National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

IBM UK LTD

IBM WebSphere MQ 5.3.0.2 with

Corrective Service Diskette (CSD) 6

Report Number: CCEVS-VR-04-0059

Dated: 27 April 2004

Version: 2.0

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

Donald Phillips, Lead Validator, Mitretek Systems

Common Criteria Testing Laboratory

Science Applications International Corporation

Columbia, MD

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of WebSphere MQ version 5.3.0.2 with Corrective Service Diskette (CSD) 6. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory, and was completed during April 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by SAIC. The evaluation team determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of the **EAL2** assurance requirements**.**

The TOE, IBM WebSphere MQ 5.3.0.2 with Corrective Service Diskette (CSD) 6 (WMQ) allows application programs to use *message queuing* to participate in message-driven processing. Application programs can communicate across different platforms by using WMQ.

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.

IBM MQ 5.3.0.2 with Corrective Service Diskette (CSD) 6 (WMQ) is considered to be a software-only TOE, and a subset of the actual product. The TOE consists of the MQ Server, which is responsible for maintaining the queues that it owns, and for storing all the messages it receives onto the appropriate queues. The server also 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.

The TOE is supported on several operating system platforms that are identified in section 8 of this document. It is assumed that all hardware and operating systems platforms used within the operating

environment are secured such that no potential vulnerabilities could be introduced that would circumvent the functionality described within the security target (ST).

The product has several features that were excluded from the target of evaluation boundary (TOE). The TOE does not support the administrator GUI interface. The command line administrator interface is only supported for the TOE. Also, the TOE does not reference or make any evaluation claims for JVM or cryptographic functionality. Please refer to section 9 of this document for further detail.

The primary security features for the IBM WebSphere MQ version 5.3.0.2 are:

- **User Data Protection**: The TOE ensures that access to an object is given to a process acting on behalf of a user, if the associated user and group Ids associated with the user, has been granted permission to access to that object. The user and group Ids are gained from the operating system and cached in memory for any subsequent access requests. Each process contains the user ID within the message descriptor part of the process, which is used to confirm the group permissions. Permission is confirmed by checking that either the UID or GID is contained within the object's Access Control List (ACL)

- **Security Audit**: In the TOE, an instrumentation event is a logical combination of conditions that is detected by a queue manager. Such an event causes the queue manager to put a special message, called an event message, on an event queue. One type of instrumentation event is the Authority event. This event reports authorization failures, such as an application trying to open a queue for which it does not have the required authority, or a command being issued from a user ID that does not have the required authority. If an attempt to access an object has not been authorized then an audit event is generated. The Type of event, the user identity and application ID data are gained from the process that attempted to access the object and recorded in the event message (audit record). The Event messages are stored in an event queue, which is protected in the same way as all other queues. Only the administrator (member of MQM group) is able to access the event queue.

- **Security Management**: The TOE is managed through a Command Line Interface (CLI). The command line interface is used to enable administrators to provide management of the queue manager. The CLI is used to administer and issue commands. The CLI provides the ability for the administrator to modify/delete event messages, update the ACLs to grant or revoke access to users/groups, viewing of the event queue contents for authorization failures and viewing of the default attributes assigned to an object upon creation. The administrator command line prevents unauthorized deletion and modifications of event messages by ensuring that only administrators (i.e. members of the MQM group) have access to the event queue.

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all

of the functional requirements and assurance requirements defined in the Security Target (ST) for an EAL2 evaluation. Therefore, the validation team concludes that the SAIC CCTL findings are accurate, the conclusions justified.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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 EAL 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
Target of Evaluation	IBM WebSphere MQ 5.3.0.2 with Corrective Service Diskette (CSD) 6
Protection Profile	Not applicable
Security Target	*WebSphere MQ EAL2 Security Target, Version 2.8, dated 4 May 2004.*
Evaluation Technical Report	*Evaluation Technical Report for IBM WebSphere MQ 5.3.0.2 with Corrective Service Diskette (CSD) 6;* Version 1.0, April 20, 2004
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	IBM UK LTD
Developer	IBM UK LTD
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD

CCEVS Validator(s)	Donald Phillips, Lead, Mitretek Systems

3. SECURITY POLICY

- The TOE must ensure that only those users with the correct authority are able to access objects by user and processes. The TOE must also allow administrators of the TOE to effectively manage the TOE and ensure that this is only performed by authorized users. The TOE also supports environmental objectives to further support the security policy. Those responsible for the TOE are assumed to be competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains. Those responsible for the TOE must ensure that each user on the supporting operating system has a unique user ID and that the operating system is configured to ensure that only approved groups of users may access the system. Those responsible for administering the TOE must also ensure that the supporting operating system is installed and configured in accordance with the manufacturer's instructions to ensure the evaluated configuration is secure.

4. ASSUMPTIONS

4.1 Personnel Assumptions

- There will be 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.

4.2 Physical Assumptions

- 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.

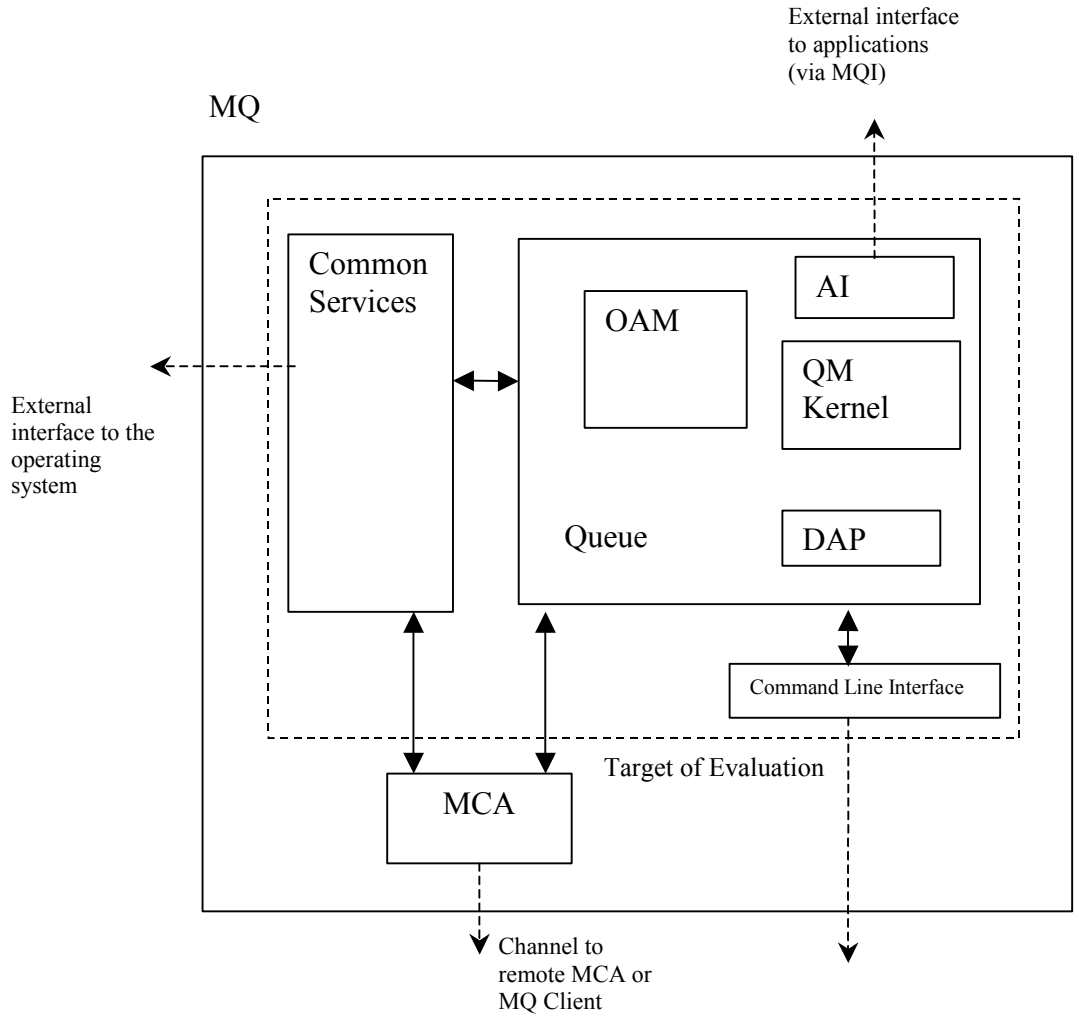
- All software and hardware, including network and peripheral devices, have been approved for the transmittal of protected data. Such items are to be physically protected against threats to the confidentiality and integrity of the data.

5. ARCHITECTURAL INFORMATION

The TOE consists of the MQ Server, which is responsible for maintaining the queues that it owns, and for storing all the messages it receives onto the appropriate queues. The server also 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.

The following diagram illustrates the physical scope and boundaries of the TOE. It should be noted that the TOE does not include the MQ Client or MQI components. The TOE is a subset of the product and the dotted line within figure 2.1 illustrates the boundary of the TOE in relation to the components.



6. DOCUMENTATION

Design documentation

Document	Version	Date
WebSphere MQ EAL2 Functional Specification	Issue 2.3	31 March 2004
WebSphere MQ EAL2 High Level Design	Issue 2.2	22 March 2004

* Representation Correspondence Embedded in the Functional Specification and the High Level Design

Guidance documentation

Document	Version	Date
WebSphere MQ System Administration Guide	Version 5 Release 3	May 2004[1]
WebSphere MQ Messages	Version 5 Release 3	October 2002
WebSphere MQ Programmable Command Formats and Administration Interface	Version 5 Release 3	March 2003
WebSphere MQ Script (MQSC) Command Reference	Version 5 Release 3	March 2003
WebSphere MQ Application Programming	Version 5 Release 3	March 2003
WebSphere MQ Event Monitoring	Version 5 Release 3	December 2002
WebSphere MQ Security	Version 5 Release 3	October 2002

Configuration Management documentation

Document	Version	Date
WebSphere MQ EAL2 Configuration Management	Issue 2.2	11 February 2004
Mq5302csd06rev4.txt	Configuration Items	

	Supplement	

Delivery and Operation documentation

Document	**Version**	**Date**
WebSphere MQ EAL2 Delivery Documentation	Issue 1.4	14 April 2004
WebSphere MQ for Linux for Intel and Linux for zSeries Quick Beginnings	Version 5.3	October 2002
WebSphere MQ for AIX Quick Beginnings	Version 5.3	May 2004
WebSphere MQ for HP-UX Quick Beginnings	Version 5.3	October 2002
WebSphere MQ for Solaris Quick Beginnings	Version 5.3	May 2004
WebSphere MQ for Windows Quick Beginnings	Version 5.3	October 2002

Test documentation

Document	**Version**	**Date**
WebSphere MQ EAL2 Developer Testing	Issue 2.3	15 April 2004

Vulnerability Assessment documentation

Document	**Version**	**Date**
WebSphere MQ EAL2 Vulnerability Analysis	Issue 2.1	17 March 2004

7. IT PRODUCT TESTING

7.1 Developer Testing

IBM's approach to security testing for WebSphere MQ is security function based. A set of test suites was developed that corresponded to each security function. Each test suite targets the specific security behavior associated with that security function. The test procedures are designed to be exercised by running a script that has been designed to test the applicable security function described in the test scenarios.

Test depth is addressed by analyzing the functionalities addressed in the high-level design and associating test cases that cover the addressed functionalities. The high-level design addressed the general functions of the TOE components. Each security function maps to the appropriate test suite, and the test rationale demonstrates why the test suites provide adequate test coverage of a given security function.

The vendor provided the evaluation team with the expected and actual results for all the operating system platforms identified in section 8 of this document.

7.2Evaluator Testing

The evaluation team applied each EAL2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a complete test of the vendor's automated test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The following hardware is used to create the test configurations:

AIX:

- *Any IBM machine that supports AIX V5.2 Power 32 bit only operating system.*
- *Typical storage requirements are as follows:*
  - *Server installation: 50 MB*
  - *Data storage: 50 MB*

Microsoft Windows:

- *Any IBM PC machine (or compatible), based on a 32–bit Intel processor, that is year 2000 compliant and that is certified as Windows 2000 compatible.*
- *Typical storage requirements are as follows:*
  - *Minimum of 85 megabytes (MB) of disk space for Server installation and data*
  - *Minimum of 30 MB for working space.*
- *A suitable monitor for the operating system with a screen size of at least 800×600).*

Solaris:

- *Sun SPARC or Sun UltraSPARC.*
- *Typical storage requirements are as follows:*
  - *Server installation: 50 MB*
  - *Data storage: 50 MB*

Software: The following software is required for the test configuration:

Operating Systems:

- *Microsoft Windows 2000 (With Service Pack 2)*
- *Sun Solaris 8 (The patches listed for Sun Solaris 7, plus the following patches or equivalent superseding levels, 108827–12, 111177–06*
- *AIX V5.2*

Supporting Software:

- *Windows platforms: Microsoft Visual C++ 6.0 or later;*
- *Sun Solaris platforms: Sun Forte Developer 6 update 2 or later;*
- *AIX platforms: IBM VisualAge C/C++ professional V6 or later*
- *make (obtained from GNU website: www.gnu.org)*
- *Perl Interperter Pearl 5.6.1 or later (ActivePearl from www.activestate.com)*
- *Pearl Packages: FreezeTjaw-0.43 for all platforms; WinSecurity and Win32-API for Windows platforms only*

Regression Test Suite Source Code

WebSphere MQ 5.3.0.2 with CSD 6

8. EVALUATED CONFIGURATION

The evaluated configuration consists of the IBM WebSphere MQ 5.3.0.2 with Corrective Service Diskette (CSD) 6, which includes the MQ server and MQ client and Message Queue Interface (MQI) as the TOE components. MQ is supported on the following operating system platforms, however the operating systems platforms are not considered part of the physical TOE boundary.

- IBM AIX 5.1 & 5.2;
- HP-UX 11i;
- SUSE Linux Enterprise Server 8 (for Linux Intel and Linux zSeries);
- RedHat Enterprise Linux AS 2.1 (for Linux Intel);
- Sun Solaris 8 & 9;
- Microsoft Windows 2000 (this includes all combinations of Advanced Server, Sever, Professional, Service Packs and hotfixes);
- Microsoft Windows 2003 (this includes all combinations of Standard Enterprise, Service Packs and hotfixes)

The evaluation team determined the product to be **CC Part 2 conformant, CC Part 3 conformant,** and to meet the requirements of **EAL 2**. This implies that the product satisfies the security technical requirements specified in *WebSphere MQ EAL2 Security Target, dated 4 May 2004.*

9. VALIDATOR COMMENTS

The Validation Team would like to note that for the purpose of this CC evaluation, the Target of Evaluation (TOE) is considered to be a software-only TOE and is a subset of the actual product. The product in general is comprised of many parts. The TOE defines the server portion of the product and does not make any references to the MQ Client or MQI components that are available for this product. The product also has an administrator GUI interface feature that was considered outside the bounds of this evaluation. The TOE, as defined for this evaluation supports the user command line interface. Also the TOE does not support any claims or references to integrated Java Messaging Support (JMS). Also, the TOE does not support any claims for security cryptographic operations, such as Secure Sockets Layer (SSL) for secure communications between supported platforms. Also, the user should be aware that the evaluation team did not perform independent tests for SUSE Linux Enterprise Server 8 (for Linux Intel and Linux zSeries) or RedHat Enterprise Linux AS 2.1 (for Linux Intel) platforms. The evaluation team reviewed the expected and actual test results provided by the developer.

10. SECURITY TARGET

The ST, *IBM WebSphere MQ EAL2 version 2.8 dated 4 May 2004* is included here by reference.

11. GLOSSARY

ACL	Access Control List

Administrator	A user with membership to the MQM administrator group within the operating system.
Authorised User	A user who may, in accordance with the TSP, perform an operation.
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
Channel	Channels are objects that provide a communication path from one queue manager to another.
CSD	Corrective Service Diskette. This is a fix pack, which contains a collection of fixes and is cumulative e.g. all fixes within CSD5 are contained within CSD6.
DAP	Data Abstraction and Persistence
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIFO	First In First Out
IT	Information Technology
ITSEC	IT Security Evaluation Criteria
MCA	Message Channel Agent. A program that transmits prepared messages from a transmission queue to a communication link, or from a communication link to a destination queue.
Message	A message is a string of bytes that is meaningful to the applications that use it. Messages are used to transfer information from one application program to another (or between different parts of the same application).
MQ	Message Queue
MQI	Message Queue Interface
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency

OAM	Object Authority Manager
Object	Objects are queues, process definitions and namelists
OS	Operating System
OSP	Organisational Security Policy
PP	Protection Profile
Queue	A queue is a data structure used to store messages. Each queue is owned by a queue manager.
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.
SF	Security Function. A part or parts of the TOE that have been relied upon for enforcing a closely related subset of rules from the TSP.
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TACACS+	Terminal Access Controller Access Control System Plus
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy. A set of rules that regulate how assets are managed, protected and distributed within the TOE.

12. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Evaluation Technical Report for IBM WebSphere MQ 5.3.0.2 with Corrective Service Diskette (CSD) 6 Part 2.

[8] WebSphere EAL2 Security Target, Issue 2.8, 4 May 2004.

[9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

13. NATIONAL AND INTERNATIONAL INTERPRETATIONS

The evaluation team performed an analysis of the international interpretations and identified those that are applicable and had impact to the TOE evaluation. The table summarized the set of interpretations determined to have an impact on the evaluation and identifies the impact.

Impact on Security Target Requirement	Impact on ETR Work Unit	Interpretation ID
New element added after ACM.CAP.4.3C		RI #003
ACM_SCP.2.1D and ACM_SCP.2.1C changed		RI #004
	ASE_DES.1.1C changed (no work unit change indicated)	RI #038
	ASE_OBJ.1.2C and ASE_OBJ.1.3C changed (no work unit change indicated)	RI #043
ADO_IGS.1.1C and AVA_VLA changed		RI #051
FMT_SMF, family		RI #065

Impact on Security Target Requirement	Impact on ETR Work Unit	Interpretation ID
addition to CC Part 2		
	ASE_REQ.1-20 work unit changed	RI #084
	ASE_REQ.1.10C (ASE_REQ.1-16 work unit changed)	RI #085
FDP_ACF.1 modified		RI #103