

# National Information Assurance Partnership



## Common Criteria Evaluation and Validation Scheme Validation Report

### BEA WebLogic Integration V8.1 SP6

**Report Number:** CCEVS-VR-VID10029-2007  
**Dated:** 19 October 2007  
**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

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

**ACKNOWLEDGEMENTS**

**Validation Team**

**Franklin Haskell  
The MITRE Corporation  
Bedford, Massachusetts**

**Dr. Jerome F. Meyers  
The Aerospace Corporation  
Columbia, Maryland**

**Common Criteria Testing Laboratory**

**SAIC  
Columbia, Maryland**

## Table of Contents

1	Executive Summary .....	1
1.1	Evaluation Details .....	2
1.2	Interpretations .....	3
1.3	Threats to Security .....	3
2	Identification .....	4
3	Security Policy .....	4
3.1	Access Control .....	4
3.2	Identification and Authentication .....	4
3.3	Auditing .....	4
3.4	Security Management .....	5
4	Assumptions.....	5
4.1	Physical Assumptions .....	5
4.2	Personnel Assumptions .....	5
4.3	Operational Assumptions.....	5
4.4	Clarification of Scope .....	5
5	Architectural Information .....	6
6	Documentation.....	7
7	Product Testing .....	8
7.1	Developer Testing.....	8
7.2	Evaluation Team Independent Testing .....	9
7.3	Penetration Testing .....	11
8	Evaluated Configuration .....	11
9	Results of the Evaluation .....	11
10	Validator Comments/Recommendations .....	11
11	Annexes.....	12
12	Security Target.....	12
13	Glossary .....	12
14	Bibliography .....	12

## List of Tables

Table 1 – Evaluation Details.....	2
Table 2 – Threats .....	3
Table 3 – Physical Assumptions .....	5
Table 4 – Personnel Assumptions.....	5
Table 5 – Operational Assumptions.....	5

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

## 1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of BEA WebLogic Integration V8.1 SP6 with BEA07-169.00 security advisory patch. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process. The criteria against which the WebLogic Integration V8.1 SP6 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.2 and International Interpretations effective on 3 September, 2004. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2. A validator on behalf of the CCEVS Validation Body monitored the evaluation carried out by SAIC. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. The evaluation was completed in September 2007.

The SAIC evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 2 augmented with ALC\_FLR.1 family of assurance requirements.

BEA WebLogic Integration V8.1 SP6 with BEA07-169.00 security advisory patch is an application server that provides a foundation for an enterprise to build and integrate applications and databases. The TOE consists of the following subsystems that are used in combination to support an end-user developed application: WebLogic Server and WebLogic Integration.

The TOE is supported on the following Java 2 environments: BEA JRockit 1.4.2\_10 SDK; and Sun Java 2 SDK 1.4.2\_11 with Java HotSpot™ Client VM. The TOE is dependent on the correct operation of the Java 2 environment and on its underlying operating system, neither of which are included within the scope of the evaluation. It should also be noted that the access control policy implemented by the TOE is enforced only on access attempts made through the TOE's interfaces. The TOE does not and cannot control attempts to access data directly (e.g., via the underlying operating system).

The product, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the BEA WebLogic Integration 8.1 Security Target.

The validation team monitored the activities of the evaluation team, examined evaluation testing procedures, 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 ETR are consistent with the evidence produced.

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

**1.1 Evaluation Details**

**Table 1 – Evaluation Details**

<b>Evaluated Product:</b>	BEA WebLogic Integration V8.1 SP6 with BEA07-169.00 security advisory patch
<b>Sponsor:</b>	BEA Systems, Inc 2315 North First Street San Jose, CA 95131
<b>Developer:</b>	BEA Systems, Inc 2315 North First Street San Jose, CA 95131
<b>CCTL:</b>	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
<b>Kickoff Date:</b>	September 3 2004
<b>Completion Date:</b>	September 11 2007
<b>CC:</b>	Common Criteria for Information Technology Security Evaluation, Version 2.2
<b>Interpretations:</b>	RI-137
<b>CEM:</b>	Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and General Model, Version 0.6, January 1997; Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 2.2, August 1999.
<b>Evaluation Class:</b>	EAL 2
<b>Description:</b>	BEA WebLogic Integration V8.1 SP6 with BEA07-169.00 security advisory patch comprises an application server that provides a foundation for an enterprise to build and integrate applications and databases. The TOE consists of the following subsystems that are used in combination to support an end-user developed application: WebLogic Server and WebLogic Integration.
<b>Disclaimer:</b>	The information contained in this Validation Report is not an endorsement of the BEA WebLogic Integration V8.1 SP6 product by any agency of the U.S. Government and no warranty of the WebLogic Integration product is either expressed or implied.
<b>PP:</b>	None

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

**Evaluation Personnel:** Science Applications International Corporation:  
 Anthony J. Apted  
 Keith W. Beatty  
 Terrie L. Diaz  
 Katie Sykes

**Validation Team:** Franklin Haskell  
 The MITRE Corporation  
 202 Burlington Road  
 Bedford, MA 01730-1420

**1.2 Interpretations**

Interpretation ID	Impact on CC Requirements	Impact on CEM Work Units	Comment
RI-137	FIA_USB.1 changed	None	Applied

**1.3 Threats to Security**

The following are the threats that the evaluated product addresses:

**Table 2 – Threats**

Threat Identifier	Threat Description
T.BYPASS	An attacker may be able to bypass TOE protection mechanisms through unprotected interfaces in order to inappropriately access protected data and services.
T.EXCESS_AUTHORITY	An unauthorized user may be able to exercise administrator authorities to inappropriately manage the TOE.
T.NO_TIME	Those responsible for the TOE may not be able to determine the sequence of audited security relevant events.
T.NOCRYPTO	An attacker may be able to observe authentication data transmitted in the clear due to cryptographic services not being available.
T.STORAGE	An attacker may be able to cause the loss or destruction of Audit and other TSF data.
T.TAMPER	An attacker may be able to inappropriately modify or otherwise tamper with TSF programs and data.
T.TSF_COMPROMISE	A user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.UNACCOUNTABLE	Users of the TOE may not be held accountable for their security-relevant actions.

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

Threat Identifier	Threat Description
T.UNAUTHORIZED_ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policies.
T.UNDETECTED_ACTIONS	The administrator may not have the ability to detect potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
T.UNIDENTIFIED_USERS	An attacker may gain access to the TOE without being reliably identified allowing them to gain unauthorized access to data or TOE resources.

## 2 Identification

The evaluated product is **BEA WebLogic Integration V8.1 SP6 with BEA07-169.00 security advisory patch.**

## 3 Security Policy

WebLogic Integration V8.1 SP6 enforces the following security policies as described in the Security Target.

*Note: Much of the description of the WebLogic Integration V8.1 SP6 security policy has been extracted and reworked from the BEA WebLogic Integration Security Target and Final ETR.*

### 3.1 Access Control

Policies are created by administrators but use attributes maintained by the product: username, group membership, role, resource type, resource identity, and time of day. The resources to which access is permitted or denied include Java constructs (beans, APIs, jars, etc.), the administrative console, servers, and WebLogic Integration objects.

### 3.2 Identification and Authentication

The TOE supports multiple identification and authentication mechanisms: username and password; token-based (using either X.509 certificates or CORBA Common Secure Interoperability version 2 (CSIv2) identity assertion); and credential mapping which provides a capability by which legacy applications use their own I&A mechanisms to authenticate to a WebLogic Server (WLS) resource.

### 3.3 Auditing

The TOE generates audit records of security relevant events as they occur within the security framework. They are stored by the underlying operating system and, hence, the TOE is dependent upon that OS for proper protection of the audit trail.



### 3.4 Security Management

The TOE supports a number of security management or administrative roles, although from the security evaluation perspective, they are all considered equivalent to an ‘administrator’, regardless of any apparent limitations. The TOE restricts the ability to manage the access control policy, user accounts and user security attributes, and the configuration of the TOE to the administrator.

## 4 Assumptions

### 4.1 Physical Assumptions

The following physical assumptions are identified in the Security Target:

**Table 3 – Physical Assumptions**

Assumption Identifier	Assumption Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the IT environment.

### 4.2 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

**Table 4 – Personnel Assumptions**

Assumption Identifier	Assumption Description
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.

### 4.3 Operational Assumptions

The following operational assumptions are identified in the Security Target:

**Table 5 – Operational Assumptions**

Assumption Identifier	Assumption Description
A.NO_UNTRUSTED	There are no untrusted user accounts or malicious software on the server platform.

### 4.4 Clarification of Scope

The product being evaluated and consequently the TOE is entirely software. It runs utilizing the functionality (identical) of one of two Java runtime systems which, in turn run on a variety of operating systems. This makes the TOE entirely dependent upon the correct operation of the Java systems as well as the operating system, neither of which are included in the scope of the evaluation. The access policy features implemented by the TOE are enforced only on access attempts generated by supported API's connected through the TOE. The TOE does not and

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

cannot control access to data from other applications. Administrators are advised not to authorize access to TOE data to other applications running on the server. If other applications must share TOE data sources, then the applications should be “trusted applications” only.

Note that certain resources allow access based upon the operation being requested. This capability is not mentioned in the ST nor was any comprehensive testing of it performed; therefore no statements can be made regarding it in this Validation Report.

The adjudication provider is a mandatory security provider that provides functionality for dealing with multiple authorization providers. However, since the evaluated configuration includes only a single authorization provider, the adjudication provider’s security functionality, while evaluated, is not fully utilized in the evaluated configuration.

## **5 Architectural Information**

The TOE comprises two distinct subsystems: WebLogic Server (WLS) and WebLogic Integration (WLI). The figure below shows a ‘Security Service’ which includes the basic ‘Security Framework’ of WLS and a series of security service provider ‘modules’ (note that the security provider modules in the figure are only examples). The Security Service and the associated modules, identified in section 2.2.2 of the WebLogic Integration Security Target, form the core of the TOE, while the other entities in the figure depicted above the Security Service are examples of applications supported by the TOE. The WLI subsystem is a ‘BEA Layered Product’ and represents the remainder of the TOE.

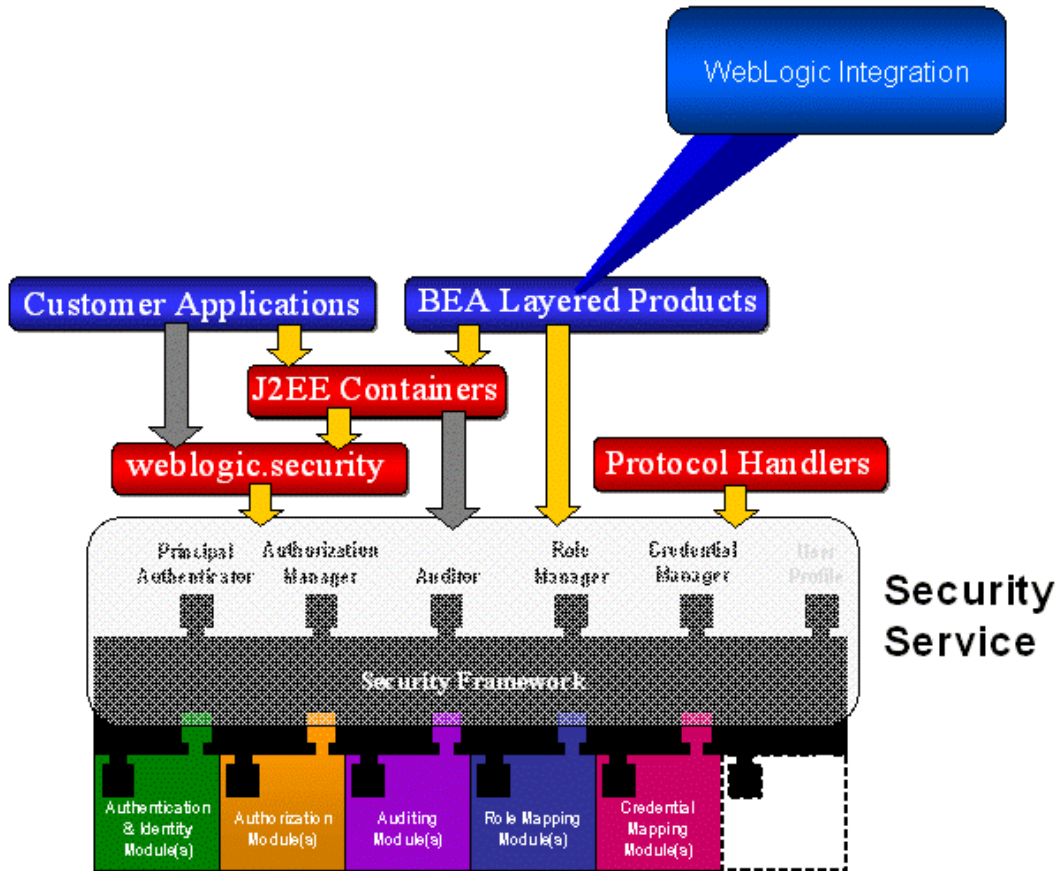
The following security providers are included in the evaluated configuration: WebLogic Auditing Provider; WebLogic Authorization Provider; WebLogic Role Mapping Provider; WebLogic Adjudication Provider; WebLogic Authentication Provider; WebLogic Identity Assertion Provider; and WebLogic Credential Mapping Provider.

In addition to the underlying Java 2 environments and their supporting operating systems, the TOE also relies on the availability of a relational database management system (RDBMS) to store and protect management data associated with trading partners.

Generally, user requests will come in from the network and will be handled by the security framework provided by WLS. If the user is attempting to access an application associated with the WLI subsystem, it will be invoked in addition to the WLS security framework and hence serves to extend or add security features relative to resources within its control.

Customer applications are acquired and installed by WLI administrators so that the appropriate controls are configured and subsequently enforced before the applications can be accessed.

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6



## 6 Documentation

BEA provides an extensive set of documentation describing the installation, configuration, management and operation of the TOE. This set comprises documentation for the WebLogic Server product (which is also part of the WebLogic Integration TOE) and for WebLogic Integration itself. The WebLogic Server documentation is available at the following URL: <http://edocs.bea.com/wls/docs81/index.html>, while the WebLogic Integration documentation is available at <http://edocs.bea.com/wli/docs81/index.html>. Additionally, the installation guide for WebLogic Platform, which also covers BEA WebLogic Integration V8.1 SP6, is available at <http://edocs.bea.com/platform/docs81/install/index.html>.

The guidance documentation examined during the course of the evaluation and therefore included in the TOE is as follows:

### Installation Guidance

- Installing BEA WebLogic Platform.

### WebLogic Server Guidance

- Administration Console Online Help
- Configuring and Managing WebLogic Server 8.1, 23 Sep 2005
- Developing Web Applications for WebLogic Server 8.1, 26 Sep 2005

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

- Introduction to WebLogic Security 8.1, Aug 2005
- Managing WebLogic Security 8.1, 9 Dec 2004
- Programming WebLogic Enterprise JavaBeans 8.1, 28 April 2006
- Programming WebLogic jCOM 8.1, 07 April 2006
- Programming WebLogic Security 8.1, Aug 2005
- Programming WebLogic Server J2EE Connectors 8.1, 1 Jul 2003
- Programming WebLogic Web Services 8.1, 25 Jun 2004
- Securing a Production Environment 8.1, 21 Jun 2004
- Securing WebLogic Resources 8.1, 13 Feb 2006
- WebLogic Server Command Reference 8.1, 15 Mar 2004.

### **WebLogic Integration Guidance**

- Managing WebLogic Integration Solutions, 8.1, Oct 2005
- Deploying WebLogic Integration Solutions, 8.1 Oct 2005
- Introducing Application Integration, 8.1, Oct 2005
- Introducing Trading Partner Integration, 8.1, Oct 2005
- Using the Application Integration Design Console, 8.1, Oct 2005
- Using Integration Controls, 8.1, Jan 2005.

## **7 Product Testing**

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for BEA WebLogic Integration 8.1 SP6, Version 1.0, 11 September 2007.

### **7.1 Developer Testing**

BEA's approach to testing for WebLogic Integration is based on TSF interface testing. BEA developed a test suite comprising various automated tests to exercise the TSF at the interfaces described in the WebLogic Integration Functional Specification.

The vendor ran the automated test suite in various configurations, consistent with the test environment described in the Testing Documentation, and provided the evaluation team with the actual results. The test configurations were representative of both the operating systems supported and the application environment (JVM). All tests passed.

In addition, the evaluation team examined the results of testing the adjudication provider, whose function could not be fully tested without taking the TOE outside the evaluated configuration. Testing this functionality required the use of multiple authorization providers. Since the TOE only includes one authorization provider, the use of additional ones took the TOE outside of the evaluated configuration. The evaluators confirmed that those test results were in accordance with the behavior specified for the adjudication provider in the Security Target.

While performing the ATE\_FUN work units, the evaluation team examined in detail a sample (amounting to slightly over 20%) of the vendor test cases and determined that all actual results matched the expected results. These results provided sufficient confidence that the entire test suite results match as well.

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

## 7.2 Evaluation Team Independent Testing

The evaluation team used two test configurations: one for repeating the vendor tests; and a separate configuration for evaluation team functional and vulnerability testing.

The test configuration for repeating the vendor tests comprised a vendor-supplied laptop computer equipped as follows:

- Dell Latitude Laptop with:
  - Pentium 4 – M CPU 2.20 GHz
  - 1GB RAM
  - 37 GB Disk, with 15 GB free
  - Microsoft Windows XP Professional Version 2002 Service Pack 2
- BEA WebLogic Integration 8.1 SP6 with BEA07-169.00 security advisory patch (the TOE)
- BEA JRockit 1.4.2\_10 SDK
- MKS Toolkit – provides a Unix shell on Windows
- Perl – a perl script is used to help setup the environmental variables that the test system uses in order to run
- Apache Ant build tool – the test harness is driven by an Ant task
- JUnit Test Framework – a regression testing framework used to execute unit tests implemented in Java
- Coconut Test Framework – a regression testing framework used to execute unit tests implemented in Java
- Oracle 91R2 with Oracle 10g XA driver.

The configuration used for evaluation team tests comprised:

- Dell Dimension 370 workstation with Intel Pentium 4 3.4GHz processor, 1GB RAM and 150GB hard disk
- Windows Server 2003 (Enterprise Edition) Version 5.2 SP1
- BEA WebLogic Integration 8.1 SP6 with BEA07-169.00 security advisory patch (the TOE)
- BEA JRockit 1.4.2\_10 SDK
- Microsoft SQL Server 2000.

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The Product Environment described above was used with team generated test procedures and team analysis to determine the expected results. All actual results matched the expected results.

The evaluation team performed the following additional functional tests:

- Generation of specified audit records: The vendor's Testing Documentation identifies the audit records generated by the various tests and the tests that contribute to the generation

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

of audit records. The Testing Documentation identifies the following audit event that is specified in the ST but not specifically generated by the vendor's tests: USERLOCKOUTEXPIRED. The team tests showed the TSF generates all audit records specified in the ST.

- Security management auditing: During the Final Validation Oversight Review for the TOE, the validators queried if any security management actions are audited, even though no claims for such auditing are made in the ST. The evaluation team examined the "Configuration Auditing" capability of the TOE, which is described in the functional specification evidence and the guidance documentation. Configuration Auditing provides for auditing of the security configuration of the TOE via auditing of actions on MBeans. The test demonstrated that the TSF generates Configuration Auditing events and information as described in the guidance documentation.
- Access to WLI resources: The ST identifies various resources that are provided by the WebLogic Integration component of the TOE and are subject to the WebLogic Server Access Control SFP, but are not clearly covered by the developer's testing. These resources are: Application Views; Trading Partner Profiles; Trading Partner Services. The test demonstrated that WebLogic Integration resources are protected according to the access control SFP.
- Minimum password length: The vendor's strength of function analysis is based partly on the assumption that passwords have a minimum length of 8 characters, but it was unclear if this is an absolute minimum, or if it is configurable. The test demonstrated that the minimum password length has a default value of eight, but that an administrator can modify the minimum password length to be less than eight. Guidance documentation warns the administrator that a minimum length of 8 characters is required in the evaluated configuration.
- Password alphabet: The vendor's strength of function analysis is based partly on the assumption that the available password alphabet comprises 94 characters. The test demonstrated that all 94 printable characters of the standard typewriter keyboard can be used in a password
- Default configuration: The vendor's strength of function analysis is based partly on the assumption that by default the TOE is configured with User Lockout enabled and configured to lock users out after 5 failed login attempts within 5 minutes for 30 minutes duration. The test demonstrated that the default configuration for the User Lockout mechanism is as specified in the documentation and that the mechanism operates as described
- Provided security management functions: The vendor's testing is at the programmatic interfaces to the TSFI. The vendor does not specify any tests at the administrator or user interface. It is not clear that the vendor tests adequately demonstrate the provision of security management functions specified in FMT\_SMF.1. The test demonstrated that the TSF provides all the security functions specified in FMT\_SMF.1
- Functional specification validation: The WebLogic Integration functional specification provides details of the various security management capabilities provided by the WebLogic Integration Administration Console, covering: User and Group Management; Role Management; Policy Management on Resources; Trading Partner Management; Password Store Management. Since the developer's testing is based on unit level tests at the underlying TSFIs, there is no evidence that the descriptions in the functional

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

specification for these capabilities are validated. The test demonstrated the WebLogic Integration Administration Console behaves as described in the functional specification.

### 7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product and found none not already known to and addressed by the developer through security advisories and patches. They also examined the vendor's vulnerability assessment and identified one vulnerability relevant to the evaluated version of the TOE in its evaluated configuration. This vulnerability is addressed by the BEA07-169.00 security advisory patch that is part of the TOE evaluated configuration.

## 8 Evaluated Configuration

The evaluated configuration is the Java 2 environment. The BEA JRockit 1.4.2\_10 SDK and Sun Java 2 SDK 1.4.2\_11 with Java HotSpot™ Client VM are specifically supported. As customer applications and dataset sizes vary tremendously no configuration guidelines can be given here. Potential customers are encouraged to seek very competent assistance to size their hardware.

## 9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.2 and CEM version 2.2. The evaluation determined the BEA TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements augmented with ALC\_FLR.1. The rationale supporting each CEM work unit verdict is recorded in the **Evaluation Technical Report for WebLogic Integration V8.1 SP6 Part 2** which is considered proprietary.

## 10 Validator Comments/Recommendations

BEA WebLogic Integration is a product with functionality intended to provide a foundation for an enterprise to build and integrate applications and databases. As such its implementation has to be robust.

The validation team believes that the claims made and successfully evaluated for the product represent a set of requirements that are a reasonable selection covering, to a certain depth, the functionality of the product. The product, while extensive in functionality, only runs at the application level. It relies upon the underlying operating system for several types of support: audit review and storage, cryptographic facilities, security management, time stamps, and separation of the product and its users. Also, the usual training and physical assumptions apply. Because of this product construction, purchasers should be very careful to follow the configuration guidance. Controlling access, both physical and network, is very important; as is the injunction not to allow anything other than the TOE and its required supporting environment to run on the server machine.

The adjudication provider is part of the TOE but its primary security functionality consists of adjudicating decisions from multiple authorization providers. Since the TOE only includes one authorization provider in the evaluated configuration, this functionality cannot be effectively used without taking the TOE outside of the evaluated configuration. Testing and analysis confirmed that this functionality worked as claimed. However, the use of multiple authorization providers

VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6

will require a supplemental assessment of the impact of the additional authorization providers on the TOE.

No claims are made for the network connections that must be in place between remote applications and the server or those between servers on different machines. It is up to the customer to put measures in place to appropriately secure these data paths.

## 11 Annexes

Not applicable.

## 12 Security Target

The security target for this product's evaluation is **BEA WebLogic Integration 8.1 Security Target**, Version 1.0, dated September 13, 2007.

## 13 Glossary

No definitions beyond those in the CC or CEM are supplied.

## 14 Bibliography

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

- [1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.2, January 2004, CCIMB-2004-01-001.
- [2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.2, January 2004, CCIMB-2004-01-002.
- [3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.2, January 2004, CCIMB-2004-01-003.
- [4] Common Methodology for Information Technology Security: Evaluation Methodology, Version 2.2, January 2004, CCIMB-2004-01-004.
- [5] Evaluation Technical Report for BEA WebLogic Integration V8.1 SP6 Part 1, Version 1.0, 11 September 2007.
- [6] Evaluation Technical Report for BEA WebLogic Integration V8.1 SP6 Part 2, Version 1.0, 11 September 2007.
- [7] Evaluation Team Test Report for BEA WebLogic Integration V8.1 SP6 ETR Part 2 Supplement, Version 1.0, 11 September 2007.
- [8] BEA WebLogic Integration 8.1 Security Target, Version 1.0, 13 September 2007.
- [9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.



VALIDATION REPORT  
BEA WebLogic Integration V8.1 SP6