# National Information Assurance Partnership


TM

# Common Criteria Evaluation and Validation Scheme Validation Report

# IBM UK Ltd

# IBM WebSphere MQ Version 6.0.1.1

**Report Number:** CCEVS-VR-06-0031
**Dated:** 2 October 2006
**Version:** 1.0

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6740**
**Fort George G. Meade, MD 20755-6740**

## ACKNOWLEDGEMENTS

**Validation Team**

**Victoria A. Ashby**
**The MITRE Corporation**
**McLean, VA**

**Common Criteria Testing Laboratory**

**Science Applications International Corporation**
**Columbia, Maryland**

# Table of Contents

# 1 Executive Summary

The evaluation of IBM WebSphere MQ (WMQ) was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 2 October 2006. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.3 and the Common Methodology for IT Security Evaluation (CEM), Version 2.3, dated August 2005.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.2). The TOE, which is the WebSphere MQ, allows application programs to use *message queuing* to participate in message-driven processing. Application programs can communicate across different platforms by using WMQ. For example, AIX and Sun Solaris applications can communicate through WMQ. The applications are shielded from the mechanics of the underlying communications.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC. The TOE is a software-only TOE consisting of a WMQ Server and WMQ clients. WMQ is divided into operating system-specific editions and the specific version for this evaluation is WMQ for AIX 5.2. Each of the operating system-specific editions can support the following components: WMQ server (which includes the queue manager); WMQ C Client and JMS/Java clients. The WMQ Server and WMQ C Client use the GSKit software to enable support for TLS/SSL. GSKit is a set of tools and C/C++ programming interfaces that can be used to add secure channels using the SSLv3 and TLSv1 protocols to TCP/IP applications (products). It provides the cryptographic functions, the protocol implementation, and key generation and management functionality for this purpose. GSKit has been separately evaluated and the results of that evaluation have been reused in accordance with CCEVS Policy Letter 8. This Validation Report applies only to the specific version of the TOE as evaluated.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the IBM WebSphere MQ product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the

conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.2) have been met.

## 1.1 Interpretations

This evaluation used the Common Criteria for Information Technology Security Evaluation Parts 2 and 3, Version 2.3, August 2005. The evaluation started in August 2005; therefore, no additional interpretations existed be applied.

# 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant;
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| **Evaluation Scheme** | United States NIAP Common Criteria Evaluation and Validation Scheme |
| **TOE**: | IBM WebSphere MQ Version 6.0.1.1 |
| **Protection Profile** | Not applicable. |
| **ST**: | IBM WebSphere MQ EAL 4 Security Target, Version 1.0, 25 July 2006 |
| **Evaluation Technical Report** | *Evaluation Technical Report for IBM WebSphere MQ version 6.0.1.1,* Version 2.0, 16 August 2006 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 |

| Item | Identifier |
|---|---|
| **Conformance Result** | CC Part 2 extended with FAU_GEN_MQ.1 and FMT_MSA_MQ.3 and Part 3 conformant |
| **Sponsor** | IBM UK LTD |
| **Developer** | IBM UK LTD |
| **Common Criteria Testing Lab (CCTL)** | SAIC, Columbia, MD |
| **CCEVS Validator** | Vicky Ashby, The MITRE Corporation |

# 3 Organizational Security Policy

The TOE complies with the following Organizational Security Policy:

- The right to access a specific object is determined on the basis of:
  - The identity of the subject attempting to access the object; or
  - Membership of a group that has access rights to the object.

# 4 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organizational security policies which the product is designed to comply.

Following are the assumptions are identified in the Security Target:

- It is assumed that the operating system has been configured in accordance with the manufacturer's installation guides and where applicable, in its evaluated configuration. It is securely configured such that the operating system protects the TOE from any unauthorized users or processes.
- It is assumed that all software and hardware, including peripheral devices, have been approved for the transmittal of protected data. Such items are to be physically protected against threats to the confidentiality and integrity of the data.

- It is assumed that there are one or more competent individuals that are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, willfully negligent or hostile.

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- A user of the TOE may gain access to an object without the correct authority to access that object or may gain administrative privileges and these attempts may go undetected.
- Data that is being transferred between platforms (TOE components) is disclosed and/or modified.
- The operating system on which the TOE is installed becomes compromised.

The Security Target also identifies the following threats that the IT environment supporting the TOE is expected to address:

- An unidentified user gains access to the TOE and its objects.
- A non-privileged user gains administrative privileges.
- The operating system on which the TOE is installed becomes compromised.

The scope of this evaluation includes the WMQ product as described in the next section. It is important to note that the encryption services required by the TOE are provided in two different ways, one within the TOE boundary and one outside of the TOE boundary. The two methods are as follows:

- For the WMQ Server product and for the WMQ C Client, GSKit has been separately evaluated and the results of that evaluation have been reused in accordance with CCEVS Policy Letter 8. This Validation Report applies only to the specific version of the TOE as evaluated.
- For the WMQ Java/JMS Clients, encryption services are provided by the IBM® Java JSSE FIPS provider (IBMJSSEFIPS or IBMJSSE2) cryptographic modules that have been FIPS 140-2 certified. The JSSE and the Java JSSE FIPS provider are outside the TOE boundary, but must be present in the TOE environment.

More details are given in the section that follows.

# 5 Architectural Information

WMQ allows application programs to use *message queuing* to participate in message-driven processing. Application programs can communicate across different platforms by

using WMQ. For example, AIX and Sun Solaris applications can communicate through WMQ. The applications are shielded from the mechanics of the underlying communications.

Messages are used to transfer information from one application program to another (or between different parts of the same application). The applications can be running on the same platform, or on different platforms.

Each queue is owned by a *queue manager*. The queue manager is responsible for maintaining the queues it owns, and for storing all the messages it receives onto the appropriate queues. The messages might be put on the queue by application programs, or by a queue manager as part of its normal operation.

The TOE is indicated by the thick black line shown in the figure below. IBM WebSphere MQ consists of the WMQ server (which includes the queue manager, and is shown as the larger block at top in the figure), and the WMQ C Client and JMS/Java clients (shown as the smaller blocks at the bottom of the figure).

The WMQ server contains the queue manager, which is responsible for maintaining the queues that it owns, and for storing all the messages it receives onto the appropriate queues. The server contains components that:

- Interface with the operating system to retrieve information (Common Services),
- Provides a command line interface for administration of the queues; and
- Interface to remote queue managers (Message Channel Agent (MCA)). This component is responsible for sending and receiving of messages to remote queues. Messages are transmitted between queue managers on a *channel*. *Channels* are objects that provide a communication path from one queue manager to another or from a client to a queue manager; this is secured in the evaluated configuration using TLS or SSL protocols.

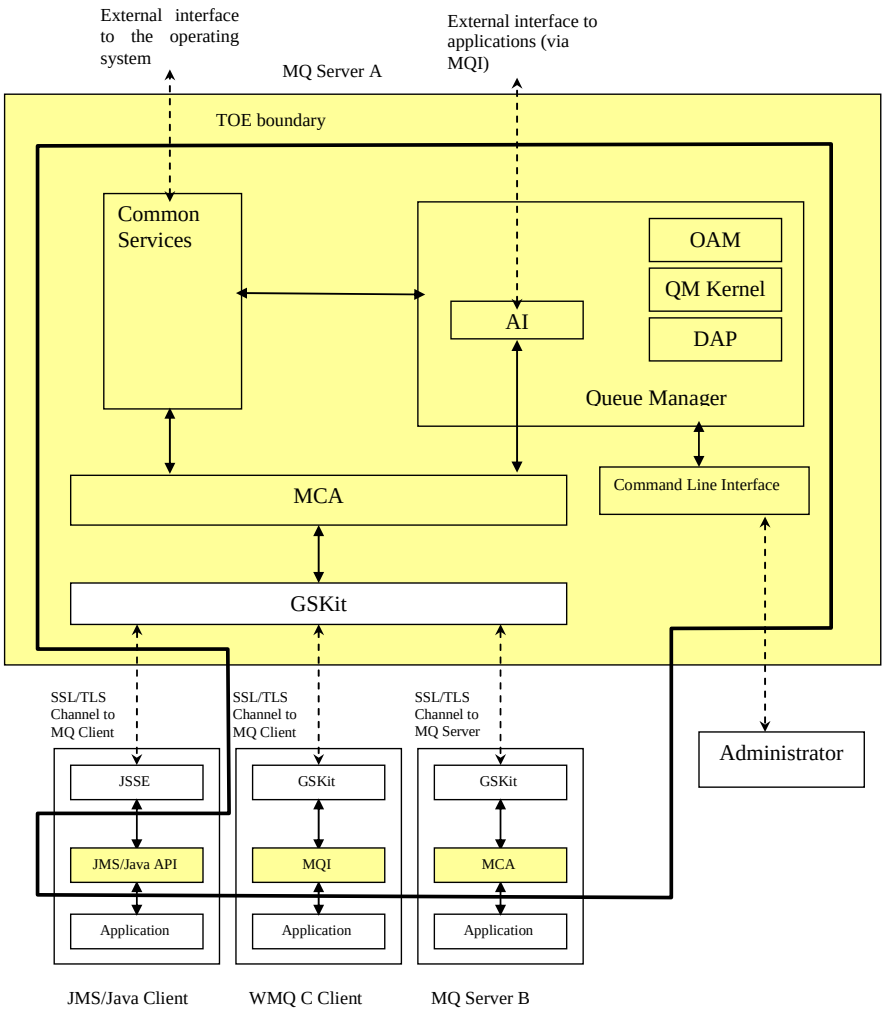
The WMQ C client is part of the WMQ product that can be installed on its own, on a separate machine from the server. A WMQ user application can be built and run on a WMQ C client system and it can interact with one or more WMQ servers and can connect to their queue managers by transmitting messages on channels that are secured using TLS or SSL protocols in the evaluated configuration.

WMQ classes for Java (also referred to as WMQ base Java or WMQ Java) allow a Java application to connect to WMQ as a WMQ client or connect directly to a WMQ server. WMQ base Java encapsulates the Message Queue Interface (MQI), the native WMQ API.

WMQ classes for Java Message Service (also referred to as WMQ JMS) are a set of Java classes that implement Sun's Java Message Service (JMS) interfaces to enable JMS programs to access WMQ systems. As with WMQ classes for Java, WMQ classes for JMS allow a WMQ JMS application to connect to WMQ either as a WMQ client or directly to a WMQ server.

WMQ JMS and Java clients can be installed as WMQ clients either on the WMQ server machine or on a separate machine. A WMQ Java application uses TLS/SSL in the evaluated configuration to obtain a secure connection to a queue manager, with authentication, message integrity, and data encryption. The IBM® Java JSSE FIPS provider (IBMJSSEFIPS or IBMJSSE2) provides the ability to use TLS/SSL connections with cryptographic modules that have been FIPS 140-2 certified. The JSSE and the Java JSSE FIPS provider are outside the TOE boundary.

The WMQ Server product and the WMQ C Client use the IBM® Global Security Kit's TLS/SSL API to request TLS/SSL connections. The JMS/Java Clients use the IBM® Java JSSE FIPS (IBMJSSEFIPS) or the IBMJSSE2 providers to request TLS/SSL connections. Only FIPS 140-2 certified TLS/SSL cipher specs are permitted within the TOE. GSKit version 7.0.3.18 is within the TOE boundary and was evaluated as a component TOE evaluation. As such, this evaluation reused the GSKit component evaluation per CCEVS Policy Letter 8.




# 6 Documentation

IBM offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features. Following is the list of documentation that was evaluated and is provided to the end user. All methods of receiving the documentation were verified by the evaluation team.

**Guidance Documentation**

| **Document** | **Version** | **Date** |
|---|---|---|
| WebSphere MQ System Administration Guide Version 6.0, SC34-6584-01 | 2nd Edition | July 2006 |
| Install instructions and standalone help downloadable package is available at: | | |

| Document | Version | Date |
|---|---|---|
| http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp<br>The Installation instructions are included with the CD package and is part of the zip file download if the customer selects delivery via download. | | |

**Delivery and Operation Documentation**

| Document | Version | Date |
|---|---|---|
| IBM WebSphere MQ 6.0 Delivery, Operation, and Guidance | Issue 1.2 | 10 March 2006 |
| DSW Secure Media Delivery<br>*Installation Guidance at,*<br>http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp | Version 1.2 | |

**Security Target**

| Document | Version | Date |
|---|---|---|
| IBM WebSphere MQ EAL 4 Security Target | Version 1.0 | 1 August2006 |

# 7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

## 7.1 Developer Testing

The vendor's test suite was organized by security function and included both automated and manual tests. Prior to independent testing, the evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected. The Evaluation Team added tests to the team test plan in cases where additional tests were indicated to ensure complete test coverage.

Before testing, the vendor provided a complete set of expected and actual test results for analysis. The evaluation team examined the vendor's actual test results for the TOE configuration on AIX 5.2. During analysis of the vendor test suite prior to actual testing, the vendor test suite, expanded by the team tests, was shown to adequately address all security functions claimed in the ST for the TOE.

## 7.2 Evaluation Team Independent Testing

The evaluation team re-ran the entire vendor test suite on the AIX platform during testing. In addition to rerunning the vendor's tests, the Evaluation Team developed a set of independent team tests to address areas of the ST that did not seem completely addressed

by the vendor's test suite, or areas where the ST did not seem completely clear. Most were run as manual tests, but for others, scripts were developed to automate the tests.

The vendor provided the TOE configuration at a local site for installation and testing. The tests were executed on a machine connected to a closed lab network. Also on this network were an LDAP server for use in the access control tests, and sniffers used in tests described below.
. The following hardware is necessary to create the test configuration:

AIX 5.2:

Any machine that supports the AIX5L V5.2 or AIX5L V5.3 operating systems capable of running 64-bit programs whether from IBM® or other vendors.

Typical storage requirements are as follows:

- Server installation: 325 MB
- Disk storage is also required for:
- Prerequisite software
- Optional software
- Your application programs

The following software is required to be installed on the machines used for the test:

Operating Systems:
- AIX V5.2 with Maintenance level 3;

TOE Software:
- IBM WebSphere Message Queue 6.0.1.1
- GSKit version 7.0.3.18

The following software is required in order that the tests can be run. Versions are not important, unless stated:

- C and C++ compilers (platform dependent).
- Perl Interperter v5.8 (ActivePerl from http://www.activestate.com) is required for Windows and Linux. For AIX 5, Solaris 2.8 and 9 perl comes with the operating system. For other platforms Perl V5 or higher is required
- 'make' (obtained from GNU website: http://www.gnu.org).
- Perl Package Win32-API for windows platforms only.
- IBM Java SDK 1.4.2 included as an optional installable component of the WebSphere MQ V6 Product

The Evaluation Team installed the TOE using the vendor's installation documentation and media delivered using the normal customer delivery process. While installing each TOE configuration, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration. Some issues were noted during the set up and testing. Updates to the vendor documentation have corrected the cause of these issues.

The Evaluation Team determined that the evaluation team's actual test results matched the vendor's expected and actual results. All API calls were executed when the user had the proper authorities, and access denied when the user did not have the proper authorities. A user was added and removed from the identified groups accordingly. This revealed the appropriate authorities before and after the refresh command was executed. All communication was secured using FIPS 140-2 CipherSuites. The evaluation team has determined the TOE behaves as expected and all test suites have been successfully executed on the identified platform. In addition, during team testing, the evaluation team confirmed the GSKit component TOE was installed and configured in accordance with the supplied guidance, and that the password stash file was properly protected by access control. The team tests also verified self-protection of the TOE, which is provided in part by the IT environment in which the TOE operates.

## 7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of vulnerability test tools, open-source vulnerability documentation, and a set of test procedures proposed by the Evaluation Team to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests. The penetration test ensured that communication between the TOE components was in fact encrypted and therefore protected from modification and disclosure. The penetration test also confirmed a that the user with all privileges could not cascade those privileges to other untrusted users (not an administrator of the mqm group).

The Evaluation Team's Final ETR, Part 2 Supplement, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

# 8 Evaluated Configuration

Each of the TOE components described above is a software application designed to execute within an operating system context provided by the environment. Only one platform is included in the evaluated configuration, as follows:

- AIX Version 5.2.

As noted above, the TOE includes GSKit 7.0.3.18, which was separately evaluated as a component. Evaluation evidence for that prior component evaluation was included per CCEVS Policy Letter 8.

In addition, there are three expectations on the TOE environment for the evaluated configuration:

- The TOE can retrieve CRLs using an LDAP client and server provided by the TOE environment. The connection between the LDAP client and the LDAP server must be an internal communication link within a trusted network. Additionally, the JMSAdmin tool requires an LDAP server or file system to store the JNDI objects.

- The TOE environment includes an application to read audit records produced by the TOE.

- The GSKit key database file is protected by a password. In order to allow unattended access to the key database file GSKit provides a stash file to store the password. This stash file must be protected by an ACL or permission bits while it resides on the system and by encrypting the stash file when it is backed up.

# 9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.3 and the Common Evaluation Methodology (CEM) Version 2.3 and all applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component and the ALC_FLR.2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

"Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the IBM WebSphere MQ EAL4 Security Target is a CC compliant ST."

In addition,

"The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "PASS". Therefore, when configured according to the following guidance documentation:

- *WebSphere MQ for (platform specific) Quick Beginnings Guide, Version 6.0, Second Edition October 2006*

The IBM WebSphere MQ TOE satisfies the *IBM WebSphere MQ EAL4 Security Target*, Version 1.0, dated 25 July 2006."

The rationale supporting each CEM work unit verdict is recorded in the *Evaluation Technical Report for IBM WebSphere MQ Version 6.0.1.1, Part 2*, which is considered proprietary.

The validation team followed the procedures outlined in the *Common Criteria Evaluation and Validation Scheme (CCEVS) Publication # 3* for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

# 10 Validator Comments/Recommendations.

This evaluation followed Policy Letter 8 to include GSKit as a previously-evaluated component. The vendor had planned to use the results of a new evaluation of a new version of GSKit. As of November 2006, this new evaluation had not completed. Therefore, the vendor chose to use the results of the previous evaluation of GSKit 7.0.3.18. This limited the choice of evaluated platforms for this IBM WebSphere MQ evaluation to AIX 5.2. During independent team testing, the vendor provided additional platforms for testing. All testing, including re-run of the vendor test suite and the team tests, were run on the additional platforms as well as on AIX 5.2. The vendor intends to use the results of these tests to perform an Assurance Continuity action and add two additional platforms to the evaluated configuration on completion of the on-going GSKit evaluation. However, this VR only covers the TOE using GSKit 7.0.3.18 on the AIX 5.2 platform.

Policy Letter 8 was met by including the GSKit documentation, including *IBM Global Security Kit Version 7c Security Target*, version 3.4, *GSKit Functional Specification and Partial Representation Correspondence*, version 2.8, and *IBM Global Security Kit Version*

*7.03.14 Composition Requirements Definition*, v1.02, 4 November 2005 (CRD). Both the GSKit ST and the Functional Specification were included in the IBM WebSphere MQ vulnerability analysis and in the preparation for penetration testing. The CRD was used to prepare team tests that concentrated on protection of the TSF data that was transmitted between the TOE components. The IBM WebSphere MQ ST has been updated to reflect the results of these team tests. The results of the analysis that supports these team tests and shows the use of the CRD can be found in *Evaluation Technical Report for IBM WebSphere MQ Version 6.0.1.1, Part 1*.

# 11 Annexes

Not applicable.

# 12 Security Target

The Security Target is identified as *IBM WebSphere MQ EAL 4 Security Target*, Version 1.0, dated 25 July 2006. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.2.

# 13 Glossary

The following definitions are used throughout this document:

*Hardware*: the physical equipment used to process programs.

*Software*: the programs and associated data that can be dynamically written and modified.

*Target of Evaluation (TOE)* - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

*IBM WebSphere MQ* refers to the TOE.

# 14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation* Part 1: Introduction and general model, Version 2.3, August 2005
- *Common Criteria for Information Technology Security Evaluation* Part 2: Security Functional Requirements, Version 2.3, August 2005
- *Common Criteria for Information Technology Security Evaluation* Part 3: Security Assurance Requirements, Version 2.3, August 2005

Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005

Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R

- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.
- *IBM WebSphere MQ EAL 4 Security Target*, Version 1.0, 25 July 2006.
- *Evaluation Technical Report for IBM WebSphereMQ Version 6.0.1.1, Part 1* (Non-Proprietary), Version 2.0, 16 August 2006.
- *Evaluation Technical Report for IBM WebSphereMQ Version 6.0.1.1, Part 1*, Version 1.0, 16 August 2006
- IBM Global Security Kit Version 7.03.14 Composition Requirements Definition, v1.02, 4 November 2005
- IBM Global Security Kit Version 7c Security Target, version 3.4
- GSKit Functional Specification and Partial Representation Correspondence, version 2.8