National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902)

Report Number: CCEVS-VR-VID10266-2009
Dated: 4 May 2009
Version: 3.5

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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Scott Shorter, Lead Validator

Olin Sibert, Senior Validator

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary 4
2 Identification 5
3 Organizational Security Policy 6
3.1 Security audit 6
3.2 Identification and authentication 7
3.3 User data protection 7
3.4 Security management 8
3.5 Protection of the TSF 9
4 Assumptions and Clarification of Scope 9
5 Architectural Information 10
6 Documentation 12
6.1 Design documentation 12
6.2 Guidance documentation 12
6.3 Configuration Management documentation 13
6.4 Delivery and Operation documentation 13
6.5 Life Cycle Support documentation 14
6.6 Test documentation 14
6.7 Vulnerability Assessment documentation 14
6.8 Security Target 14
7 IT Product Testing 14
7.1 Developer Testing 14
7.2 Evaluation Team Independent Testing 15
7.3 Vulnerability Testing 16
8 Evaluated Configuration 16
9 Results of the Evaluation 22
9.1 Evaluation of the Security Target (ASE) 22
9.2 Evaluation of the Configuration Management Capabilities (ACM) 22
9.3 Evaluation of the Delivery and Operation Documents (ADO) 22
9.4 Evaluation of the Development (ADV) 23
9.5 Evaluation of the Guidance Documents (AGD) 23
9.6 Evaluation of the Life Cycle Support Activities (ALC) 23
9.7 Evaluation of the Test Documentation and the Test Activity (ATE) 23
9.8 Vulnerability Assessment Activity (AVA) 23
9.9 Summary of Evaluation Results 24
10 Validator Comments/Recommendations 24
11 Security Target 24
12 Glossary 24
13 Bibliography 26

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902).

The Validation Report presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902) was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 29 January 2009.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and meets the assurance requirements of EAL2 augmented with ALC_FLR.1. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902). The TOE, BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902) is a product suite for business process management (BPM), or creating, executing, and optimizing business processes. It enables collaboration, business, and information technology (IT) to automate and optimize business processes.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

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, 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 conduct security evaluations.

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; and
- 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:	BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902)
Protection Profile	Not applicable
ST	BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902) Security Target, Version 1.0, 31 March 2009
Evaluation Technical Report	Evaluation Technical Report For BEA AquaLogic BPM Suite Version 6.0 MP4 (Non-Proprietary), Version 2.0 31 March 2009, Part 2 (Proprietary), Version 3.0 30 March 2009

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Conformance Result	CC Part 2 conformant and Part 3 conformant, EAL2 augmented with ALC_FLR.1
Sponsor	Oracle, Inc
Developer	Oracle, Inc
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Evaluation Personnel	Science Applications International Corporation: Terrie Diaz, Dawn Campbell
Validation Body	NIAP CCEVS: Scott Shorter, Lead Validator Olin Sibert, Senior Validator

3 Organizational Security Policy

This section summarizes the security functions provided by BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902) that are evident at the various identified network interfaces. It is based on information provided in the Security Target.

3.1 Security audit

The Process Execution Engine can be configured to generate audit records of all, or a subset of, activities in a business process associated to a particular process instance. The records generated correspond to the following events:

- start-up and shutdown of the audit functions;
- process instance creation;
- manual assignment of an activity to a participant for execution;
- manual removal of a process instance from another participant;
- activity task start and end events;
- entering and exiting an activity;
- performance (execution of) an activity task by a participant;
- manual release of an activity previously assigned for execution by a participant; and
- the completion of a activity.

Audit records are generated on a per-process basis. The BEA AquaLogic BPM developer who designs a process can, for purposes of testing the process while it is being developed,

configure audit records to be generated for that process or what activities within the process should generate the events. Audit records may include messages from the Process Execution Engine.

An administrator can override the default auditing event level defined by the developer. When a process is published and deployed, there are options to: (a) accept the existing auditing rules specified in the business process design, (b) to avoid any event auditing, or (c) to force the auditing of all process activity events. Because only administrators can publish and deploy processes, the auditing options they select ultimately determine the audit-generation behavior of the TOE for that process instance.

In addition, the Process Execution Engine can log execution events in a log file. The events logged in that log file are assigned with a severity that is one of; Fatal, Severe, Warning, Info, and Debug (from greatest to least severe). A BEA AquaLogic BPM administrator can change the type of information being recorded in the log. These logs are not associated with the main audit generation function described above for the TOE; however, these logs can contain records related to the same security-relevant events that are recorded in the audit trail. These log files are not accessible to non-administrative users.

3.2 Identification and authentication

Users accessing the TOE as participants through the WorkSpace are authenticated via an instantiation of the FDI within that component. Users accessing the TOE as administrators are authenticated via an instantiation of the FDI implemented through the Process Administrator component. In other words, the TOE requires users to provide a unique user name and password prior to accessing services to the Process Administrator, Archive View, WorkSpace Administrator, and WorkSpace or any custom application using any of the available public APIs (PAPI or PAPI-WS) prior to users being granted logical access. Users in the developer role have access to the Studio component, which are hosted on a separate workstation. Authentication for these users is performed via the local operating system authentication mechanism. Developers typically do not interact with the TOE's runtime environment directly. In addition, the IT environment identifies and authenticates the administrators' access Log Viewer and Admin Center.

The Process Execution Engine maintains a session to represent an interaction with an end user. Session information includes session identification, participant identification, and the organizational unit and roles associated with the user. The same information is maintained on the API Client side.

User attributes are bound to TOE subjects after the user completes I&A and establishes a participant session. When the participant session is created, organizational units, process roles, permissions associated with each role, and a hierarchical category associated with each role are assigned to the subject. These attributes are static for the lifetime of the subject. Changes to user security attributes do not take effect until the user logs in again and creates a new participant session.

3.3 User data protection

BEA AquaLogic BPM constrains a participant's ability to:

- View an instance and its tasks
- Select an instance
- Execute a task associated with an instance
- Modify the instance variables through the implementation of an activity task using Studio
- Route an instance
- Abort an instance
- Suspend an instance
- Delegate an instance to another participant
- Peer-assign an instance to another participant
- Re-assign an instance from one participant to another participant
- Escalate an instance to another participant
- Create a new process instance

The constraints above describe the logical access control for the TOE in both configurations. The logical processing behaves exactly the same regardless of whether the TOE is in a standalone or applications server configuration. When in the applications server configuration, there are some internal communications and protection differences, because J2EE container mechanisms can be extended to the Process Execution Engine (e.g., security descriptors, Enterprise Java Bean communications, and transaction management). Analogous capabilities and protection is provided in the standalone configuration, but via different mechanisms. In addition, the processes of publishing and deploying a process instance are internally different. However, from an external perspective the security infrastructure and behavior are exactly the same for both configurations, by intent.

The constraints are based on attributes associated with the end user's session and the instance of an interactive activity. The detailed rules for implementing the constraints are specified in FDP_ACF.1.2. This section does not repeat these rules but rather provides additional implementation details. There are certain actions that are enabled at modeling time as part of the activity definition such as whether the instance is ABORTABLE, SUSPENDABLE or AUTOCOMPLETE (automatic routing to the next activity in the process) and are inherited. In addition, task markings (read-only, mandatory) are defined aspects of the task set at modeling time. These permissions are crosschecked with those associated with a person through Role assignment (ABORT, EXECUTE, ROUTE, SELECT, DELEGATE, REASSIGN, ESCALATE, and PEER ASSIGNMENT). The intersection of the subject and object permissions determines the ability to execute these actions.

3.4 Security management

The TOE provides two types of administrators: a system administrator, called simply an "administrator", and a more restricted type of administrator, called an "end user

administrator". A system administrator has access to the entire project, whereas an end user administrator has privileges limited to creating and modifying participants and monitoring processes". The TOE also supports Developer and the BPM participant roles. A BEA AquaLogic BPM administrator performs most of the typical administrative tasks (as described below). A BEA AquaLogic BPM developer (sometimes referred to as a business analyst and business architect) designs and implements business processes with the aid of the Studio component. Part of this design task is to assign abstract roles used for access control to the processes' activity instances, which are the top-level decomposition units of the business process.

3.5 Protection of the TSF

All changes to the Business Processes data and state of the system are centralized through the Process Execution Engine. The Engine authenticates the subject and validates authorization for every request to perform an operation. No user interface or API allows a user to do any of these operations without going to the Engine. The Engine maintains a session to represent an interaction with an end user. This includes interaction with the user through WorkSpace and for each web service application that performs web service operations. The Process Execution Engine prevents one session from interfering with other sessions. The session mechanism also helps ensure the security functions are invoked and succeed before the BEA AquaLogic BPM provides service to an end user.

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 deployed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed the TOE will be located within controlled facilities which will prevent unauthorized physical access and modification.
- It is assumed Authorized users of the TOE will keep all their authentication data private.
- It is assumed those responsible to manage the TOE are competent individuals that only authorized users can gain access to the TOE, and will follow and abide by the instructions provided by the TOE documentation.
- It is assumed that the operating systems have 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 systems protect the TOE from any unauthorized users or processes.

Following are the organizational security policies levied against the TOE and its environment as identified in the Security Target.

- Users of the system shall be held accountable for their security relevant actions within the system.

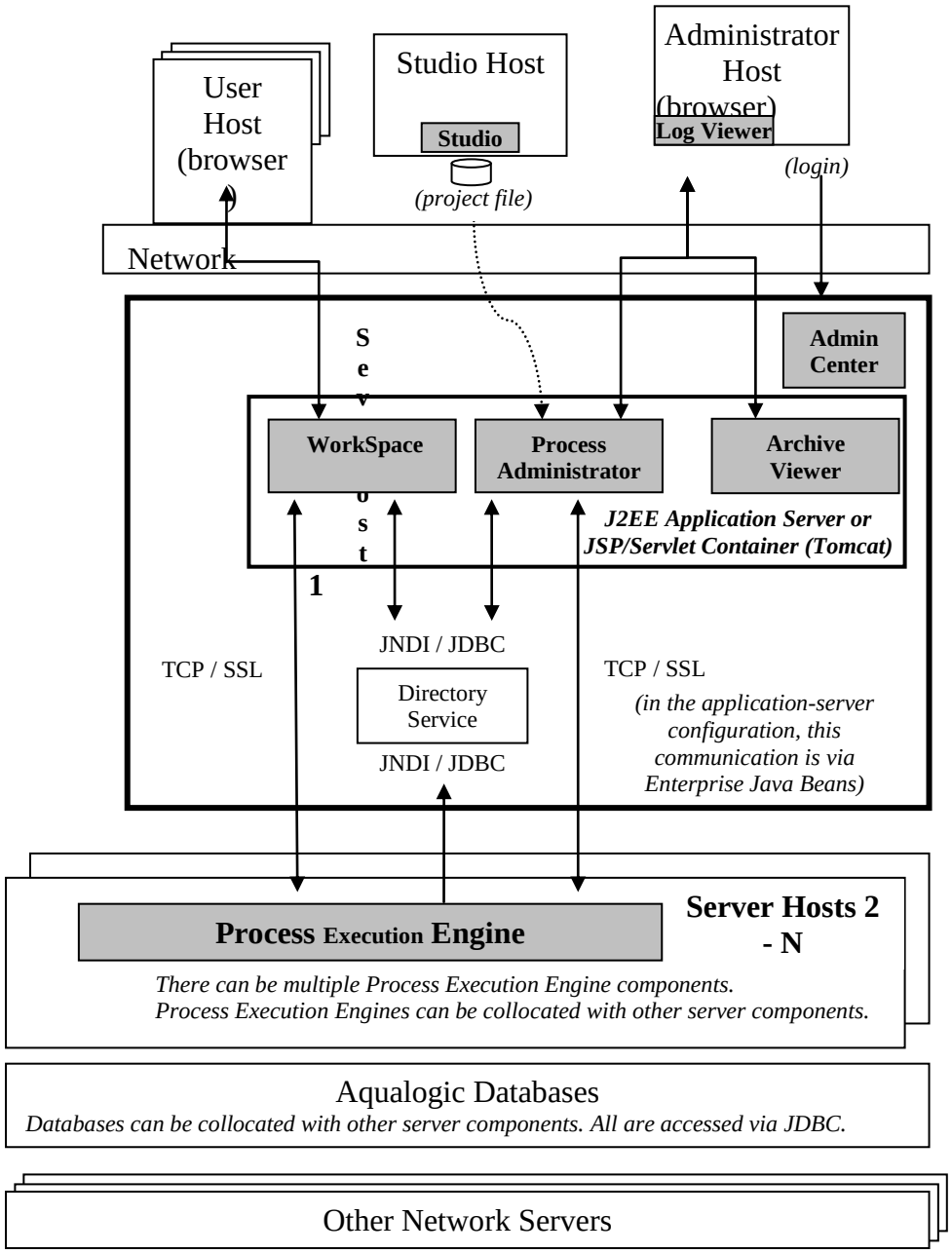
BEA AquaLogic BPM Suite is a product suite for business process management (BPM), or creating, executing, and optimizing business processes. It enables collaboration, business, and information technology (IT) to automate and optimize business processes. The TOE provides security functions that control user access to business process definitions and active instances of those processes. Users may be granted or denied access based on their organization affiliation, assigned group, assigned role, assigned groups, or identity, which is verified by the TOE. In addition, the TOE provides functions to securely manage BPM objects and process participants.

5 Architectural Information[1]

The components of BEA AquaLogic BPM Suite comprise: BEA AquaLogic BPM Studio (Studio), BEA AquaLogic BPM Process Execution Engine (Engine), BEA AquaLogic BPM WorkSpace (WorkSpace), BEA AquaLogic BPM Process Administrator (Process Administrator), BEA AquaLogic BPM Log Viewer (Log Viewer), BEA AquaLogic BPM Archive Viewer (Archive Viewer), BEA AquaLogic BPM Admin Center (Admin Center), BEA AquaLogic Process Application Programming Interface for Web Services (PAPI-WS).

There are two configurations of the Process Execution Engine TOE component in the evaluated configuration – a stand-alone configuration and an application-server configuration. The figure below shows a high-level view of the TOE components as they are distributed in the physical environment. Note that this view shows the TOE components in only the "standalone" configuration in its other configuration (the "application server" configuration) the Process Execution Engine component is implemented as a Java Enterprise application and is hosted by the same J2EE application server that presents the Workspace, WorkSpace Administrator, Process Administrator, and Archive Viewer components. In the standalone configuration, the Process Execution Engine is implemented as a standalone Java application. In either configuration, the Directory Service can be hosted remotely, in which case communications are protected by SSL[2].

[1] Extracted from SAIC Final ETR Part 1 Version 2.0, 18 November 2008
[2] If configured to use HTTPS, the IT environment is relied upon to provide the certificates for secure SSL communications.



In the stand-alone configuration, the Process Execution Engine component can reside on a separate server host from the auxiliary application server, or they can reside on the same server host. In either case, the Process Execution Engine is a separate Java application that is directly accessible as a service. The application server in the stand-alone configuration provides the service interfaces for access to other TOE components such as the Process Administrator and WorkSpace. In the application-server configuration, an application server provides the service interface for all TOE components that are part of the runtime infrastructure (i.e., including the Process Execution Engine but excluding Studio, Admin Center, and Log Viewer, which are Swing applications).

The logical functionality provided by one configuration is identical to that provided by the other configuration. The application server provided in the stand-alone configuration is the Tomcat private distribution, specifically integrated to service the supported TOE components. In this configuration, communications between the TOE components and the Process Execution Engine are external to the applications server, and are protected using TCP/SSL. In the application-server configuration, the application server is one of two supported products: BEA WebLogic or IBM WebSphere. These application servers are capable of hosting other applications simultaneously with the TOE. In this configuration, communications between the TOE components and the Process Execution Engine are internal to the applications server via internal "container" protocols (Enterprise JavaBeans communications). In this configuration, TOE communications are protected from other applications via J2EE file security descriptors, and rely on the J2EE Security Framework to restrict access to TOE-related applications. In addition, the TOE always performs an authorization check for each request it receives, to protect against unauthorized requests.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

6.1 Design documentation

Document	Version	Date
BEA AquaLogic BPM Suite Version 6.0.4 Functional Specification (ADV_FSP)	Version 7.0	16 December 2008
BEA AquaLogic BPM Suite Version 6.0 MP4 High Level Design (ADV_HLD)	Version 7.0	16 December 2008
BEA AquaLogic BPM Suite Common Criteria Representation Correspondence (RCR)	Version 3.0	22 December 2008

6.2 Guidance documentation

Document	Version	Date
http://e-docs.bea.com/albsi/docs60/admin_center/index.html; ALBPM Admin Center, Version 6.0 (PDF)	Version 6.0	3 October 2008
http://e-docs.bea.com/albsi/docs60/workspace_admin/index.html; ALBPM WorkSpace Administrator Guide, Version 6.0 (PDF)	Version 6.0	3 October 2008

Document	Version	Date
http://e-docs.bea.com/albsi/docs60/process_admin/index.html; ALBPM Process Administrator Reference, Version 6.0 (PDF)	Version 6.0	3 October 2008
http://e-docs.bea.com/albsi/docs60/logviewer/index.html; ALBPM Log Viewer, Version 6.0 (PDF)	Version 6.0	3 October 2008
http://e-docs.bea.com/albsi/docs60/archiveviewer/index.html; ALBPM Archive Viewer, Version 6.0 (PDF)	Version 6.0	3 October 2008
http://edocs.bea.com/albsi/docs60/admin_guide/index.html; AquaLogic BPM Enterprise Administration Guide, Version 6.0 (PDF)	Version 6.0	3 October 2008
AquaLogic BPM Process API Developer Guide, Version 6.0 (PDF)	Version 6.0	3 October 2008
ALBPM WorkSpace, Version 6.0 (PDF)	Version 6.0	3 October 2008
ALBPM WorkSpace Administrator Guide, Version 6.0 (PDF)	Version 6.0	3 October 2008
ALBPM Workspace Customization Guide, Version 6.0 (PDF)	Version 6.0	3 October 2008
ALBPM Studio Help, Version 6.0 (PDF)	Version 6.0	3 October 2008

6.3 Configuration Management documentation

Document	Version	Date
BEA AquaLogic BPM Suite Version 6.0.4 Configuration Management	Version 3.0	09/04/2008

6.4 Delivery and Operation documentation

Document	Version	Date
BEA AquaLogic BPM Suite Version 6.0.4 Delivery and Operation	Version 3.0	09/3/08
Common Criteria Configuration Notice for BEA AquaLogic BPM Suite 6.0.4	Version 2.0	December 16, 2008
ALBPM Product Installation Guide, Version 6.0 AquaLogic BPM Enterprise Configuration Guide BEA WebLogic Edition	Version 6.0	November 17, 2008

Document	Version	Date
AquaLogic BPM Enterprise Configuration Guide Standalone Edition, Version 6.0	Version 6.0	November 17, 2008

6.5 Life Cycle Support documentation

Document	Version	Date
BEA AquaLogic BPM Suite Version 6.0 Flaw Remediation (ALC_FLR)	Version 2.0	July 15, 2008

6.6 Test documentation

Document	Version	Date
BEA AquaLogic BPM Suite Testing Documentation (ATE) Submission to Common Criteria Process	Version 3.0	12 November 2008

The actual test results have been submitted to the evaluation team in various log files.

6.7 Vulnerability Assessment documentation

Document	Version	Date
BEA AquaLogic BPM Suite, Version 6.0, Vulnerability Assessment (AVA)	Version 7.0	03/09/2009

6.8 Security Target

Document	Version	Date
BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902) Security Target	Version 1.0	31 March 2009

7 IT Product Testing

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

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, User data protection, Identification and authentication, Security management, and Protection of the TSF. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team re-ran the entire automated test suite and a subset of the of the vendor's manual tests in both configurations, stand-alone configuration and an application-server configuration. In addition to re-running 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. All were run as manual tests.

Though not tested, the TOE offers the ability to secure communications between the browsers and TOE components via HTTPS. If configured to use HTTPS, the IT environment is relied upon to provide the certificates for secure SSL communications.

The vendor provided the TOE software and the necessary computers, hubs, and cabling for the test environment.

The following hardware is necessary to create the test configuration:

- TOE Hardware
    - TOE Hardware
        - Any hardware that supports the TOE components is acceptable.
    - IT Environment Hardware
        - Any hardware that supports the non-TOE IT components is acceptable.
    - Test Hardware
        - No specific test hardware is required
    - Ethernet router, CAT 5e cabling, and any other items required to create a functional Ethernet network environment.

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

- TOE Software
- BEA AquaLogic BPM Suite Version 6.0 MP4
    - BEA AquaLogic BPM Studio (Studio)
    - BEA AquaLogic BPM Process Execution Engine (Engine)
    - BEA AquaLogic BPM WorkSpace (WorkSpace)
    - BEA AquaLogic BPM Process Administrator (Process Administrator)
    - BEA AquaLogic BPM Log Viewer (Log Viewer)
    - BEA AquaLogic BPM Archive Viewer (Archive Viewer)
    - BEA AquaLogic BPM Admin Center (Admin Center)

  - BEA AquaLogic Process Application Programming Interface for Web Services (PAPI-WS)

- IT Environment Software
  - Microsoft Windows Server 2003 SP1
  - Linux SUSE 10.0 or Linux RHEL 4.x
  - Oracle 9i and 10g or MS SQL Server 2005, IBM DB2 UDB 8.1 and 9.1 using DataDirect Embedded JDBC Drivers (DataDirect 3.6)
  - Tomcat Servlet 5.5.15, BEA WebLogic Server 9.2.1 and 9.2.2, BEA WebLogic Server 10.0, IBM WebSphere 6.1.0.5
  - Microsoft Internet Explorer 6.0 and 7.0 or Mozilla Firefox 2.0
  - LDAP compliant directory products
  - Microsoft Active Directory, as provided by supported Microsoft operating systems

7.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8 Evaluated Configuration

There are two configurations of the Process Execution Engine TOE component in the evaluated configuration – a stand-alone configuration and an application-server configuration. In the stand-alone configuration, the Process Execution Engine component can reside on a separate server host from the auxiliary application server[3], or they can reside on the same server host. In either case, the Process Execution Engine is a separate Java application that is directly accessible as a service. The application server in the stand-alone configuration provides the service interfaces for access to other TOE components such as the Process Administrator and WorkSpace. In the application-server configuration, an application server provides the service interface for all TOE components that are part of the runtime infrastructure (i.e., including the Process Execution Engine but excluding Studio, Admin Center, and Log Viewer, which are Swing applications).

The logical functionality provided by one configuration is identical to that provided by the other configuration. The application server provided in the stand-alone configuration is the Tomcat private distribution, specifically integrated to service the supported TOE components. In this configuration, communications between the TOE components and the Process Execution Engine are external to the applications server, and are protected using

[3] The "auxiliary" application server is the application server that hosts other runtime components of the TOE, such as the Process Administrator component. It is auxiliary in the sense that it is part of the IT environment and it supports the TOE, but it does not exclusively support the TOE as a dedicated component.

TCP/SSL. In the application-server configuration, the application server is one of two supported products: BEA WebLogic or IBM WebSphere. These application servers are capable of hosting other applications simultaneously with the TOE. In this configuration, communications between the TOE components and the Process Execution Engine are internal to the applications server via internal "container" protocols (Enterprise JavaBeans communications). In this configuration, TOE communications are protected from other applications via J2EE file security descriptors, and rely on the J2EE Security Framework to restrict access to TOE-related applications. In addition, the TOE always performs an authorization check for each request it receives, to protect against unauthorized requests.

The IT environment and the TOE both work together to provide transaction protection. A transaction begins when the Process Execution Engine begins the processing of a request. In the application server configuration, the J2EE Container Transaction Manager provides rollback protection in the case where a request does not terminate correctly. In the standalone configuration, the Process Execution Engine has an internal, integrated transaction manager to provide the same protection.

The TOE components have the software dependencies on the IT environment as described below.

Table 1: TOE Component Physical Requirements

Configuration	Requirement
Studio	Recommended: • 2 GB RAM or more • 4 GB or greater free disk space • 1.8 GHz or faster Pentium Core Duo CPU or similar Minimum: • 1 GB RAM • 2.5 GB or greater free disk space • 1.5 GHz Pentium M CPU or similar
Enterprise Standalone	Recommended: For high-volume deployment (more than 500 concurrent users), consult with ALBPM Professional Services. For testing and low volume deployment (up to 500 concurrent users): • 4 GB RAM or more • 5 GB or greater free disk space • 2.0 GHz or faster Pentium Dual-Core Xeon CPU or similar Minimum (testing only): • 2 GB RAM • 3 GB or greater free disk space • 1.5 GHz Pentium M CPU or similar

The BEA WebLogic and IBM WebSphere application servers are not part of the TOE. Rather for the purposes of this evaluation, they are considered as supporting IT infrastructure outside the scope of the evaluation. Supporting database and directory service components are considered part of the IT environment, too. A complete list of acceptable supporting components can be found in the BEA AquaLogic BPM installation guide. However, the definitive list for support components that are applicable to the TOE definition is provided below, in Table 2.

TOE Component	IT Support Components	Platform(s)
ALBPM Process Execution Engine Standalone (v6.0)	Operating System(s)	Windows Server 2003 SP1 (x86-32), Linux SUSE 10.0 (x86-32, x86-64, Itanium-64), Linux RHEL 4.x (x86-32, x86-64, Itanium-64), AIX 5.3, Solaris 9 and 10 (SPARC), HP-UX 11.23 (Itanium-64)
	Application Server	WorkSpace: Tomcat Servlet 5.5.15, BEA WebLogic Server 9.2.1 and 9.2.2, WebLogic Server 10.0, IBM WebSphere 6.1.0.5; Process Administrator: Tomcat Servlet 5.5.15; WorkSpace Administrator: Tomcat Servlet 5.5.15, BEA WebLogic Server 9.2.1 and 9.2.2, WebLogic Server 10.0, IBM WebSphere 6.1.0.5; Archive Viewer: Tomcat Servlet 5.5.15, BEA WebLogic Server 9.2.1 and 9.2.2, WebLogic Server 10.0, IBM WebSphere 6.1.0.5 (other patch levels introduced problems); PAPI-WS: Tomcat Servlet 5.5.15, BEA WebLogic Server 9.2.1 and 9.2.2, BEA WebLogic Server 10.0, IBM WebSphere 6.1.0.5; RSS Feeds: Tomcat Servlet 5.5.15, BEA WebLogic Server 9.2.1 and 9.2.2, BEA WebLogic Server 10.0, IBM WebSphere 6.1.0.5;
	Directory Service Database	Oracle 9i, 10g (including RAC), MS SQLServer 2005, IBM DB2 UDB 8.1 and 9.1 using DataDirect Embedded JDBC Drivers (DataDirect 3.6)
	JMS Provider	N/A

TOE Component	IT Support Components	Platform(s)
	LDAP Directory Service	Sun ONE System Directory Server 5.2 MS Active Directory 2003
	Identity Service	AquaLogic Interaction Identity Service (for use with the AquaLogic User Interaction Portal)
	Browsers	On Microsoft Windows: • Microsoft Internet Explorer 6.0 and 7.0 • Mozilla Firefox 2.0 On Linux: Mozilla Firefox 2.0 On Apple Mac OS X: • Apple Safari 3.0 • Mozilla Firefox 2.0
	JVM Version for each operating system	Sun 1.5.0_12^ for Windows Server 2003 SP1 (x86-32), SUSE Linux 10.0 (x86-32), Red Hat Enterprise Linux 4 (x86-32), Solaris 9 and 10 (SPARC), JRockit 5 for Red Hat Enterprise Linux 4 (Itanium-64 and x86-64) and Suse 10.0 (Itanium-64 and x86-64), IBM 1.5.0 64 bits for AIX 5.3 running 32 bit JVM, HP-UX 11.23 Itanium-64 using HP-UX JVM 1.5.0_05
Process Execution Engine for WebLogic (v6.0)	Operating System(s)	Microsoft Windows Server 2003 SP1 or R2 (x86-32) Novell SUSE Linux 10.0 (x86-32, x86-64, IA-64) Red Hat Enterprise Linux 4.x (x86-32, x86-64, IA-64) IBM AIX 5.3 Sun Solaris 9 and 10 (SPARC) HP-UX 11.23 (IA-64)
	Application Server	The following versions are supported for all Enterprise applications except Process Administrator, which runs only in the built-in Tomcat Servlet/JSP Container: BEA WebLogic Server 9.2 (MP1 or MP2) BEA WebLogic Server 10.0.
	Engine Database	Oracle 9i, 10g (including RAC), MS SQLServer 2005, IBM DB2 UDB 8.2 and 9.1 using BEA WebLogic Server Embedded DataDirect JDBC Drivers.
	JMS Provider	TIBCO EMS 4.1, WebLogic 8.1 Embedded Messaging and WebLogic 9.2 Embedded. (XA Compliant Resources)

TOE Component	IT Support Components	Platform(s)
	Directory Service Database	Single Source JDBC Plugins: Oracle 9i and 10g, MS SQLServer 2005, IBM DB2 UDB 8.2 and 9.1 using DataDirect JDBC Drivers 3.6; Hybrid Plugins: Sun ONE System Directory Server 5.2 and Oracle 9i, Sun ONE System Directory Server 5.2 and Oracle 10g, MS Active Directory 2003 and Oracle 9i, MS Active Directory 2003 and Oracle 10g, MS Active Directory 2003 and MS SQL Server 2005, Sun ONE System Directory Server 5.2 and IBM DB2 8.2 or 9.1
	Browsers	On Microsoft Windows: • Microsoft Internet Explorer 6.0 and 7.0 • Mozilla Firefox 2.0 On Linux: Mozilla Firefox 2.0 On Apple Mac OS X: • Apple Safari 3.0 • Mozilla Firefox 2.0
	JVM Version	JRockit 5 for Windows Server 2003 SP1, Red Hat Enterprise Linux 4 (x86-32, x86-64 and Itanium-64) and Suse 10.0 (x86-32, x86-64 and Itanium-64), Sun 1.5.0_12^ Solaris 9 and 10 (SPARC), IBM 1.5.0 64 bits for AIX 5.3 running 32 bits JVM, HP-UX 11.23 Itanium-64 using HP-UX JVM 1.5.0_05,
ALBPM Enterprise 6.0 for WebSphere	Operating System(s)	Windows Server 2003 SP1 (x86-32), Linux SUSE 10.0 (x86-32, x86-64, Itanium-64), Linux RHEL 4.x (x86-32, x86-64, Itanium-64), AIX 5.3, Solaris 9 and 10 (SPARC).
	Application Server	WorkSpace: Tomcat 5.5.15, IBM WebSphere 6.1.0.5; Process Administrator: Tomcat 5.5.15; WorkSpace Administrator: Tomcat 5.5.15, IBM WebSphere 6.1.0.5; Archive Viewer: Tomcat 5.5.15, IBM WebSphere 6.1.0.5; BPM Deployer: IBM WebSphere 6.1.0.5; PAPI-WS: Tomcat 5.5.15, IBM WebSphere 6.1.0.5; RSS Feeds: Tomcat 5.5.15, IBM WebSphere 6.1.0.5; ALSB Custom Transport EAR: N/A
	Engine Database	Oracle 9i, 10g (including RAC), MS SQLServer 2005, IBM DB2 UDB 8.2 and 9.1 using DataDirect Embedded JDBC Drivers (DataDirect 3.6).
	JMS Provider	TIBCO EMS 4.1, WebSphere 6.1.0.5 (other versions presented problems) Embedded Messaging, IBM MQ Series 5.3 (XA Compliant Resources)

TOE Component	IT Support Components	Platform(s)
	Directory Service Database	Single Source JDBC Plugins: Oracle 9i and 10g, MS SQLServer 2005, IBM DB2 UDB 8.2 and 9.1 using DataDirect JDBC Drivers 3.6; Hybrid Plugins: Sun ONE System Directory Server 5.2 and Oracle 9i, Sun ONE System Directory Server 5.2 and Oracle 10g, MS Active Directory 2003 and Oracle 9i, MS Active Directory 2003 and Oracle 10g, MS Active Directory 2003 and MS SQL Server 2005, Sun ONE System Directory Server 5.2 and IBM DB2 8.2 or 9.1
	Browsers	On Microsoft Windows: • Microsoft Internet Explorer 6.0 and 7.0 • Mozilla Firefox 2.0 On Linux: Mozilla Firefox 2.0 On Apple Mac OS X: • Apple Safari 3.0 • Mozilla Firefox 2.0
	JVM Version	Sun 1.5.0_12^ for Solaris 9 and 10 (SPARC); IBM 1.5.0 for Windows Server 2003 SP1 (x86-32), SUSE Linux 10.0 (x86-32, x86-64), Red Hat Enterprise Linux 4 (x86-32, x86-64), IBM 1.5.0 64 bits for AIX 5.3 running in 32 bits JVM
Studio (v6.0)	Operating System(s)	Microsoft Windows XP SP2 (x86-32) Microsoft Windows 2003 Server SP1 or R2 (x86-32) Novell SUSE Linux 10.0 (x86-32) Red Hat Enterprise Linux 4 (x86-32)
	Application Server	Tomcat Servlet/JSP Container
	Database	Embedded Derby DB
	Browsers	On Microsoft Windows: • Microsoft Internet Explorer 6.0 and 7.0 • Mozilla Firefox 2.0 On Linux: Mozilla Firefox 2.0 On Apple Mac OS X: • Apple Safari 3.0 • Mozilla Firefox 2.0

Table 2 IT Environment Support-Component Requirements

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on March 2007. The evaluation confirmed that the BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902) product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 conformant, and assurance requirements (Part 3) for EAL2 Augmented with ALC_FLR.1. The details of the evaluation are recorded in the CCTL's evaluation technical report; Evaluation Technical Report for BEA AquaLogic BPM Suite Version 6.0 MP4, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902) Security Target, Version 1.0, 31 March 2009.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the BEA AquaLogic BPM Suite Version 6.0 MP4 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. In addition, the evaluation team ensured changes to the implementation representation are controlled and that TOE associated configuration item modifications is properly controlled.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

The evaluation team followed the Common Criteria Configuration Notice for BEA AquaLogic BPM Suite 6.0.4, ALBPM Product Installation Guide, Version 6.0 AquaLogic BPM Enterprise Configuration Guide BEA WebLogic Edition, and AquaLogic BPM Enterprise Configuration Guide Standalone Edition, Version 6.0 the installation procedures to ensure the procedures result in the evaluated configuration.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL2 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The ALBPM Product Installation Guide, Version 6.0 (PDF), AquaLogic BPM Process API Developer Guide, Version 6.0 (PDF), ALBPM WorkSpace, Version 6.0 (PDF), ALBPM WorkSpace Administrator Guide, Version 6.0 (PDF), ALBPM Workspace Customization Guide, Version 6.0 (PDF), and ALBPM Studio Help, Version 6.0 (PDF) were assessed during the design and testing phases of the evaluation to ensure it was complete.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied the ALC_FLR.1 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that systematic procedures exist for managing flaws discovered in the TOE.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

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 exercised the complete Vendor 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.

9.8 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis, the evaluation team's misuse analysis, the

evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 Summary of Evaluation Results

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

10 Validator Comments/Recommendations

The validation team observed that the evaluation was performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR. The validation team therefore recommends that the evaluation results be accepted.

It is important to note that the implementation of TLS to provide HTTPS is not part of the TOE, it is provided by the IT Environment. It is important for customers to consider the need for protection of information flow in transit and plan their deployments accordingly.

The TOE is designed for deployment in an intranet environment, and assumes that TOE administrators do not act maliciously. The EAL2 assurance level is not intended to protect against highly sophisticated technical threats.

The validators find that the product's data protection functions appear to be a good match with the product's functional objectives, and that the architecture integrates well with the security capabilities of the hosting IT environments. In addition to the specific results of vulnerability analysis and testing, the vendor appears to have made a sound engineering effort to reduce risks associated with flaws commonly found in web-based applications. The configuration rules required for the evaluated TOE do not appear to introduce significant administrative difficulties or to materially impact the product's capabilities.

11 Security Target

The Security Target is identified as BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902) Security Target, Version 1.0, dated 31 March 2009. 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 2 augmented with ALC_FLR.1.

12 Glossary

The following definitions are used throughout this document:

ACL Access Control List

AES Advanced Encryption Standard

ALBPM AquaLogic Business Process Management

ALUI AquaLogic User Interaction

API Application Programming Interface

BAM Business Activity Monitoring

BPEL Business Process Execution Language

BPM Business Process Management

CC Common Criteria

CM Configuration Management

EAL Evaluation Assurance Level

FIPS Federal Information Processing Standard

IBM International Business Machines

ID Identification

IT Information Technology

JDBC Java Database Connectivity

JNDI Java Naming and Directory Interface

JVM Java virtual machine

NIST National Institute of Standards and Technology

PAPI Process Application Programming Interface

PAPI-WS Process Application Programming Interface Web Services

PC Personal Computer

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

XML Extensible Markup Language

13 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 2.3, August 2005.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] BEA AquaLogic BPM Suite Version 6.0 MP4 Final Proprietary ETR – Part 2, Version 3.0 dated 30 March 2009 and Supplemental Team Test Report, Version 2.0, 30 March 2009.

[6] BEA AquaLogic BPM Suite Version 6.0 MP4 Final Non-Proprietary ETR – Part 1, Version 2.0, 31 March 2009.

[7] BEA AquaLogic BPM Suite Version 6.0 MP4 (Build 95902) Security Target, Version 1.0, 31 March 2009.

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