MQ Channel Encryption for z/OS Overview

Last Updated: July 2020.
© Copyright Capitalware Inc. 2010, 2020.

Table of Contents

1 Introduction

1.1 Overview

MQ Channel Encryption for z/OS (z/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.

z/MQCE provides encryption for message data, which flows between IBM MQ resources. z/MQCE operates with MQ v5.3.1, v6.0, v7.0, v7.1, v8.0, v9.0, v9.1 and v9.2 for z/OS environments. It operates with Sender, Receiver, Server, Requester, Cluster-Sender, Cluster-Receiver, Server Connection and Client Connection channels of the MQ queue managers.

z/MQCE is a simple drop-in solution that provides cryptographic protection for MQ 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 MQ client application and queue manager will be encrypted.

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

z/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.

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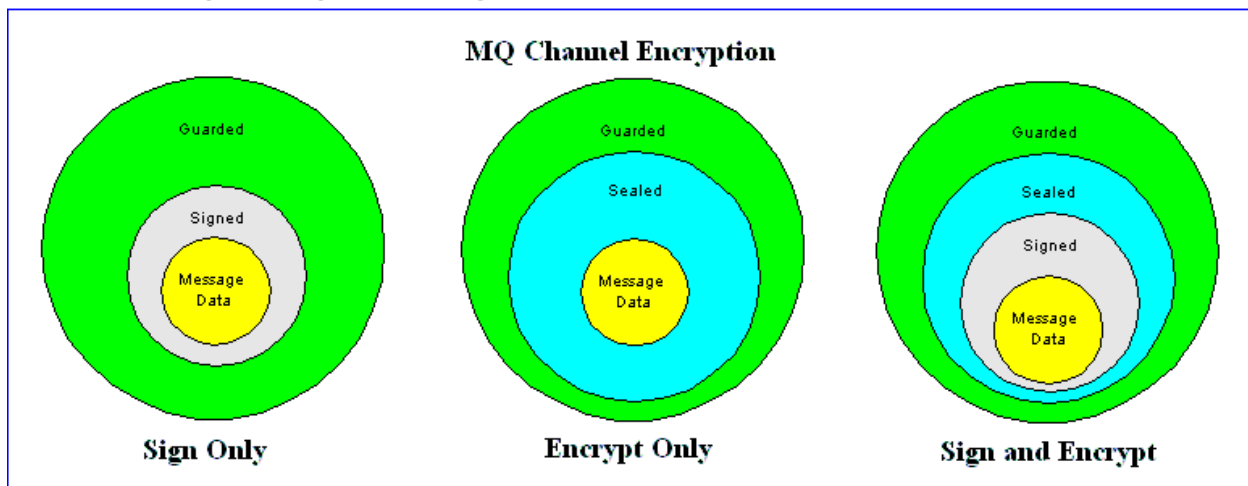
1.2 Executive Summary

The z/MQCE solution is an MQ encryption exit. It is available for z/OS v1.4 or higher environments.

Major Features of MQCE for z/OS:

- ➢ 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 logging capability via Write To Operator (WTO) facility.

1.3 Message Diagram (Logical View)

1.4 Context Diagram (Logical View)

Queue Manager to Queue Manager : Wire Encryption

Client Application to a Queue Manager : Wire Encryption
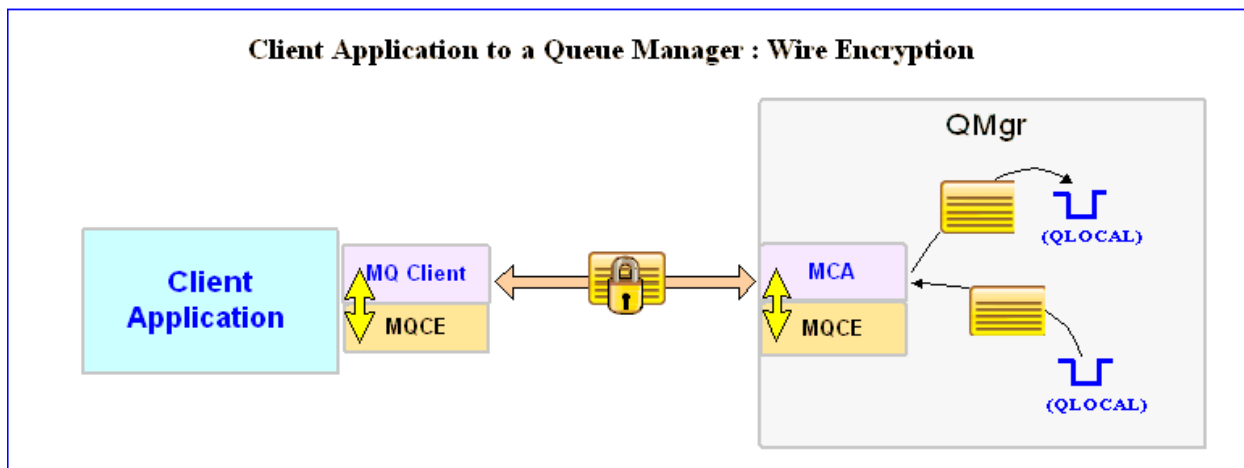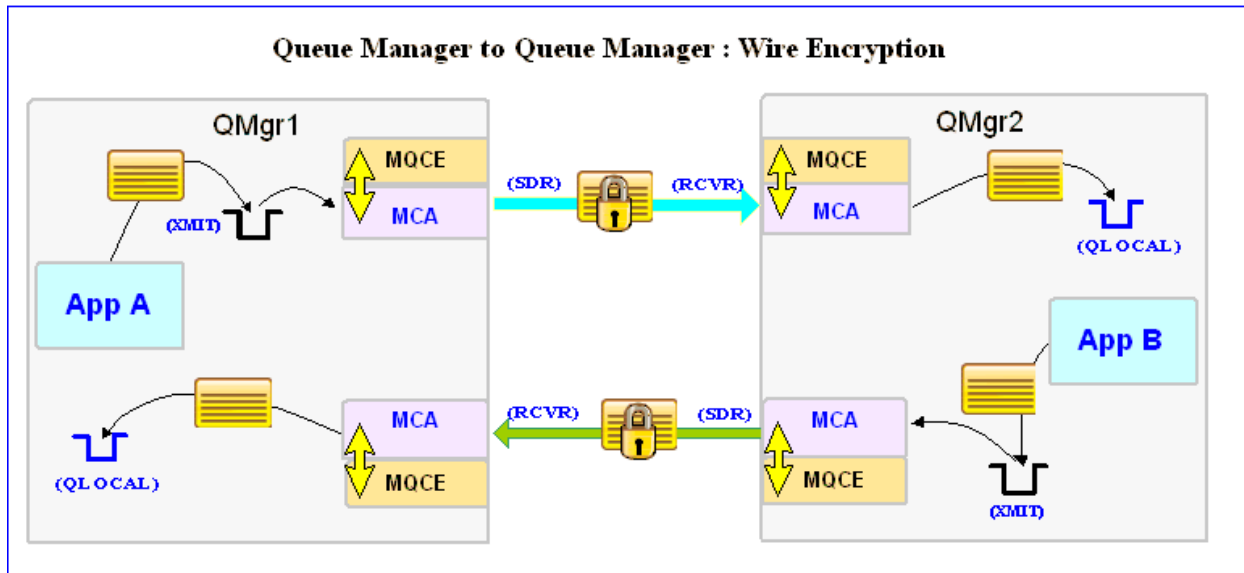
1.5 Prerequisites

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

1.5.1 Operating System

MQ Channel Encryption for z/OS can be installed on any of the following supported servers:

1.5.1.1 IBM z/OS
➢ IBM z/OS v1.4 or higher

1.5.2 IBM MQ
➢ IBM MQ for z/OS v5.3.1, v6.0, v7.0, v7.1, v8.0, v9.0, v9.1 and v9.2