

# ***MQ Instant Secure Data Overview***



Capitalware Inc.  
90 Morrison Crescent,  
Markham, Ontario, Canada  
L3R 9K9  
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.....	1
1.3 CONTEXT DIAGRAM (LOGICAL VIEW).....	2
1.4 PREREQUISITES.....	4
1.4.1 <i>Operating System</i> .....	4
1.4.2 <i>WebSphere MQ</i> .....	5

# 1 Introduction

## 1.1 Overview

*MQ Instant Secure Data* (MQISD) 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.

MQISD is a solution that allows a company to encrypt message data, which flows between WebSphere MQ (WMQ) resources. MQISD operates with WMQ v5.3 or v6.0 (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.

MQISD is a simple drop-in solution that provides cryptographic protection for WMQ queue managers. The protection can be Node-to-Node or End-to-End.

- Node-to-Node protection means all messages flowing over a channel between 2 queue managers will be encrypted.
- End-to-End protection means application-level message data flowing between 2 WMQ Client applications will be encrypted.

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

MQISD uses TEA Variant to encrypt the data. The TEA Variant is a fast block cipher algorithm with a 128-bit key. The algorithm is simple, fast and secure.

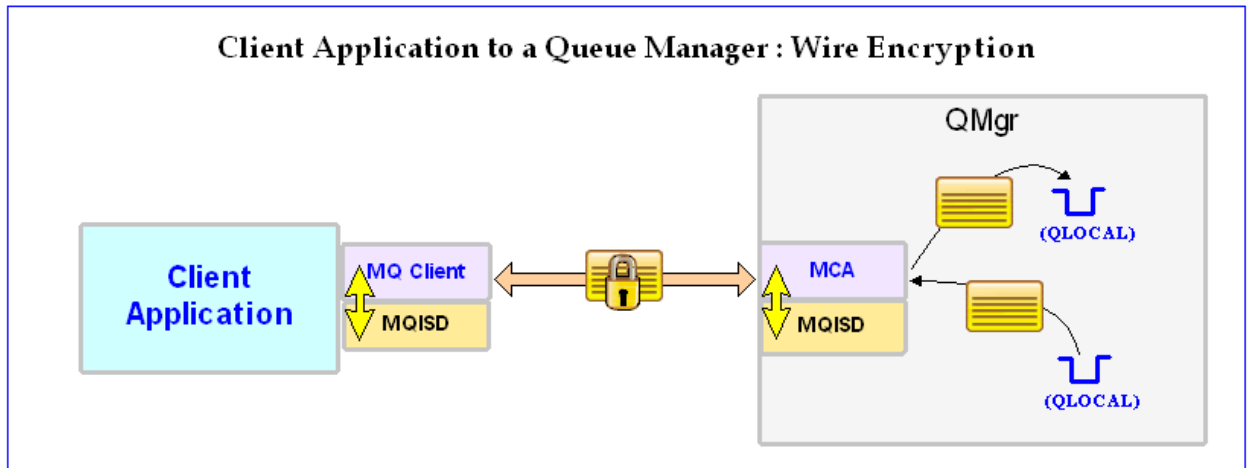
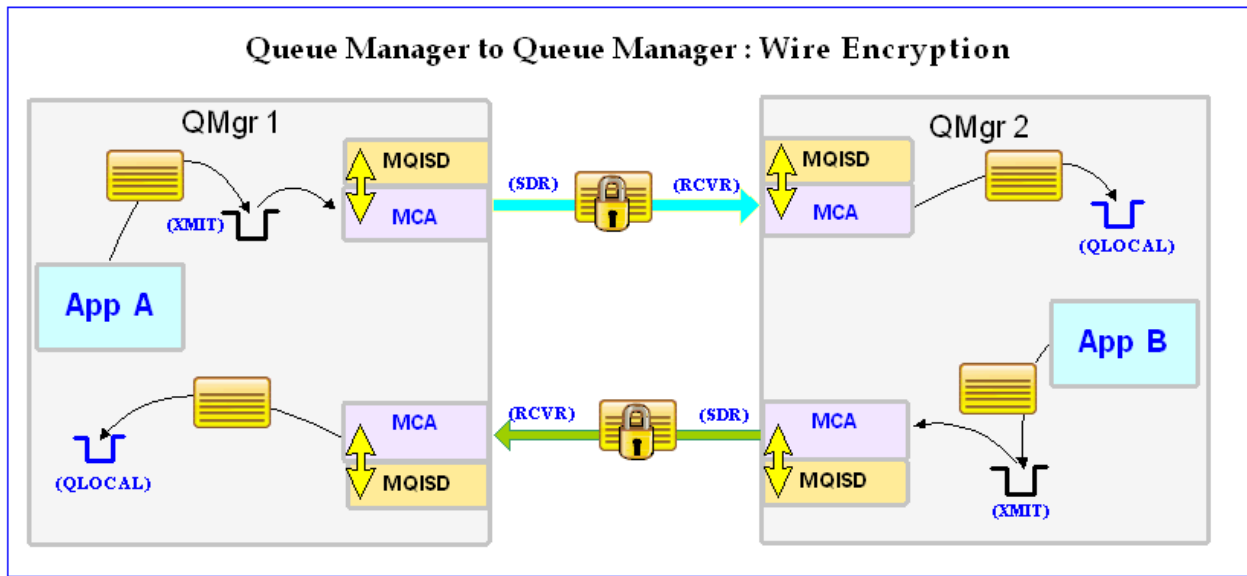
## 1.2 Executive Summary

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

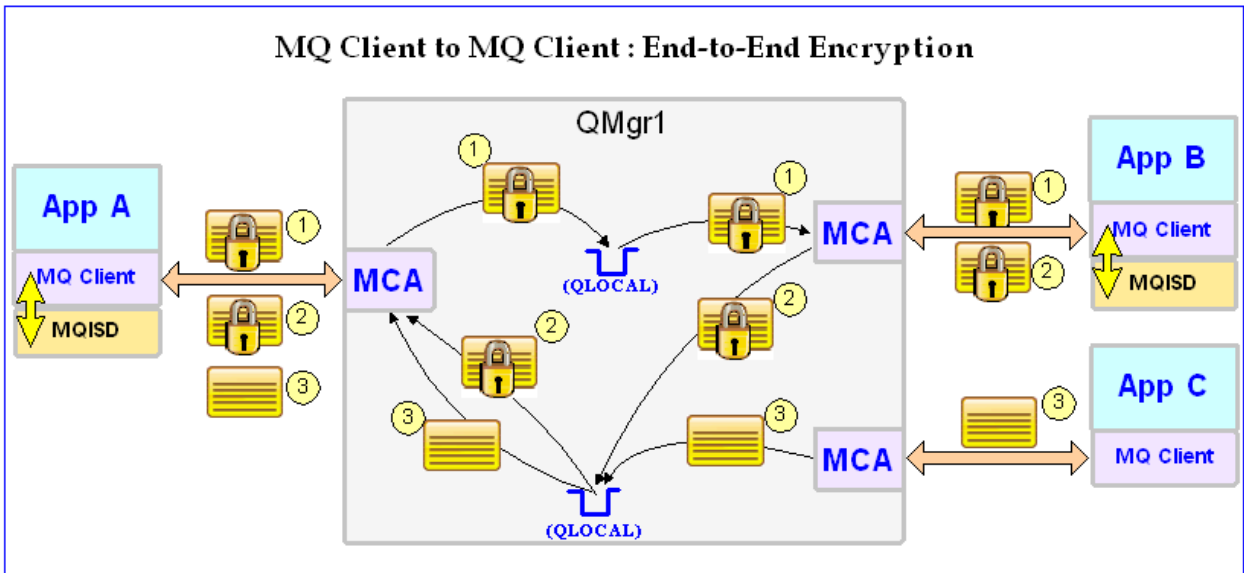
Major Features of MQ Instant Secure Data:

- Easy to set up and configure (unlike SSL)
- No application changes required
- Can be configured as either Node-to-Node or End-to-End solution
- In Node-to-Node mode, all message data flowing over a channel will be encrypted (nothing missed or forgotten)
- Extremely fast encryption/decryption methodology using TEA Variant 128-bit key
- Standard MQ feature, GET-with-Convert, is supported
- Provides high-level logging capability for encryption / decryption processing

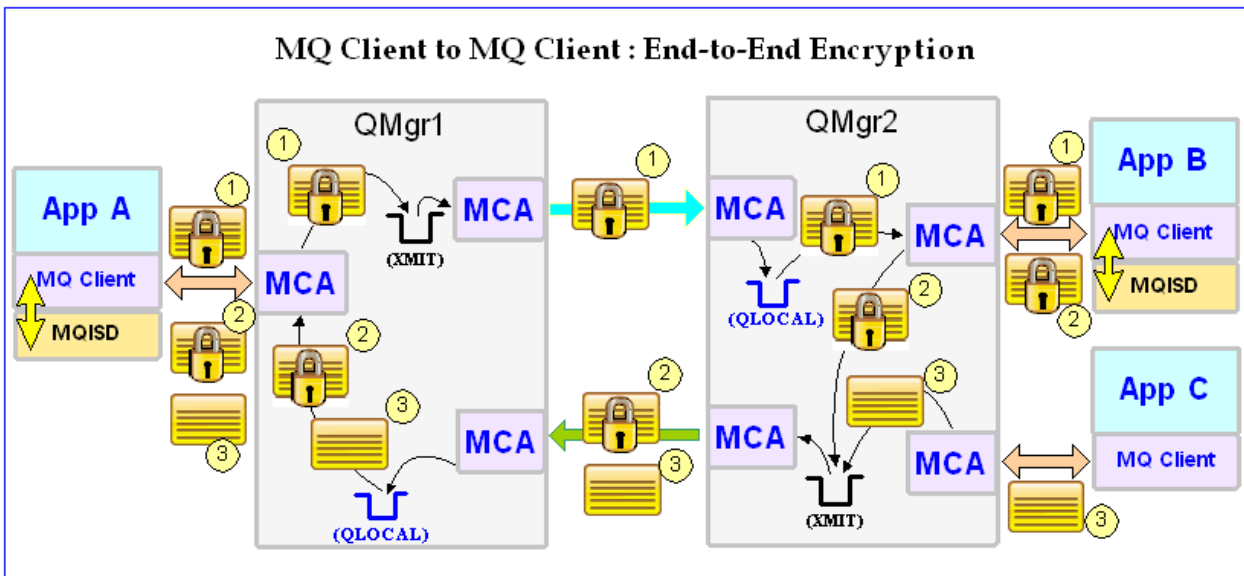
### 1.3 Context Diagram (Logical View)



### MQ Client to MQ Client : End-to-End Encryption



### MQ Client to MQ Client : End-to-End Encryption



## 1.4 Prerequisites

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

### 1.4.1 Operating System

MQ Instant Secure Data can be installed on any of the following supported servers:

#### 1.4.1.1 IBM AIX

- IBM AIX 5L version 5.1 or higher

#### 1.4.1.2 HP-UX IA64

- HP-UX v11.23 or higher

#### 1.4.1.3 HP-UX PA-RISC

- HP-UX v11.00 or higher

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

- IBM i V5R3 or higher

#### 1.4.1.5 Linux x86

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

Sample distributions:

- Red Hat Linux v7.3
- SuSE Linux Enterprise Server v7

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

Sample distributions:

- Red Hat Enterprise Linux v4.0
- SUSE Linux Enterprise Server v9

#### 1.4.1.7 Linux on POWER

Sample distributions:

- Red Hat Enterprise Linux v3.0 (with Update 2)
- Red Hat Enterprise Linux v4.0
- SUSE Linux Enterprise Server v9

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

- Linux kernel, version 2.4
  - glibc version 2.2.5 or greater
- Sample distributions:
- Red Hat Enterprise Linux v3.0 (with Update 2)
  - SUSE Linux Enterprise Server v8 (with Service Pack 3)
  - SUSE Linux Enterprise Server v9

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

Sample distributions:

- Red Hat Enterprise Linux v4.0
- SUSE Linux Enterprise Server v9

#### 1.4.1.10 Sun Solaris

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

#### 1.4.1.11 Windows

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

#### 1.4.2 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	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