National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

IBM WebSphere Application Server

Report Number: **CCEVS-VR-06-0024**
Dated: **June 3, 2006**
Version: **1.3**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

IBM Corporation
New Orchard Road
Armonk, NY 10504
USA

Evaluation Personnel:
SAIC Common Criteria Testing Laboratory, Columbia, Maryland

Reese, Cynthia
Diaz, Terrie
Thompson, Dave

Validation Personnel:

Geoff Beier, Orion Security Solutions
Bill Hohle, Orion Security Solutions
Santosh Chokhani, Orion Security Solutions

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the IBM WebSphere Application Server. It 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 the IBM WebSphere Application Server was performed by the SAIC Common Criteria Testing Laboratory in the United States and was completed during April 2006. 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 IBM. 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 extended and Part 3 augmented, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 4, augmented with Basic Flaw Remediation (ALC_FLR.1) have been met.

The WebSphere Application Server product consists of several editions of the WebSphere Application Server 6.0.2.3 (hereafter referred to as *the product*) with specific patches as specified in Table 1. The product is a Java™ 2 Enterprise Edition (J2EE) 1.4 compliant run-time environment. The primary purpose of the product is to provide an environment for running and managing user-supplied enterprise applications. J2EE is a comprehensive set of specifications for designing, developing and deploying multi-tier, server-based applications.

The WebSphere Application Server TOE, which is software-only, enforces identification of request to protected resources, controls access to protected resources based upon based upon security attributes, allows for the management of the security attributes associated with protected resources and users, and provides an invocation of SSL that requires a remote caller to invoke SSL using the configured algorithms so that the session is encrypted when the remote caller issues a request to the TOE over the remote interface of the IBM HTTP Server component. Note that the TOE does not perform the actual SSL encryption.

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 4, augmented with Basic Flaw Remediation (ALC_FLR.1) evaluation. Therefore the validation team concludes that the SAIC CCTL findings are accurate, and the conclusions justified.

2 Identification

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

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's 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 organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	WebSphere Application Server version V6.0.2.3 (32-bit) WebSphere Application Server Express V6.0.2.3 WebSphere Application Server Network Deployment (32-bit) V6.0.2.3 WebSphere Application Server for z/OS V6.0.1, service level 6.0.2.3 WebSphere Application Server V6.0.2.3, WebSphere Application Server Express V6.0.2.3, and WebSphere Application Server Network Deployment V6.0.2.3 requires interim fixes for APARs PK15487, PK16977, PK13494, PK13653, PK15059, PK18574, PK18576, and PK18991. WebSphere Application Server for z/OS 6.01, service level 6.0.2.3 requires the fix to APAR AK17408.
Security Target	WebSphere Application Server EAL4+ Security Target, V9.3, May 11, 2006
Evaluation Technical Report	Evaluation Technical Report for WebSphere Application Server; Part 1, Version 0.5, May 23, 2006.
Conformance Result	CC Part 2 extended, CC Part 3 conformant, EAL 4 augmented with ALC_FLR.1
Sponsor	IBM Corporation New Orchard Road Armonk, NY 10504
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, Maryland 21046

Item	Identifier
CCEVS Validator(s)	Geoff Beier, Bill Hohle, Santosh Chokhani Orion Security Solutions 1489 Chain Bridge Road, Suite 300 Mclean, Virginia 22101

3 Security Policy

The TOE identifies a client before performing any other TSF mediated action for the client. The TOE relies upon the IT environment to perform authentication using any one of the following methods: passwords-based, certificate-based, and LPTA token.

The TOE permits a client to access a protected resource only if a user or group ID of the user is mapped to a role that has permission to access the resource. The resources protected by the TOE are:

- Protected methods of web server applications
- Protected methods of enterprise beans
- Configuration data, files and runtime state
- Naming directory
- Transactions and activities
- Protected resources of the built-in JMS Provider (the local bus, queue destination, temporary destination, topic space, topic space root and topics)
- Protected resources of the UDDI registry directory
- Protected location service resources

The TOE provides security management functions that provide a mechanism for dynamically configuring some security attributes used by TOE access control functions

The TOE provides an invocation of SSL function that requires a remote caller to invoke SSL using the configured algorithms so that the session is encrypted when the remote caller issues a request to the TOE over the remote interface of the IBM HTTP Server component. This function does not perform the actual SSL encryption, yet provides a mechanism for requiring requests from remote callers to be encrypted.

4 Assumptions

- It is assumed that the applications and operating system that the TOE interfaces, will not compromise the security of the TOE and where applicable, that they have been configured in accordance with manufacturer's installation guides and/or its evaluated configuration.
- It is assumed that the developers of all trusted user applications (user web server applications and user enterprise beans), resource adapters, and providers will comply with all the guidelines and restrictions specified in the User Guidance document.

- It is assumed that all software and hardware, including network and peripheral devices, have been approved for the transmittal of protected data. Such items are to be physically protected against threats to the confidentiality and integrity of the data.
- It is assumed that all hardware used in the operating environment is physically secured.
- It is assumed that there are one or more competent individuals that are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, willfully negligent or hostile.
- It is assumed that the IT Environment supporting the TOE provides at least one of the supported authentication mechanisms identified within the evaluated configuration of the TOE.

5 Architectural Information

Figure 1 below illustrates the TOE; components of the TOE are in the shaded boxes. The non-shaded components are required in the software environment of the TOE. The dashed areas are optional.

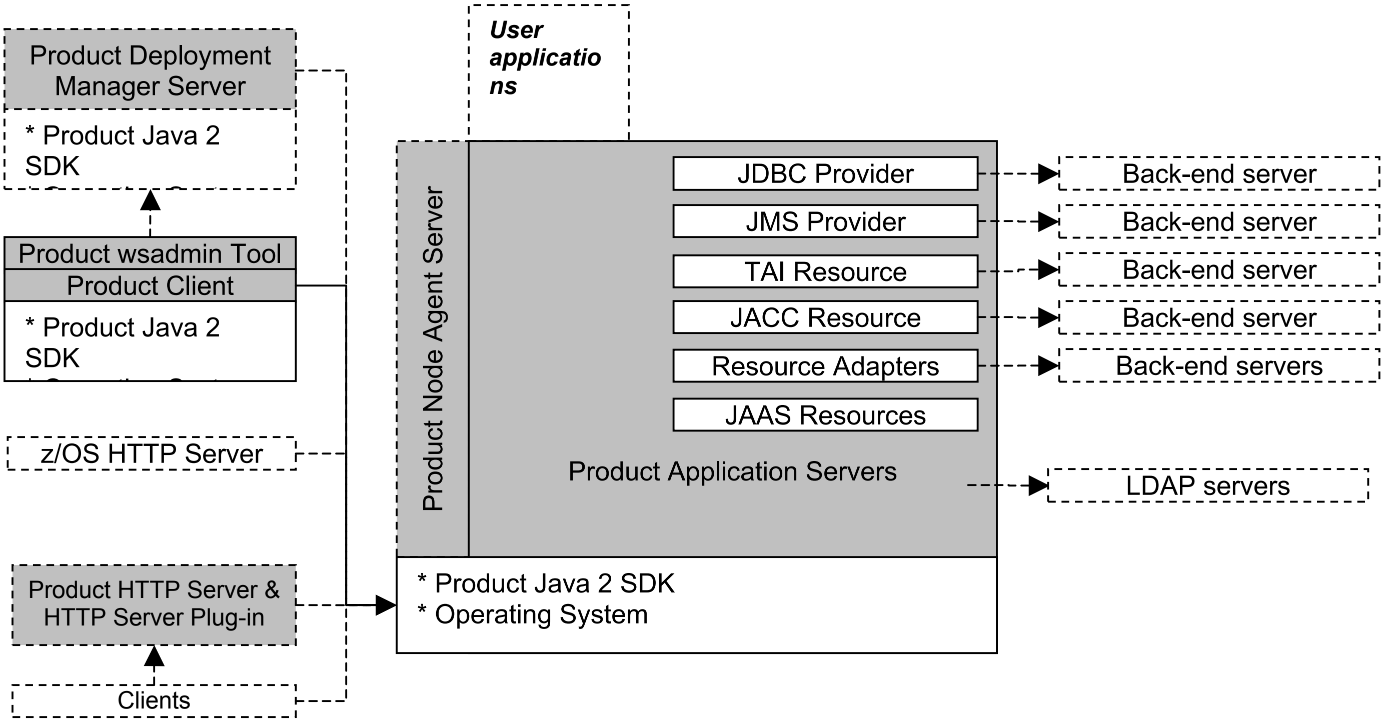

Figure 1: TOE Overview

The following subsections describe the TOE components.

5.1 Product Application Server

The Product Application Server component is a set of containers, services, and resources that provide an environment for running enterprise applications and their components and for programmatically managing enterprise applications and their components.

The Product Application Server is included in the TOE because it implements the primary purpose of the product, which is to provide an environment for running enterprise applications and their components and for programmatically managing enterprise applications and their components.

The Product Application Server performs the following functions:

- Starts up
- Loads local components
- Accepts local and remote requests
- Processes requests for services
- Processes requests for mapped methods and HTML pages

Starts up: The Product Application Server is started using the Java command provided by the Product Java 2 SDK. The Product Application Server is run in a single operating system process and JVM.

Loads local components: The Product Application Server starts the following components:

- User applications, and
- UDDI Registry Application.

These components are run in the same operating system process and JVM that the Product Application Server is using. Therefore, these components are called "local components."

Accepts local and remote requests: The Product Application Server accepts requests over its local and remote interfaces. The requests over its local interfaces come from the local components (web server applications and enterprise beans). The Product Application Server receives these requests directly. The requests over its remote interfaces come from clients. The Product Application Server receives these requests indirectly by means of the Product Java 2 SDK.

Processes requests for services: If the Product Application Server receives a request for a service, the Product Application Server processes any required security and, if security is successful, processes the requested service.

Processes requests for mapped methods and HTML pages: If the Product Application Server receives a request for a mapped method or HTML page in an user application or the UDDI Registry Application, the Product Application Server processes any required security and then, if security processing is successful, invokes the mapped method or HTML page.

5.2 Product Wsadmin Tool

The Product Wsadmin Tool is a tool that provides a scripting interface for managing enterprise applications and their components.

The Product Wsadmin Tool is included in the TOE because it provides a scripting tool that facilitates the management of enterprise applications.

The Product Wsadmin Tool is a Java client application and must reside on the same operating system as the Product Client and is run in the same operating system process and JVM as the Product Client. In the evaluated configuration the product Wsadmin tool and the product client must run on the same machine and under the same operating system as the product application server.

An administrator can use this tool to execute administrative scripting commands. The Product Wsadmin Tool processes these commands by calling the AdminClient API of the Product client.

5.3 Product Client

The Product Client component is a set of application programming interfaces (APIs) that provide an environment for running clients to enterprise applications.

The Product Client is included in the TOE because it is required by the Wsadmin Tool.

In the evaluated configuration, the administrator starts the Product Client using the Wsadmin command file. The Wsadmin command file causes the Java 2 SDK to start the Product Client and then causes the Product Client to start the Product Wsadmin Tool. Both the Product Client and the Product Wsadmin Tool run in a single process and use a single JVM. After the Product Client starts, it accepts AdminClient API requests from the Product Wsadmin Tool and processes these requests by calling a remote interface to the Administration Service of the Product Application Server.

5.4 Product Deployment Manager Server and Product Node Agent Server

The Product Deployment Manager Server and Product Node Agent Server each contain one service, which is an administration service. Each Product Deployment Manager Server and Product Node Agent Server accepts requests to its administration service, processes any required security and processes the request only if security processing is successful.

5.5 Product HTTP Server and Product HTTP Server Plug-in

The Product HTTP Server and Product HTTP Server Plug-in are included in the TOE. Both reside in the same process, which is separate from the process in which the Product Application Server resides. The Product HTTP Server receives HTTP requests by remote HTTP Clients. The Product HTTP Server Plug-in forwards the requests to the Product Application Server.

6 Documentation

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

Configuration Item	Identification
Security Target	**IBM ST EAL 4 93.doc,** V 9.3 dated 11 May 2006
Configuration Management	**WAS EAL4 ACM v 11.doc,** Version 1.1 Dated 15 March 2006 **Configuration List: WAS EAL4 Config List v17.doc** V1.7 Dated: 11 May 2006
Delivery and Operation	**WAS EAL4 ADO v50.doc,** V5.0 dated 10 March 2006
LifeCycle Documents	**WAS EAL4 ALCv30.doc,** V3.0 dated 13 March 2006 **WAS EAL4 FLR 30.doc,** V3.0 dated 13 March 2006

Configuration Item	Identification
Guidance	**WAS EAL4 AGD 92.doc,** V9.2 dated 27 April 2006
Design	**Reference Material**: CD- JavaDocs buildo0525.05 **WAS EAL4 Jsclient_fap20.doc** dated 30 Jun 2005 **WS-AtomicTransaction.pdf** dated November 2004 **Messaging_Engine_Corespi_javadoc.zip** created 28June 2005 **WAS EAL4 Messaging_Interface_Javadoc.zip** Created 16 September 2005 **rmm-javadoc.zip** Created 7 November 2005 **GSK7c_sslapi.pdf** Edition dated 28 July 2005 **WASEAL4Source_1201.zip** Created 01 December 2005 **RCR: WAS EAL4 RCR v30.doc,** V3.0 dated 9 December 2005 **Security Policy Model: IBM WAS EAL4 ADV_SPM v3.0.doc,** 6 February 2006 **Functional Specification: WAS EAL4 FS 50.doc,** 6 March 2006 **High Level Design: WAS EAL4 HLD 50.doc,** 7 March 2006 **WAS EAL4 TRM-HLD10.doc,** JetStream Component (TRM) HLD, V1.0 dated October 2004, Updated 8 February 2005 **Low Level Design:** **|WASEAL4LLD-AA-OverviewRelevantComponents1v30.doc,** 01 March 2006 **WASEAL4LLD-EJBCollaboratorv30.doc,** 01 March 2006 **WASEAL4LLD-WebCollaborator30.doc,** 01 March 2006 **WASEAL4LLD-WSSecurity30.doc,** 01 March 2006 **WAS EAL4 LLD NR 20.doc,** 1 November 2005 **WAS EAL4LLD-ORBExtensionsv10.doc**, 1 July 2005 **WASEAL4LLD-AA-OverviewRelevantComponents2v20.ppt,** 7 November 2005 **WASEAL4LLD-Activityv10.doc** 1 July 2005 **WASEAL4LLD-Adminv10.doc,** 1 July 2005 **WASEAL4LLD-Authenticationv10.doc,** 8 Apr 2005 **WASEAL4LLD-CSIv2-v10.doc,** 24 Mar 2005 **WASEAL4LLD-EJBContainerv10.doc,** 1 Jul 2005 **WASEAL4LLD-FileTransferServletv20.doc,** 27 October 2005 **WASEAL4LLD-HAMv20.doc,** 13 October 2005 **WASEAL4LLD-HttpChannelv20.doc,** 14 Mar 2005 **WASEAL4LLD-HTTPServerv20.doc,** 1 July 2005 **WASEAL4LLD-Messagingv20.doc,** 1 Jul 2005 **WASEAL4LLD-Namingv20.doc,** 1 July 2005 **WASEAL4LLD-RoleBasedAuthz-v20.doc,** 2 April 2005 **WASEAL4LLD-zOS-CSIv210.doc,** 1 July 2005 **WASEAL4LLD-SSLChannel20.doc,** 1 July 2005 **WASEAL4LLD-TAM-JAAS10.doc,** 5 May 2005 **WASEAL4LLD-TAM-JACC10.doc,** 1 Jul 2005 **WASEAL4LLD-TAM-TAI10.doc,** 5 May 2005 **WASEAL4LLD-TCPChannel20.doc,** 1 July 2005 **WASEAL4LLD-Transaction10.doc,** 1 Jul 2005

Configuration Item	Identification
Test Documents	**WASEAL4LLD-UDDI10.doc,** 12 May 2005 **WASEAL4LLD-WebContainer10.doc,** 1 Jul 2005 **WASEAL4LLD-WebEngine10.doc,** 1 Jul 2005 **WASEAL4LLD-WSAdmin10.doc,** 24 Mar 2005 **WASEAL4LLD-zProxyMbean10.doc,** 1 Jul 2005 **WASEAL4LLD-zRuntime20.doc,** 5 May 2005 **WASEAL4LLD-zTransactions20.doc,** 7 November 2005 **IBM-WAS-ADV_LLD-ETR -response.rtf,** 7 November 2005 **Functional Test:** **WAS EAL4 ATE 70.doc,** Functional Test / Test Coverage Analysis V7.0, 14 March 2006 **WAS EAL4 ATE 20 MSGADMIN.doc,** Messaging Admin Scripting Test Plan, V2.0, 9 December 2005 **WAS EAL4 ATE 30 TATP.doc,** Transactions and Activities Test Plan, V3.0, 15 February 2006 **WAS EAL4 ATE 10 Messaging TestPlan.doc** Messaging Security Test Plan V1.0, 7 October 2005 **Test Logs:** **07 March 2006-** **ZOS_Logs_Official_Part2.zip** **z/OS (last 4 of 11) CFG5** **06 March 2006-** **ZOS_Logs_Official_Part1.zip** **z/OS (7 of 11) CFG5** **27 February 2006** – **logs_cfg3_Linux_weblnx16r_was-na-2.zip** **logs_cfg3_Linux_weblnx13_was-na-1.zip** RHEL-Z CFG3 **24 February 2006** – **logs_cfg3_Linux_weblnx14s_was-na-2.zip** **logs_cfg3_Linux_weblnx18_was-na-1.zip** SUSE-Z CFG3 **20 February 2006** – **logs_cfg2_Linux_weblnx14s_was-na-1.zip** **logs_cfg1_Linux_weblnx18_was-na-1.zip** SUSE-Z CFG1, CFG2 **16 February 2006** – **logs_cfg2_Linux_weblnx13_was-na-1.zip** **logs_cfg1_Linux_weblnx16r_was-na-1.zip** RHEL-Z CFG1, CFG2 **logs_cfg2_Linux_hoodpin_was-na-1.zip** **logs_cfg1_Linux_swaybar_was-na-1.zip** **logs_cfg3_Linux_swaybar_was-na-2.zip** **logs_cfg3_Linux_hoodpin_was-na-1.zip** SUSE LINUX-PPC CFG1, CFG2, CFG3

Configuration Item	Identification
	logs_cfg2_Linux_t50_was-na-1.zip **logs_cfg3_Linux_cc01rhel_was-na-1.zip** **logs_cfg3_Linux_cc02rhel_was-na-2.zip** **logs_cfg1_Linux_cc01rhel_was-na-1.zip** RHEL-INTEL, CFG1,CFG2,CFG3 **logs_cfg3_Linux_t35_was-na-2.zip** **logs_cfg3_Linux_kamakazi_was-na-1.zip** **logs_cfg1_Linux_kamakazi_was-na-1.zip** **logs_cfg2_Linux_t35_was-na-1.zip** RHEL-PPC CFG1, CFG2, CFG3 **logs_cfg3_Win2003_eh5a_was-na-1.zip** **logs_cfg3_Win2003_eh5b_was-na-2.zip** **logs_cfg2_Win2003_eh5c_was-na-1.zip** **logs_cfg1_Win2003_t52_was-na-1.zip** WINDOWS CFG1, CFG2, CFG3 **logs_cfg1_AIX_wsbvt150_was-na-1.zip** **logs_cfg2_AIX_t31_was-na-1.zip** **logs_cfg3_AIX_t43_was-na-2.zip** **logs_cfg3_AIX_t40_was-na-1.zip** AIX CFG1, CFG2, CFG3 **logs_cfg3_HP-UX_wsbvt157_was-na-2.zip** **logs_cfg3_HP-UX_wssechp1_was-na-1.zip** HP CFG3 **14 February 2006** – **logs_cfg1_HP-UX_hpcst3_was-na-1.zip** **logs_cfg2_HP-UX_wsbvt189_was-na-1.zip** HP CFG1, CFG2 **7 February 2006** – **logs_cfg3_SunOS_t25_was-na-1.zip** **logs_cfg3_SunOS_t26_was-na-2.zip** **logs_cfg1_SunOS_sun1_was-na-1.zip** **logs_cfg2_SunOS_sun2_was-na-1.zip** Solaris CFG1, CFG2, CFG3
Vulnerability Documents	**WAS MSU Analysis30.doc,** Misuse Analysis, V3.0 , 8 March 2006 **WASv6 EAL4 VLAv30.doc,** Vulnerability Analysis, V3.0, 16 March 2006
Source Code	**WASEAL4SOURCE_0320.zip,** Delivered 20 March 2006 **apr.h,** Delivered 03 March 2006 **SelectedSource Description2.doc,** Delivered 01 March 2006 **WASEAL4SOURCE_1201.zip,** Delivered 02 December 2005

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 all the security functional requirements in the ST including: invocation of SSL, Identification, Access Control, and Security Management which are all the security functions for the TOE. 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 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 developer test documentation sufficiently addresses the TSFI and security functions as described in the functional specification. The evaluation team performed all of the developer's test suite. The evaluation team devised and conducted an independent set of team tests and penetration tests.

8 Evaluated Configuration

The product TOE consists of a subset of the components provided with the product. This subset is comprised of those product components that are used to deploy and run user-supplied enterprise applications and to manage these applications by means of a scripting tool. Table 2 below lists the product components for the various evaluated editions. All product TOE components must be installed on the same machine running a single operating system.

TABLE 2: TOE Components in Evaluated Configuration

Product Component	WebSphere Application Server Express V6.0.2.3	WebSphere Application Server V6.0.2.3 (32-bit)	WebSphere Application Server Network Deployment (32-bit) V6.0.2.3	WebSphere Application Server for z/OS V6.0.1, service level 6.0.2.3
Product Application Server	Required	Required	Required	Required
Product Client	Required	Required	Required	Required
Product Tools and applications	Required – only the product wsadmin tool	Required – only the product wsadmin tool	Required – only the product wsadmin tool	Required – only the product wsadmin tool
Product HTTP Server	Optional	Optional	Optional	Not in TOE
Product HTTP Server Plug-Ins	Optional – only the plug-ins for the Product HTTP Server	Optional – only the plug-ins for the Product HTTP Server	Optional – only the plug-ins for the Product HTTP Server	Not in TOE
Product Java 2 SDK	Not in TOE	Not in TOE	Not in TOE	Not in TOE
Product Deployment	Not applicable	Not	Required	Required

Product Component	WebSphere Application Server Express V6.0.2.3	WebSphere Application Server V6.0.2.3 (32-bit)	WebSphere Application Server Network Deployment (32-bit) V6.0.2.3	WebSphere Application Server for z/OS V6.0.1, service level 6.0.2.3
Manager Server	to this edition.	applicable to this edition.		
Product Node Agent Server	Not applicable to this edition.	Not applicable to this edition.	Required	Required
Product Dynamic Caching Server	Not in TOE	Not in TOE	Not in TOE	Not in TOE

Table 3 below lists the non-TOE components for the evaluated configuration.

Non-TOE component in the environment	WebSphere Application Server Express	WebSphere Application Server	WebSphere Application Server Network Deployment	WebSphere Application Server for z/OS
Product Java 2 SDK	Required	Required	Required	Required
Operating system	Required	Required	Required	Required
JDBC resource and any back-end servers	Optional	Optional	Optional	Optional
Alternate JMS resource and any back-end servers	Optional	Optional	Optional	Optional
z/OS HTTP Server	Not applicable	Not applicable	Not applicable	Optional
LDAP server	Required	Required	Required	Not applicable
TAI resource and any back-end servers	Optional	Optional	Optional	Optional
JACC resource and any back-end servers	Optional	Optional	Optional	Optional
JAAS resources	Optional	Optional	Optional	Optional
Resource adapters and back-end servers	Optional	Optional	Optional	Optional
User applications	Optional	Optional	Optional	Optional
Callers	Optional	Optional	Optional	Optional

The evaluated configuration does not impose any restrictions upon hardware other than the hardware must support the operating system.

9 Validator Comments

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

The users should be aware that the TOE only identifies users, but does no authentication. The TOE depends on the Environment (i.e., underlying operating system for this feature).

For token based authentication, and for transport security, the TOE relies on the Environment to generate the keys, protect the keys, to perform the basic cryptographic functions, and to carry out applicable cryptographic protocols. Thus, any of these security critical functions have not been evaluated as a part of this evaluation.

10 Security Target

See Table 1.

11 List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTML	Hyper Text Markup Language
ID	Identifier
IBM	International Business Machines
J2EE	Java 2 Enterprise Edition
JVM	Java Virtual Machine
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
SAIC	Science Applications International Corporation
SDK	Software Development Kit
ST	Security Target
TOE	Target Of Evaluation
TSF	**TOE** Security Function
VR	Validation Report

.

12 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.2 Revision 256, January 2004.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.2 Revision 256, January 2004.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, Version 2.2 Revision 256, January 2004.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.2 Revision 256, January 2004.

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

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, Version 2.2, January 2004.

[7] Final Evaluation Technical Report for IBM WebSphere Application Server EAL4+ Part 2, Version 0.5, May 5 2006.

[8] WebSphere Application Server EAL4 Security Target, Version 9.3. May 11, 2006.

[9] Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.

13 Interpretations

13.1 International Interpretations

The evaluation team performed an analysis of the international interpretations and applied those that were applicable and had impact to the TOE evaluation as the CEM work units were applied.

The following international interpretations were applied to the IBM WebSphere Application Server EAL4 Security Target:

- 058 – Confusion over Refinement
- 064 – Apparent Higher Standard for Explicitly Stated Requirements
- 065 – No Component to Call Out Security Function Management
- 103 – Association of Access Control Attributes with Subjects and Objects

13.2 NIAP Interpretations

The Evaluation Team determined that the no NIAP interpretations were applicable to this evaluation:

13.3 Interpretations Validation

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.