVR/SVRCONN channels**
  - SSL handshake uses /etc/ssl/mq/mq.conf
  - Since the SSL Handshake is done before we know the channel name.
  - Once the channel name is known the SSLCONF channel parameter is used to determine the override file to verify the connection settings. (Using correct cipher, version, etc.)

Change required to z/TPF WebSphere MQ INETD

- **WebSphere MQ uses a single port for all traffic SSL/non-SSL**
- **Current listener MQS, uses activate_on_receipt_with_length()**
  - s-mqs pgm-cmql model-aor p-tcp aorl-8 port-1414
- **A new model was needed so that we can peek at the data and determine SSL or non-SSL traffic using activate_on_accept()**
- **Procedure for applying PJ34481**
  - Define the new listener (MQAOA)
    - zinet add s-mqaoa pgm-cmql model-aoa2 p-tcp port-1414
  - Required regardless of the use of SSL or non-SSL

Migration

- **All existing and new definitions will default to not using SSL**
- **Converting existing channels to use SSL**
  - SDR/RCVR channel pairs
    - Both channel definitions will need to be modified to use SSL, and then restarted.
  - SVRCONN channels
    - Once the channel is altered to use SSL all new clients must use SSL in order to connect. New non-SSL connections will fail.
- **Ways to migrate client connections**
  - Define a new SVRCONN channel and convert clients to the new channel.
  - Enable SSL and force all clients to be changed to use SSL

z/TPF WebSphere MQ Minimum Setup

- **Ensure SSL Server side has a certificate. (RCVR/SVRCONN).**
- **Ensure an Application configuration file for SSL (/etc/ssl/mq/mq.conf) is created with the correct parameters specified. (CERTIFICATE, CIPHER, VERSION, etc.)**
- **Ensure channel has been modified to use SSL.**
- **Start the channel.**

SSL Daemon process control

- Shared SSL provides a load balancing mechanism by specifying which daemon processes an application can use through **/etc/sslshared.txt**
- The default for MQ is “MQ ALL” if there is no entry in /etc/sslshared.txt
- For Example:

  “MQ 2,3” will use daemon process two and three.

Conclusion

- z/TPF WebSphere MQ provides a mechanism to secure your channels that is integrated into the product.
- Does not involve any changes to your MQ applications in order to use
- Set up as part of your channel configuration and provides a built in mechanism to address
  - Eavesdropping
  - Tampering
  - Impersonation
- Uses a well known and extensively tested security protocol. (OpenSSL)

Trademarks

- IBM and WebSphere are trademarks of International Business Machines Corporation in the United States, other countries, or both.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Other company, product, or service names may be trademarks or service marks of others.

- Notes
- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

- This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.