Here encryption, there encryption, simple encryption everywhere

Roger Lacroix
roger.lacroix@capitalware.com
http://www.capitalware.com

Background and Problem Statement

- Does your company want its message data in a viewable format?
- Does your company require that sensitive data be stored and/or transmitted in a secure format that complies with PCI security requirements?

Data Protection

- Data Protection for Channels (data in flight)
- Data Protection for Queues (data at rest)

Data Protection for Channels

MQ Channel Encryption (MQCE) vs MQ SSL/TLS:

- MQ SSL/TLS is included with MQ but requires SSL/TLS certificates and is used to encrypt data as it passes over MQ channels (between 2 points only)
- MQCE is used by MQ channels to encrypt/decrypt data that passes over the channel (between 2 points only)
- MQCE as a direct competitor to MQ SSL/TLS.

Data Protection for Channels (2)

Major Features of MQCE:

- Easy to set up and configure (unlike SSL/TLS)
- No application changes required – Simply update CCDT file or MQ JNDI
- Can be configured as either queue manager to queue manager or client application to queue manager solution
- All message data flowing over a channel will be encrypted
- Secure encryption methodology using AES with 128, 192 or 256-bit keys
- Standard MQ feature, GET-with-Convert, is supported
- Provides high-level logging capability
- Cost is $299.00 (cheaper in volume) per queue manager plus 15% yearly maintenance and support fee
- Yearly cost per queue manager: $45 vs $400

Data Protection for Channels (3)

Here are some MQ SSL/TLS disadvantages:

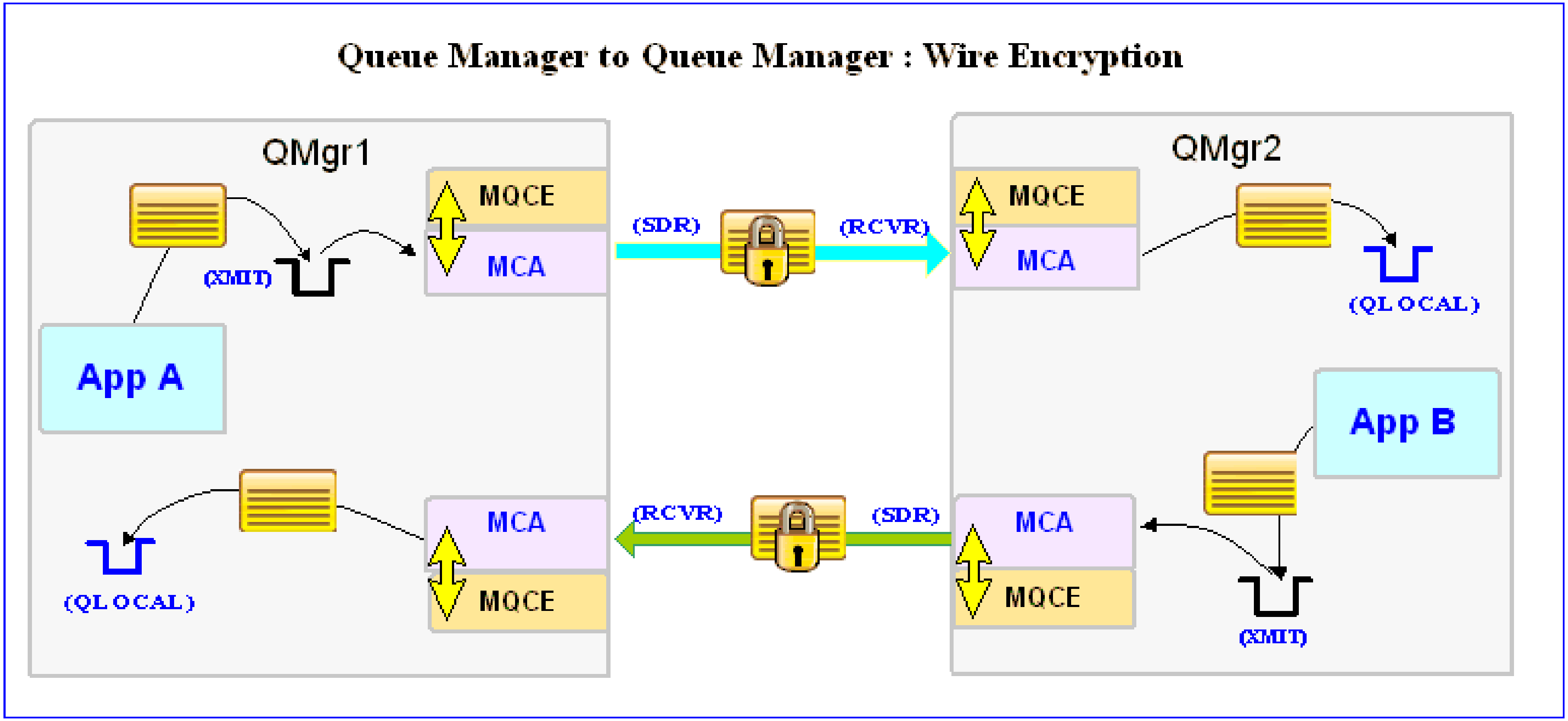
- SSL/TLS certificates must be purchased YEARLY at a cost of roughly $400
- SSL/TLS certificates expire, requiring regular repurchase, renewal and then the MQAdmin needs to deploy the new SSL/TLS certificates.
- There is no logging capability for SSL/TLS to see who accessed which queue manager.
- This form of security is only as secure as the integrity of the client side certificates. Anyone who possesses a copy of the certificate will have full access (It is extremely easy to copy a keystore on a Windows Server).
- SSL/TLS is Node-to-Node security and NOT End-to-End security. Node-to-Node security that any application running on the server can connect to the queue manager. It is far better to control each application that is connecting to a queue manager (i.e. End-to-End).

Data Protection for Channels (4)

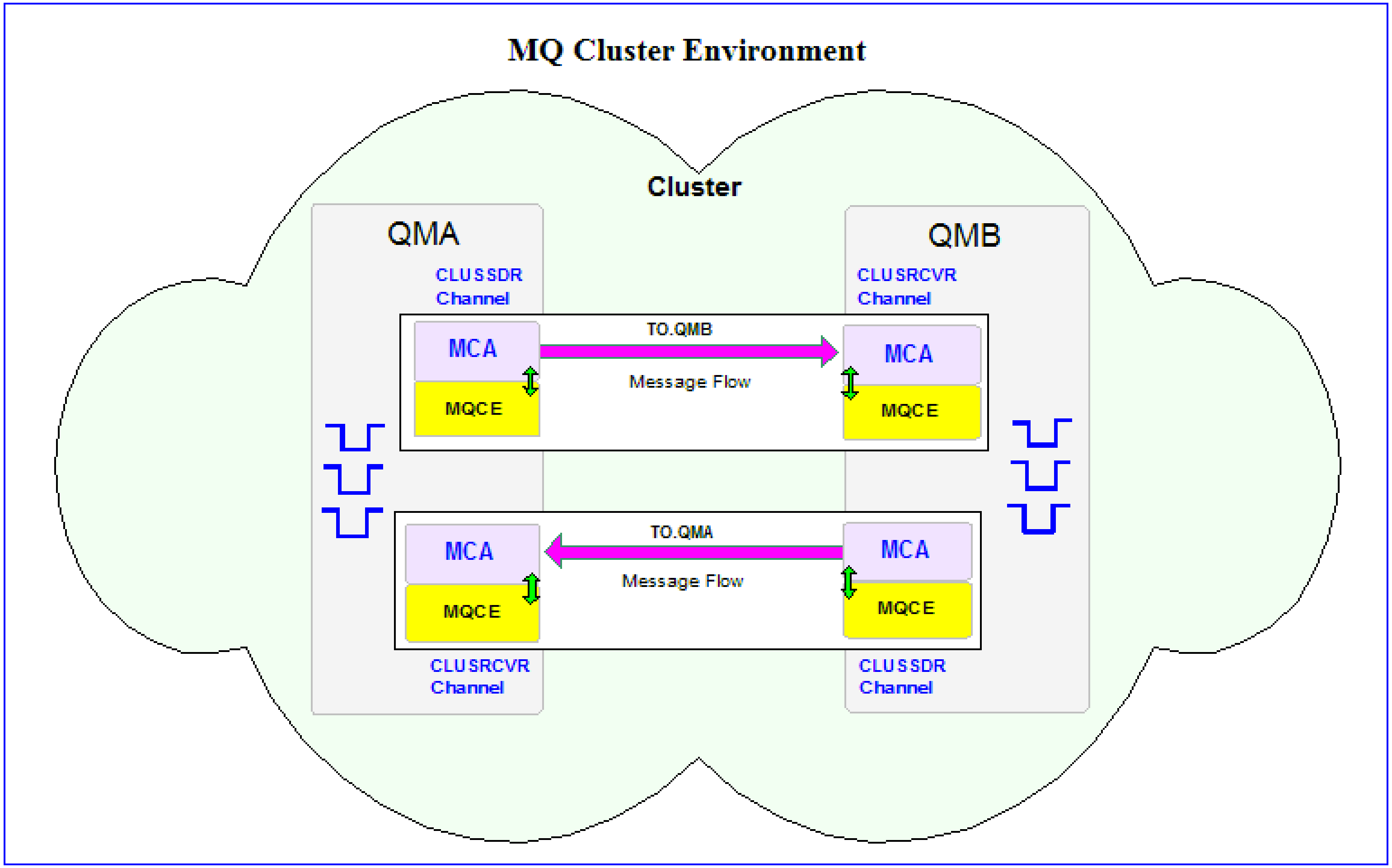
Configuration / Management:

- When a customer purchases MQCE license(s), they get permanent MQCE license keys that do NOT expire.
- SSL/TLS Certs expire yearly. If you forgot to update a queue manager's SSL/TLS certificate, when it expires your channels will stop working.

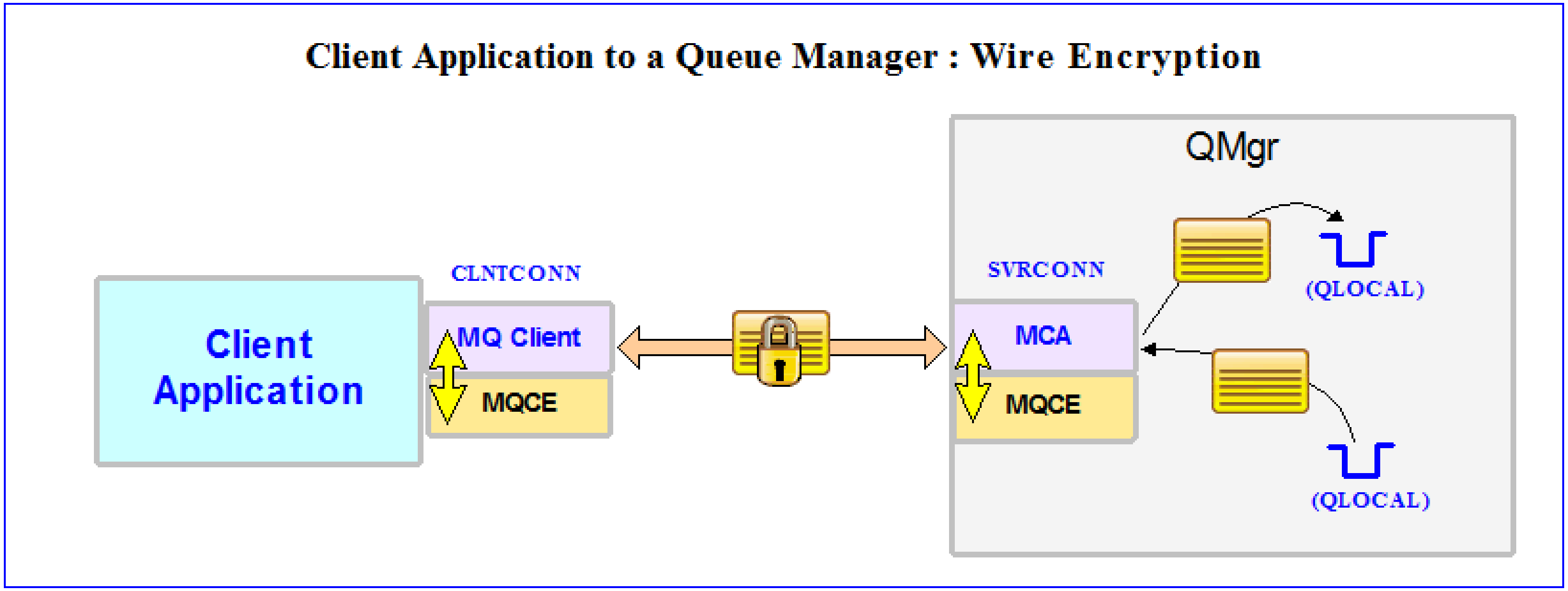
Data Protection for Channels (5)



Data Protection for Channels (6)



Data Protection for Channels (7)



Data Protection for Queues

MQ Message Encryption (MQME) vs IBM MQ AMS (Advanced Message Security)

- IBM MQ AMS included with the MQ Advanced license. (Previously, required a separate license purchase)
- MQME is $299.00 (cheaper in volume) per queue manager plus 15% yearly maintenance and support fee

Data Protection for Queues (2)

Major Features of MQME:

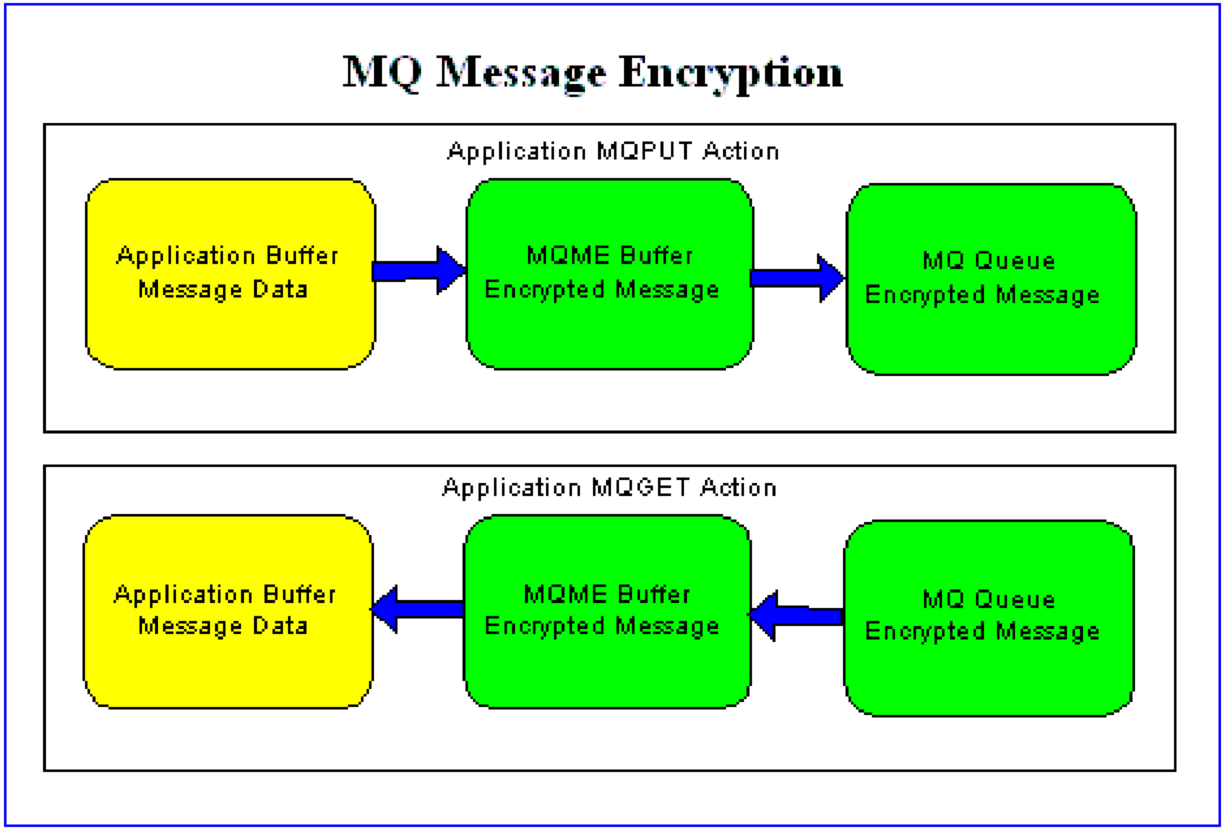
- Easy to set up and configure (unlike SSL/TLS)
- No application changes required
- All message data written to a selected queue will be encrypted
- Secure encryption methodology using AES with 128, 192 or 256-bit keys
- Uses the SHA-2 to create a cryptographic hash function (digital signature)

Data Protection for Queues (3)

Major Features of MQME (cont'd):

- Support for MQ clustering
- Group authority checking against the local OS groups or a group file
- Standard MQ feature, GET-with-Convert, is supported
- Provides high-level logging capability for encryption / decryption processing
- Yearly cost per queue manager: $45 vs $400

Data Protection for Queues (4)



MQ Message Encryption

Application MQPUT Action

Application Buffer
Message Data

MQME Buffer
Encrypted Message

MQ Queue
Encrypted Message

Application MQGET Action

Application Buffer
Message Data

MQME Buffer
Encrypted Message

MQ Queue
Encrypted Message

Data Protection for Queues (5)

	MQME	MQ AMS
End-to-End Encryption	Yes	Yes
Supported Encryption	AES128, AES192, AES256	RC2, DES, 3DES, AES128, AES256
Digital Signature	SHA-2	MD5, SHA-1, SHA-2
Requires the purchase of an SSL certificate for each end point (~$400 USD)	**NO**	Yes
PCI compliant for separation of digital signature and message data in the message payload	Yes	No
Show encrypted message data to unauthorized users	**NO**	Yes

Data Protection for Queues (6)

	MQME	MQ AMS
Support Publish/Subscribe	Yes	**NO**
Support for Cluster Queues	Yes	Yes
MQGet with Convert for C/COBOL applications	Yes	Yes
MQGet with Convert for C++ applications	Yes	Yes
MQGet with Convert for Java applications	Yes	Yes
MQGet with Convert for .NET (C#) applications	Yes	Yes
Distribution lists	Yes	**NO**
IBM MQ classes for .Net in a managed mode	Yes	**NO**

Data Protection for Queues (7)

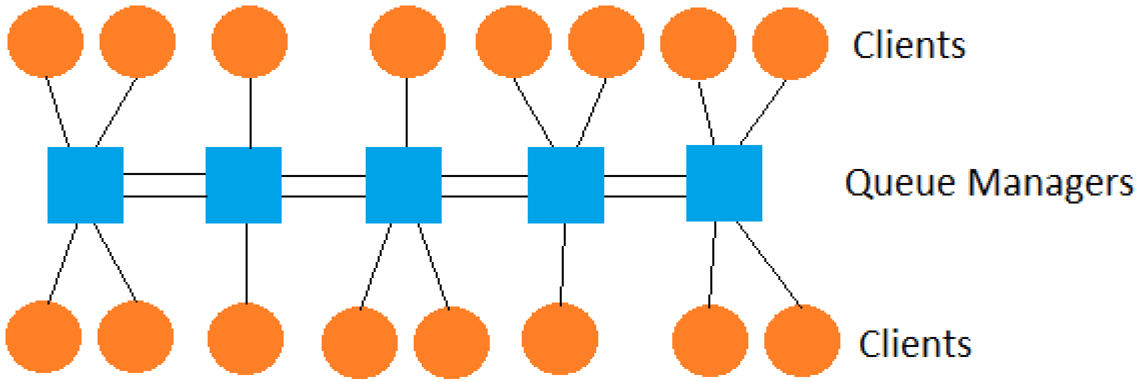
	MQME	**MQ AMS**
Message Service client for .Net (XMS) applications	Yes	**No**
Message Service client for C/C++ (XMS) applications	Yes	**No**
Protection of SYSTEM.* queues	Yes	Yes
Require application code changes	No	No
Supported Platform: Unix (AIX, HP-UX & Solaris)	Yes	Yes
Supported Platform: Linux (x86, x86-64, Power & System z)	Yes	Yes
Supported Platform: Windows	Yes	Yes
Supported Platform: IBM i (OS/400)	Yes	Yes

MQ Security Grid

- A “quick drop and go” way to have protected queues and protected messages across multiple queue managers:
  - Remote queues
  - Cluster queues
  - Even works with messages that originate from a client connection
  - And of course, local and alias queues

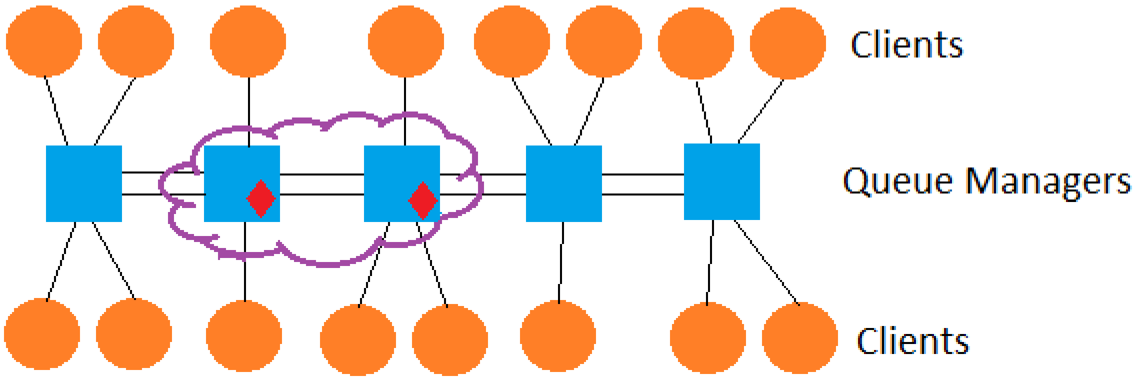
MQ Security Grid (2)

A standard MQ environment:



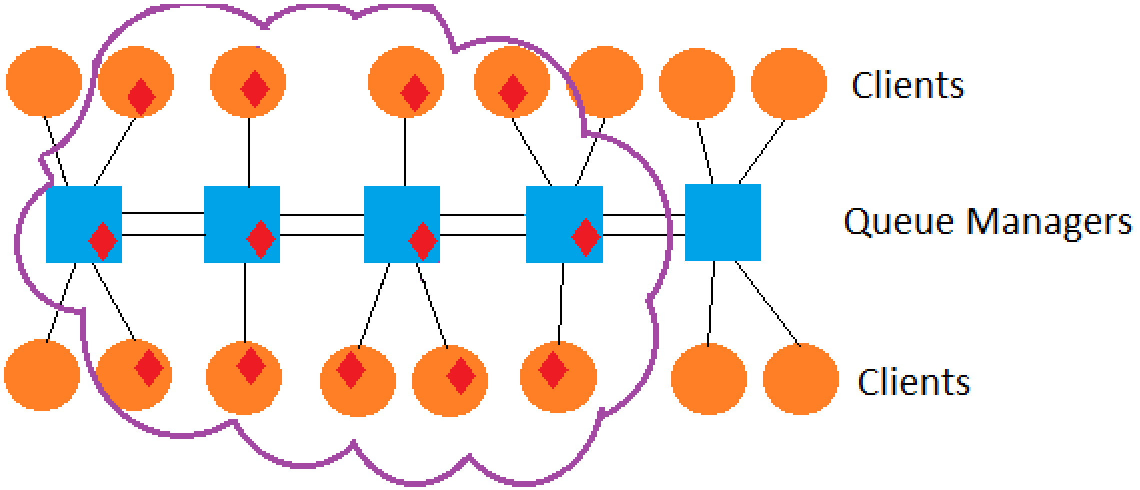
MQ Security Grid (3)

MQME deployed to 2 queue managers:



MQ Security Grid (4)

MQME deployed to 4 queue managers & 9 clients:



MQ Security Grid (5)

- Messages that “hop” between queue managers “can” stay encrypted if the user wishes.
- Will require MQME on the “final” queue manager for decryption but not on the intermediary queue managers.
- Does not require SSL/TLS for channel encryption!
- Does not require MQCE for channel encryption!

Questions & Answers