What's new in MQ Message Encryption

Roger Lacroix
roger.lacroix@capitalware.com
https://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 and/or GDPR security requirements?
- MQ Message Encryption provides protection of data in a queue and/or topic (data at rest).
What’s new in MQ Message Encryption v4

- Added Topic section so that MQME will protect topics.
- Added UseExcludeTopics and ExcludeTopics keywords to explicitly exclude topics from being protected.
- Added EncPassPhrase keyword to support the use of encrypted PassPhrase. Added ‘enc_pp’ program that will create an encrypted PassPhrase.
- Changed when the authorization is perform. Now it is done during the MQOPEN rather than MQGet and/or MQPUT/1.
What’s new in MQ Message Encryption v4

- Support for MQ clients performing Pub/Sub
- Support for AMQP clients performing Pub/Sub
- Support for MQTT clients performing Pub/Sub
Data Protection for Queues & Topics

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 & Topics (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 & Topics (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 & Topics (4)
# Data Protection for Queues & Topics (5)

<table>
<thead>
<tr>
<th>Feature</th>
<th>MQME</th>
<th>MQ AMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-to-End Encryption</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supported Encryption</td>
<td>AES128, AES192, AES256</td>
<td>RC2, DES, 3DES, AES128, AES256</td>
</tr>
<tr>
<td>Digital Signature</td>
<td>SHA-2</td>
<td>MD5, SHA-1, SHA-2</td>
</tr>
<tr>
<td>Requires the purchase of an SSL certificate for each end point (~$400 USD)</td>
<td>NO</td>
<td>Yes</td>
</tr>
<tr>
<td>PCI compliant for separation of digital signature and message data in the message payload</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Show encrypted message data to unauthorized users</td>
<td>NO</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# Data Protection for Queues & Topics (6)

<table>
<thead>
<tr>
<th>Feature</th>
<th>MQME</th>
<th>MQ AMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Publish/Subscribe</td>
<td>Yes</td>
<td>NO</td>
</tr>
<tr>
<td>Support for Cluster Queues</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MQGet with Convert for C/COBOL applications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MQGet with Convert for C++ applications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MQGet with Convert for Java applications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MQGet with Convert for .NET (C#) applications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Distribution lists</td>
<td>Yes</td>
<td>NO</td>
</tr>
<tr>
<td>IBM MQ classes for .Net in a managed mode</td>
<td>Yes</td>
<td>NO</td>
</tr>
</tbody>
</table>
## Data Protection for Queues & Topics (7)

<table>
<thead>
<tr>
<th>Feature</th>
<th>MQME</th>
<th>MQ AMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Service client for .Net (XMS) apps</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Message Service client for C/C++ (XMS) apps</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Protection of SYSTEM.* queues</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Require application code changes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supported Platform: Unix (AIX, HP-UX &amp; Solaris)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supported Platform: Linux (x86, x86-64, Power &amp; System z)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supported Platform: Windows</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supported Platform: IBM i (OS/400)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
[default]
License=
LicenseFile=C:\Capitalware\MQME\mqme_licenses.ini
LogMode=N
LogFile=C:\Capitalware\MQME\mqme.log
RotateLogDaily=Y
Active=Y
IniFileRecheckTime=60
ExitPath=C:\Capitalware\MQME\User
UserIDFormatting=A
Perform=E
KeySize=128
UseExcludeQueues=N
UseExcludeTopics=N
UseExcludeUserIDs=Y
ExcludeUserIDs=abcd; tester
UseExcludeApplications=N
ExcludeApplications=mqexplorer; mqve
#

[Q:TEST.*]
ApplicationsForGet = aq1
ApplicationsForPut = ap1
GroupFileForGet = C:\Capitalware\MQME\groupsForGet.ini
GroupFileForPut = C:\Capitalware\MQME\groupsForPut.ini
GroupsForGet = grp1; grp2
GroupsForPut = GrpA; GrpB
KeySize = 256
UseApplicationsForGet = Y
UseApplicationsForPut = Y
UseGroupFileForGet = Y
UseGroupFileForPut = Y
UseGroupsForGet = Y
UseGroupsForPut = Y
UserIDsForGet = roger
UserIDsForPut = Test1; Test2
#

[Q:ABC.*]
KeySize = 256
UserIDsForGet = appl01; appl02; appl03
#

[T:TEST/ABC]
UserIDsForGet = fred; Barney; Wilma
MQME-GUI (2)
MQME-GUI (4)

![MQME-GUI screenshot](image-url)

Keywords and Values:
`UserID=Fred;Barney;Wilma`
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 (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!
MQ Security Grid (4)

MQME deployed to 4 queue managers & 9 clients:
Questions & Answers