

# *MQ Channel Encryption Overview*



Capitalware Inc.  
1673 Richmond Street, Suite 524  
London, Ontario N6G2N3  
Canada  
sales@capitalware.biz  
<http://www.capitalware.biz>

# Table of Contents

---

<b>1 INTRODUCTION.....</b>	<b>1</b>
1.1 OVERVIEW.....	1
1.2 EXECUTIVE SUMMARY.....	2
1.3 MESSAGE DIAGRAM (LOGICAL VIEW).....	2
1.4 CONTEXT DIAGRAM (LOGICAL VIEW).....	3
1.5 PREREQUISITES.....	4
<i>1.5.1 Operating System</i> .....	<i>4</i>
<i>1.5.2 WebSphere MQ</i> .....	<i>5</i>

# 1 Introduction

## 1.1 Overview

*MQ Channel Encryption* (MQCE) provides encryption for MQ message data. In cryptography, encryption is the process of transforming information into an unreadable form (encrypted data). Decryption is the reverse process. It makes the encrypted information readable again. Only those with the key (PassPhrase) can successfully decrypt the encrypted data.

MQCE provides encryption for message data, which flows between WebSphere MQ (WMQ) resources. MQCE operates with WMQ v5.3, v6.0 and v7.0 (and MQSeries v5.2) in Windows, Unix, IBM i (OS/400) and Linux environments. It operates with Sender, Receiver, Server, Requestor, Cluster-Sender, Cluster-Receiver, Server Connection and Client Connection channels of the WMQ queue managers.

MQCE is a simple drop-in solution that provides cryptographic protection for WMQ queue managers. The protection can be queue manager to queue manager or client application to queue manager.

- Queue manager to queue manager protection means all messages flowing over a channel between 2 queue managers will be encrypted.
- Client application to queue manager protection means application-level message data flowing between a WMQ client application and queue manager will be encrypted.

The MQCE can be configured as a queue manager channel message exit or as a channel sender/receive exit pair.

MQCE uses Advanced Encryption Standard (AES) to encrypt the data. AES is a data encryption scheme, adopted by the US government, that uses three different key sizes (128-bit, 192-bit, and 256-bit). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year standardization process.

MQCE uses the SHA-2 to create a cryptographic hash function (digital signature) for the message data.

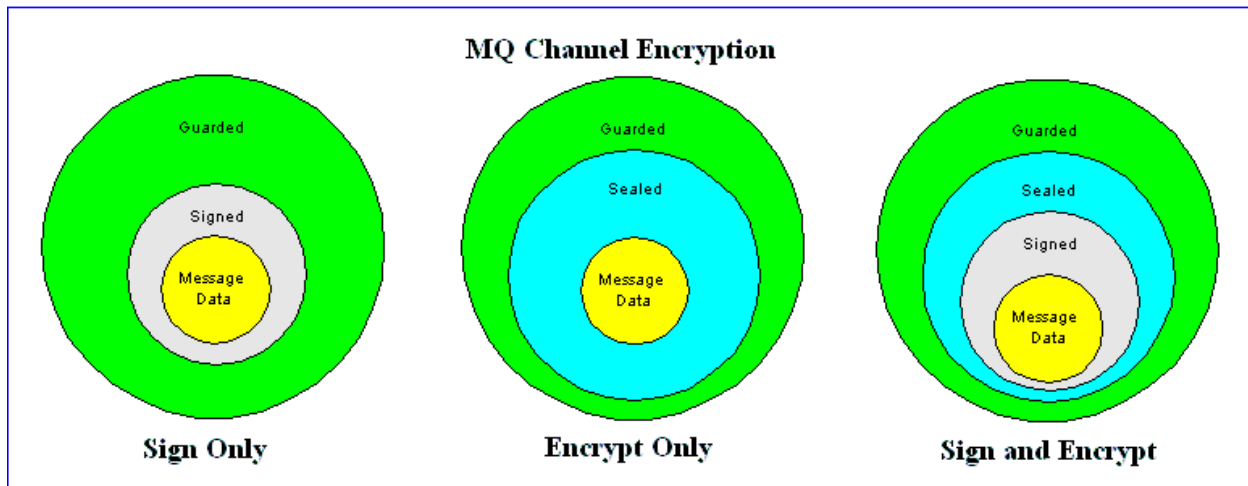
## 1.2 Executive Summary

The MQCE solution is an MQ encryption exit. It is available for a wide range of platforms: AIX, HP-UX, IBM i, Linux, Solaris and Windows.

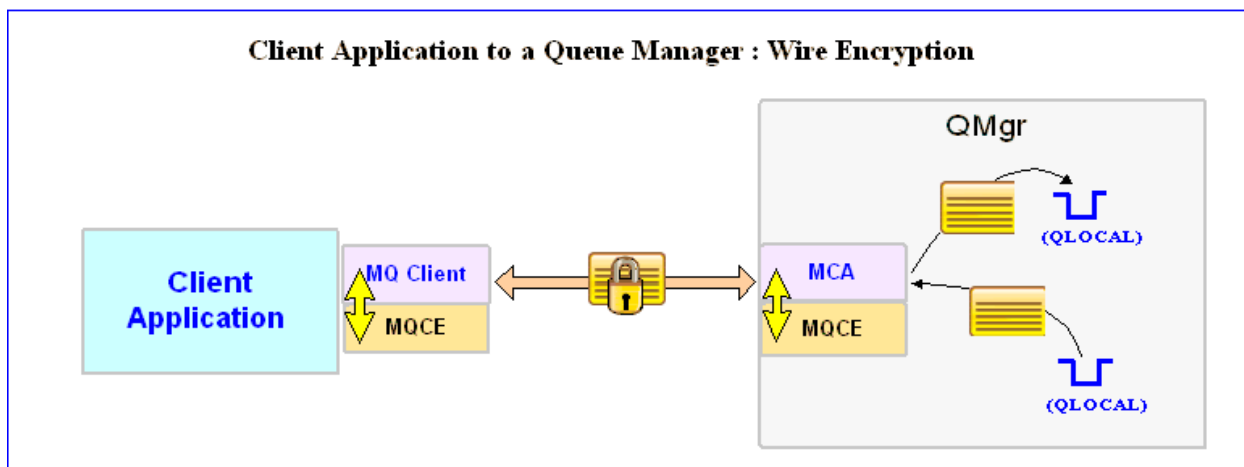
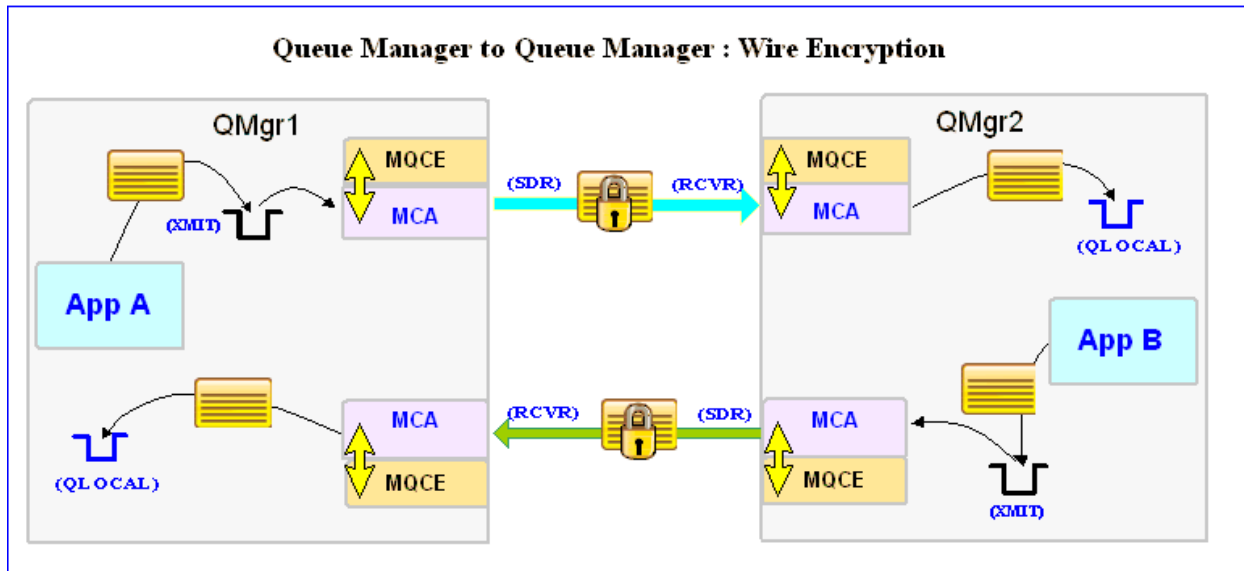
Major Features of MQCE:

- Easy to set up and configure (unlike SSL)
- No application changes required
- Can be configured as either queue manager to queue manager or client application to queue manager solution
- For both modes, all message data flowing over a channel will be encrypted (nothing missed or forgotten)
- Secure encryption/decryption methodology using AES with 128, 192 or 256-bit keys
- Uses the SHA-2 to create a cryptographic hash function (digital signature)
- Standard MQ feature, GET-with-Convert, is supported
- Provides high-level logging capability for encryption / decryption processing

## 1.3 Message Diagram (Logical View)



## 1.4 Context Diagram (Logical View)



## 1.5 Prerequisites

This section details the minimum supported software levels. These prerequisites apply to both client-side and server-side installations of MQ Channel Encryption.

### 1.5.1 Operating System

MQ Channel Encryption can be installed on any of the following supported servers:

#### 1.5.1.1 IBM AIX

- IBM AIX 5L version 5.1 or higher

#### 1.5.1.2 HP-UX IA64

- HP-UX v11.23 or higher

#### 1.5.1.3 HP-UX PA-RISC

- HP-UX v11.00 or higher

#### 1.5.1.4 IBM i (OS/400)

- IBM i V5R3 or higher

#### 1.5.1.5 Linux x86

- Linux kernel, version 2.4
- glibc version 2.2.5 or greater

Sample distributions:

- Red Hat Enterprise Linux v4, v5
- SuSE Linux Enterprise Server v9, v10, v11

#### 1.5.1.6 Linux x86\_64 (64-bit)

Sample distributions:

- Red Hat Enterprise Linux v4, v5
- SUSE Linux Enterprise Server v9, v10, v11

#### 1.5.1.7 Linux on POWER

Sample distributions:

- Red Hat Enterprise Linux v4, v5
- SUSE Linux Enterprise Server v10, v11

#### 1.5.1.8 Linux on zSeries (32-bit)

- Linux kernel, version 2.4
- glibc version 2.2.5 or greater

Sample distributions:

- Red Hat Enterprise Linux v4, v5
- SUSE Linux Enterprise Server v10, v11

### 1.5.1.9 Linux on zSeries (64-bit)

Sample distributions:

- Red Hat Enterprise Linux v4, v5
- SUSE Linux Enterprise Server v9, v10, v11

### 1.5.1.10 Sun Solaris

- Solaris SPARC v8 or higher
- Solaris v10 x86\_64 (64-bit)

### 1.5.1.11 Windows

- Windows NT, 2000, 2003 or 2008 Server (32-bit)
- Windows XP Professional, Vista or 7 (32-bit)

## 1.5.2 WebSphere MQ

- WebSphere MQ v5.3 (or MQSeries v5.2)
- WebSphere MQ v6.0 and v7.0 (both 32-bit and 64-bit)

Operating System	WMQ v5.3 (or MQ 5.2)	WMQ v6.0 & v7.0
AIX v5.1 or higher	32-bit	64-bit
HP-UX IA64 v11.23 or higher	n/a	64-bit
HP-UX PA-RISC v11.00 or higher	32-bit	64-bit
IBM i (OS/400)	64-bit	64-bit
Linux x86	32-bit	32-bit
Linux x86_64	n/a	64-bit
Linux on POWER	n/a	64-bit
Linux on zSeries	32-bit	64-bit
Solaris SPARC v8 or higher	32-bit	64-bit
Solaris x86_64 v10	n/a	64-bit
Windows NT, 2000, 2003, XP Pro, Vista & 7	32-bit	32-bit