Swedish Certification Body for IT Security

Certification Report - Oracle WebLogic

Issue: 1.0, 2016-dec-21

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Executive Summary

The TOE is Oracle WebLogic Server Version 12.1.3. It is a Java Enterprise Edition (Java EE) application server.

The WebLogic Server is a complete implementation of the Java EE 6 specification which provides a standard set of APIs for creating distributed Java applications that can access a wide variety of services, such as databases, messaging services, and connections to external enterprise systems. End-user clients access these applications using Web browser clients or Java clients.

The TOE comprises the following components:

- Oracle WebLogic Server version 12.1.3
- JDK Java Cryptographic Extension (JCE) provider
- JDK Java Secure Socket Cryptographic Extension (JSSE) provider
- RSA Java Cryptographic Extension (JCE) provider, included in RSA Crypto-J version 6.1.1
- RSA Java Secure Socket Extension (JSSE) provider, included in RSA SSL-J version 6.1.2

The TOE does not include the hardware, firmware, operating system or Java virtual machine used to run the software components.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT Security Evaluation, version 3.1, release 4.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 2 + ALC_FLR.1

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2014011
Name and version of the certified IT product	Oracle WebLogic Server 12.1.3
Security Target Identification	ST Oracle WebLogic Server 12.1.3 Security Target, version, 1.30, 2016-12-05
EAL	EAL 2 + ALC_FLR.1
Sponsor	Oracle America, Inc.
Developer	Oracle America, Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
Certification date	2016-10-12-21

3 Security Policy

The following sections briefly describe the security functionality provided by the TOE. A more detailed explanation can be found in [ST] Chapter 7, TOE Summary Specification.

3.1 Identification and Authentication

The TOE provides single and multiple identification and authentication using one or more of the following credentials:

- Username and password credential pairs
- X.509 digital certificates
- Identity Assertion tokens

The TOE implements this functionality with the WebLogic Security Framework and the following security providers:

- Authentication providers
- Identity Assertion providers
- Credential Mapping providers

3.2 Authorization

The TOE provides a role-based access control policy, applicable to all type of resources, management related or application related. Authorization for performing a certain action on a given resource is defined though security roles, security policies and access decisions.

The TOE implements this functionality with the WebLogic Security Framework and the following security providers:

- Role Mapping provider
- Authorization providers
- Adjudication provider

3.3 User Data Protection

The TOE provides protection of user data transmitted between the TOE and IT entities, and between TOE instances within the same application server domain through the use of secure channels with the TLS protocol, which is provided by the operational environment. Establishment of a secure channel in the different communication paths is optional; protection can be assured by other security measures in the operational environment.

The TOE also supports Web Service Security, which provides integrity and confidentiality of web service payloads.

3.4 Auditing

The TOE generates audit records on application and management related events.

The TOE implements this functionality with the WebLogic Security Framework and the following security providers:

- Auditing provider

3.5 Security Management

The TOE provides the WebLogic Admin Console for all administrative activities (start/stop of servers, domain configuration, user and group management, role management, policy management, application deployment etc.). The TOE also provides a Java Extension Management (JMX) interface, which allows the use of other JMX clients to perform management activities through the use of Managed Beans (MBeans). The WebLogic Scripting Tool (WLST) is one of these JMX clients.

MBeans are considered JMX resources in the access control policy.

The TOE enforces authentication and authorization for security management actions using the same security framework.

3.6 Cryptographic support

The TOE incorporates the following components for cryptographic support:

- The Java Secure Socket Extension (JSSE) is the Java standard framework for the SSL and TLS protocols, including functionality for data encryption, server authentication, message integrity, and optional client authentication.
- The Java Cryptographic Extension (JCE) provides a framework and a default implementation for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms.

The TOE requires cryptography for supporting the following functionality:

- Signature generation and verification for SAML 1.1 and 2.0 assertions.
- Validation of X.509 certificates
- Digest Authentication (only for Web Service Security Username Token Profile 1.0 and 1.1)
- SPNEGO Authentication
- Establishment of secure channels using the TLS protocol for communication between instances of the TOE (admin and managed servers, clustered managed servers) and the TOE with external IT entities (application clients, web browsers, LDAP servers, etc).
- XML signature and encryption for Web Service Security.

Correctness of the cryptographic algorithms has been verified as part of the testing process of the TOE, whose test cases cover the following functionality:

- Single Sign-on (SSO) using SAML 1.1, SAML 2.0 and SPNEGO.
- Encryption and decryption of sensitive data (e.g. passwords)
- Processing of web services with policies including XML signing and encryption.
- Certificate validation
- TLS communication

It is to note that the TOE can be set in FIPS 140-2 mode, and for that purpose, it uses the RSA BSAFE® Crypto-J JSAFE and JCE Software Module version 6.1.1, which is a FIPS-140-2 validated, security level 1 cryptographic module (certificate #2058).

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes two assumptions on the usage of the TOE.

A.ADMIN - It is assumed that there are one or more competent individuals who are assigned to manage the TOE, the operational environment, and the security of the information it contains. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

A.DEVEL - The developer of user applications executed by the TOE, including web server applications and enterprise beans, is trustworthy and will comply with all instructions set forth by the user guidance and evaluated configuration guidance of the TOE.

4.2 Environmental Assumptions

Seven assumptions on the environment are made in the Security Target.

A.PROTECT - The TOE and the hardware and software executing the TOE will be physically protected from unauthorized modification including unauthorized modifications by potentially hostile outsiders.

A.SYSTEM - The operating system and the Java virtual machine operate according to their specification.These external systems are configured in accordance with the installation guidance and the evaluated configuration guidance of the TOE.

A.CLOCK - The real time clock of the underlying operating system provides reliable time stamps.

A.PKI - It is assumed that digital certificates, CRLs used for certificate validation and private and public keys are generated externally and imported into the TOE, meeting the corresponding standards and providing sufficient security strength through the use of appropriate key lengths and cryptographic algorithms.

A.IDENTITY_PROVIDER - External entities configured in the TOE to provide identity assertions for authentication of users operate according to the specification. Successful verification of the origin of the identity assertion and trust of the external entity are sufficient to authenticate a user in the TOE.

A.DS - External entities providing storage for TSF data in the operational environment like LDAP servers or database servers are trusted, and are protected against unauthorized physical access and modification.

A.COMM_PROT - Communication between the TOE instances that constitute an application server domain, and between the TOE and external entities providing services to the TOE, is protected from eavesdropping and modification.

4.3 Organizational Security Policies

The Security Target [ST] makes two Organizational Security Policies on the usage of the TOE.

P.ACCOUNTABILITY - The users of the system shall be held accountable for security-relevant actions within the system.

P.CONSISTENCY - Configuration information and TSF data of the administration domain shall be kept consistent in all TOE instances that are part of that domain.

4.3.1 Threats countered by the TOE

The Security Target [ST] contains three threats, which have been considered during the evaluation.

T.IMPERSONATE_USER - An unauthenticated individual may impersonate a user of the TOE to gain access to protected TSF data or user data.

T.UNAUTHORIZED_ACCESS - An authenticated user may gain access to resources or perform operations on resources for which no access rights have been granted.

T.DATA_COMPROMISE - An unauthorized user is able to eavesdrop on, or manipulate without detection, the data exchanged between the TOE and a remote trusted IT product, or data in transit between instances of the TOE in the same application server domain.

5 Architectural Information

Oracle WebLogic Server is an application server that allows users to access applications over various network protocols. WebLogic Server executes Java applications which are registered and are executed by the application server.

WebLogic Server provides a Java EE-compliant environment which is consistent with the Java EE 6 specification as defined by JSR-316, with additional support of selected Java EE 7 APIs. The applications developed for and served by the TOE are to be written in Java. Developers of the Java application implement the business logic and are free to utilize the supporting functionality of Java EE.

As part of the Java EE framework implemented by WebLogic Server, applications can provide their logic to remote clients through the following network protocols:

- HTTP/HTTPs protocols: Java servlets, Enterprise Java Beans, JMS queues, Web Services and WebSockets provide their functionality based on URLs requested by the client.
- RMI, RMI over IIOP and T3 protocols: Enterprise Java Beans (EJB) and JMS queues can provide services through these protocols.

6 Documentation

Guidance Supplement for Oracle (R) Weblogic Server 12.1.3 [CCGUIDE]	Version 1.2. August 2016
Understanding Oracle WebLogic Server [INTRO]	E41937-04, August 2015
Understanding Oracle Fusion Middleware Concepts [ASCON]	E48202-01, May 2014
Understanding Domain Configuration for Oracle WebLogic Server [DOMCF]	E41943-04, August 2015
Release Notes for Oracle WebLogic Server [WLSRN]	E41931-13, April 2016
Planning an Installation of Oracle Fusion Middleware [ASINS]	E48353-01, May 2014
Installing and Configuring Oracle WebLogic Server and Coherence [WLSIG]	E48355-02, July 2014
Installing Software with the Oracle Universal Installer [OUIRF]	E48351-01, May 2014
Creating WebLogic Domains Using the Configuration Wizard [WLDCW]	E41890-02, August 2015
Domain Template Reference for Fusion Middleware 12.1.3 [WLDTR]	E41892-02, August 2015
Administering Server Environments for Oracle WebLogic Server [CNFGD]	E41942-07, August 2015
Administering Server Startup and Shutdown for Oracle WebLogic Server [START]	E41938-05, May 2016
Administering JDBC Data Sources for Oracle WebLogic Server [JDBCA]	E41864-09, May 2016
Administering JMS Resources for Oracle WebLogic Server [JMSAD]	E41859-04, August 2015
Administering the JMS Resource Adapter for Oracle WebLogic Server [JMSRA]	E41853-02, August 2015
Administering Clusters for Oracle WebLogic Server [CLUST]	E41944-06, August 2015
Administering Node Manager for Oracle WebLogic Server [NODEM]	E41941-05, May 2016
Understanding Security for Oracle WebLogic Server [SCOVR]	E42028-02, August 2015
Administering Security for Oracle WebLogic Server [SECMG]	E41905-08, April 2016
Securing a Production Environment for Oracle WebLogic Server [LOCKD]	E41900-06, March 2016
Securing Resources Using Roles and Policies for Oracle WebLogic Server [ROLES]	E41904-02, August 2015

Securing WebLogic Web Services for Oracle WebLogic Server [WSSOV]	E42030-02, August 2015
Deploying Applications to Oracle WebLogic Server [DEPGD]	E41940-03, August 2015
Developing Enterprise JavaBeans for Oracle WebLogic Server [EJBAD]	E47839-05, August 2015
Developing Enterprise JavaBeans, Version 2.1, for Oracle WebLogic Server [EJBPG]	E47840-04, August 2015
Developing JAX-RPC Web Services for Oracle WebLogic Server [WSRPC]	E47707-03, August 2015
Developing JAX-WS Web Services for Oracle WebLogic Server [WSGET]	E47706-04, August 2015
Developing and Securing RESTful Web Services for Oracle WebLogic Server [RESTF]	E47709-02, August 2015
Developing JDBC Applications for Oracle WebLogic Server [JDBCP]	E41865-04, August 2015
Developing Resource Adapters for OracleWebLogic Server [ADAPT]	E41877-02, August 2015
Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server [WBAPP]	E41936-07, August 2015
Developing Applications with the WebLogic Security Service [SCPRG]	E42029-04, August 2015
Command Reference for Oracle WebLogic Server [ADMRF]	E42026-03, August 2015
WLST Command Reference for WebLogic Server [WLSTC]	E35669-03, February 2016
The WebLogic Server MBean Reference [WLMBR]	E41843-02, February 2015

7 IT Product Testing

7.1 Test Configuration

The developer testing was performed at the developer site in Burlington, Massachusetts, USA.

The evaluator used the same testing environment as the one used by the developer for testing. The testing hardware / software configuration is as follows:

- Oracle Linux 6.7 and Solaris Platform 11.3 with the Oracle Java SDK v 1.8.0_91 with Java HotSpotTM Client VM installed.
- Oracle Fusion Middleware 12c (12.1.3.0.0) WebLogic Server and Coherence [V44413-01.zip] downloaded from (https://edelivery.oracle.com) are installed, along with 12.1.3.0.160719 Patch Set Update (PSU) for WebLogic Server 12.1.3.0 from Master Note on WebLogic Server Patch Set Updates (PSUs) (Doc ID 1470197.1) (https://support.oracle.com/epmos/faces/DocContentDisplay?id=1470197.1)
- WLS 12.1.3 is configured according to the WLS 12.1.3 Security Target and associated guidance documents, including the deserialization blacklist setting provided in Chapter 3 of the Guidance Supplement for Oracle Weblogic Server 12.1.3, version 1.2, August 2016.
- The test environment needs following prerequisites:
  - bash shell
  - The perforce (Source Code Control System used for WebLogic product Development).
- All tests are carried out on a single machine with a test client interacting with a WebLogic Server instance on the same machine.

The evaluator testing was performed at the evaluation facility in Stockholm. The following testing environment was used, which has been found to be compliant with the requirements stated in the [ST]:

- Oracle Linux 6, latest version
- Oracle Java Development Kit (JDK) version 8, latest update

Furthermore, in order to access functionality on the TOE and deployed applications, an additional workstation is used. It has no specific requirements other than a working Java (JDK 8) environment and network access to the TOE. The evaluator therefore used a standard Linux Debian installation. The TOE was installed according to the provided TOE guidance [CCGUIDE] and the therein referenced documents.

7.2 Developer Testing

7.2.1 Testing Effort

The test suites are grouped according to the TOE security functionality:

- Auditing
- Authorization
- Identification and Authentication
- User Data Protection
- Security Management

Testing is automated, and written in Java to directly exercise the TOE functionality. Most tests can be parametrized using XML files. The expected outcome is part of the test code. All results are collected and summarized as a HTML page.

Testing of the TOE was performed on one of the supported platforms, Oracle Linux. The evaluator considered this sufficient since the TOE is written in Java, in which case the JDK provides an abstraction layer to the underlying platform.

7.2.2 Test results

All test cases completed successfully.

7.3 Evaluator Testing Effort

7.3.1 Testing Effort

The developer tests focused on the most visible interfaces and those exposed to user applications.

The evaluator test cases were selected based on the TOE security functionality, considering existing test coverage provided by the developer.

7.3.2 Test results

All developer and evaluator test cases were found to be completed successfully. No issues were identified.

7.4 Evaluator Penetration Testing

Based on the analysis performed in work unit AVA_VAN.2-5, the evaluator did not identify any potential vulnerability. No additional penetration testing was therefore required.

Please note that since the search was intended to identify possible potential vulnerabilities in the TOE (CEM para. 1459), the public vulnerability search was not performed on the underlying non-TOE platform (Oracle Linux 6.7, Oracle Solaris 11.3, or Java Runtime Environments).

8 Evaluated Configuration

The following security providers are allowed in the evaluated configuration:

Security provider	Description
XACML Authorization Provider	Authorization provider based on XACML. This is the default authorization provider.
WebLogic Adjudication Provider	This provider tallies the potentially differing results rendered by multiple Authorization providers' Access Decisions and renders a final verdict on granting access to a resource. This is the default adjudication provider.
XACML Role Mapping Provider	Role Mapping provider based on XACML. This is the default rolemapping provider.
WebLogic Auditing Provider	This provider records information from a number of security requests, which are determined internally by the Security Framework. It must be configured in the evaluated configuration.
WebLogic Credential Mapping Provider	This provider maps a user's authentication credentials (username and password) to those required for legacy applications, so that the legacy application gets the necessary credential information.
PKI Credential Mapping Provider	This provider maps a subject (the initiator) and target resource (and an optional credential action) to a key pair or public certificate that can be used by applications when accessing the targeted resource. The PKI Credential Mapping provider uses the subject and resource name to retrieve the corresponding credential from the keystore.
SAML 1.1 Credential Mapping Provider Version 2	This provider generates SAML 1.1 assertions for authenticated subjects based on relying party/destination site configuration.
SAML 2.0 Credential Mapping Provider	This provider generates SAML 2.0 assertions that can be used to assert identity in the following use cases: SAML 2.0 Web SSO Profile WS-Security SAML Token Profile version 1.1
WebLogic CertPath Provider	This provider completes certificate paths and validates certificates using the trusted CA configured for a particular server instance. This is the default certificate and validation provider.
Certificate Registry	This provider allows explicit registration of the list of trusted certificates that are allowed to access the TOE. Only certificates that are registered in the Certificate Registry will be considered valid. The Certificate Registry provides an inexpensive mechanism for performing revocation checking.
WebLogic Authenticat-	This provider uses the embedded LDAP server to store user

ion Provider	and group membership information. This is the default authentication provider.
Oracle Internet Directory Authentication Provider	This provider uses the Oracle Internet Directory server to store user and group membership information
Oracle Virtual Directory Authentication Provider	This provider uses the Oracle Virtual Directory server to store user and group membership information
iPlanet Authentication Provider	This provider uses the iPlanet LDAP server to store user and group membership information
Active Directory Authentication Provider	This provider uses Active Directory server to store user and group membership Information
Open LDAP Authentication Provider	This provider uses the Open LDAP server to store user and group membership information
Novell LDAP Authentication Provider	This provider uses the Novell LDAP server to store user and group membership information
SQL Authenticator Provider	This provider uses a SQL database and allows both read and write access.
Read-only SQL Authenticator Provider	This provider uses a SQL database and allows only read access
SAML Authenticator Provider	This provider may be used in conjunction with the SAML 1.1 or SAML 2.0 Identity Assertion provider to allow virtual users to log in via SAML, or create an authenticated subject using the username and groups retrieved from a SAML assertion
Password Validation Provider	This provider manages and enforces a set of configurable password composition rules, and is automatically invoked by a supported authentication provider whenever a password is created or updated for a user. This the default password validation provider.
WebLogic Identity Asserter	This provider supports identity assertion with X.509 certificates and CORBA Common Secure Interoperability version 2 (CSI v2). This is the default identity assertion provider.
LDAP X.509 Identity Asserter	This provider receives an X509 certificate, looks up the LDAP object for the user associated with that certificate, ensures that the certificate in the LDAP object matches the presented certificate, and then retrieves the name of the user from the LDAP object.
Negotiate Identity Asserter	This provider enables single sign-on (SSO) with Microsoft clients. It decodes Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) tokens to obtain Kerberos tokens, validates the Kerberos tokens, and maps Kerberos tokens to WebLogic users.

SAML Identity Asserter (for SAML 1.1) Version 2	This provider acts as a consumer of SAML 1.1 security assertions, allowing the TOE to act as a destination site for using SAML 1.1 for single sign-on. It validates SAML 1.1 assertions by checking the signature and validating the certificate for trust in the certificate registry maintained by the provider.
SAML 2.0 Identity Asserter	This provider acts as a consumer of SAML 2.0 security assertions, allowing the TOE to act as a Service Provider for: - Web single sign-on - WebLogic Web Services Security: accepting SAML tokens for identity through the use of the appropriate WS-SecurityPolicy assertions

Table 1: Supported Security Providers

The following features are not allowed in the evaluated configuration:

- Resources:
  - Common Object Model
- Security providers:
  - Custom RDBMS Authenticator Authentication provider
  - WebLogic Authorization Provider
  - Windows NT Authentication provider
  - WebLogic Role Mapping Provider
  - Custom Security Providers
- Protocols:
  - Simple Network Management Protocol (SNMP)
  - Distributed Common Object Model (DCOM)
- Java Standards:
  - Java Authentication Service Provider Interface for Containers (JASPIC)

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Enhanced-Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarized in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE Design	ADV_TDS.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Flaw Remediation	ALC_FLR.1	PASS
Security Target Evaluation	ASE	PASS
ST introduction	ASE_INT	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product or using the product.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	A set of software, firmware and/or hardware possibly accompanied by guidance.

12 Bibliography

[CCGUIDE]	Guidance Supplement for Oracle (R) Weblogic Server 12.1.3 Version 1.2. August 2016
[INTRO]	Understanding Oracle WebLogic Server E41937-04, August 2015
[ASCON]	Understanding Oracle Fusion Middleware Concepts E48202-01, May 2014
[DOMCF]	Understanding Domain Configuration for Oracle WebLogic Server E41943-04,August 2015
[WLSRN]	Release Notes for Oracle WebLogic Server E41931-13, April 2016
[ASINS]	Planning an Installation of Oracle Fusion Middleware E48353-01, May 2014
[WLSIG]	Installing and Configuring Oracle WebLogic Server and Coherence E48355-02, July 2014
[OUIRF]	Installing Software with the Oracle Universal Installer E48351-01, May 2014
[WLDCW]	Creating WebLogic Domains Using the Configuration Wizard 41890-02, August 2015
[WLDTR]	Domain Template Reference for Fusion Middleware 12.1.3 E41892-02, August 2015
[CNFGD]	Administering Server Environments for Oracle WebLogic Server, E41942-07, August 2015
[START]	Administering Server Startup and Shutdown for Oracle WebLogic Server E41938-05, May 2016
[JDBCA]	Administering JDBC Data Sources for Oracle WebLogic Server E41864-09, May 2016
[JMSAD]	Administering JMS Resources for Oracle WebLogic Server E41859-04, August 2015
[JMSRA]	Administering the JMS Resource Adapter for Oracle WebLogic Server E41853-02, August 2015
[CLUST]	Administering Clusters for Oracle WebLogic Server E41944-06, August 2015
[NODEM]	Administering Node Manager for Oracle WebLogic Server E41941-05, May 2016
[SCOVR]	Understanding Security for Oracle WebLogic Server E42028-02, August 2015
[SECMG]	Administering Security for Oracle WebLogic Server E41905-08, April 2016
[LOCKD]	Securing a Production Environment for Oracle WebLogic Server E41900-06, March 2016

[ROLES]	Securing Resources Using Roles and Policies for Oracle WebLogic Server E41904-02, August 2015
[WSSOV]	Securing WebLogic Web Services for Oracle WebLogic Server E42030-02, August 2015
[DEPGD]	Deploying Applications to Oracle WebLogic Server E41940-03, August 2015
[EJBAD]	Developing Enterprise JavaBeans for Oracle WebLogic Server E47839-05, August 2015
[EJBPG]	Developing Enterprise JavaBeans, Version 2.1, for Oracle WebLogic Server E47840-04, August 2015
[WSRPC]	Developing JAX-RPC Web Services for Oracle E47707-03, August 2015WebLogic Server
[WSGET]	Developing JAX-WS Web Services for Oracle WebLogic Server E47706-04, August 2015
[RESTF]	Developing and Securing RESTful Web Services for Oracle WebLogic Server E47709-02, August 2015
[JDBCP]	Developing JDBC Applications for Oracle WebLogic Server E41865-04, August 2015
[ADAPT]	Developing Resource Adapters for OracleWebLogic Server E41877-02, August 2015
[WBAPP]	Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server E41936-07, August 2015
[SCPRG]	Developing Applications with the WebLogic Security Service E42029-04, August 2015
[ADMRF]	Command Reference for Oracle WebLogic Server E42026-03, August 2015
[WLSTC]	WLST Command Reference for WebLogic Server E35669-03, February 2016
[WLMBR]	The WebLogic Server MBean Reference E41843-02, February 2015

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
1.20	2016-10-20	No impact
1.19.3	2016-06-02	No impact
1.19.2	2016-04-28	No impact
1.19.1	2016-03-07	No impact
1.19	2016-02-05	No impact
1.18.1	2015-08-21	No impact
1.18	2015-06-18	No impact
1.17.3	2015-01-29	No impact
1.17.2	2015-01-13	No impact
1.17.1	2014-12-02	Original version

A.2 Scheme Notes

Version	Introduced	Impact of changes
4.0	Application	Original version