National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

IBM UK Ltd

IBM WebSphere Business Integration Message Broker Version 5.0, Fix Pack 4

Report Number: CCEVS-VR-05-0087
Dated: 15 December 2005
Version: 0.2

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 1
1.1 Interpretations 2
1.2 Threats to Security 2
2 Identification 3
3 Security Policy 4
4 Assumptions 5
5 Architectural Information 5
6 Documentation 7
7 IT Product Testing 8
7.1 Developer Testing 8
7.2 Evaluation Team Independent Testing 8
7.3 Evaluation Team Penetration Testing 9
8 Evaluated Configuration 9
9 Results of the Evaluation 10
10 Validator Comments/Recommendations. 11
11 Annexes 12
12 Security Target 12
13 Glossary 12
14 Bibliography 12

1 Executive Summary

The evaluation of IBM WebSphere Business Integration (WBI) Message Broker was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 15 December 2005. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

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 2.1). The TOE, which is the WBI Message Broker, enables information, packaged as messages, to flow between different business applications, ranging from large legacy systems through to unmanned devices such as sensors on pipelines.

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 five components that make up the WBI Message Broker provided by IBM. These components are the Message Broker Toolkit, the Broker itself, the Configuration Manager, the User Name Server, and the Applications or Clients. The TOE also requires that a database that uses the ODBC protocol and IBM WebSphere Message Queue (MQ) be available in the IT environment. 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 Business Integration Message Broker 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 3 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 2.1, August 1999, which incorporated all applicable interpretations at the time the evaluation started in July 2004.

1.2 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

- An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
- The sender or receiver of a message denies sending or receiving the message to avoid accountability for subsequent action or inaction
- Data transferred between workstations is disclosed to or modified by unidentified users or processes monitoring network traffic.
- A non-privileged user may gain administrative privileges and bypasses the security policy.
- A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted) by changing access to the configuration data.
- A user may gain unauthorized access (view, modify, delete) to user data by bypassing access controls.
- Failure of the IT system to detect and record unauthorized actions may occur.

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 Business Integration Message Broker, Version 5.0 Fix Pack 4
Protection Profile	Not applicable.
ST:	IBM WebSphere Business Integration Message Broker Security Target, Version 1.0, 21 November 2005
Evaluation Technical Report	*Evaluation Technical Report for IBM WebSphere Business Integration Message Broker,* Version 2.0, November 21, 2005
CC Version	Common Criteria for Information Technology Security

Item	Identifier
	Evaluation, Version 2.1, August 1999
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	Vicky Ashby, The MITRE Corporation

3 Security Policy

The TOE logically supports the following security functions at its interfaces: Security audit, Communication, Authentication, Access Control, Security Management, and Protection of the TSF. Each is discussed in more detail as follows:

Security Audit: WMB performs security auditing for all authentication attempts made to the TOE. Audit records are generated when audit events occur, including the responsible user, date, time, and other details. The audit data is recorded into the operating system for protection.

Communication: WMB provides the ability to verify the sender and receiver of messages. Support for the authenticity of the sender and/or receiver is proved through the use of SSL.

Authentication: WMB provides authentication services between client applications that use the WebSphere MQ Real-Time Transport and WebSphere MQ Message Broker Real-Time Input and Real-time Optimized Flow nodes. The WMB Message Broker identification and authentication services verify that a broker and a client application are who they claim they are, and can participate in a publish/subscribe session; where each participant uses an authentication protocol to prove to the other that they are who they say they are and are not an intruder impersonating a valid participant. The WMB supports the following three protocols: mutual challenge-response password authentication; asymmetric Secure Socket Layer (SSL); and symmetric SSL.

Access Control: WMB uses topic-based security to control which applications in the environments publish/subscribe system can access information on which topics. For each topic for restricted access, the principals (i.e., user IDs and groups of user IDs) can be specified where this information can be published to determine which principals can subscribe to a given topic. Principals can also be specified on persistent messages (i.e., stored messages). WMB also has an access policy to control who can create the topology

of the domain. Like the topic-based access policy, access decisions are based on groups IDs.

Security Management: WMB provides security management functionality for the management of the access control policies. Management is performed from the Broker Toolkit and the command line.

Protection of the TSF: WMB protects itself and ensures that its policies are enforced in a number of ways. First, WMB interacts with users through well-defined interfaces designed to ensure that the WMB security policies are always enforced. Next, WMB encrypts all communications between physically separate parts of the TOE to ensure that no data is disclosed or modified.

4 Assumptions

The following assumptions are identified in the Security Target:

- The Message Brokers Toolkit must be installed on the same platform as the Configuration Manager because the two components do not encrypt traffic when communicating via a network.
- Authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
- It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
- The IT Environment underlying the TOE is assumed to fulfill the requirements for the IT Environment described in this ST. It is also assumed that the IT Environment will provide a suitable operational environment for the TOE where the TOE will be able to properly execute and the dependencies that the TOE has upon the IT Environment are properly fulfilled.

5 Architectural Information

The TOE provides two ways to act on messages: message routing and message transformation. For message routing, the TOE supports the definition of message flows. These message flows consist of a series of steps used to process a message, as defined in the message flow nodes, and connections between the nodes that define the routes through message processing. For message transformation, the steps in a message flow include changes to the format or even content of a message as part of the message processing.

The TOE consists of five components as described below:

- The Message Brokers Toolkit, which is an integrated development environment and graphical user interface used for management.
- The Broker, which routes messages sent to it by applications using rules defined in message flows and message sets, and transforms the data into the structure required by the receiving application.
- The Configuration Manager, which acts as an intermediary between the Toolkit and the Broker domain at runtime. The Configuration Manager polices which Windows users are able to perform actions within the Broker domain.
- The User Name Server provides authentication of users and groups performing the publish/subscribe operations.
- The Applications are clients that send messages to the Broker using MQ queues and connections.

The following diagram illustrates the physical scope and boundaries of the TOE. The five components can be on different platforms. For more detail on the evaluated configuration, see Section 8.

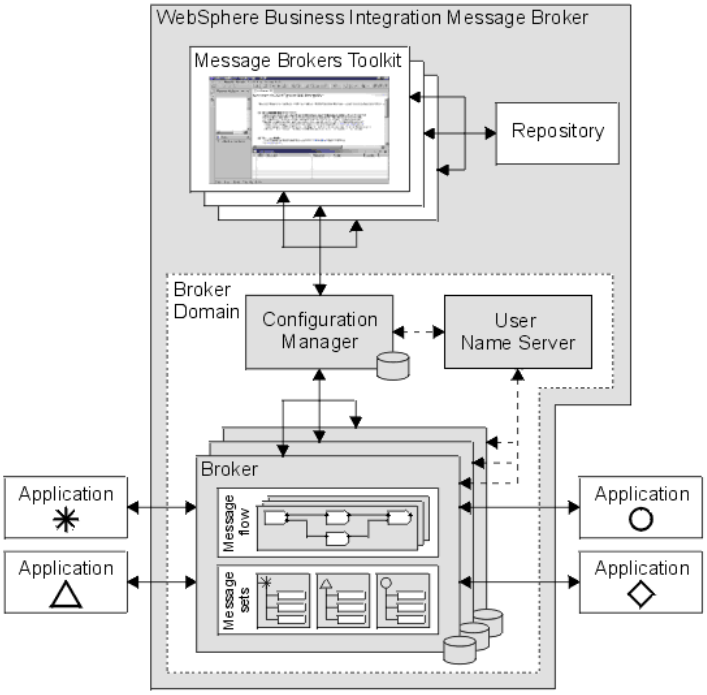

Figure 1 – WebSphere Message Broker

6 Documentation

Design Documentation

Document	Version	Date
WebSphere Message Broker v5.0 Fix Pack 4 EAL3 Functional Specification	Issue 1.4	16 November 2005
WebSphere Message Broker v5.0 Fix Pack 4 EAL3 High Level Design	Issue 1.4	16 November 2005

Guidance Documentation

Document	Version	Date
System Administration online help located at InfoCenter www.ibm.com (http://publib.boulder.ibm.com/infocenter/wbihelp/index.jsp) (This document includes installation procedures and User guidance)	Version 5 Release 0	May 2004
IBM WebSphere Business Integration Message Broker v5.0 with Fix Pack 4 CC Addendum	Version 2.2	22 November 2005

Configuration Management Documentation

Document	Version	Date
IBM WebSphere Business Integration Message Broker V5.0 Configuration Management	Issue 1.3	21 November 2005
WBIMB5.0files221105.txt (supplemental text file that identifies the configuration items under CM)		22 November 2005

Delivery and Operation Documentation

Document	Version	Date
IBM WebSphere Business Integration Message Broker v5.0 Delivery, Operation and Guidance	Issue 1.0	21 October 2004
DSW Secure Media Delivery (SMD),	1.2	10 January 2005
Installation documents located at http://publib.boulder.ibm.com/infocenter/wbihelp/index.jsp	Version 5 Release 0	May 2004

Test Documentation

Document	Version	Date

Document	Version	Date
WebSphere Message Broker v5.0 Fix Pack 4 EAL3 Developer Testing	Issue 1.7	15 November 2005
Actual Test results for all supported platforms	N/A	

Vulnerability Assessment Documentation

Document	Version	Date
Vulnerability Analysis for WebSphere Message Broker v5.0 with Fix Pack 4	1.2	27 September 2005

Security Target

Document	Version	Date
IBM WebSphere Business Integration Message Broker Security Target	1.0	21 November 2005

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.

The evaluation team examined the vendor's actual test results for the TOE configuration on all supported platforms.

7.2 Evaluation Team Independent Testing

The vendor provided three TOE configurations at a local site for installation and testing. The Evaluation Team installed the TOEs 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. SAIC and the developer consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a description of the vendor's test configurations in the ETR, Part 2.

The Evaluation Team chose to run all of the tests that the developer performed for the three of the supported platforms; AIX, Solaris, and Windows. This ensured that the Evaluation Team adequately addressed all security functions.

The vendor provided a complete set of expected and actual test results for analysis. The Evaluation Team determined that the evaluation team's actual test results matched the vendor's expected and actual results.

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. The independent team tests were run on all of the TOE configurations. Most were run as manual tests, but for others, scripts were developed to automate the tests.

Some issues were noted during the set up and testing. Updates to the vendor documentation have corrected the cause of these issues. In addition, use of a sniffer during the rerun of the vendor tests showed that, for one TOE configuration, encryption did not work as expected. A retest period was scheduled after documentation and ST updates were made. The retest period resulted in a clarified description of encryption being included in the ST. A selection of vendor tests was rerun on the three of the supported platforms; Linux, Solaris, and Windows. The retest period showed that updates to the Access Control section of the ST were needed, and these updates have been made.

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 Evaluation Team's ETR, Part 2, 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. The following platforms are included in the evaluated configuration:

For the Broker, User Name Server, and Application:

- Windows 2000 (this includes all combinations of Advanced Server and Server with recommended Service Pack and hotfixes),
- Windows Server 2003 (this includes all combinations of Standard and Enterprise with recommended Service Pack and hotfixes),

- AIX Version 5.1 (maintenance level 3) or AIX Version 5.2 (maintenance level 2),
- HP-UX, V11.11 (December 2002 Quality Pack),
- Sun Solaris 2.8 (with the SunSolve recommended patch level),
- Red Hat Enterprise Linux AS 3.0 (for Linux Intel),
- SuSE Linux Enterprise Server (SLES) 8 (for Linux Intel).

The Message Broker Toolkit must be installed on the same platform as the Configuration Manager in the evaluated configuration since communication between the two is not encrypted. The Configuration Manager is supported on Windows 2000 only.

The TOE also requires that the following be available in the IT environment:

- any database that uses the ODBC protocol on another platform, and
- IBM WebSphere MQ

9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.1 and the Common Evaluation Methodology (CEM) Version 1.0 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 3 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 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

"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 entire set of the vendor's test suites, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST."

The rationale supporting each CEM work unit verdict is recorded in the *Evaluation Technical Report for IBM WebSphere Business Integration Message Broker Version 5.0, Fix Pack 4, Part 2,* which is considered proprietary.

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

"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 Business Integration Message Broker Configuration, Administration, and Security document,*

The IBM WebSphere Business Integration Message Broker TOE (see product identification below) satisfies the *IBM WebSphere Business Integration Message Broker Security Target*, Version 1.0, dated 21 November 2005."

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.

All users of the TOE are administrative users. There are no general or unprivileged users. The Authentication Server authenticates client processes, not users.

Communications between components of the TOE that reside on separate platforms is protected by SSL. This protection can be provided by either the TOE itself, or by the IBM WebSphere MQ product, as determined by the message flow connection definition. When the message flow connection calls for real-time, the TOE provides its own SSL protection, using the IBM Java Secure Sockets Extension (JSSE) cryptographic library in the Broker directory. When the message flow connection calls for non-real-time, then the IBM WebSphere MQ transport capability is used to provide the connection and the SSL protection for that connection.

In addition to the message flow connection definition, when a Topic Access Policy (that is, to control access between users and topics for subscription or publishing) is being enforced, the Quality of Protection permission must be set to "Encrypted" for the evaluated configuration to ensure that these communications are encrypted.

Both real-time and non-real-time modes are included in the evaluated configuration, and IBM WebSphere MQ is required in the IT environment for the evaluated configuration. Authentication, a security function provided by the TOE as described in section 3 above, is supported by the TOE for message flow connections using real-time.

The evaluation team provided extensive independent test procedures to determine exactly how encryption was provided to protect communication between TOE components, and saw that this understanding was reflected in an updated ST.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *IBM WebSphere Business Integration Message Broker Security Target,* Version 1.0, dated 21 November 2005. 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 3 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 Business Integration (WBI) Message Broker 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*, Version 2.1, August 1999, Parts 1, 2, and 3.
- 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.
- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 97/01/11, CEM-97/017.
- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999, CEM-99/045.

- *IBM WebSphere Business Integration Message Broker Security Target,* Version 1.0, 21 November 2005.
- *Evaluation Technical Report for IBM WebSphere Business Integration Message Broker Version 5.0*, *Fix Pack 4, Part 1* (Non-Proprietary), Version 4.0, 13 December 2005.