WebSphere® Application Server for z/OS EAL4+ Security Target

Date: February 16, 2007
Issue: V19a.0
Reference: WAS-ZOS/EAL4/ST/19a

This Page Intentionally Left Blank.

Table of Contents

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States and other countries, or both:

AIX®
DB2®
Domino®
IBM®
Lotus®
Power PC®
Tivoli®
WebSphere®
z/OS®

The following terms are trademarks of other companies:

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Glossary and Terminology

ACL	Access Control List
AllAuthenticatedUsers	A value that is used by some of the TOE access control functions to determine authorization. The value of "AllAuthenticatedUsers" represents a special group consisting of all users that have been successfully identified (caller has presented its identity and the TOE has validated its identity). When the value of "AllAuthenticatedUsers" is mapped to a role with permission on a resource, the applicable TOE access control function grants access to the caller only if the caller has been successfully identified. In the evaluated configuration, all callers must be successfully identified by a TOE identification function before reaching a TOE access control function. Therefore, in the evaluated configuration, when the value of

	"AllAuthenticatedUsers" is mapped to a role with permission on a resource, the applicable TOE access control function always grants access to the resource. In other words, in the evaluated configuration, there are only positive scenarios for AllAuthenticatedUsers as processed by the applicable TOE access control functions. Furthermore, the behavior of these positive scenarios is the same as those in which a group ID is mapped to a role with permission on a resource and the caller is a member of this group. Note: AllAuthenticatedUsers is used interchangeably with AllAuthenticated.
API	Application Programming Interface
Authorised Client	A client user who may, in accordance with the TSP, perform an operation.
Certified applications, resource adapters, and providers	Enterprise applications, resource adapters, and providers that have been certified at an EAL4 level or higher to run in the environment of the TOE.
CC	Common Criteria
CCIMB	Common Criteria Interpretations Management Board
Channel chain	Channel chain refers to the channel transport chain such as that used by DCS. For details on the DCS channel transport chain options, reference the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/urun_chain_typedcs.html
CN	Common Name (CN) is part of the Distinguished Name (DN) that uniquely identifies an entry in a directory.
CORBA	Common Object Request Broker Architecture (CORBA) is an architecture specification for distributed object-oriented computing that separates client and server programs with a formal interface definition. For additional information see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/rorb_r4lno.html
COSNaming	The CORBA Naming Service is also known as the Common Object Services Naming Service – COSNaming for short. For details, reference the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tnam_ovr2.html

CMVC	The Configuration Management Version Control (CMVC) is used for WebSphere Application Server version control, change control and defect tracking.
CSIv2	Common Secure Interoperability Version 2 is an authentication protocol developed by the Object Management Group (OMG) that supports interoperability, authentication delegation and privileges. For details on authentication protocols for EJB security on the Application server see http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/csec_corba.html
DB	DataBase
DCS	The Distribution and Consistency Services is a component of the WebSphere Application Server high availability network which uses the Channel Framework as the default network protocol and allows configuration of a transport channel. For details on configuring the DCS transport channel reference the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/urun_chain_typedcs.html
DN	Distinguished Name is a set of attribute:value pairs that uniquely identifies an entry in a directory such as the LDAP directory.
Distributed platforms	All the WebSphere Application Server operating systems supported for the evaluation except for z/OS®.
EAL	Evaluation Assurance Level
EJB	Enterprise JavaBeans is a component architecture defined by Sun Microsystems for the development and deployment of object-oriented, distributed enterprise-level applications. For details on EJB applications, reference the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6tech_ejb.html
EJBHome	The EJBHome is an interface which must be extended by all remote home interfaces of enterprise beans. For details see http://java.sun.com/j2ee/1.4/docs/api/javax/ejb/EJBHome.html
EJBObject	The EJBObject interface is extended by all remote interfaces of enterprise beans. For details see http://java.sun.com/j2ee/1.4/docs/api/javax/ejb/EJBObject.html Enterprise bean component A server application component that conforms to the J2EE V1.4 specification. The component contains one or more enterprise beans. The enterprise beans are packaged in a JAR file and configured with an ejb-jar.xml file.

Enterprise application	A server application that conforms to the J2EE V1.4 specification. The application consists of one or more web server application components, enterprise bean components, or both. The components optionally can be packaged in an EAR file and configured with an application.xml file.
Enterprise bean	A server module that is included in an enterprise bean component. The module is coded in the Java programming language and conforms to the EJB architecture identified in the J2EE V1.4 specification.
Everyone	A value that is used by some of the Target of Evaluation (TOE) access control functions to determine authorization. The value of "Everyone" represents a special group consisting of all users. When value of "Everyone" is mapped to a role with permission to access a resource, the applicable TOE access control function allows any caller to access the resource. In the evaluated configuration, for all identification functions except Ident.1, each caller must be successfully identified before the applicable access control function is processed. Therefore, in the evaluated configuration, for all identification functions except Ident.1, mapping "Everyone" to a resource has the same effect as mapping "AllAuthenticatedUsers" to a resource. (See "AllAuthenticatedUsers.")
FIPS	Federal Information Processing Standards (FIPS) are standards used by NIST for Federal Government Computer systems. For details, reference the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/rovr_fips.html
GSSUP	Generic Security Services Username Password (GSSUP) token is discussed in the Common Object Request Broker: Architecture and Specification version 2.6, Chapter 26 at http://www.omg.org/cgi-bin/doc?formal/01-12-01
HA	HA refers to High Availability as in the High Availability Manager component of the WebSphere Application Server. See HA Manager.
HA Manager	The High Availability (HA) Manager component of the WebSphere Application Server. For details, reference the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/crun_ha_hamanager.html
HLD	High Level Design: The document entitled “WebSphere Application Server EAL4 High Level Design”
HTML	Hypertext Markup Language

HTTP	Hypertext Transfer Protocol (HTTP) an internet protocol that is used to transfer and display hypertext and XML documents on the Web.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is an internet protocol that is used by Web servers and Web browsers to transfer and display hypermedia documents securely across the internet.
HTTP/S	Refers to both the HTTP and HTTPS protocols.
ICC	IBM Cryptography for C (ICC) is an approved FIPS 140-2 provider. More information on ICC can be found in certificate 384 at http://csrc.nist.gov/cryptval/140-1/1401val2004.htm#384
IDL	Interface Definition Language (IDL) is a declarative language in Common Object Request Broker (CORBA) that is used to describe object interfaces, without regard to object implementation.
IETF	Internet Engineering Task Force
IBM HTTP Server	IBM HTTP Server. For details, see the IBM HTTP Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.ihs.doc/info/welcome_ihs.html
IIOP	Internet Inter-ORB Protocol (IIOP) is a protocol used for communication between Common Object Request Broker Architecture (CORBA) Object Request Brokers. For information on the IIOP protocol, reference Chapter 15 of the CORBA 2.3.1 specification at http://www.omg.org/docs/formal/99-10-07.pdf
IOR	Interoperable object reference (IOR) is an object reference with which an application can make a remote method call on a CORBA object. This reference contains all the information needed to route a message directly to the appropriate server.
IT	Information Technology
J2EE	Java™ 2 Enterprise Edition (J2EE) provides a standard for developing multi-tier, enterprise services. For information on J2EE 1.4 see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/covr_j2ee.html
J2SE	Java 2 Standard Edition. WebSphere Application Server supports the Java 2 Standard Edition (J2SE) 5 specification as described in the Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tovr_migratingjava.html

JAAS	Java Authentication and Authorization Service (JAAS) is the package through which services can authenticate and authorized users while enabling the applications to remain independent from underlying technologies. For details see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/csec_jaas.html
JACC	Java Authorization Contract for Containers (JACC) is a J2EE specification that enables third party security providers to manage authorization in the application server. For details, see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/csec_jaccauthorization.html
JAX-RPC	Java API for XML-based RPC (JAX-RPC) is a specification that describes application programmer interfaces and conventions for supporting XML based remote procedure call (RPC) protocols in the Java platform. For more information, see http://jcp.org/en/jsr/detail?id=101
JCA	J2EE Connector Architecture (JCA) is a standard architecture for connecting the J2EE platform to heterogeneous enterprise information systems (EIS). For information see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tdat_jdbcconnect.html
JDBC	Java Database Connectivity (JDBC) is an industry standard for database-independent connectivity between Java code and a wide range of databases. The JDBC provides a call-level application programming interface (API) for SQL-based database access. For information on creating and configuring a JDBC provider for WebSphere Application Server, see the Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tdat_tccrtprovds.html
JDK	Java Development Kit
JFAP	JetStream Client Formats and Protocol (JFAP) is a communication protocol used by the Remote Secure Messaging Interface. The specification for the JFAP protocol is provided as an attachment to the WebSphere Application Server EAL4 Functional Specification document.
JMS	Java Message Service (JMS) is a Java API that supports the creation and communication of various messaging implementations. For more on messaging and WebSphere Application Server see the Information Center at

	http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tm_learn.html
JNDI	Java Naming Directory Interface (JNDI) is a Java extension that provides an interface for various directory and naming services in an enterprise. For details on Naming and JNDI see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6tech_nam.html
JSP	JavaServer Page files, a server module that is included in a web server application component. The module is coded in the Java scripting language and conforms to the JSP architecture identified in the J2EE V1.4 specification. For information on JavaServer Pages and WebSphere Application Server, see the Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/cweb_jov2.html
JVM	Java virtual machine (JVM) is a software implementation of a central processing unit that runs compiled Java code (applets and applications).
LDAP	Lightweight Directory Access Protocol (LDAP) is an open protocol that uses TCP/IP to provide access to information directories that support an X.500 model and it does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory. For information on configuring LDAP as the user registry with WebSphere Application Server, see http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tsec_ldap.html
LTPA	Lightweight Third Party Authentication (LTPA) is a method that the product uses to generate and validate identification information. The method supports the use of an LTPA token for passing identification information.
LTPA Token	Lightweight Third Party Authentication (LTPA) Token is a data structure containing the user ID of the caller, along with the caller's unique signature and date generated, that the TOE client code generates and passes to the TOE server code. The signature in the LTPA token is generated with the RSA algorithm using the TOE LTPA key. The TOE LTPA key is generated by the environment from a random number when the TOE is configured in the evaluated configuration.
LSD	Location Service Daemon as described in the WebSphere Application Server EAL4 Functional Specification document.
MBean	Managed Bean (MBean). See the WebSphere Application Server Information Center Glossary at

	http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/glossary.html
MDB	Message-driven bean is an enterprise bean that provides asynchronous message support and clearly separates message and business processing.
NIAP	National Information Assurance Partnership
ORB	Object Request Broker (ORB) in object-oriented programming, software that serves as an intermediary by transparently enabling objects to exchange requests and responses. For details, see the WebSphere Application Server Information Center at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6tech_orb.html
OS	Operating System
OSP	Organisational Security Policy
Permission	Indicating that one has authorization to access a resource. Privilege and permission are used to mean the same thing.
PP	Common Criteria Protection Profile.
PPC	Power PC®
Protected Resources	Methods in enterprise beans, methods and HTML pages in web server applications, the Administration Service, the Naming Service, UDDI naming resources, and messaging resources.
Remote	Any entity outside the local network address.
RMI	Remote Method Invocation (RMI) is a protocol that is used to communicate method invocations over a network. Java Remote Method Invocation is a distributed object model in which the methods of remote objects written in Java programming language can be invoked from other Java virtual machines, possibly on different hosts.
Role	A logical grouping of users that are defined by an application component provider or assembler
RPC	Remote procedure call (RPC) is a protocol that allows a program on a client computer to run a program on a server.
SAAJ	SOAP with Attachments API for Java (SAAJ) provides a standard way to send XML documents over the Internet from the Java platform. For details see http://java.sun.com/webservices/saaj/
SDK	Software Development Kit
Servlet	A server module that is included in a web server application component. The module is coded in the Java programming language and conforms to the servlet architecture identified in the J2EE V1.4 specification.

SF	Security Function. A part or parts of the TOE that have been relied upon for enforcing a closely related subset of rules from the TSP.
SFR	Security Functional Requirement
SOAP	Simple Object Access Protocol (SOAP) is described in the specification at http://www.w3.org/TR/soap/
SOF	Strength Of Function
SPI	System Programming Interface
SSL	Secure Sockets Layer (SSL) is a security protocol that provides transport layer security: authenticity, integrity, and confidentiality, for a secure connection between a client and a server. The protocol runs above TCP/IP and below application protocols.
SSO	Single signon (SSO is an authentication process in a client and server relationship in which the user can enter one name and password, and have access to more than one application. For more information on using single signon with WebSphere Application Server, see http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/tsec_msso.html
ST	Security Target
TAI	Trust association interceptor (TAI) is a mechanism by which trust is validated in the product environment for every request received by the proxy server. The method of validation is agreed upon by the proxy server and the interceptor. For information on trust associations in WebSphere Application Server, see http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/csec_trust.html
TAI Plus /TAI ++	TAI Plus refers to the Tivoli Access Manager Trust Association Interceptor Plus which is described at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/csec_trust.html
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard nonproprietary set of communication protocols that provide reliable end-to-end connections between applications over interconnected networks of different types.
TLS	Transport Layer Security (TLS) is an Internet Engineering Task Force (IETF) –defined security protocol that is based on Secure Sockets Layer (SSL). See the WebSphere Application Server Information Center for details at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/cwbs_clienttransport.html

TOE	Target Of Evaluation. An IT product or system and its associated administrator and user guidance documentation that is the subject of the evaluation.
Trusted applications, resource adapters, and providers	Enterprise applications, resource adapters, and providers that have been written by a developer who adhered to all the guidelines described in the User Guidance document.
TSF Scope of Control	
TSF	TOE Security Function. A set consisting of all hardware, software and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TSP	TOE Security Policy. A set of rules that regulate how assets are managed, protected and distributed within the TOE.
UDB	Universal Database
UDDI	Universal Description, Discovery, and Integration (UDDI) defines a way to publish and discover information about Web Services. Refer to the WebSphere Application Server Information Center for more details on the UDDI registry for WebSphere Application Server http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/cwsu_over.html
URL	Uniform Resource Locator (URL) is the unique address of a file that is accessible in a network such as the Internet. The URL includes the abbreviated name of the protocol used to access the information resource and the information used by the protocol to locate the information resource
User Guidance document	The document entitled "WebSphere Application Server AGD - Guidance". This document contains installation and configuration guidance as well as guidance for the administrator and developer. This document can be found at the following URL: http://www.ibm.com/support/docview.wss?rs=180&uid=swg24013510
Web server application	A servlet, JSP, or HTML page.
Web server application component	A server application component that conforms to the J2EE V1.4 specification. The component contains one or more web server applications. The web server applications are packaged in a WAR file and configured with a web.xml file.
WS	Web Services is often abbreviated as WS in this document. See the following for details on the Web Services for J2EE specification http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.

	jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/twbs_usewbs.html
WSDL	Web Services Description Language (WSDL) is an XML based specification for describing networked services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. For more information, see http://www.w3.org/TR/wsdl
XML	Extensible Markup Lanaguage. For information, see http://www.w3.org/XML/
z/OS platform	The supported z/OS operating system.

1 Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

1.1 TOE Overview

The TOE consists of an application server, deployment manager server, node agent server, proxy server, client, and wsadmin tool, all available from the WebSphere® Application Server 6.1 product (hereafter referred to as the *product*) provided by IBM®. The primary purpose of the product is to provide an environment for running and managing the components of user-supplied enterprise applications. In addition to its primary purpose, the product provides an environment for running clients of enterprise applications and provides tools for doing useful functions such as assembling and troubleshooting enterprise applications.

1.2 Security Target, TOE and CC Identification

Security Target (ST) Title:

WebSphere Application Server for z/OS EAL4+ Security Target

Version: 19a.0

Version Date: 14 February 2007

Author : Donna Skibbie and Kristen Clarke

TOE identification:

- WebSphere Application Server for z/OS V6.1, service level 6.1.0.2. Requires fix to APAR AK30720.

Common Criteria Identification: Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01, Version 2.2, January 2004.

Evaluated Assurance Level: EAL4, augmented with ALC_FLR.1 (Basic Flaw Remediation).

1.3 CC Conformance

This ST is [CC] Part 2 extended and Part 3 augmented to a claimed Evaluation Assurance Level of EAL4, augmented with ALC_FLR.1 (Basic Flaw Remediation).

1.3.1 PP Claims

This ST does not claim conformance to any PP for the TOE.

1.4 Strength of Functions

There is no strength of function claim because the TOE does not identify any security functional requirements for which an explicit Strength Of Function (SOF) is appropriate and does not identify any functions that are of a permutational or probabilistic nature. Therefore, a minimum SOF claim is not included for the TOE.

1.5 References

[CC] Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01, Version 2.2, January 2004.

1.6 Document Conventions

Application Notes: An application note is additional informative and non-normative text that assists the intended audience to better understand the intent of the TOE and its security features.

Application notes are identified as a footnote to the corresponding item requiring further clarification with a number in the upper-right position (e.g. FAU_GEN.1[1]). The accompanying text of the application note is then displayed at the bottom of the page containing the corresponding item.

Assignment: An assignment allows the specification of an identified parameter.

Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).

Explicitly Stated An explicitly stated requirement is a requirement which is stated outside the scope of any predefined requirements within the Common Criteria. Explicitly stated requirements are often used for identifying specific capabilities, which are not common covered by the Common Criteria. Explicitly stated requirements are identified with ".EXP" following by the component name (FIA_OBO.EXP.1).

Interpretation:	An interpretation is a clarification or further definition to a security functional or assurance requirement that has been reviewed and approved by CCIMB or the associated Common Criteria scheme representative as being acceptable to incorporate into a complying ST. CCIMB and NIAP interpretations are identified by inserting a footnote next to the corresponding security requirement component which indicates the interpretation affecting the component.
Iteration:	An iteration allows for the use of a component more than once with varying operations. Iterations are indicated with a lowercase alphabetic character (e.g. FAU_GEN.1a).
Refinement:	A refinement allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Refinements resulting from an interpretation are additionally indicated with a red font.
Selection:	A selection allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).

1.7 Structure

The structure of this document is as defined by [CC] Part 1, Annex C:

- Section 2 is the TOE description;
- Section 3 provides a statement of the TOE security environment;
- Section 4 provides the statement of IT security objectives;
- Section 5 provides a statement of IT security requirements;
- Section 6 provides the TOE summary specification, which includes the detailed specification of the IT functions; and
- Section 7 provides the rationale for the security objectives, security requirements and TOE summary specification.

2 TOE Description

This section provides the following information:

- Description of the product;
- Identification of the TOE;
- Description of the TOE evaluated configuration;
- Description of the TOE security functions.

2.1 Description of the Product

The product is a J2EE V1.4 compliant run-time environment. The primary purpose of the product is to provide an environment for running and managing user-supplied enterprise applications and their components. In addition to its primary purpose, the product provides an environment for running clients of enterprise applications and provides tools for doing useful functions such as assembling and troubleshooting enterprise applications.

The product consists of the following components:

- Product Application Server;
- Product Client;
- Product Tools and Applications;
- Product HTTP Server Plug-Ins
- Product Java 2 Software Development Kit (SDK).
- Product Deployment Management Server;
- Product Node Agent Server;
- Product Proxy Server.

Note: See the Glossary of this document for a definition of enterprise applications and for definitions of enterprise application components, which are web server applications and enterprise bean components.

The TOE was tested on the following operating system. However, the operating system is outside the scope of the TOE.

- z/OS 1.7.

The TOE was tested on this operating system. It is assumed that all hardware used within the operating environment is secured such that no potential vulnerabilities could be introduced that would circumvent the functionality described within this ST.

2.1.1 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 containers are runtime wrappers that handle system functions, such as communications and security, for enterprise application components and some types of resources. The following containers are included:

- Enterprise bean container--handles system functions for enterprise beans.
- Web server container (contains an embedded HTTP server)--handles system functions for web server applications.
- Resource adapter container--handles system functions for resources that conform to the J2EE Connector Architecture (JCA).

The services are Java API and remote interface implementations. They provide useful functions, such as directory and security that components of enterprise applications can use. A few of these services also are remotely available so that clients also can use them. The following services are included:

- Services defined and documented in Java specifications. These services are identified in the formal product documentation.
- Services defined and documented in the formal product documentation.

The resources are software modules that are used by some of the services for back-end processing. The following resources are included:

- A built-in Java Database Connectivity (JDBC) provider, which is sometimes referred to as the “WebSphere Relational Resource Adapter”-- handles back-end processing for the product JDBC API service and uses its own built-in database server for storing and retrieving storage.
- A built-in Java Message Service (JMS) Provider, which is sometimes referred to as the “JMS Provider for WebSphere”--handles back-end processing for the product messaging service.
- A naming resource--handles back-end processing for the product JNDI and COSNaming services.
- The UDDI Registry Application, which provides a directory for storing web services endpoints.
- Security resources--handles back-end processing for the product security services using a user registry in the environment.

In this evaluation, it has been tested that each available service in the Application Server is protected if the service can be accessed remotely and can be used to access a protected resource, and if the Application Server is configured in the evaluated configuration. See the glossary for a definition of the term “remote.” See Section 2.4 for a list of the protected resources. See Section 2.3 for a description of the evaluated configuration.

2.1.2 Product Client

The Product Client component is a set of containers, services, and resources that provide an environment for running clients of enterprise applications.

2.1.3 Product Tools and Applications

The Product Tools and Applications component is a set of system tools, system applications, and sample applications. Included are the following:

- The Product Administrative Console Tool, which provides a graphical user interface for managing enterprise applications and their components.
- The Product wsadmin tool, which provides a scripting interface for managing enterprise applications and their components.
- Tools for doing the following functions:
    - Installing, upgrading, and migrating the product
    - Assembling enterprise applications
    - Monitoring and tuning the runtime environment of enterprise applications
    - Troubleshooting the runtime environment of enterprise applications

2.1.4 Product HTTP Server Plug-Ins

The Product HTTP Server Plug-Ins component is a set of plug-ins for external HTTP servers. An HTTP Server Plug-in re-routes requests from an external HTTP server to the embedded HTTP server included in the web server container of the Product Application Server component.

2.1.5 Product Java 2 Software Development Kit (SDK)

The Product Java 2 SDK component is software that implements all the Java APIs defined in the Java 2 Standard Edition (J2SE) V1.4 specification. The Product Java 2 SDK is sometimes referred to as the "JDK."

2.1.6 Product Deployment Manager and Product Node Agent Servers

The Product Deployment Manager Server and Product Node Agent Server components provide additional functionality for managing multiple Product Application Servers in a distributed environment.

In this evaluation, it has been tested that each available service in the Node Agent Server and Deployment Manager Server is protected if the service can be accessed remotely and can be used to access a protected resource, and if the server is configured in the evaluated configuration. See the glossary for a definition of the term "remote." See Section 2.4 for a list of the protected resources. See Section 2.3 for a description of the evaluated configuration.

2.1.7 Product Proxy Server

The Product Proxy Server components provide additional functionality for managing the routing of HTTP requests to Application Servers in a distributed environment.

2.2 Identification of the TOE

The following table lists the product components and indicates whether each component is included in or excluded from the TOE. Both the "required" and the "optional" components are part of the TOE. This is clarified in Section 2.3.

Product Component	**WebSphere Application Server for z/OS**
Product Application Server	Required
Product Client	Required
Product Tools and applications	Required – only the product wsadmin tool
Product HTTP Server Plug-Ins	Not in TOE
Product Java 2 SDK	Not in TOE
Product Deployment Manager Server	Required
Product Node Agent Server	Required
Product Proxy Server	Optional

2.3 Description of the TOE Evaluated Configuration

2.3.1 TOE Components

The TOE components are:

- Product Application Server
- Product Client
- Product wsadmin Tool
- Product Deployment Manager Server
- Product Node Agent Server
- Product Proxy Server

2.3.1.1 Product Application Server

The Product Application Server is included in the TOE. Multiple instances of the Product Application Server can be configured on the network and in a single operating system. Each instance of the Product Application Server runs in its own process and JVM.

The Product Application Server is briefly described in the section 2.1.1 of this document. The following provides additional information about the Product Application Server and its required configuration.

2.3.1.1.1 Description of the Product Application Server

In the evaluated configuration, 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. In the evaluated configuration, the Product Application Server processes security for the following services:

- Administration service
- Naming service
- Messaging service, when the Product Application Server is configured to use the Built-In JMS Provider
- UDDI 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 a 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.

2.3.1.1.2 Required configuration of the Product Application Server

In the evaluated configuration, the Product Application Server must be configured as described in the document, "WebSphere Application Server EAL4 – AGD Guidance". In subsequent sections, this document will be references as the User Guidance document.

2.3.1.2 Product Client

The Product Client is included in the TOE. Multiple instances of the Product Client can be configured in the network or in a single node. Each instance of the Product Client runs in its own operating system process and JVM.

The Product Client is briefly described in section 2.1.2 of this document. The following provides additional information about the Product Client and how it is used and configured in the evaluated configuration.

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 Product wsadmin Tool.

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, Product Node Agent Server, or Product Deployment Manager Server.

2.3.1.3 Product wsadmin Tool

The Product wsadmin Tool is included in the TOE. It must reside in the same system unit as the Product Client and runs in the same operating system process and JVM as the Product Client.

The Product wsadmin Tool is briefly described in section 2.1.3 of this document. The following provides additional information about the Product wsadmin Tool and how it is configured in the evaluated configuration.

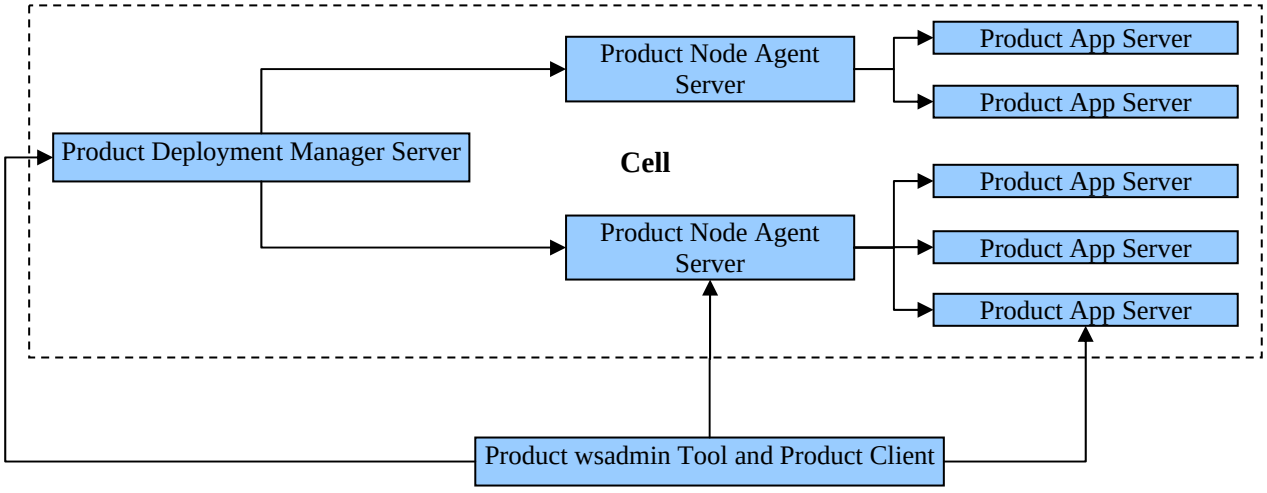
The Product wsadmin Tool is a Java client application. The administrator starts the Product wsadmin Tool by running a wsadmin.bat file as described in the next section. After the Product wsadmin Tool starts, an administrator can use this tool to execute administrative scripting commands for the purpose of managing any or all of the following servers: Product Application Server, Product Node Agent Server, or Product Deployment Manager Server. The Product wsadmin Tool processes these commands by calling the AdminClient API of the Product Client, which, in turn, calls a remote interface of the server being managed. The Product wsadmin Tool must be configured as described in the User Guidance document.

2.3.1.4 Product Deployment Manager Server and Product Node Agent Server

The Product Deployment Manager Server and Product Node Agent Server are included in the TOE. Multiple instances Product Node Agent Server can be configured on the network. Each instance runs in its own operating system process and JVM.

The Product Deployment Manager Server and Product Node Agent Server each contain one service, which is an administration service. The administration service of each server must be configured in a logical unit called a cell. Each cell consists of one Product Deployment Manager, one or more Product Node Agent Servers, and each Product Application Server residing on the same node as a Product Node Agent Server. Using this configuration, an entire cell can be managed from a single client using the Product wsadmin Tool and Product Client, as shown in the following figure:

Figure 2-1: Cell Architecture



Each Product Deployment Manager Server and Product Node Agent Server accepts requests to its administration service, processes any required security as described for AC.3 in section 6.1.2.3, and processes the request only if security processing is successful.

Each Product Deployment Manager Server and Product Node Agent Server must be configured as described in the User Guidance document.

2.3.1.5 Product Proxy Server

The Product Proxy Server is included in the TOE. Multiple instances of the Product Proxy Server can be configured on the network. Each instance runs in its own operating system process and JVM. The Product Proxy Server receives HTTP requests by remote HTTP Clients and forwards the requests to the Product Application Server.

The Product Proxy Server must be configured as described in the User Guidance document.

2.3.2 Components in the Environment during Evaluation

The following software components are not included in the TOE but were configured in the TOE environment during the evaluation of the TOE:

- Product Java 2 SDK
- Operating system
- JDBC resource and any back-end servers
- MQ JMS provider

2.3.2.1 Product Java 2 SDK

The TOE was evaluated with the Product Java 2 SDK that is included with the product. This Product 2 SDK was configured in each TOE component.

The TOE uses the following resources of the Java 2 SDK:

- APIs
- Java launcher (distributed platforms only)

2.3.2.2 Operating System

The TOE was evaluated with each of the operating systems listed in the section "Description of Product." The operating system was configured on each system unit in which a TOE component resides.

The TOE components use the following resources of the operating system:

- Process, threads, and mutex
- User registry
- File system
- TCP

- Operating system APIs

2.3.2.3 JDBC Provider and Back-end Servers

The TOE was evaluated with the following JDBC provider, as well as the back-end server used by this provider:

- IBM DB2 UDB for z/OS v8

The provider was configured to run inside the Product Application Server component of the TOE and to access data stored in the back-end server.

The UDDI and Built-in JMS Resource services of the TOE use the provider and back-end server to store UDDI and messaging data.

2.3.2.4 MQ JMS Provider

The TOE was evaluated with the following MQ provider, which was configured in the environment of the Product Application Server:

- IBM WebSphere MQ 5.3.1 for z/OS

This provider was not used for JMS functions during the evaluation because the Built-In Messaging JMS Provider was used instead. However, this provider was configured in the environment to ensure that all claimed security functions worked properly with the provider configured.

2.4 Description of the TOE Security Functions

The TOE provides a set of identification, access control, and security management functions. These functions are designed to protect sensitive resources from malicious remote callers. A sensitive resource is defined as a resource that:

- Resides in a server TOE component
- Can be accessed by a remote caller, which is an entity residing outside the server TOE component in which the sensitive resource resides.
- Could be used by a remote caller to compromise the security of a deployed web server application or deployed enterprise bean.

The following are the sensitive resources of the TOE:

- Methods and static web content of deployed user web server applications (user web server applications that are deployed in the TOE)
- Methods of deployed user enterprise beans (user enterprise beans that are deployed in the TOE)
- Transactions and activities of deployed user web server applications, deployed enterprise beans, and the TOE
- The TOE naming directory
- The TOE UDDI registry directory
- TOE configuration data

- TOE files
- TOE runtime state
- TOE local bus, queue destinations, temporary destinations, topic space, topic space root, and topics
- TOE location service entries

2.4.1 Identification and Re-Identification

The TOE provides functions that identify a remote caller when the caller requests access to a sensitive resource. These functions are:

- Ident.1—This function identifies a remote caller that requests access to a sensitive resource using a remote HTTP/S Interface of the TOE.
- Ident.2—This function identifies a remote caller that requests access to a sensitive resource using a remote ORB interface of the TOE.
- Ident.3—This function identifies a remote caller that requests access to a sensitive resource using a remote JMS interface of the TOE.
- Ident.4—This function re-identifies a remote caller that requests access to a sensitive resource using a remote web services interface of the TOE.
- Ident.5—This function identifies a remote caller that requests access to a connection to the remote HA Manager interface of the TOE.
- Ident.6—This function permits a method in a deployed user web server application or enterprise bean to assume the identity of another user.
- Ident.7—This function identifies a remote caller when the remote caller attempts to access a sensitive transaction using the remote Web Services Transactions (WS-Transactions) interface of the TOE.

See Section 6.1.1, "Identification and Re-Identification" for more information.

2.4.2 Access Control

The TOE provides access control functions that allow only authorized remote callers to access to the sensitive resources. The following are the access control functions:

- AC.1—This function controls access from remote callers to methods and HTML pages in deployed web server applications.
- AC.2—This function controls access from remote callers to Methods in deployed enterprise beans (including methods that are deployed as web services endpoints).
- AC.3—This function controls access from remote callers to TOE configuration data and TOE runtime state. The function also controls access from remote callers to TOE files.
- AC.4—This function controls access from remote callers to the TOE naming directory.
- AC.5—This function controls access from remote callers to transactions and activities.
- AC.6—This function controls access from remote callers to messaging resources (local bus, queue destinations, temporary destinations, topic space, topic space root, and topics).
- AC.7—This function controls access from remote callers to UDDI resources.
- AC.8—This function controls access from remote callers to location service resources.
- AC.9—This function controls access from remote callers to methods and attributes in user MBeans.

See Section 6.1.2, "Access Control" for more information.

2.4.3 System Management

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

See Section 6.1.3, "System Management (SM.1.1, SM.1.2, SM.1.3, and SM.1.4)" for more information.

3 TOE Security Environment

3.1 Introduction

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 employed.

The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organisational security policies which the product is designed to comply.

3.2 Threats

The assumed security threats are listed below:

3.2.1 Threats countered by the TOE

[T.ACCESS_RES] A caller gains access to a resource without the correct authority to access that resource.

[T.ACCESS_TOE] An unidentified caller gains access to a protected resource.

[T.NETWORK] Data transferred between workstations is disclosed to, or modified by unidentified users or processes, either directly or indirectly.

3.2.2 Threats countered by the TOE Environment

[T.APP] The misconfiguration, inappropriate installation, or inappropriate development of applications and operating system that the TOE interfaces with, compromises the TOE security policies or security functions used to protect sensitive resources from access by unauthorized remote callers.

3.3 Organisational Security Policies (OSPs)

The TOE complies with the following OSP:

[P.ACCESS] The right to access a resource is determined on the basis of association of user or group IDs to roles and of roles to resources.

3.4 Assumptions

This section provides the minimum connectivity, physical, and procedural measures required to maintain security of the WebSphere Application Server product.

3.4.1 IT environment aspects

[A.AUTH] 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.

[A.APP] 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 also 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.

3.4.2 Physical aspects

[A.PROTECT] 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 secured.

3.4.3 Personnel Aspects

[A.ADMIN] 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 also is assumed that this individual will comply with all the guidelines specified in the User Guidance document.

4 Security Objectives

4.1 Security Objectives for the TOE

[O.ACCESS] The TOE must ensure that only those callers with the correct authority are able to access an object.

[O.IDENTIFY] The TOE must ensure that all callers are identified before they access a protected resource.

[O.MANAGE] The TOE must allow administrators to effectively manage the TOE and that this can be performed remotely only by authorised callers.

4.2 Security Objectives for the TOE Environment

[O.ADMIN] Those responsible for the TOE and its environment are competent and trustworthy individuals, capable of managing the TOE and its environment, and the security of the information it contains. In addition, those responsible for the TOE and its environment must comply with the guidelines listed in the assumption A.ADMIN.

[O.APP] Those responsible for the TOE must ensure that the interfacing applications do not compromise the security of the TOE and that they are installed and configured in accordance with the manufacturer's instructions and/or the evaluated configuration where applicable. In addition, those responsible for the TOE must ensure that the developers of the applications are trusted to comply with the Guidelines listed in the assumption A.APP.

[O.ATTR] The IT Environment shall maintain User and Group mappings for callers.

[O.AUTH] The IT Environment shall process authentication requests by remote callers.

[O.PROTECT] Those responsible for the TOE must ensure that procedures exist to ensure that data transferred between workstations is secured from disclosure, interruption or tampering.

[O.RECOVER] Those responsible for the TOE must ensure that procedures are provided to ensure that after system failure or other discontinuity, recovery without a security compromise is obtained.

[O.TRANSFER] The IT Environment shall provide data encryption to protect network traffic.

5 Security Requirements

This section specifies the Security Functional Requirements (SFRs) for the TOE and organises the SFRs by class.

Within the text of each SFR, the selection, assignment, and refinement operations (as defined within [CC]) are formatted according to the conventions specified in Section 1.6.

Note: FIA_OBO.EXP.1 is an explicitly stated TOE security requirement, and although based on [CC], it has not been specified using CC Part 2 functional components.

5.1 TOE Security Functional Requirements

The following table summarises the SFRs:

Table 1: TOE Security Functional Requirements

CLASS	FAMILY	COMPONENT	ELEMENT
FDP	FDP_ACC	FDP_ACC.1a	FDP_ACC.1a.1
			FDP_ACC.1a.2
		FDP_ACC.1b	FDP_ACC.1b.1
			FDP_ACC.1b.2
		FDP_ACC.1c	FDP_ACC.1c.1
			FDP_ACC.1c.2
		FDP_ACC.1d	FDP_ACC.1d.1
			FDP_ACC.1d.2
		FDP_ACC.1e	FDP_ACC.1e.1
			FDP_ACC.1e.2
		FDP_ACC.1f	FDP_ACC.1f.1
			FDP_ACC.1f.2
		FDP_ACC.1g	FDP_ACC.1g.1
			FDP_ACC.1g.2

CLASS	FAMILY	COMPONENT	ELEMENT
		FDP_ACC.1h	FDP_ACC.1h.1
			FDP_ACC.1h.2
		FDP_ACC.1i	FDP_ACC.1i.1
			FDP_ACC.1i.2
	FDP_ACF	FDP_ACF.1a	FDP_ACF.1a.1
			FDP_ACF.1a.2
			FDP_ACF.1a.3
			FDP_ACF.1a.4
		FDP_ACF.1b	FDP_ACF.1b.1
			FDP_ACF.1b.2
			FDP_ACF.1b.3
			FDP_ACF.1b.4
		FDP_ACF.1c	FDP_ACF.1c.1
			FDP_ACF.1c.2
			FDP_ACF.1c.3
			FDP_ACF.1c.4
		FDP_ACF.1d	FDP_ACF.1d.1
			FDP_ACF.1d.2
			FDP_ACF.1d.3
			FDP_ACF.1d.4
		FDP_ACF.1e	FDP_ACF.1e.1
			FDP_ACF.1e.2
			FDP_ACF.1e.3
			FDP_ACF.1e.4
		FDP_ACF.1f	FDP_ACF.1f.1

CLASS	FAMILY	COMPONENT	ELEMENT
			FDP_ACF.1f.2
			FDP_ACF.1f.3
			FDP_ACF.1f.4
		FDP_ACF.1g	FDP_ACF.1g.1
			FDP_ACF.1g.2
			FDP_ACF.1g.3
			FDP_ACF.1g.4
		FDP_ACF.1h	FDP_ACF.1h.1
			FDP_ACF.1h.2
			FDP_ACF.1h.3
			FDP_ACF.1h.4
		FDP_ACF.1i	FDP_ACF.1i.1
			FDP_ACF.1i.2
			FDP_ACF.1i.3
			FDP_ACF.1i.4
FIA	FIA_OBO.EXP	FIA_OBO.EXP.1	FIA_OBO.EXP.1.1
	FIA_UID	FIA_UID.1	FIA_UID.1.1
			FIA_UID.1.2
	FIA_USB	FIA_USB.1	FIA_USB.1.1
FMT	FMT_MSA	FMT_MSA.1a	FMT_MSA.1a.1
		FMT_MSA.1b	FMT_MSA.1b.1
		FMT_MSA.1c	FMT_MSA.1c.1
		FMT_MSA.3a	FMT_MSA.3a.1
			FMT_MSA.3a.2
		FMT_MSA.3b	FMT_MSA.3b.1

CLASS	FAMILY	COMPONENT	ELEMENT
			FMT_MSA.3b.2
		FMT_MSA.3c	FMT_MSA.3c.1
			FMT_MSA.3c.2
		FMT_MSA.3d	FMT_MSA.3d.1
			FMT_MSA.3d.2
	FMT_SMF	FMT_SMF.1	FMT_SMF.1.1
	FMT_SMR	FMT_SMR.1	FMT_SMR.1.1
			FMT_SMR.1.2

5.1.1 Access Control (FDP)

FDP_ACC.1a: Subset access control

FDP_ACC.1a.1 The TSF shall enforce the [**web server applications access control policy**] on [

a) Subjects

a) Remote caller

b) Objects

a) Protected methods of web server applications

c) Operations

a) Defined by the application developer].

FDP_ACC.1b: Subset access control

FDP_ACC.1b.1 The TSF shall enforce the [**enterprise beans access control policy**] on [

a) Subjects

a) Remote caller

b) Objects

a) Protected methods of enterprise beans

c) Operations

a) Defined by the application developer].

FDP_ACC.1c: Subset access control

FDP_ACC.1c.1 The TSF shall enforce the [**configuration data, files, and runtime state access control policy**] on [

a) Subjects

a) Remote caller

b) Objects

a) TOE configuration data

b) TOE files

c) TOE runtime state

c) Operations

a) Read TOE configuration data

b) Write to non-sensitive areas within the TOE configuration data

c) Write to highly sensitive areas within the TOE configuration data

d) Upload and download TOE files

e) Read the TOE runtime state

f) Modify the TOE runtime state].

FDP_ACC.1d: Subset access control

FDP_ACC.1d.1 The TSF shall enforce the [**naming directory access control policy**] on [

a) Subjects

a) Remote caller

b) Objects

a) TOE naming directory

c) Operations

a) Delete an entry from the TOE naming directory

b) Create an entry into the TOE naming directory

c) Write to an entry within the TOE naming directory

d) Read an entry within the TOE naming directory].

FDP_ACC.1e: Subset access control

FDP_ACC.1e.1 The TSF shall enforce the [**transactions and activities access control policy**] on [

a) Subjects

a) Remote caller

b) Objects

a) Transactions and activities

c) Operations

a) All transactions and activities operations].

FDP_ACC.1f: Subset access control

FDP_ACC.1f.1 The TSF shall enforce the [**messaging access control policy**] on [

a) Subjects

a) Remote caller

b) Objects

a) Protected resources of the built-in JMS Provider (the local bus, queue destination, temporary destination, topic space, topic space root and topics)

c) Operations

a) Browse

b) Connect

c) Create

d) Receive

e) Send].

FDP_ACC.1g: Subset access control

FDP_ACC.1g.1 The TSF shall enforce the [**UDDI access control policy**] on [

a) Subjects

a) Remote caller

b) Objects

a) Protected resources of the UDDI registry directory

c) Operations

a) All operations on the UDDI SOAP V1, V2 and V3 Publish API through the HTTP interface

b) All operations on the UDDI SOAP V3 Custody Transfer API through the HTTP interface

c) All operations on the UDDI SOAP V3 Security API through the HTTP interface

d) All operations on the V2 Publish API through the ORB interface].

FDP_ACC.1h : Subset access control

FDP_ACC.1h.1 The TSF shall enforce the [**location service access control policy**] on [

a) Subjects

a) Remote caller

b) Objects

a) Protected location service resources

c) Operations

a) Register Server

b) Unregister Server

c) Register Object Adapters

d) Unregister Object Adapters].

FDP_ACC.1i: Subset access control

FDP_ACC.1i.1 The TSF shall enforce the [**user MBean access control policy**] on [

a) Subjects

a. Remote caller

b) Objects

a) Protected methods and attributes of user MBeans

c) Operations

a) Invoke, read, write].

FDP_ACF.1a: Security attribute based access control[1]

FDP_ACF.1a.1 The TSF shall enforce the [**web server applications access control policy**] to objects based on the following **information provided in** Table 2:

Table 2: Mapping of Subjects/Objects to Security Attributes for the Web Server Applications Access Control Policy

Subjects	***Objects***	***Operations***	***Security Attributes***
Remote caller[2]	*Protected methods of Web Server Applications*	*Defined by the application developer*	*Application-Specific Role*

FDP_ACF.1a.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if**: [

- **The user ID of the caller is mapped to an application-specific role; or**
- **A group ID of the caller is mapped to an application-specific role;**

and

- **The application-specific role has permission to access the protected resource.**]

FDP_ACF.1a.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

[1] Elements 3 and 4 of this requirement have been modified per NIAP interpretation I-0407.

[2] A caller is a user from a remote JVM.

FDP_ACF.1a.4 The TSF shall explicitly deny access of subjects to objects based on the: [***no additional rules***].

FDP_ACF.1b: Security attribute based access control[3]

FDP_ACF.1b.1 The TSF shall enforce the [**enterprise beans access control policy**] to objects based on the following **information provided in Table 3:**

Table 3: Mapping of Subjects/Objects to Security Attributes for the Enterprise Beans methods Access Control Policy

Subjects	***Objects***	***Operations***	***Security Attributes***
Remote caller[4]	*Protected methods of enterprise beans*	*Defined by the application developer*	*Security attributes defined by Application-Specific Role*

FDP_ACF.1b.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if**: [

- **The user ID of the caller is mapped to an application-specific role; or**
- **A group ID of the caller is mapped to an application-specific role;**

and

- **The application-specific role has permission to access the protected resource.**].

FDP_ACF.1b.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1b.4 The TSF shall explicitly deny access of subjects to objects based on the: [***no additional rules***].

FDP_ACF.1c: Security attribute based access control[5]

FDP_ACF.1c.1 The TSF shall enforce the [**configuration data, files, and runtime state access control policy**] to objects based on the following **information provided in** Table 4:

[3] Elements 3 and 4 of this requirement have been modified per NIAP interpretation I-0407.

[4] A caller is a user from a remote JVM.

[5] Elements 3 and 4 of this requirement have been modified per NIAP interpretation I-0407.

Table 4: Mapping of Subjects/Objects to Security Attributes for the Configuration Data, Files, and Runtime State Access Control Policy

Subjects	***Objects***	***Operations***	***Security Attributes***[6]
Remote caller[7]	*TOE configuration data*	*Read*	*Administrator role* *Configurator role* *Monitor role* *Operator role* *Deployer (configuration data for applications only)*
		Modify *Applies to all attributes except the attributes that map user/group IDs to administration roles.* *Note: This includes the attributes listed in SM 1.4 except for the runtime attribute that stores the list of registered UDDI publishers.*	*Administrator role* *Configurator role* *Deployer (configuration data for applications only)*
		Modify attributes that map user/group IDs to administration roles.	*AdminSecurityManager role*

[6] The security attributes to objects within the Configuration Data, Files, and Runtime State Access Control Policy consist of the pre-defined roles implemented in WebSphere Application Server. These pre-defined roles are hardcoded with a pre-defined set of privileges. Therefore, the only way a remote caller can inherit the appropriate permission to perform an operation is for the user ID or group ID of the remote caller to be mapped to a role that has sufficient permissions. See section 6.1.2.3 for further information.

[7] A caller is a user from a remote JVM.

	TOE files	*Upload and download files*	*Administrator role* *Configurator role* *Monitor role* *Operator role* *Deployer role* *AdminSecurityManager role*
	TOE runtime state	*Read*	*Administrator role* *Configurator role* *Monitor role* *Operator role* *Deployer(application runtime state only)*
		Modify *Note: this includes the runtime attribute that stores the list of registered UDDI publishers.*	*Administrator role* *Operator role* *Deployer(application runtime state only)*

FDP_ACF.1c.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if**: [

- **The requested resource is TOE configuration data and:**
  - **The requested operation is to read TOE configuration data and**
    - **The user ID of the caller is mapped to one of the following administration roles (Administrator, Configurator, Monitor, Operator, or Deployer (configuration for applications data only));**

      or
    - **A group ID of the caller is mapped to one of the following administration roles (Administrator,**

Configurator, Monitor, Operator, or Deployer (configuration for applications data only));

or

- **The requested operation is to modify any attributes except the attributes that map user/group IDs to administration roles.**
  - **The user ID of the caller is mapped to one of the following administration roles (Administrator, Configurator, or, for application data only, Deployer);**

    or

  - **A group ID of the caller is mapped to one of the following administration roles (Administrator, Configurator, or, for application data only, Deployer);**

or

- **The requested operation is to modify attributes that map user/group IDs to administration roles and**
  - **The user ID of the caller is mapped to the following administration role (AdminSecurityManager);**

    or

  - **A group ID of the caller is mapped to the following administration role (AdminSecurityManager);**

or

- **The requested resource is TOE files and:**
  - **The requested operation is to upload or download TOE files and**
    - **The user ID of the caller is mapped to one of the following administration roles (Administrator, Configurator, Monitor, Operator, Deployer, or AdminSecurityManager);**

      or

    - **A group ID of the caller is mapped to one of the following administration roles (Administrator, Configurator, Monitor, Operator, Deployer, or AdminSecurityManager);**

or

- **The requested resource is TOE runtime state and:**

- **The requested operation is read access to the TOE runtime state and**
  - **The user ID of the caller is mapped to one of the following administration roles (Administrator, Configurator, Monitor, Operator, or Deployer (for the runtime state of applications only));**

    or
  - **A group ID of the caller is mapped to one of the following administration roles (Administrator, Configurator, Monitor, Operator, or Deployer (for the runtime state of applications only));**

  or
- **The requested operation is to modify the TOE runtime state and**
  - **The user ID of the caller is mapped to one of the following administration roles (Administrator, Operator, or Deployer (for the runtime state of applications only));**

    or
  - **A group ID of the caller is mapped to one of the following administration roles (Administrator ,Operator, or Deployer (for the runtime state of applications only)).**]

FDP_ACF.1c.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1c.4 The TSF shall explicitly deny access of subjects to objects based on the: [***no additional rules***].

FDP_ACF.1d: Security attribute based access control[8]

FDP_ACF.1d.1 The TSF shall enforce the [**naming directory access control policy**] to objects based on the following **information provided in** Table 5:

Table 5: Mapping of Subjects/Objects to Security Attributes for the Naming Directory Access Control Policy

Subjects	***Objects***	***Operations***	***Security Attributes***[9]

[8] Elements 3 and 4 of this requirement have been modified per NIAP interpretation I-0407.

[9] The security attributes to objects within the Naming Directory Access Control Policy consist of the pre-defined roles implemented in WebSphere Application Server. These pre-defined roles are hardcoded with a pre-defined set of privileges. Therefore, the only way a remote caller can inherit the appropriate permission to perform an operation is for the user ID or group ID of the remote caller to be mapped to a role that has sufficient permissions. See section 6.1.2.4 for further information.

Remote caller[10]	*TOE naming directory*	*Delete access*	*COSNamingDelete Role*
		Create access	*COSNamingDelete Role* *COSNamingCreate Role*
		Read access	*COSNamingDelete Role* *COSNamingCreate Role* *COSNamingRead Role* *COSNamingWrite Role*
		Write access	*COSNamingDelete Role* *COSNamingCreate Role* *COSNamingWrite Role*

FDP_ACF.1d.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if**: [

- **The requested operation is to delete an entry from the TOE naming directory and**
  - **The user ID of the caller is mapped to the following naming role (COSNamingDelete);**

    or
  - **A group ID of the caller is mapped to the following naming role (COSNamingDelete);**

  or
- **The requested operation is to create an entry in the TOE naming directory and**
  - **The user ID of the caller is mapped to one of the following naming roles (COSNamingDelete or COSNamingCreate);**

    or
  - **A group ID of the caller is mapped to one of the following naming roles (COSNamingDelete or COSNamingCreate);**

  or

[10] A caller is a user from a remote JVM.

- **The requested operation is to write to an entry within the TOE naming directory and**
  - **The user ID of the caller is mapped to one of the following naming roles (COSNamingDelete, COSNamingCreate, or COSNamingWrite);**

    or
  - **A group ID of the caller is mapped to one of the following naming roles (COSNamingDelete, COSNamingCreate, or COSNamingWrite);**

or

- **The requested operation is to read from an entry within the TOE naming directory and**
  - **The user ID of the caller is mapped to one of the following naming roles (COSNamingDelete, COSNamingCreate, COSNamingRead, or COSNamingWrite);**

    or
  - **A group ID of the caller is mapped to one of the following naming roles (COSNamingDelete, COSNamingCreate, COSNamingRead, or COSNamingWrite).**]

FDP_ACF.1d.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1d.4 The TSF shall explicitly deny access of subjects to objects based on the: [***no additional rules***].

FDP_ACF.1e: Security attribute based access control[11]

FDP_ACF.1e.1 The TSF shall enforce the [**transactions and activities access control policy**] to objects based on the following **information provided in** Table 6:

Table 6: Mapping of Subjects/Objects to Security Attributes for the Transactions and Activities Access Control Policy

Subjects	***Objects***	***Operations***	***Security Attributes[12]***

[11] Elements 3 and 4 of this requirement have been modified per NIAP interpretation I-0407.

[12] The security attributes to objects within the Transactions and Activities Access Control Policy consists of the pre-defined role, Administrator, implemented in WebSphere Application Server. This pre-defined role is hardcoded with a pre-defined set of privileges. Therefore, the only way a remote caller can inherit the appropriate permission to perform an operation is for the user ID or group ID of the remote caller to be mapped to a role that has sufficient permissions. See section 6.1.2.5 for further information.

Remote caller[13]	*Transactions and activities*	*All operations of transactions and activities*	*Administrator Role*

FDP_ACF.1e.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if**: [

- **The requested operation is to perform an operation on a TOE transaction or activity and**
  - **The user ID of the caller is mapped to the following administration role (Administrator);**

    or
  - **A group ID of the caller is mapped to the following administration role (Administrator).**]

FDP_ACF.1e.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1e.4 The TSF shall explicitly deny access of subjects to objects based on the: [***no additional rules***].

FDP_ACF.1f: Security attribute based access control[14]

FDP_ACF.1f.1 The TSF shall enforce the [**messaging access control policy**] to objects based on the following **information provided in Table 7**:

Table 7: Mapping of Subjects/Objects to Security Attributes for the Messaging Access Control Policy

Subjects	***Objects***	***Operations***	***Security Attributes***[15]
Remote caller	*Local Bus*	*Connect to the local bus for messaging services.*	*Bus connector Role*
	Queue destination	*Create a queue destination.*	*Creator Role*

[13] A caller is a user from a remote JVM.

[14] Elements 3 and 4 of this requirement have been modified per NIAP interpretation I-0407.

[15] The security attributes to objects within the Special Messaging Access Control Policy consist of the pre-defined roles implemented in WebSphere Application Server. These pre-defined roles are hardcoded with a pre-defined set of privileges. Therefore, the only way a remote caller can inherit the appropriate permission to perform an operation is for the user ID or group ID of the remote caller to be mapped to a role that has sufficient permissions. See section 6.1.2.6 for further information.

		Send a message to a queue destination.	*Sender Role*
		Receive a message from a queue destination.	*Receiver Role*
		Browse messages within a queue destination.	*Browser Role*
	Temporary destination	*Create a temporary destination.*	*Creator Role*
		Send a message to a temporary destination.	*Sender Role*
		Receive a message from a temporary destination.	*Receiver Role*
		Browse messages within a temporary destination.	*Browser Role*
	Topic Space	*Send a message to a topic space*	*Sender Role*
		Receive a message from a topic space	*Receiver Role*
	Topic Space Root	*Send a message to a topic space root*	*Sender Role*
		Receive a message from a topic space root	*Receiver Role*
	Topics	*Send a message to a topic*	*Sender Role*
		Receive a message from a topic	*Receiver Role*

FDP_ACF.1f.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if**: [

- **The Built-in JMS Provider is installed and configured on the TOE;**

and

- **The requested resource is Local Bus and:**
  - **The requested operation is to connect to the local bus for messaging services. and**
    - **The user ID of the caller is mapped to the Bus Connector messaging role;**

      or
    - **A group ID of the caller is mapped to the Bus Connector messaging role;**

  or

- **The requested resource is protected Queue Destination and:**
  - **The requested operation is to create a queue destination and**
    - **The user ID of the caller is mapped to the Creator messaging role;**

      or
    - **A group ID of the caller is mapped to the Creator messaging role;**

    or
  - **The requested operation is to send a message to a queue destination and**
    - **The user ID of the caller is mapped to the Sender messaging role;**

      or
    - **A group ID of the caller is mapped to the Sender messaging role;**

    or
  - **The requested operation is to receive a message from a queue destination and**
    - **The user ID of the caller is mapped to the Receiver messaging role;**

      or
    - **A group ID of the caller is mapped to the Receiver messaging role;**

or

- **The requested operation is to browse messages within a queue destination and**
  - **The user ID of the caller is mapped to the Browser messaging role;**

    or

  - **A group ID of the caller is mapped to the Browser messaging role;**

or

- **The requested resource is protected Temporary Destination and:**
  - **The requested operation is to create a temporary destination and**
    - **The user ID of the caller is mapped to the Creator messaging role;**

      or

    - **A group ID of the caller is mapped to the Creator messaging role;**

    or
  - **The requested operation is to send a message to a temporary destination and**
    - **The user ID of the caller is mapped to the Sender messaging role;**

      or

    - **A group ID of the caller is mapped to the Sender messaging role;**

    or
  - **The requested operation is to receive a message from a temporary destination and**
    - **The user ID of the caller is mapped to the Receiver messaging role;**

      or

    - **A group ID of the caller is mapped to the Receiver messaging role;**

    or
  - **The requested operation is to browse messages within a temporary destination and**
    - **The user ID of the caller is mapped to the Browser messaging role;**

or

- **A group ID of the caller is mapped to the Browser messaging role;**

or

- **The requested resource is Topic Space and:**
  - **The requested operation is to send a message to a topic space and**
    - **The user ID of the caller is mapped to the Sender messaging role;**

      or

    - **A group ID of the caller is mapped to the Sender messaging role;**

    or

  - **The requested operation is to receive a message from a topic space and**
    - **The user ID of the caller is mapped to the Receiver messaging role;**

      or

    - **A group ID of the caller is mapped to the Receiver messaging role;**

or

- **The requested resource is Topic Space Root and:**
  - **The requested operation is to send a message to a topic space root and**
    - **The user ID of the caller is mapped to the Sender messaging role;**

      or

    - **A group ID of the caller is mapped to the Sender messaging role;**

    or

  - **The requested operation is to receive a message from a topic space root and**
    - **The user ID of the caller is mapped to the Receiver messaging role;**

      or

    - **A group ID of the caller is mapped to the Receiver messaging role;**

or

- **The requested resource is Topics and:**
  - **The requested operation is to send a message to a topic and**
    - **The user ID of the caller is mapped to the Sender messaging role;**

      or
    - **A group ID of the caller is mapped to the Sender messaging role;**

    or
  - **The requested operation is to receive a message from a topic and**
    - **The user ID of the caller is mapped to the Receiver messaging role;**

      or
    - **A group ID of the caller is mapped to the Receiver messaging role.]**

FDP_ACF.1f.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1f.4 The TSF shall explicitly deny access of subjects to objects based on the: [***no additional rules***].

FDP_ACF.1g: Security attribute based access control[16]

FDP_ACF.1g.1 The TSF shall enforce the [**UDDI access control policy**] to objects based on the following **information provided in Table 8:**

Table 8: Mapping of Subjects/Objects to Security Attributes for the UDDI Access Control Policy

Subjects	***Objects***	***Operations***	***Security Attributes[17]***
Remote caller	*Protected UDDI registry resources through the HTTP interface*	*All operations on the SOAP V1, V2 and V3 Publish API*	*SOAP_Publish_User or V3SOAP_Publish_User_Role, and* *List of registered UDDI Publishers*

[16] Elements 3 and 4 of this requirement have been modified per NIAP interpretation I-0407.

[17] The security attributes to objects within the Special UDDI Access Control Policy consists of the pre-defined UDDI Publisher roles, implemented in WebSphere Application Server. These pre-defined roles are hardcoded with a pre-defined set of privileges. Therefore, the only way a remote caller can inherit the appropriate permission to perform an operation is is for the user ID or group ID of the remote caller to be mapped to a role that has sufficient permissions. See section 6.1.2.7 for further information.

		All operations on the SOAP V3 Custody Transfer API	*V3SOAP_CustodyTransfer _User_Role, and* *List of registered UDDI*
		All operations on the SOAP V3 Security API	*V3SOAP_Security_User_R ole* *List of registered UDDI Publishers*
	Protected UDDI registry resources through the ORB interface	*All operations on the V2 Publish API*	*EJB_Publish_Role*

FDP_ACF.1g.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if**: [

- **The UDDI Registry Application is installed and configured on the TOE;**

and

- **The requested resource is protected UDDI registry resources :**
  - **The requested operation is an operation on the UDDI SOAP V1, V2, or V3 Publish API through the HTTP interface**
    - **The user ID of the caller is mapped to one of the following UDDI roles (SOAP_Publish_User or V3SOAP_Publish_User_Role) and is identified within the list of registered UDDI Publishers;**

    or
  - **The requested operation is an operation on the UDDI SOAP V3 Custody Transfer API through the HTTP interface**
    - **The user ID of the caller is mapped to one of the following UDDI roles (V3SOAP_CustodyTransfer_User_Role) and is identified within the list of registered UDDI Publishers;**

    or
  - **The requested operation is an operation on the UDDI V3SOAP Security User API through the HTTP interface**

- **The user ID of the caller is mapped to one of the following UDDI roles (V3SOAP_Security_User_Role) and is identified within the list of registered UDDI Publishers;**

or

- **The requested operation is an operation on the V2 Publish API through the ORB interface**
  - **The user ID of the caller is mapped to the following UDDI role (EJB_Publish_Role).**]

FDP_ACF.1g.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1g.4 The TSF shall explicitly deny access of subjects to objects based on the: [***no additional rules***].

FDP_ACF.1h: Security attribute based access control[18]

FDP_ACF.1h.1 The TSF shall enforce the [**location service access control policy**] to objects based on the following **information provided in Table 9:**

Table 9: Mapping of Subjects/Objects to Security Attributes for the Location Service Access Control Policy

Subjects	***Objects***	***Operations***	***Security Attributes[19]***
Remote caller	*Protected location service resources*	*Register a server*	*WebSphere Application Server ID*
		Unregister a server	
		Register an object adapter	
		Unregister an object adapter	

FDP_ACF.1h.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if**: [

- **The requested resource is protected location service resources and:**
  - **The requested operation is to register a server and**

[18] Elements 3 and 4 of this requirement have been modified per NIAP interpretation I-0407.

[19] The security attributes to objects within the Location Service Access Control Policy consists of the pre-defined user, the WebSphere server ID, implemented in WebSphere Application Server. This pre-defined user is hardcoded with a pre-defined set of privileges. Therefore, the only way a remote caller can inherit the appropriate permission to perform an operation is to become authenticated with the WebSphere server ID. See section 6.1.2.8 for further information.

- **The user ID of the caller is mapped to the following identity (WebSphere Application Server ID);**

or

- **The requested operation is to unregister a server and**
  - **The user ID of the caller is mapped to the following identity (WebSphere Application Server ID);**

or

- **The requested operation is to register an object adapter and**
  - **The user ID of the caller is mapped to the following identity (WebSphere server ID);**

or

- **The requested operation is to unregister an object adapter and**
  - **The user ID of the caller is mapped to the following identity (WebSphere server ID).]**

FDP_ACF.1h.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1h.4 The TSF shall explicitly deny access of subjects to objects based on the: [***no additional rules***].

FDP_ACF.1i: Security attribute based access control[20]

FDP_ACF.1i.1 The TSF shall enforce the [**user MBean access control policy**] to objects based on the following **information provided in Table 10**:

Table 10: Mapping of Subjects/Objects to Security Attributes for the User MBean Access Control Policy

Subjects	***Objects***	***Operations***	***Security Attributes***
Remote caller[21]	*Protected methods in user MBeans*	*invoke*	*One or more Administration roles*[22]
	Protected attributes in	*read*	*One or more Administration roles*

[20] Elements 3 and 4 of this requirement have been modified per NIAP interpretation I-0407.

[21] A caller is a user from a remote JVM.

[22] The Administration roles are: AdminSecurityManager, Administrator, Configurator, Deployer, Operator, and Monitor.

	user MBeans	*write*	*One or more Administration roles*

FDP_ACF.1i.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if**: [

- **The user ID of the caller is mapped to an administration role; or**
- **A group ID of the caller is mapped to an administration role;**

and

- **The administration role has permission to access the protected resource.**]

FDP_ACF.1i.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1i.4 The TSF shall explicitly deny access of subjects to objects based on the: [***no additional rules***].

5.1.2 Identification & Authentication (FIA)

FIA_OBO.EXP.1: Perform actions on behalf of another user

FIA_OBO.EXP.1.1 The TSF shall provide applications which have previously been successfully authenticated by the environment with the capability to perform operations on behalf of another user as follows:

a) The application shall obtain all privileges assigned to the claimed identity only if the user is successfully re-authenticated by the environment as the other user; or

b) The application shall obtain all privileges assigned to the TSF supplied identity only if specifically allowed by the TSF to operate with a TSF supplied identity."

FIA_UID.1: Timing of identification

FIA_UID.1.1 The TSF shall allow [**access to a method or static web content that is not configured with a security constraint or access to a method or static web content that is configured with the security constraint of the "Everyone" role**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1: User-subject binding[23]

FIA_USB.1.1 The TSF shall associate the **following** user security attributes with subjects acting on the behalf of that user**: [roles]**.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [none].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [none].

[23] FIA_USB.1 has been modified per international interpretation 137.

5.1.3 Security Management (FMT)

FMT_MSA.1a: Management of security attributes

FMT_MSA.1a.1 The TSF shall enforce the [**web server applications access control policy, the enterprise beans access control policy, the naming directory access control policy, and the messaging access control policy**] to restrict the ability to [***write or delete***] the security attributes

- [**Mappings of user/group IDs to application-defined roles,**
- **Mappings of user/group IDs to messaging roles,**
- **Mappings of user/group IDs to naming roles**]

to [**only the callers that are mapped to either the Administrator role or Configurator role**].

FMT_MSA.1b: Management of security attributes

FMT_MSA.1b.1 The TSF shall enforce the [**configuration data, files, and runtime state access control policy and transactions and activities access control policy and user MBean access control policy**] to restrict the ability to [***write or delete***] the security attributes

- [**Mappings of User/Group IDs to Administration Roles**]

to [**only the callers that are mapped to the AdminSecurityManager role**].

FMT_MSA.1c: Management of security attributes

FMT_MSA.1c.1 The TSF shall enforce the [**UDDI access control policy**] to restrict the ability to [***write or delete***] the security attributes

- [**Registered UDDI Publishers**]

to [**only the callers that are mapped to either the Administrator role or Operator role**].

FMT_MSA.3a: Static attribute initialization

FMT_MSA.3a.1 The TSF shall enforce the [**UDDI access control policy**] to provide [***restrictive***] default values for the

- **Registered UDDI Publishers**

security attributes that are used to enforce the SFP.

FMT_MSA.3a.2 The TSF shall allow the [**Administrator role or Operator role**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3b: Static attribute initialization

FMT_MSA.3b.1 The TSF shall enforce the [**web server application access control policy, enterprise bean access control policy, messaging access control policy**] to provide [***restrictive***] default values for **the:**

- **Mappings of user/group IDs to application-defined roles,**
- **Mappings of user/group IDs to messaging roles,**

security attributes that are used to enforce the SFP.

FMT_MSA.3b.2 The TSF shall allow the [**Administrator role or Configurator role**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3c: Static attribute initialization

FMT_MSA.3c.1 The TSF shall enforce the [**configuration data, files, and runtime state access control policy and transactions and activities access control policy**] to provide [***restrictive***] default values for **the:**

- **Mappings of user/group IDs to administration roles**

security attributes that are used to enforce the SFP.

FMT_MSA.3c.2 The TSF shall allow the [**AdminSecurityManager role**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3d: Static attribute initialization

FMT_MSA.3d.1 The TSF shall enforce the [**naming directory access control policy**] to provide [***permissive***] default values for the

- **Mappings of user/group IDs to naming roles**

security attributes that are used to enforce the SFP.

FMT_MSA.3d.2 The TSF shall allow the [**Administrator role or Configurator role**] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions **on the Product Application Server component**: [

a) Configuring the attributes that map user and group IDs to roles,
b) Configuring the attribute that stores the list of registered UDDI publishers,
c) Configuring the attribute that sets the inherit defaults flag for each Messaging queue, topic space, and topic,
d) Configuring the attribute that sets the topic space access check flag for each Messaging topic space,
e) Configuring the attribute that maps a user ID and password to a run-as role,
f) Configuring the attribute that sets the inherit Sender flag for new topics,
g) Configuring the attribute that sets the inherit Receiver flag for new topics].

FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [

- **administration roles,**
  - **Administrator**
  - **Configurator**
  - **Monitor**
  - **Operator**
  - **Deployer**
  - **AdminSecurityManager**
- **application-defined roles,**
- **messaging roles,**
  - **Browser**
  - **Bus Connector**
  - **Creator**
  - **Receiver**
  - **Sender**
- **naming roles,**
  - **COSNamingCreate**
  - **COSNamingDelete**
  - **COSNamingRead**
  - **COSNamingWrite**
- **UDDI roles**
  - **SOAP_Publish_User**
  - **V3SOAP_CustodyTransfer_User_Role**
  - **V3SOAP_Publish_User_Role**
  - **V3SOAP_Security_User_Role**
  - **EJB_Publish_Role**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2 Strength Of Function (SOF)

There is no strength of function claim because the TOE does not identify any non-cryptographic security functional requirements for which an explicit Strength of Function (SOF) is appropriate and does not identify any non-cryptographic functions that are of a permutational or probabilistic nature. Therefore, a minimum SOF claim is not included for the TOE.

5.3 TOE Security Assurance Requirements

The target evaluation assurance level for this product is EAL4, augmented with ALC_FLR.1 (Basic Flaw Remediation)

5.4 Security Requirements for the IT Environment

This section specifies the Security Requirements for the IT environment.

5.4.1 Cryptographic Support (FCS)

FCS_CKM.1: Cryptographic key generation

FCS_CKM.1.1	The **IT environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**DSA or RSA**] and specified cryptographic key sizes [**512-bit or 1024-bit for DSA, or 1024-bit for RSA**] that meet the following: [**FIPS 186-2 for DSA or none for RSA**].

FCS_CKM.4: Cryptographic key destruction

FCS_CKM.4.1	The **IT environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**that provides a zeroization method that is sufficient not to compromise plaintext secret and private keys**] that meets the following: [**FIPS 140-1 or FIPS 140-2 standard with a minimum of a Level 1 of assurance**].

5.4.2 Identification and Authentication (FIA)

FIA_ATD.1: User attribute definition

FIA_ATD.1.1 The **IT environment** shall maintain the following list of security attributes belonging to individual users: [**User ID, Group ID(s), and a Password, or Certificate**].

FIA_UAU.1: Timing of authentication

FIA_UAU.1.1 The **IT environment** shall allow [**validation of the password of individual users or mapping of the DN in a certificate to a user identity, or verification of signature in LTPA token**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The **IT environment** shall require each user to be successfully authenticated **using a password-based, token-based, or certificate-based authentication mechanism** before allowing any other TSF-mediated actions on behalf of that user.

5.4.3 Security Management (FMT)

FMT_MSA.2: Secure security attributes

FMT_MSA.2.1 The **IT environment** shall ensure that only secure values are accepted for security attributes.

6 TOE Summary Specification

6.1 Security Functions (SF)

6.1.1 Identification and Re-Identification (Ident)

The following describes the TOE identification and re-identification security functions.

6.1.1.1 Remote HTTP/S Identification (Ident.1)

This security function identifies a remote caller when the TOE is **not** configured to use a TAI or TAI plus resource and the caller attempts to access a sensitive resource using a remote HTTP/S interface of the TOE. A remote caller can use the remote HTTP/S interface to access any of the following sensitive resources:

> Methods and static web content of deployed user web server applications that are configured with any security constraint except for the role of "Everyone." (The Ident.1 security function is not processed if a method or static web content is not configured with a security constraint or if the method or static web content is configured with the security constraint of the "Everyone" role.)

The behaviour of this security function depends on whether the TOE is configured for Single Signon (SSO) and whether a caller passes a valid LTPA token with the request. In the evaluated configuration, Single Signon must be configured so the remaining description assumes that Single Signon is configured. An LTPA token is valid if the token is signed by the TOE LTPA key and the date in the token has not expired. (The TOE relies on the environment to authenticate that the signature in the LTPA token was generated using the TOE LTPA key.) While the TOE does not perform the verification of an LTPA token's digital signature, the TOE makes its determination based on the response returned by the IT environment indicating whether the digital signature is valid or not valid.

- **Valid LTPA token passed.** The TOE does one of the following, depending on whether the TOE is configured to use propagated attributes and propagated attributes are passed with the LTPA token:
    - **Propagated attribute passed:** The TOE gets the user ID from the token and any group IDs from the propagated attributes. The TOE then associates the user ID and any group IDs with the caller.
    - **Propagated attributes not passed:** The TOE gets the user ID from the token and then uses environment to get all group IDs of which the user ID is a member. The TOE then associates the user ID and any group IDs with the caller.
- **No valid LTPA token passed.** The TOE does one of the following, depending on the configuration of the "authentication method" attribute of the sensitive web

resource. (In the evaluated configuration, a user web server application can be configured for BASIC, FORM, CLIENT CERTIFICATE, or no authentication method. The UDDI registry application is configured for no authentication method. The file transfer capability within the TOE, used to upload and download TOE files, is configured for BASIC authentication method.)

- **FORM Authentication Method.** The TOE queries the caller for a user ID and password using an HTML form and does not continue processing until it receives this. The TOE then queries the environment to determine whether the user ID and password is valid. (The user ID and password are valid if they are configured for a user in the user registry. The TOE relies on the environment to authenticate the user ID and password.) If invalid, the TOE does not process the caller request. Otherwise, the TOE uses the environment to get all group IDs of which the caller is a member and associates the user ID and any group IDs with the caller

- **CLIENT-CERT Authentication Method.** The TOE gets the client certificate in one of the following ways:

  - If the caller passes a client certificate in the HTTP header and the Trusted property is configured in the environment, the TOE gets the client certificate from the HTTP header.

  - In all other cases (caller does not pass client certificate in HTTP header or Trusted property is not configured in the environment), the TOE uses the environment to get the client certificate from the SSL protocol and then uses the environment to authenticate the client certificate. (The TOE relies on the environment to authenticate that the client certificate belongs to the client and was signed by a trusted certificate authority.) If unsuccessful, the TOE returns and error to the caller and does not process the caller request.

  The TOE then uses the environment to map the identity in the certificate to a user ID. If no mapping exists, the TOE returns an error to the caller and does not process the caller request. Otherwise, the TOE uses the environment to get all group IDs of which the caller is a member and associates the user ID and any group IDs with the caller.

- **BASIC Authentication Method.** The TOE queries the caller for a user ID and password using the BASIC Authentication Protocol and does not continue processing until it receives this. The TOE then continues with the same processing as described previously for the "Form Authentication Method."

- **No Authentication Method[24].** The TOE allows processing of data without querying the caller for a user ID and password.

6.1.1.2 Remote ORB Identification (Ident.2)

This security function identifies a remote caller when the caller attempts to access a sensitive resource of the TOE using a remote ORB interface of the TOE. The following sensitive resources can be accessed using a remote ORB interface of the TOE:

- Methods of deployed user enterprise beans
- Transactions and activities of deployed web server applications, deployed enterprise beans, or the TOE
- The TOE naming directory
- The TOE UDDI registry directory
- TOE configuration data
- TOE runtime state

The function will attempt to receive and validate identification information from the remote caller. The specific way that the function will do this depends on the type of identification information that the remote caller passes and whether this information is supported in the TOE configuration. The following table lists the types of identification that could be passed and how the TOE will retrieve and validate each type of information.

Identification Information	**How Identification Information is Validated**
User ID and password	Must be a valid user ID and password stored in the user registry. (The TOE relies on the environment to authenticate the user ID and password.)
Client certificate	For LDAP, must contain a subject DN that matches a subject DN that is stored in the LDAP user registry. Fo LocalOS, must contain a common name (CN) from a subject DN that matches a user ID in the user registry. (The TOE relies on the environment to authenticate that the client certificate belongs to the client and was signe by a trusted certificate authority.)
LTPA token	Must be a valid LTPA token. An LTPA token is valid when it is signed with the configured LTPA key and the date in the token has not expired. (The TOE relies on the environment to authenticate the signature in the

[24] Although a "No Authentication Method" option is available for certain cases such as access to the UDDI registry application, a remote caller is still subject to authentication via the BASIC Authentication Method, which is automatically enforced when Global Security is enabled.

	LTPA token was generated using the TOE LTPA key.)
Propagated attributes	Must be sent with a valid token (either an LTPA token or an asserted identity token) (The TOE does not rely on the environment for authentication.)
Asserted identity	Must be sent with server identification information (either user ID/password or X509Certificate) and the server's ID must be present on a trusted ID list to establish trust in the sending server. The client's asserted ID must be present in the target server's user registry. (If sent with server ID/password, the TOE relies on the environment to authenticate the server ID and password. If sent with a server X509Certificate, the TOE relies on the environment to authenticate that the client certificate belongs to the server and was signed by a trusted certificate authority.)

If the identification information is valid, the results of the identification function are successful. The TOE associates identification attributes with the caller. These attributes include the user ID of the caller and all groups ID of which the user is a member.

If the remote caller does not provide identification information, the TOE returns an error to the caller.

If the remote caller provides invalid identification information, the TOE returns an error to the caller.

6.1.1.3 Remote JMS Identification (Ident.3)

This security function identifies a remote caller when the TOE is configured to use the Built-In JMS Provider Resource and the remote caller attempts to identify itself to the remotely accessible, proprietary messaging interface. The protocol used by this interface (JFAP) is not externally documented but is used internally by:

- The application client, to provide access to the sensitive JMS resources of the TOE to client applications.
- Peer servers (messaging engines) belonging to the same 'bus', to propagate the sensitive JMS resources around the messaging infrastructure.

The TOE will not process requests that access the protected resources unless the remote caller has previously successfully identified itself, using an identification request. The following sensitive resources can be accessed using the remote JMS interface of the TOE:

- Buses, queues, topic spaces and topics

When the remote caller issues an identification request, it provides either a user ID and password or an LTPA token to the TOE. If the remote caller provides a user ID and password, the TOE then queries the environment to determine whether the user ID and

password is valid. (The user ID and password are valid if they are configured for a user in the user registry or are both null, indicating an anonymous login.) If invalid, the TOE will reject the identification request.

If the remote caller provides an LTPA token, the TOE determines if the LTPA token is valid. An LTPA token is valid when it is signed with the configured LTPA key and the date in the token has not expired. (The TOE relies on the environment to authenticate the signature in the LTPA token was generated using the TOE LTPA key.) If invalid, the TOE will reject the identification request.

6.1.1.4 Remote Web Services Re-Identification (Ident.4)

This security function attempts to re-identify a remote caller when the remote caller attempts to access a sensitive resource using the remote web services interface of the TOE. A remote caller can access only one type of sensitive resource using a remote web services interface, which is in a deployed enterprise bean that is configured as a web services endpoint.

Before a request from a remote caller gets to a remote web services interface of the TOE, the request passes through a remote HTTP/S (Ident.1) of the TOE. Therefore, the caller already has been identified by the Ident.1 identification function of the TOE before being processed by this security function (Ident.4). This security function attempts to re-identify the caller. Re-identification occurs using an identification token, and optionally also a trust token.

An identification token is a data structure that is used to pass a username token, x.509 token, or LTPA token. A username token is a data structure that contains a user name and password. An x.509 token is a data structure that contains an x.509 certificate. An LTPA token is a data structure that contains a user id.

A trust token is a data structure used to pass a username token. A username token contains a user name and password.

The specific behaviour of this security function depends on the configuration of the web services endpoint for this security function. In the evaluated configuration, five configurations are supported. The following table defines the five configurations. The meanings of the columns are as follows:

- Configuration Identifier—an identifier number that is referenced in the next table.

- Identification Token Required—indicates whether the client is required to send an identification token with the request.

- Identification Token Type—indicates the type and contents of the identification token.

- Asserted Identity—indicates whether the identification token contains an asserted identity.

- Trust Token Required—indicates whether the client is required to send a trust token, in addition to the Identification Token, with the request.

- Trust Token Type—indicates the type and contents of the trust token

Configuration Identifier	Identification token required?	Identification token type	Asserted identity?	Trust token required?	Trust token type
1	No	not applicable	not applicablee	not applicable	not applicable
2	Yes	username token containing user ID	yes	yes	user name token containing user ID and password
3	Yes	user name token containing user ID and password	no	no	not applicable
4	Yes	X509 token containing client certificate	no	no	not applicable
5	Yes	LTPA token	no	no	not applicable

For configuration 1, the TOE does not attempt to re-identify the remote caller, so the identification attributes inserted by the Ident.1 security function are not replaced.

For all other configurations (configurations 2-5), the TOE attempts to obtain new identification information from the caller, determine whether the information is valid, and, if valid, replace the identification attributes of the caller with new identification attributes.

The following table defines how the TOE does this. The meanings of the columns are as follows:

- Configuration identifier—a reference to a configuration identifier number in the previous table.

- Logic for determining if information is valid—the logic that the TOE uses to determine whether the information in the identification token is valid.

- Associated IDs if valid—the IDs that are associated with the client connection if the TOE determines that the information in the identification token is valid.

Configuration Identifier	**Logic for determining if information is valid**	**Associated IDs if valid**
2	(1)User registry must contain an entry with a user ID and password that matches the user ID and password in the trust token. (The TOE relies on the environment to authenticate the user ID and password.) (2) The user ID from the trust token must be in the trusted list of the target server.	* the user ID contained in the username identification token * all group IDs that are configured in the user registry with the user ID as a member.
3	User registry must contain an entry with a user ID and password that matches the user ID and password in the identification token. (The TOE relies on the environment to authenticate the user ID and password.)	* the user ID contained in the username identification token * all group IDs that are configured in the user registry with the user ID as a member.
4	* If the user registry is in LDAP, the client certificate must contain a subject DN that matches a DN in the LDAP user registry. * If the user registry is in the local OS, the client certificate must contain a common name (CN) from a subject DN that matches a user ID in the user registry. (The TOE relies on the environment to authenticate that the client certificate belongs to the client and was signed by a trusted certificate authority.)	* the user ID contained in the user registry that is mapped to the client certificate in the x509 identification token * all group IDs that are configured in the user registry with the user ID as a member.

5	(1) Signature of token must be valid and (2) Token must not have an expired date. (The TOE relies on the environment to authenticate that the signature in the token was generated using the TOE LTPA key.)	* user ID contained in the LTPA identification token * all group IDs that are configured in the user registry with the user ID as a member.

If the TOE is unable to obtain the required identification attributes from the caller or if the identification attributes are not valid, the TOE returns an error and does not process the caller request.

6.1.1.5 Remote HA Manager Identification (Ident.5)

This security function determines whether a remote caller has a trusted identity when the remote caller attempts to access a sensitive resource by means of a remote High Availability (HA) Manager interface. The remote caller can access only one sensitive resource by means of a remote HA Manager interface, which is a remote HA Manager connection.

When a remote caller issues a connection request to the remote HA Manager interface, first, the interface validates the LTPA token. (The TOE relies on the environment to authenticate that the signature in the LTPA token was generated using the TOE LTPA key.) If the LTPA token is invalid, the security function terminates the connection.

6.1.1.6 Run-As Identification (Ident.6)

This security function is processed each time the TOE invokes a method in a deployed web server application or enterprise bean on behalf of a remote caller. Before a request from a remote caller gets to invoke the Run-As Identification function, the request passes through a remote HTTP/S (Ident.1) or Remote ORB Identification function (Ident.2) of the TOE. Therefore, the caller already has been identified by the Ident.1 or Ident.2 identification function of the TOE before being processed by this security function (Ident.6). This security function associates identification attributes with the invoke method.

To determine which identification attributes to associate with the method, the TOE uses the configured “Run-As” identity or, if no Run-As identity is configured, the identification attributes of the remote caller. The configured Run-As identity can be configured for any of the following:

- Client
- System (applicable only for a method in an enterprise bean)
- Specified Identity

If Client is configured, the TOE associates with the method the identification attributes of the remote caller that requested the method. If System is configured, the TOE associates

with the method the identification attributes of the TOE component in which the method resides. If Specified Identity is configured, the user ID and password of this specified user must also be configured. The TOE uses the environment to determine whether the user ID and password are valid. If the user ID and password are valid, the TOE uses the environment to get the identification attributes of the user and associates with the method these attributes (which include the user ID of the user and all group IDs of which the user is a member). If not valid, the identification attributes of the remote caller are used.

6.1.1.7 Remote WS-Transactions Identification (Ident.7)

This security function attempts to identify a remote caller when the remote caller attempts to access a sensitive transaction using the remote Web Services Transactions (WS-Transactions) interface of the TOE. When the remote caller uses this interface, the TOE requires the remote caller to identify itself using an LTPA token. The TOE then determines whether the LTPA token is valid based on the response returned by the IT environment. The LTPA token is valid if it is signed by the LTPA key of WebSphere Application Server and the date in the token has not expired. If not valid, the TOE does not process the caller request. Otherwise, the TOE uses the environment to get all group IDs of which the caller is a member and associates the user ID and any group IDs with the caller.

6.1.2 Access Control (AC)

The following describes the TOE access control security functions.

6.1.2.1 Protection of Methods and HTML pages in Deployed Web Server Applications (AC.1)

This function controls access to the following sensitive resources:

- Methods and HTML pages in deployed web server applications

This protects a method or HTML page in a deployed web server application from being invoked by an unauthorized remote caller. When a remote caller issues a request to a method or HTML page in a deployed web server application, the TOE invokes the method or HTML page on behalf of the caller if one of the following conditions are true:

- A user or group ID of the user is mapped to a role that has permission to access the method or HTML page.
- The special group ID of "Everyone" is mapped to a role that has permission to access the method or HTML page.
- The special group ID of "AllAuthenticatedUsers" is mapped to a role that has permission to access the method or HTML page and the remote caller has been successfully identified.
- The method is not configured with a permission (security constraint).

If none of these conditions are true, the TOE does not invoke the method or HTML page.

The application roles and permissions (if any) are configured before the Web Server application is deployed into the evaluated configuration. The application mappings are described in the System Management functions.

6.1.2.2 Protection of Methods in Deployed Enterprise Beans (AC.2)

This function controls access to the following sensitive resources:

- Method in deployed enterprise beans (including methods that are deployed as web services endpoints)

This protects a method in deployed enterprise bean (including a method that has been deployed as a web services endpoint) from being invoked by an unauthorized remote caller. When a remote caller issues a request to a method in a deployed enterprise bean (including a method that has been deployed as a web services endpoint), the TOE invokes the method on behalf of the caller if one of the following conditions are true:

- A user or group ID of the user is mapped to a role that has permission to access the method.
- The special group ID of "Everyone" is mapped to a role that has permission to access the method
- The special group ID of "AllAuthenticatedUsers" is mapped to a role that has permission to access the method and the remote caller has been successfully identified.
- The method is not configured with a permission.

If none of these conditions are true, the TOE does not invoke the method.

The application roles and permissions (if any) are configured before the Enterprise Beans is deployed into the evaluated configuration. The application mappings are described in the System Management functions.

6.1.2.3 Protection of TOE Configuration Data, Files, and TOE Runtime State (AC.3)

This function controls access to the following sensitive resources:

- TOE configuration data
- TOE runtime state

This protects the TOE configuration data and TOE runtime state from a read or write operation that is initiated by an unauthorized remote caller. When a remote caller requests the TOE to read or write configuration data or runtime state, the TOE performs the operation only if one of the following conditions is true:

- A user or group ID of the user is mapped to a role that has permission to perform the operation.
- The special group ID of "Everyone" is mapped to a role that has permission to perform the operation.
- The special group ID of "AllAuthenticatedUsers" is mapped to a role that has permission to perform the operation and the remote caller has been successfully identified.
- The special group ID of "PrimaryAdmin" is mapped to a role that has permission to perform the operation and the remote caller is the primary administrator ID.
- The special group ID of "Server ID" is mapped to a role that has permission to perform the operation and the remote caller is the server ID.

If none of these conditions are true, the TOE does not perform the operation.

The following are the administration roles and permissions.

Administration Role	**Permission**
Monitor	Permission to read configuration attributes and runtime state, and to manage TOE files.
Operator	Monitor permission plus permission to affect runtime state, and to manage TOE files. Permission to modify the attribute that stores the list of registered UDDI publishers.
Configurator	Monitor permission plus permission to: Modify attributes that map user/group IDs to application-defined roles, messaging roles, naming roles, and UDDI roles . Modify the attribute that sets the inherit defaults flag for each Messaging queue, topic space, and topic. Modify the attribute that sets the topic space access check flag for each Messaging topic

	space. Modify the attribute that maps a user ID and password to a run-as role. Modify the attribute that sets the inherit Sender flag for new topics. Modify the attribute that sets the inherit Receiver flag for new topics.
Administrator	Operator and Configurator permission.
Deployer	Operator plus Configurator permission on applications.
AdminSecurityManager	Permission to modify attributes that map user/group IDs to administration roles. Also, when fine grained admin security is used, permission to manage authorization groups. (As stated in the guidance document, managing authorization groups is not allowed in the evaluated configuration.)

The administration mappings are described in the SM functions.

6.1.2.4 Protection of TOE Naming Directory (AC.4)

This function controls access to the following sensitive resources:

- TOE naming directory

This protects the TOE naming data from a read or write operation that is initiated by an unauthorized remote caller. When a remote caller requests the TOE to read from or write to the TOE naming directory, the TOE performs the operation only if one of the following conditions is true:

- A user or group ID of the user is mapped to a role that has permission to perform the operation.
- The special group ID of “Everyone” is mapped to a role that has permission to perform the operation.
- The special group ID of “AllAuthenticatedUsers” is mapped to a role that has permission to perform the operation and the remote caller has been successfully identified.
- The special group ID of “PrimaryAdmin” is mapped to a role that has permission to perform the operation and the remote caller is the primary administrator ID.
- The special group ID of “Server ID” is mapped to a role that has permission to perform the operation and the remote caller is the server ID.

If none of these conditions are true, the TOE does not perform the operation.

The following are the naming roles and permissions:

Naming Role	Permission
COSNamingRead	Permission to read from the naming directory
COSNamingWrite	COSNamingRead permission plus permission to write to the naming directory
COSNamingCreate	COSNamingWrite permission plus permission to insert entries in the naming directory
COSNamingDelete	COSNamingCreate permission plus permission to delete entries in the naming directory

The naming mappings are described in the SM functions.

6.1.2.5 Protection of Transactions and Activities (AC.5)

This function allows a remote caller to invoke a TOE operation that affects a transaction or activity only if the TOE has identified the remote caller, this identity has been validated, and the authenticated identity of the remote caller is mapped to the administrator role. Transactions and activities are invoked via the Transactions interface, which is accessible through the remote ORB or HTTP/S interface.

6.1.2.6 Protection of Messaging Destinations (AC.6)

> Note: The product documentation describes an additional messaging role, identity adopter, which is not mentioned in this document. The reason the identity adopter role is not mentioned in this document is because this role is not permitted to be configured in the evaluated configuration (as specified in the User Guidance document) and, therefore, this role is not relevant to the evaluation.

This security function protects the messaging resources (local bus, queue destination, temporary destination, topic space, topic space root, and topics) of the Built-in JMS Provider from a connect, send, receive, browse, or create operation that is initiated by an unauthorized remote caller.

When a remote caller requests the TOE to perform a connect, send, receive, browse, or create, operation on messaging resource of the Built-in JMS Provider, the TOE evaluates the following conditions and performs the operation only if one of them is true (the conditions are evaluate in the order below, until one is discovered to be true, if any):

1. The special group ID of “Everyone” is mapped to a role that has permission to perform the operation. Use of this group for any messaging role is not permitted in the TOE. (In the User Guidance document, the administrator is instructed not to map the special group of “Everyone” to a role that has permission to a Messaging operation, so this condition should never occur in the evaluated configuration. If “Everyone” is mapped to a role with permission, any caller will be allowed to perform the requested operation.)
2. The user ID is mapped to a role that has permission to perform the operation.

3. The special group ID of "AllAuthenticated" is mapped to a role that has permission to perform the operation and the remote caller has been successfully identified.
4. At this point the user ID to group ID mappings are determined. A group ID to which the user belongs is mapped to a role that has permission to perform the operation.

In addition to these conditions, the TOE also takes into consideration any flags set that will require additional access checks or to inherit permissions.

As such, if the inheritsDefaults flag is set, then the above conditions also take into account any User/Group ID to messaging role mappings that are inherited from the Default values. The inheritsDefaults flag is independently settable for each Queue and Topic Space destination. It informs the TOE to take into account all mappings configured for the Defaults values as well as for the target destination. For example, if the caller requests an operation on a target destination, the inheritsDefault flag is set, and the Defaults values contains a mapping between the user ID of the caller and a role with permission to the requested operation, the TOE will perform the requested operation.

If the inheritSender flag is set, then the above conditions also take into account any User/Group ID to the Sender messaging role mappings that are inherited from the parent topic. The inheritSender flag is independently settable for each topic destination. It informs the TOE to take into account all mappings configured for Send role of the parent destination as well as the mappings configured for the target destination. For example, if the caller requests a send operation on a target destination, the inheritSender flag is set, and the parent destination contains a mapping between the user ID of the caller and the Send role, the TOE will perform the requested operation.

If the inheritReceiver flag is set, then the above conditions also take into account any User/Group ID to the Receiver messaging role mappings that are inherited from the parent topic. The inheritReceiver flag is independently settable for each topic destination. It informs the TOE to take into acocunt all mappings configured for the Receive role of the parent destination as well as the mappings configured for the target destination. For example, if the caller requests a receive operation on a target destination, the inheritReceiver flag is set, and the parent destination contains a mapping between the user ID of the caller and the Receive role, the TOE will perform the requested operation.

If the topicAccessCheck flag is set, then the above conditions also take into account any User/Group ID to messaging role mappings configured for each topic within a topic space, in addition to the role mappings configured on the Topic Space. The topicAccessCheck flag is independently settable for each topic space destination. For example, if the caller requests an operatoin on a topic and the topicAccessCheck flag is set, the TOE will take into account the mappings configured for the topic as well as the topic space.

If none of these conditions are true, the TOE does not perform the operation.

6.1.2.7 Protection of UDDI Registry (AC.7)

The UDDI Registry can be accessed by two remote interfaces: HTTP/S and ORB. This security function protects the UDDI Registry so that it can be accessed by remote callers only by means of the remote HTTP/S interface and so that only remote callers that the TOE has identified using the Ident.1 security function can perform a protected UDDI registry operation. The protected UDDI registry operations are:

- All operations over HTTP on the
  - UDDI SOAP V1, V2, and V3 Publish API
  - UDDI SOAP V3 Custody Transfer API
  - UDDI SOAP V3 Security API
- All operations over the ORB interface on the
  - UDDI V2 Publish API

When a remote caller issues a request to the TOE to access the UDDI registry by means of the remote ORB interface, the TOE always denies the request.

When a remote caller issues a request to the TOE to access the UDDI registry by means of the remote HTTPS interface, the TOE will accept the request but if the request is to perform a protected UDDI registry operation, the TOE will perform the operation only if both of the following conditions are true:

- The TOE has identified the user and validated this identity
- The user is registered as a UDDI publisher. This means that the user is configured on the list of registered UDDI publishers.

If all of these conditions are not true, the TOE will not perform the operation.

The configuration of the user to role mappings are part of the evaluated configuration and are restricted to only those mappings defined within the evaluated configuration guidance. The configuration of users that are registered as UDDI publishers is also part of the evaluated configuration and may be configured as desired.

6.1.2.8 Protection of Location Service (AC.8)

This function allows a remote caller to invoke a method on the location service only if the TOE has identified the remote caller and the identity of the caller is the security principal having the WebSphere Application Server ID. The location service methods are invoked through the Location service interface, which is accessible through the ORB interface.

6.1.2.9 Protection of Methods and Attributes in User MBeans (AC.9)

This function controls access to the following sensitive resources:

- Methods and Attributes in User MBeans

This protects a method and attributes in User MBeans from being invoked by an unauthorized remote caller. When a remote caller issues a request to a method in a User Mbean, the TOE invokes the method on behalf of the caller if one of the following conditions are true:

- A user or group ID of the user is mapped to a role that has permission to access the method.
- The special group ID of "Everyone" is mapped to a role that has permission to access the method
- The special group ID of "AllAuthenticatedUsers" is mapped to a role that has permission to access the method and the remote caller has been successfully identified.
- The method is not configured with a permission.

If none of these conditions are true, the TOE does not invoke the method.

The application roles and permissions (if any) are configured before the User Mbean is deployed into the evaluated configuration. The Administration role mappings are described in the System Management functions.

6.1.3 Security Management (SM)

The following describes the TOE security management security functions.

6.1.3.1 Management of the Product Application Server (SM.1)

SM.1.1 The TOE shall maintain the following roles:

Administration roles:

- *Administrator*
- *Configurator*
- *Monitor*
- *Operator*
- *Deployer*
- *AdminSecurityManager*

Messaging roles:

- *Browser*
- *Bus Connector*
- *Creator*
- *Receiver*
- *Sender*

Naming roles:

- *COSNamingCreate*
- *COSNamingDelete*
- *COSNamingRead*
- *COSNamingWrite*

UDDI roles:

- *SOAP_Publish_User*
- *V3SOAP_CustodyTransfer_User_Role*
- *V3SOAP_Publish_User_Role*
- *V3SOAP_Security_User_Role*
- *EJB_Publish_Role*

SM.1.2 The TOE shall maintain the security attributes:

- Mappings of user/group IDs to application-defined roles

- Mappings of user/group IDs to messaging roles
- Mappings of user/group IDs to naming roles
- Mappings of User/Group IDs to Roles Mapping to Administration Roles
- Registered UDDI publishers

SM.1.3 On initiation of the TOE by default, the following is configured for each of the security attributes defined in SM.1.2:

- Mappings of user/group IDs to application-defined roles:

Application-Defined Role	**Default user/group IDs to role mappings**
Each application-defined role	*None or defined by application developer*

- Mappings of user/group IDs to administration roles:

Administration Role	**Default user/group IDs to role mappings**
Administrator[25]	*Server ID, PrimaryAdmin User:WSADMIN,Group:CBCFG1*
Configurator	*None*
Monitor	*None*
Operator	*None*
Deployer	*None*
AdminSecurityManager[26]	*Server ID, PrimaryAdmin User:WSADMIN,Group:CBCFG1*

[25] The default mapping for the Administrator role does not associate any users to the Administrator role. However, an internal mapping is defined which assigns each server identity (Server ID and PrimaryAdmin) to the administrator role so that server operations have sufficient privileges to execute. Yet, these internal mappings are not externally visible within the configuration for mapping users to the Administrator role. (The server ID and PrimaryAdmin are externally visible with the configuration, but the mapping of the server identity and PrimaryAdmin to the Administration role is not externally visible.)

[26] The default mapping for the AdminSecurityManager role does not associate any users to the AdminSecurityManager role. However, an internal mapping is defined which assigns each server identity (Server ID and PrimaryAdmin) to the AdminSecurityManager role so that server operations have sufficient privileges to execute. Yet, these internal mappings are not externally visible within the configuration for mapping users to the AdminSecurityManager role. (The server ID and PrimaryAdmin are externally visible with the configuration, but the mapping of the server identity and PrimaryAdmin to the AdminSecurityManager role is not externally visible.)

- Mappings of user/group IDs to naming roles:

Naming Role	**Default user/group IDs to role mappings**[27]
COSNamingCreate	*Server ID*
COSNamingDelete	*Server ID*
COSNamingRead	*Server ID,* *Everyone group ID*
COSNamingWrite	*Server ID*

- Mappings of user/group IDs to messaging roles:

Messaging Role	**Default user/group IDs to role mappings**
Browser	*None*
Bus Connector	*None*
Creator	*None*
Receiver	*None*
Sender	*None*

- Registration of UDDI publishers: None

SM.1.4 A caller in the Administrator or Configurator role can configure, via the Product wsadmin Tool, the following security attributes:

- The attributes that map user/group IDs to messaging roles, and naming roles.
- The attribute that sets the inherit defaults flag for each Messaging queue and topic space (inheritsDefaults).
- The attribute that sets the topic space access check flag for each Messaging topic space (topicAccessCheck).
- The attribute that sets the inherit Sender flag for new topics (inheritSender).

[27] The default mapping for the Naming roles has the internal mapping defined which assigns each server identity (Server ID) to the naming role so that server operations have sufficient privileges to execute. Yet, this internal mappings is not externally visible within the configuration for mapping users to the Naming role. (The server ID is externally visible with the configuration, but the mapping of the server identity to the Naming role is not externally visible.)

- The attribute that sets the inherit Receiver flag for new topics (inheritReceiver).

A caller in the Administrator, Configurator or Deployer role can configure, via the Product wsadmin Tool, the following security attributes:

- The attributes that map user/group IDs to application-defined roles, messaging roles, and naming roles.
- The attribute that maps a user ID and password to a run-as role.

A caller in the Administrator or Operator role can configure, via the Product wsadmin Tool, the following security attribute:

- The attribute that stores the list of registered UDDI publishers.

A caller in the AdminSecurityManager role can configure, via the Product wsadmin Tool, the following security attribute:

- The attributes that map user/group IDs to administration roles.

6.2 Assurance Measures

Assurance measures will be adopted to address each of the EAL4, augmented with ALC_FLR.1 (Basic Flaw Remediation), assurance requirements, as summarised in table B.1 within [CC]. The following table provides a summary:

Assurance Component	Description of how Requirement will be met
ACM_AUT.1	A CM system that automates processes required for ensuring that only authorized changes are made to the TOE and for generating the TOE will be implemented and/or described. Confirmation that the automated processes that are described have been implemented is established during the onsite visit.
ACM_CAP.4	A description of the configuration management system used by the developers will be provided with a configuration list that will identify the items that comprise the TOE. This document will uniquely reference the TOE stated within Section 1 of this ST. Confirmation that the TOE is labelled with the correct reference will be provided during testing. Additionally, the configuration management system documentation will identify the controls provided which ensure that unauthorized modifications are not made to the TOE, and ensure proper functionality and use of the CM system to help maintain the integrity of the TOE. The configuration management system documentation will also describe any acceptance procedures used to confirm that any creation or modification of configuration items is authorized.
ACM_SCP.2	The list of TOE configuration items provided will identify the implementation representation of the TOE, security flaws, and evaluation evidence.
ADO_DEL.2	The developers will provide the delivery procedures used to ensure that security is maintained when distributing versions of the TOE to the user's site, including: procedures used to maintain security during distribution of the TOE to a user's site; procedures and technical measures used to detect modifications or discrepancies between the developer's master copy and the version received at the user's site; and procedures used to allow detection of attempts to masquerade as the developers, even in cases in which the developers have sent nothing to the user's site.
ADO_IGS.1	Procedures for the secure installation, generation and start-up of the TOE will be provided.
ADV_FSP.2	An informal description of the TSF and its external interfaces, describing complete effects, exceptions and error messages will be provided.

Assurance Component	Description of how Requirement will be met
ADV_HLD.2	A high-level design will be provided that informally describes the security of each component within the TSF. All hardware, software and firmware required by the TOE will be identified. A presentation of the functions provided by the supporting protection mechanisms implemented in the environment will also be included. Identification of the interfaces between the components and which of these are externally visible will be provided. A description of the security-relevant effects, exceptions and error messages of all interfaces to TSF-enforcing subsystems will be provided. All TOE subsystems, both TSF-enforcing and non-TSF-enforcing subsystems, will be identified and described.
ADV_IMP.1	A subset of the TSF implementation will be provided in such a manner that unambiguously defines the TSF to a level of detail that allows the evaluator to regenerate the TSF without further design decisions.
ADV_LLD.1	A low-level design will be provided that describes the TSF in terms of modules, describes the purpose of each module, defines the interrelationships between the modules in terms of provided security functionality and dependencies on other modules, describes how each TSP-enforcing function is provided, and identifies all interfaces to the modules of the TSF, as well as those interfaces that are externally visible
ADV_RCR.1	This correspondence information will be contained within the Functional Specification, high-level design, low-level design, and implementation representation. This will provide a correspondence analysis between the TOE summary specification, the functional specification, the high level design, the low-level design and between the low-level design and the implementation representation.
ADV_SPM.1	A security policy model will be provided that includes correspondence between the functional specification, the security policy model, and the policies of the TSP all of which assist in providing additional assurance that the security functions in the functional specification enforce the policies in the TSP.
AGD_ADM.1	The product operational documentation that describes to the administrator how to operate the TOE in a secure manner will be provided. This will describe the administrative security functions and interfaces available to the administrator. All details of any warnings about functions and privileges and assumptions about user behaviour are included.

Assurance Component	Description of how Requirement will be met
AGD_USR.1	The product user guidance documentation will be provided at the following URL: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg24011697 This document describes to trusted developers the interfaces that can be called from web server applications and enterprise beans.
ALC_DVS.1	Development security procedures will be provided, which describe the physical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE.
ALC_FLR.1	The flaw remediation procedures will be provided, which describe the procedures used to track all reported security flaws in each release of the TOE. Details of the nature and effect of each flaw will be provided as well as the status of finding a correction to that flaw. The methods used to provide flaw information; correction and guidance on corrective actions to users will be described.
ALC_LCD.1	A life-cycle model for the development and maintenance of the TOE will be provided that defines a model sufficient to ensure that the development and maintenance models implemented will contribute to the overall quality of the TOE.
ALC_TAT.1	The tools used for the development and maintenance of the TOE will be documented. The development tools documentation will identify the tools, identify the selected implementation-dependent options of the development tools, unambiguously define the meaning of all statements used in the implementation, and unambiguously define the meaning of all implementation-dependent options. This includes, but is not limited to, programming languages, documentation, implementation standards, and other parts of the TOE such as supporting runtime libraries.
ATE_COV.2	Coverage of the TSF by the developers functional testing to the functional specification will be provided as part of the testing documentation. This coverage will provide an analysis that includes correspondence between the tests identified in the test documentation and the TSF as described in the functional specification and will demonstrate that the correspondence provided is complete.
ATE_DPT.1	An analysis of the depth of the testing will be provided and will demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_FUN.1	Test documentation will be provided, which describes the functional tests performed by the developers. This document will include test plans, test procedures, expected and actual test results, It will also identify the security functions to be tested.

Assurance Component	Description of how Requirement will be met
ATE_IND.2	Resources will be made available to the evaluators so that they are able to perform additional, independent testing.
AVA_MSU.2	An analysis of the guidance documentation will be provided which demonstrates that the guidance documentation identifies all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation, the guidance documentation is complete, clear, consistent, and reasonable, the guidance documentation lists all assumptions about the intended environment, and the guidance documentation lists all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_SOF.1	There are no functions within the TOE that have an explicit strength of function claim and therefore no Strength of Function analysis will be produced.
AVA_VLA.2	A description and analysis of any potential vulnerability identified within the TOE will be performed. This will be documented together with an explanation of why the TOE is resistant to penetration attacks with regards to the identified vulnerabilities. The analysis will additionally describe the method used to search the TOE deliverables for discovering ways in which a user can violate the TSP.

7 Rationale

This chapter presents the evidence used in the ST evaluation and supports the claims that the ST is a complete and cohesive set of requirements.

7.1 Correlation of Threats, Policies, Assumptions and Objectives

The following matrix provides a correspondence of the threats, policies, assumptions and objectives:

Objectives:	O.ACCESS	O.IDENTIFY	O.MANAGE	O.ADMIN	O.APP	O.ATTR	O.AUTH	O.PROTECT	O.RECOVER	O.TRANSFER
T.ACCESS_RES	x		x			x		x	x	
T.ACCESS_TOE		x	x			x		x	x	
T.APP					x			x	x	
T.NETWORK					x			x		x
P.ACCESS	x		x	x	x	x				
A.ADMIN				x						
A.APP				x	x					
A.AUTH							x			
A.PROTECT								x		

7.2 Security Objectives Rationale

This section demonstrates that the security objectives stated in Section 4 of this ST are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them.

7.2.1 Threats

This section provides evidence demonstrating coverage of the threats by both the IT and non-IT security objectives.

[T.ACCESS_RES]

A caller gains access to a resource without the correct authority to access that resource.

The objective O.ACCESS counters this directly by ensuring that only those callers with the correct authority can access an object. This is supported by O.MANAGE, which ensures that privileged actions are performed effectively.

The following environmental objectives support O.ACCESS in countering the threat:

- O.ATTR – ensures that the correct role to resource association is maintained, and thus preventing any access to a resource that the caller is not authorised.
- O.PROTECT – ensures that no objects can be accessed by the cabling between the workstations;
- O.RECOVER – ensures that following a system failure, the TOE is not operating in an insecure state whereby an unauthorised caller can gain access to objects they are not authorised to access.

[T.ACCESS_TOE]

An unidentified caller gains access to a protected resource.

O.IDENTIFY is the primary objective that counters this threat, by ensuring that all callers are identified before they can access a protected resource. O.MANAGE also supports this by ensuring effective management of the TOE.

The following environmental objectives support O.IDENTIFY in countering the threat:

- O.ATTR – ensures that a UID is maintained thus allowing correct operation of the identification functionality;
- O.PROTECT – ensures that an unidentified caller cannot gain access to the TOE via the cabling between the workstations;
- O.RECOVER – ensures that following a system failure, the TOE is not operating in an insecure state whereby an unauthorised caller can gain access to the TOE.

[T.APP]

The applications and operating system that the TOE interfaces compromises the TOE.

It is essential that the administrator manages the applications interfacing to the TOE in a secure manner, so that vulnerabilities do not exist, which may lead to compromise of the TOE. The objectives O.APP, O.PROTECT and O.RECOVER all ensure that the operating system is managed in a secure manner.

[T.NETWORK]

Data transferred between workstations is disclosed to, or modified by unidentified callers or processes, either directly or indirectly.

Administrators must ensure that data transferred between workstations i.e. along network cabling, is suitably protected against physical or other (e.g. Sniffing) attacks that may result in the disclosure, modification or delay of information transmitted between workstations. Objective O.PROTECT ensures that this is achieved. O.APP ensures that the protocols used in the transmission of data have been correctly configured within the operating systems.

7.2.2 Security Policy

This section provides evidence demonstrating coverage of the organisational security policy by both the IT and non-IT security objectives.

[P.ACCESS]

The right to access a resource is determined on the basis of association of user or group IDs to roles and of roles to resources.

This policy is implemented through the objective O.ACCESS, which provides the means of controlling access to objects by users and processes. O.MANAGE supports this policy by the administrators ensuring that the policy is maintained.

The environmental objectives O.ADMIN and O.APP further support the policy by ensuring that the interfacing applications are configured in a secure manner so that no vulnerability may exist that enables an unauthorised caller to gain an authorised identity.

O.ATTR ensures that the association of roles to resources is maintained, and thus supporting this policy.

7.2.3 Assumptions

This section provides evidence demonstrating coverage of the assumptions by both the IT and non-IT security objectives.

[A.ADMIN]

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 also is assumed that this individual will comply with all the guidelines specified in the User Guidance document.

O.ADMIN is the primary objective that meets this assumption, which ensures that the administrator is a competent and trustworthy person whom is capable of managing the TOE in a secure manner.

[A.APP]

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 also 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.

O.APP is the primary environmental objective that satisfies the assumption. This ensures that the administrator installs and configures the supporting operating systems in accordance with:

- The manufacturers instructions; and
- Any evaluated configurations were applicable.

This also ensures that the developers of the applications comply with the guidelines defined in this document.

O.ADMIN supports this by ensuring that the Administrator is a competent and trustworthy person and that the users have been set up appropriately.

[A.AUTH]

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.

O.AUTH is the primary environmental objective that satisfies the assumption. This ensures that at least one or more authentication mechanisms are present within the environment to authenticate remote callers needing to access the TOE resources.

[A.PROTECT]

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.

The environmental objective O.PROTECT ensures that the network cabling is suitably protected against threats of modification, tampering or interruption of the data transmitted via this medium. Also, it is assumed that all hardware used within the operating environment is secured.

7.3 Security Requirements Rationale

7.3.1 Security Functional Requirements Rationale

This section demonstrates that the functional components selected for the TOE provide complete coverage of the defined security objectives. The mapping of components to security objectives is illustrated in the table below.

Security Objective	Functional Component
O.ACCESS	Subset Access Control (FDP_ACC.1a, FDP_ACC.1b, FDP_ACC.1c, FDP_ACC.1d, FDP_ACC.1e, FDP_ACC.1f, FDP_ACC.1g, FDP_ACC.1h, FDP_ACC.1i) Security Attribute Based Access Control (FDP_ACF.1a, FDP_ACF.1b, FDP_ACF.1c, FDP_ACF.1d, FDP_ACF.1e, FDP_ACF.1f, FDP_ACF.1g, FDP_ACF.1h, FDP_ACC.1i) User-subject binding (FIA_USB.1) Management of Security Attributes (FMT_MSA.1(a)(b)(c)) Static Attribute Initialisation (FMT_MSA.3(a)(b)(c)(d))
O.IDENTIFY	Perform Actions On Behalf Of Another User (FIA_OBO.EXP.1) Timing of Identification (FIA_UID.1)
O.MANAGE	Management of Security Attributes (FMT_MSA.1(a)(b)(c)) Static Attribute Initialisation (FMT_MSA.3(a)(b)(c)(d)) Specification of Management Functions (FMT_SMF.1) Security Roles (FMT_SMR.1)

[O.ACCESS]

The TOE must ensure that only those callers with the correct authority are able to access an object.

Association [FIA_USB.1] of user security attributes must be performed in order that the access control mechanism can operate.

The access control mechanism must have a defined scope of control [FDP_ACC.1a, FDP_ACC.1b, FDP_ACC.1c, FDP_ACC.1d, FDP_ACC.1e, FDP_ACC.1f, FDP_ACC.1g, FDP_ACC.1h, and FDP_ACC.1i] with defined rules [FDP_ACF.1a, FDP_ACF.1b, FDP_ACF.1c, FDP_ACF.1d, FDP_ACF.1e, FDP_ACF.1f, FDP_ACF.1g, FDP_ACF.1h, and FDP_ACF.1i]. Authorised callers [FMT_SMR.1] must be able to

control who has access to the objects [FMT_MSA.1 (a) (b) (c)]. Protection of these objects must be continuous, starting from object creation [FMT_MSA.3 (a) (b) (c) (d)].

[O.IDENTIFY]

The TOE must ensure that all callers are identified before they access a protected resource.

The TOE provides a user the ability to be identified as another user to perform a specific action on behalf of that user [FIA_OBO.EXP.1].

Before callers can access a protected resource, they need to be identified [FIA_UID.1].

[O.MANAGE]

The TOE must allow administrators to effectively manage the TOE and that this is only performed by authorised callers.

The TSF must restrict the ability to manage the TOE to authorised administrators [FMT_MSA.1 (a) (b) (c)] with default values [FMT_MSA.3 (a) (b) (c) (d)] and the security attributes [FMT_MSA.1 (a) (b) (c)]. [FMT_SMF.1] specifies the management functions provided by the TOE. [FMT_SMR.1] defines roles in order that the TOE is managed effectively.

7.3.2 Security Environment Requirements Rationale

This section demonstrates that the functional components provided by the environment for the TOE, provide complete coverage of the defined security objectives. The mapping of requirements to security objectives is illustrated in the table below.

Security Objective	Requirement for Environment
O.ATTR	User Attribute Mapping (FIA_ATD.1)
O.AUTH	Timing of authentication (FIA_UAU.1)
O.TRANSFER	Cryptographic key generation (FCS_CKM.1) Cryptographic key destruction (FCS_CKM.4) Secure security attributes (FMT_MSA.2)

[O.ATTR]

The IT Environment shall maintain User and Group mappings for callers.

The User/Group IDs mapping belonging to individual callers must be maintained in the IT Environment (FIA_ATD.1).

[O.AUTH]

The IT Environment shall process authentication requests by remote callers.

The ability to process authentication requests using one of the supported authentication mechanisms identified within the evaluated configuration must be supported by the IT Environment (FIA_UAU.1).

[O.TRANSFER]

The IT Environment shall provide data encryption to protect network traffic.

The IT Environment provides encryption capabilities and associated management support to provide SSL capabilities to the TOE.

7.3.3 Security Assurance Requirements Rationale

This ST contains assurance requirements from the CC EAL4, augmented with ALC_FLR.1 (Basic Flaw Remediation) assurance package, and is additionally augmented with the ALC_FLR.1 (Basic Flaw Remediation) SFR.

The EAL chosen is based on the impact that the statements of the security environment and objectives within this ST have on the assurance level. The administrator shall be capable of managing the TOE such that the security is maintained (O.ADMIN) particularly within the operating system that the TOE relies (O.APP), and that the physical environment protects the TOE from any potential vulnerability (O.PROTECT). This EAL level also provides a moderate to high level of independently assured security through analysis of the functional specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation to understand the security behaviour of the TOE.

While the TOE includes explicitly stated security functional requirements, the assurance requirements selected provide adequate assurance to ensure that the design and implementation details of these explicitly stated security functionalities are documented and tested. The assurance requirements selected also ensure that the explicitly stated security functional requirements are stated in a manner in which compliance can be demonstrated.

Given the amount of assurance required to meet the TOE environment and the intent of EAL4, this assurance level was considered most applicable for the TOE described within this ST.

EAL4, augmented with ALC_FLR.1 (Basic Flaw Remediation), was chosen to provide further assurance in the flaw remediation procedures provided by the developers.

7.3.4 SFR Dependencies

The matrix below identifies all of the dependencies of the SFRs included in the ST. Only those SFRs that have a dependency, or are depended upon are shown in the table.

	ADV_SPM.1	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1a	FDP_ACC.1b	FDP_ACC.1c	FDP_ACC.1d	FDP_ACC.1e	FDP_ACC.1f	FDP_ACC.1g	FDP_ACC.1h	FDP_ACC.1i	FDP_ACF.1a	FDP_ACF.1b	FDP_ACF.1c	FDP_ACF.1d	FDP_ACF.1e	FDP_ACF.1f	FDP_ACF.1g	FDP_ACF.1h	FCP_ACF.1i	FIA_ATD.1	FIA_UID.1	FMT_MSA.1a	FMT_MSA.1b	FMT_MSA.1c	FMT_MSA.2	FMT_MSA.3a	FMT_MSA.3b	FMT_MSA.3c	FMT_MSA.3d	FMT_SMF.1	FMT_SMR.1
FCS_CKM.1			x																								x						
FCS_CKM.4		x																									x						
FDP_ACC.1a													x																				
FDP_ACC.1b														x																			
FDP_ACC.1c															x																		
FDP_ACC.1d																x																	
FDP_ACC.1e																	x																
FDP_ACC.1f																		x															
FDP_ACC.1g																			x														
FDP_ACC.1h																				x													
FDP_ACC.1i																					x												
FDP_ACF.1a				x																									x				
FDP_ACF.1b					x																								x				
FDP_ACF.1c						x																								x			
FDP_ACF.1d							x																								x		
FDP_ACF.1e								x																						x			
FDP_ACF.1f									x																				x				
FDP_ACF.1g										x																	x				x		
FDP_ACF.1h											x																						
FDP_ACF.1i												x																	x				
FIA_OBO.EXP.1																							x										
FIA_ATD.1																																	
FIA_UAU.1																							x										
FIA_UID.1																																	
FIA_USB.1																						x											
FMT_MSA.1a				x	x		x		x																							x	x
FMT_MSA.1b						x		x				x																				x	x
FMT_MSA.1c										x																						x	x
FMT_MSA.2	x			x																				x									x
FMT_MSA.3a																									x								x
FMT_MSA.3b																								x									x
FMT_MSA.3c																									x								x

	ADV_SPM.1	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1a	FDP_ACC.1b	FDP_ACC.1c	FDP_ACC.1d	FDP_ACC.1e	FDP_ACC.1f	FDP_ACC.1g	FDP_ACC.1h	FDP_ACC.1i	FDP_ACF.1a	FDP_ACF.1b	FDP_ACF.1c	FDP_ACF.1d	FDP_ACF.1e	FDP_ACF.1f	FDP_ACF.1g	FDP_ACF.1h	FCP_ACF.1i	FIA_ATD.1	FIA_UID.1	FMT_MSA.1a	FMT_MSA.1b	FMT_MSA.1c	FMT_MSA.2	FMT_MSA.3a	FMT_MSA.3b	FMT_MSA.3c	FMT_MSA.3d	FMT_SMF.1	FMT_SMR.1
FMT_MSA.3d																								x								x
FMT_SMF.1																																
FMT_SMR.1																							x									

The key to the symbols used, are:

x required dependency

As shown in [CC], all dependencies are satisfied by the TOE, with the exception for the following SFRs:

- FMT_MSA.2 has a dependency on ADV_SPM.1, FDP_ACC.1 or FDP_IFC.1, FMT_MSA.1, and FMT_SMR.1, and
  - ADV_SPM.1 is included within the TOE, however, is irrelevant to FMT_MSA.2 as it is a requirement on the IT environment and ADV_SPM.1 is intended to define a security policy model for the TOE and not its IT environment.
  - FDP_ACC.1 is included in the TOE and FDP_IFC.1 is irrelevant as the TOE does not enforce an information flow control policy. However, the FDP_ACC.1 iterations included within the ST cannot satisfy the dependency on FMT_MSA.2 since they define security attributes for the TOE and not the TOE's environment.
  - FMT_MSA.1 is included within the TOE, however, is irrelevant to FMT_MSA.2 since the FMT_MSA.1 iterations define the management capabilities of the security attributes defined for the various access control policies and not for cryptographic security attributes. Furthermore, the TOE does not maintain the cryptographic security attributes and so no claim has been associated.
  - FMT_SMR.1 is included within the TOE, however, is irrelevant to FMT_MSA.2 since the FMT_SMR.1 SFR defines the roles enforced by the TOE and not the TOE's environment. Furthermore, the TOE does not maintain the cryptographic security attributes and so no claim has been associated.
- The dependency of FDP_ACF.1h on FMT_MSA.3 is not met for the following reason: In the evaluated configuration, there is nothing to manage with respect to the Location Service Access Control Policy. The WebSphere Server ID is defined during the configuration of the evaluated configuration and it is the only security attribute pertaining to access control for the Location Service.

7.3.5 Explicitly Stated Requirements

The ST includes the following explicitly stated requirements:

- FIA_OBO.EXP.1

FIA_OBO.EXP.1 was explicitly stated to address functionality for the ability of a user to perform an action on behalf of another user.

The explicitly stated SFRs are modeled after Common Criteria requirements and as such the assurance requirements as stated in the Security Target document apply to the explicitly stated SFRs. No new assurance procedures are required to evaluate the explicitly stated SFRs.

7.4 TOE Summary Specification Rationale

This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

7.4.1 TSF correspondence to SFRs

This section demonstrates that the combination of the specified TSFs works together so that the SFRs are satisfied. The matrix below shows the TOE security functions, which together satisfy each SFR element.

	AC.1	AC.2	AC.3	AC.4	AC.5	AC.6	AC.7	AC.8	AC.9	Ident.1	Ident.2	Ident.3	Ident.4	Ident.5	Ident.6	Ident.7	SM.1.1	SM.1.2	SM.1.3	SM.1.4
FDP_ACC.1a	X																			
FDP_ACC.1b		X																		
FDP_ACC.1c			X																	
FDP_ACC.1d				X																
FDP_ACC.1e					X															
FDP_ACC.1f						X														
FDP_ACC.1g							X													
FDP_ACC.1h								X												
FDP_ACC.1i									X											
FDP_ACF.1a	X																			
FDP_ACF.1b		X																		
FDP_ACF.1c			X																	
FDP_ACF.1d				X																
FDP_ACF.1e					X															
FDP_ACF.1f						X														
FDP_ACF.1g							X													
FDP_ACF.1h								X												
FDP_ACF.1i									X											
FIA_OBO.EXP.1															X					
FIA_UID.1										X	X	X	X	X		X				
FIA_USB.1										X	X	X	X	X		X				
FMT_MSA.1(a)(b)(c)																		X		
FMT_MSA.3(a)(b)(c)(d)																			X	
FMT_SMF.1																				X
FMT_SMR.1																	X			

7.4.2 TSF correspondence Rationale

This section provides rationale describing how the combination of the specified TSFs works together so that the SFRs are satisfied.

SFRs	TSFs
FDP_ACC.1a	**AC.1** is suitable to meet *FDP_ACC.1a* by ensuring that the TOE enforces an access control security function policy for remote callers requesting access to protected methods of web server applications using operations defined by an application developer. However the operations must conform to the application developer guidance supplied for the evaluated configuration.
FDP_ACC.1b	**AC.2** is suitable to meet *FDP_ACC.1b* by ensuring that the TOE enforces an access control security function policy for remote callers requesting access to protected methods of enterprise beans using operations defined by an application developer. However the operations must conform to the application developer guidance supplied for the evaluated configuration.
FDP_ACC.1c	**AC.3** is suitable to meet *FDP_ACC.1c* by ensuring that the TOE enforces an access control security function policy for remote callers requesting access to TOE configuration data, TOE files, or TOE runtime state using the set of operations defined.
FDP_ACC.1d	**AC.4** is suitable to meet *FDP_ACC.1d* by ensuring that the TOE enforces an access control security function policy for remote callers requesting access to TOE naming directory using the set of operations defined.
FDP_ACC.1e	**AC.5** is suitable to meet *FDP_ACC.1e* by ensuring that the TOE enforces an access control security function policy for remote callers requesting access to transaction and activities using the set of operations defined.
FDP_ACC.1f	**AC.6** is suitable to meet *FDP_ACC.1f* by ensuring that the TOE enforces an access control security function policy for remote callers requesting access to the local bus, queue destination, temporary destination, topic space, topic space root, and topics using the set of operations defined.

SFRs	TSFs
FDP_ACC.1g	**AC.7** is suitable to meet *FDP_ACC.1g* by ensuring that the TOE enforces an access control security function policy for remote callers requesting access to protected resources of the UDDI registry directory using the set of operations defined.
FDP_ACC.1h	**AC.8** is suitable to meet *FDP_ACC.1h* by ensuring that the TOE enforces an access control security function policy for remote callers requesting access to protected location service resources using the set of operations defined.
FDP_ACC.1i	**AC.9** is suitable to meet *FDP_ACC.1i* by ensuring that the TOE enforces an access control security function policy for remote callers requesting access to user MBeans using the set of operations defined.
FDP_ACF.1a	**AC.1** is suitable to meet *FDP_ACF.1a* by ensuring that the TOE enforces an access control policy which permits or denies remote callers requesting access to protected methods of web server applications using operations defined by an application developer, based on security attributes also defined by an application developer. However the operations and security attributes defined must conform to the application developer guidance supplied for the evaluated configuration.
FDP_ACF.1b	**AC.2** is suitable to meet *FDP_ACF.1b* by ensuring that the TOE enforces an access control policy which permits or denies remote callers requesting access to protected methods of enterprise beans using operations defined by an application developer, based on security attributes also defined by an application developer. However the operations and security attributes defined must conform to the application developer guidance supplied for the evaluated configuration.

SFRs	TSFs
FDP_ACF.1c	**AC.3** is suitable to meet *FDP_ACF.1c* by ensuring that the TOE enforces an access control policy which permits or denies remote callers requesting access to TOE configuration data, TOE files, or TOE runtime state using the set of defined operations, based on the security attributes identified. The security attributes of the TOE configuration data, TOE files, or TOE runtime state are identified as the roles belonging to the Administration roles group. These roles defined are hard-coded with a specific level of access which can only be granted by being mapped to the role. The security attributes of the remote callers include the User/Group ID to role mapping.
FDP_ACF.1d	**AC.4** is suitable to meet *FDP_ACF.1d* by ensuring that the TOE enforces an access control policy which permits or denies remote callers requesting access to the TOE naming directory using the set of defined operations, based on the security attributes identified. The security attributes of the TOE naming directory are identified as the roles belonging to the Naming roles group. These roles defined are hard-coded with a specific level of access which can only be granted by being mapped to the role. The security attributes of the remote callers include the User/Group ID to role mapping.
FDP_ACF.1e	**AC.5** is suitable to meet *FDP_ACF.1e* by ensuring that the TOE enforces an access control policy which permits or denies remote callers requesting access to transactions and activities using the set of defined operations, based on the security attributes identified. The security attributes of the transactions and activities are identified as the Administrator role. This role is hard-coded with a specific level of access which can only be granted by being mapped to the role. The security attributes of the remote callers include the User/Group ID to role mapping.

SFRs	TSFs
FDP_ACF.1f	**AC.6** is suitable to meet *FDP_ACF.1f* by ensuring that the TOE enforces an access control policy which permits or denies remote callers requesting access to the local bus, queue destination, temporary destination, topic space, topic space root, and topics using the set of defined operations, based on the security attributes identified. The security attributes of the local bus, queue destination, temporary destination, topic space, topic space root, and topics are identified as the roles belonging to the Messaging roles group. These roles defined are hard-coded with a specific level of access which can only be granted by being mapped to the role. The security attributes of the remote callers include the User/Group ID to role mapping.
FDP_ACF.1g	**AC.7** is suitable to meet *FDP_ACF.1g* by ensuring that the TOE enforces an access control policy which permits or denies remote callers requesting access to protected resources of the UDDI registry directory using the set of defined operations, based on the security attributes identified. The security attributes of the protected resources of the UDDI registry directory are identified as the list of registered UDDI publishers and the role belonging to the UDDI roles group. This role is hard-coded with a specific level of access which can only be granted by being mapped to the role. The security attributes of the remote callers include the User/Group ID to role mapping.
FDP_ACF.1h	**AC.8** is suitable to meet *FDP_ACF.1h* by ensuring that the TOE enforces an access control policy which permits or denies remote callers requesting access to protected location service resources using the set of defined operations, based on the security attributes identified. The security attributes of the protected location service resources include the WebSphere Application Server ID. The security attributes of the remote caller include the user identity in which the remote caller is authenticated with. A remote caller requesting access to the protected location service resources is only granted access if the remote caller is authenticated as the WebSphere Application Server ID.

SFRs	TSFs
FDP_ACF.1i	**AC.9** is suitable to meet *FDP_ACF.1i* by ensuring that the TOE enforces an access control policy which permits or denies remote callers requesting access to protected methods and attributes in user MBeans using the set of defined operations, based on the security attributes identified. The security attributes are identified as the roles belonging to the Administration roles group. These roles are configured for MBean methods and attributes by the application developer. The application developer must conform to the guidance supplied for the evaluated configuration.
FIA_OBO.EXP.1	**Ident.6** is suitable to meet *FIA_OBO.EXP.1* by ensuring that the TOE provides a means for a remote caller or application to be associated with an additional authenticated identity, in which operations may be performed on behalf of the additional authenticated identity.
FIA_UID.1	**Ident.1** is suitable to meet *FIA_UID.1* by ensuring that the TOE uniquely identifies remote callers by the user ID associated with the remote caller when accessing the TOE through the remote HTTP/S interface for all methods or static web content is configured with a security constraint or for method or static web content not configured with the security constraint of the “Everyone” role.
	Ident.2 is suitable to meet *FIA_UID.1* by ensuring that the TOE uniquely identifies remote callers by the user ID associated with the remote caller when accessing the TOE through the remote ORB interface.
	Ident.3 is suitable to meet *FIA_UID.1* by ensuring that the TOE uniquely identifies remote callers by the user ID associated with the remote caller when accessing the TOE through the remote JMS interface.
	Ident.4 is suitable to meet *FIA_UID.1* by ensuring that the TOE re-identifies a remote caller’s user ID from either a username token, x509 token, or LTPA token when accessing the TOE through either the remote HTTP/S interface.

SFRs	TSFs
	Ident.5 is suitable to meet *FIA_UID.1* by ensuring that the TOE uniquely identifies remote callers by the user ID associated with the remote caller as it is supplied within the LTPA token, when accessing the TOE through the remote HA manager interface.
	Ident.7 is suitable to meet *FIA_UID.1* by ensuring that the TOE uniquely identifies remote callers by the user ID associated with the remote caller as it is supplied within the LTPA token, when accessing the TOE through the remote WS-Transactions interface.
FIA_USB.1	**Ident.1** is suitable to meet *FIA_USB.1* by ensuring that when a remote caller is identified through the remote HTTP/S interface, the TOE properly maps any roles associated to the remote callers authenticated user and/or group ID.
	Ident.2 is suitable to meet *FIA_USB.1* by ensuring that when a remote caller is identified through the remote ORB interface, the TOE properly maps any roles associated to the remote callers authenticated user and/or group ID.
	Ident.3 is suitable to meet *FIA_USB.1* by ensuring that when a remote caller is identified through the remote JMS interface, the TOE properly maps any roles associated to the remote callers authenticated user and/or group ID.
	Ident.4 is suitable to meet *FIA_USB.1* by ensuring that when a remote caller is re-identified through either the remote HTTP/S interface, the TOE properly maps any roles associated to the remote callers authenticated user and/or group ID.
	Ident.5 is suitable to meet *FIA_USB.1* by ensuring that when a remote caller is identified through the remote HA manager interface, the TOE properly maps any roles associated to the remote callers authenticated user and/or group ID.
	Ident.7 is suitable to meet *FIA_USB.1* by ensuring that when a remote caller is identified through the remote WS-Transacations interface, the TOE properly maps any roles associated to the remote callers authenticated user and/or group ID.

SFRs	TSFs
FMT_MSA.1a	**SM.1** is suitable to meet *FMT_MSA.1a* by ensuring that the TOE enforces the web server applications access control policy, the enterprise beans access control policy, the naming directory access control policy, and the messaging access control policy to restrict access to write or delete the mapping of user and group IDs to an application-defined role, messaging role, and naming role to either the Administrator or Configurator role.
FMT_MSA.1b	**SM.1** is suitable to meet *FMT_MSA.1b* by ensuring that the TOE enforces the configuration data, TOE files, and runtime state access control policy and the transaction and activities access control policy to restrict access to write or delete the mapping of user and group IDs to an administration role to the Administrator role.
FMT_MSA.1c	**SM.1** is suitable to meet *FMT_MSA.1c* by ensuring that the TOE enforces the UDDI access control policy to restrict access to write or delete the registered UDDI publishers to the Administrator role or Operator role.
FMT_MSA.3a	**SM.1** is suitable to meet *FMT_MSA.3a* by ensuring that the TOE enforces the UDDI access control policy to provide restrictive default values for the registered UDDI publishers. **SM.1** also ensures that only the Administrator role or Operator role can define alternative registered UDDI publishers.
FMT_MSA.3b	**SM.1** is suitable to meet *FMT_MSA.3b* by ensuring that the TOE enforces the web server applications access control policy, the enterprise beans access control policy, and the messaging access control policy to provide restrictive default values for mapping a user or group ID to an application-defined role, or messaging role. **SM.1** also ensures that only a remote caller associated with either the Administrator role or Configurator role can define alternative role mappings to override the default role mappings.

SFRs	TSFs
FMT_MSA.3c	**SM.1** is suitable to meet *FMT_MSA.3c* by ensuring that the TOE enforces the configuration data, TOE files, and runtime state access control policy, and the transactions and activities access control policy to provide restrictive default values for the user/group IDs to administration roles. **SM.1** also ensures that only a remote caller associated with the Administrator role can define alternative role mappings to override the default administration role mappings.
FMT_MSA.3d	**SM.1** is suitable to meet *FMT_MSA.3d* by ensuring that the TOE enforces the naming directory access control policy to provide permissive default values for the mapping of user/group IDs to naming roles. **SM.1** also ensures that only a remote caller associated with either the Administrator role or Configurator role can define alternative role mappings to override the default role mappings.
FMT_SMF.1	**SM.1** is suitable to meet *FMT_SMF.1* by ensuring that the TOE provides the capability for a remote caller to configure the attribute that stores the list of registered UDDI publishers, the attribute that sets the inherit defaults flag for each Messaging queue, topic space, and topic, the attribute that sets the topic space access check flag for each Messaging topic space, the attribute that maps a user ID and password to a run-as role, the attribute that sets the inherit Sender flag for new topics, the attribute that sets the inherit Receiver flag for new topics, and the attribute that maps user and group IDs to roles..
FMT_SMR.1	**SM.1** is suitable to meet *FMT_SMR.1* by ensuring that the TOE maintains administration roles (Administrator, Configurator, Monitor, Operator, Deployer, and AdminSecurityManager), application-defined roles, messaging roles (Browser, Bus Connector, Creator, Receiver, Sender), naming roles (COSNamingCreate, COSNamingDelete, COSNamingRead, COSNamingWrite), and UDDI roles (SOAP_Publish_User, V3SOAP_CustodyTransfer_User_Role, V3SOAP_Publish_User_Role,V3SOAP_Security_User_ Role, EJB_Publish_Role).

End of Document