UK IT SECURITY EVALUATION AND
CERTIFICATION SCHEME

UKAS
PRODUCT
CERTIFICATION
122-B

COMMON CRITERIA CERTIFICATION REPORT No. P223

Oracle Application Server 10*g*

(Oracle Containers for J2EE and Oracle Internet Directory)
Release 9.0.4.0.0
running on Sun Solaris 8 2/02

Issue 1.0

May 2006

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham, GL51 0EX
United Kingdom

ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party’s claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Trademarks:

CERTIFICATION STATEMENT

The Target of Evaluation is Oracle Application Server 10*g* (Oracle Containers for J2EE and Oracle Internet Directory), Release 9.0.4.0.0. This comprises the following two components of Oracle Application Server:

- Oracle Application Server Containers for J2EE 10*g* (Release 9.0.4.1.0). This is a Java 2 Enterprise Edition environment, written entirely in Java and executes on the Java Virtual Machine.
- Oracle Internet Directory 10*g* (Release 9.0.4.0.0). This is a general purpose directory service that enables fast retrieval and centralised management of information about users and network resources. It has previously been certified to Evaluation Assurance Level EAL4 augmented by ALC_FLR.3.

Oracle Application Server 10*g* (Oracle Containers for J2EE and Oracle Internet Directory), Release 9.0.4.0.0, has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL4 (i.e. augmented by ALC_FLR.3), for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the platforms specified in Annex A.

Originator	**CESG** Certifier
Reviewer	**CESG** Deputy Certifier
Date authorised	11 May 2006

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
J2EE	Java 2 Enterprise Edition
JAAS	Java Authentication and Authorisation Service
JNDI	Java Naming and Directory Interface
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
OC4J	Oracle Application Server Containers for J2EE
OID	Oracle Internet Directory
ONS	Oracle Net Services
OPMN	Oracle Process Manager and Notification Server
OSP	Organisational Security Policy
PL/SQL	Programming Language / Structured Query Language
PWD	Password
SFR	Security Functional Requirement
SOF	Strength of Function
SQL	Structured Query Language
SSL	Secure Sockets Layer
TOE	Target of Evaluation
TSF	TOE Security Functions
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Security Target for Oracle Application Server 10*g* (9.0.4),
Oracle Corporation,
Issue 1.0, May 2006.

b. Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-001, Version 2.2, January 2004.

c. Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-002, Version 2.2, January 2004.

d. Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-003, Version 2.2, January 2004.

e. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-004, Version 2.2, January 2004.

f. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

g. CLEF Requirements - Startup and Operation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

h. CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 1.1, October 2003.

i. Common Criteria Certification Report No. P210:
Oracle Internet Directory 10*g* Release 9.0.4.0.0,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, February 2005.

j. Common Criteria Certification Report No. P178:
Oracle9*i* Database Enterprise Edition Release 9.2.0.1.0,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, September 2003.

k. Common Criteria Certification Report No. P182:
Sun Solaris Version 8 2/02,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, April 2003.

l. Task LFL/T207 Evaluation Technical Report 1,
LogicaCMG CLEF,
310.EC201092:30.1, Issue 1.0, 23 September 2004.

m. Task LFL/T207 Evaluation Technical Report 2,
LogicaCMG CLEF,
Task207.310.EC201092:30.2.4, Issue 1.0, 15 December 2005.

n. Task LFL/T207 Evaluation Technical Report 3,
LogicaCMG CLEF,
Task207.310.EC201092:30.3.10, Issue 1.0, 28 February 2006.

o. Evaluated Configuration for Oracle Application Server 10*g* (9.0.4),
Oracle Corporation,
Issue 0.3, May 2006.

p. Oracle Application Server Containers for J2EE: Security Guide, 10*g* (9.0.4),
Oracle Corporation,
Part No. B10325-02, September 2003.

q. Oracle Application Server Containers for J2EE: User’s Guide, 10*g* (9.0.4),
Oracle Corporation,
Part No. B10322-01, September 2003.

r. Security Target for Oracle Internet Directory 10*g* (9.0.4),
Oracle Corporation,
Issue 1.0, November 2004.

s. Evaluated Configuration for Oracle Internet Directory 10*g* (9.0.4),
Oracle Corporation,
Issue 0.5, September 2005.

t. Oracle Internet Directory: Administrator’s Guide, 10*g* (9.0.4),
Oracle Corporation,
Part No. B12118-01, September 2003.

u. Oracle Process Manager and Notification Server: Administrator’s Guide, 10*g* (9.0.4),
Oracle Corporation,
Part No. B12057-02, March 2004.

v. Evaluated Configuration for Oracle9*i*, Release 2 (9.2.0),
Oracle Corporation,
Issue 0.7, March 2003.

w. Solaris 8-2/02 Security Testing - Installation Procedure,
Sun Microsystems,
Issue 0.1, 5 November 2002.

x. Oracle Application Server 10*g*: Quick Installation and Upgrade Guide, 10*g* (9.0.4)
for Solaris Operating System (SPARC),
Oracle Corporation,
Part No. B10936-01, December 2003.

y. Oracle Application Server: Quick Installation and Upgrade Guide, 10*g* Release 2 (10.1.2)
for Solaris Operating System (SPARC),
Oracle Corporation,
Part No. B14089-01, December 2004.

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Oracle Application Server 10*g* (Oracle Containers for J2EE and Oracle Internet Directory), Release 9.0.4.0.0, to the Sponsor, Oracle Corporation, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

Oracle Application Server 10*g* (Oracle Containers for J2EE and Oracle Internet Directory), Release 9.0.4.0.0.

4. This comprises the following two components of Oracle Application Server:

a. Oracle Application Server Containers for J2EE 10*g* (Release 9.0.4.1.0). This report identifies it as 'OC4J'.
Note: It is obtained by applying Oracle Application Server 10*g* Patch Set 1 - July 2004 to Oracle Application Server Containers for J2EE 10*g* (Release 9.0.4.0.0).

b. Oracle Internet Directory 10*g* (Release 9.0.4.0.0). This report identifies it as 'OID'.

5. This report describes the product as the Target of Evaluation (TOE) and identifies it as 'Oracle Application Server'. The Developer was Oracle Corporation.

6. OC4J is a Java 2 Enterprise Edition (J2EE) 1.3 certified server implementation that is written entirely in Java and executes on the Java Virtual Machine (JVM). OC4J provides all of the containers, Application Programming Interfaces (APIs) and services that J2EE specifies. OC4J supports the Java Authentication and Authorisation Service (JAAS) and is Oracle Application Server's JAAS Provider. (JAAS aims to reduce development costs, by allowing developers to use a declarative security model instead of integrating security programmatically.)

7. OC4J can perform two types of authorisation checks:

a. J2EE authorisation, regarding a user's permission to access a J2EE application. (J2EE authorisation is within the scope of the evaluation.)

b. JAAS authorisation, regarding a user's permission to perform an action on a resource after the J2EE application has been entered. (JAAS authorisation is outside the scope of the evaluation.)

8. OID is a general-purpose directory service, which runs as an Oracle9*i* application. OID relies on the Oracle9*i* database for the storage of directory data and it communicates with that database using Oracle Net Services (ONS), which is Oracle's operating system-independent, database connectivity solution. OID enables fast retrieval and centralised management of data about distributed users and network resources, including security data such as user names and passwords for the Oracle9*i* product stack. OID combines the Lightweight Directory Access Protocol (LDAP) Version 3 with the performance, scalability, robustness, and availability of the Oracle9*i* Database Server. (LDAP is a standard, extensible directory access protocol that is used by LDAP clients and servers to communicate.)

9. OID has previously been certified to Evaluation Assurance Level EAL4 augmented by ALC_FLR.3 [i].

10. The security functionality in the TOE includes:

a. user identification and authentication, with password management;

b. application access control - which permits users to access applications hosted by OC4J if they have sufficient authorisation;

c. security attribute maintenance - which provides the means for creating and maintaining the security attributes for TOE users and user repository entries;

d. user repository access controls - which use Access Control Items held in the directory to define users' authorisations for user repository data access;

e. auditing.

11. Annex A summarises the evaluated configuration, including its guidance documentation. Annex B outlines the security architecture. Annex C summarises the product testing.

TOE Scope

12. The scope of the TOE comprises the following software components:

a. Oracle Application Server Containers for J2EE 9.0.4.1.0.

b. Oracle Internet Directory 9.0.4.0.0.

c. Oracle Internet Directory Server 9.0.4.0.0.

d. Oracle Internet Directory Tools 9.0.4.0.0, specifically the following command-line tools, which provide essential features by which the directory can be maintained and administered securely:

i. The following runtime tools, to run the OID Server instances:

- **`oidmon`** (i.e. the OID monitor, which initiates, monitors, and terminates the LDAP server processes);
- **`oidctl`** (i.e. the OID control utility, which communicates with **`oidmon`** by placing message data in OID Server tables.

ii. The following directory administration tools:

- **`catalog`** (i.e. the catalogue management tool);

- `bulkload`, `bulkdelete`, `bulkmodify` and `ldifwrite` (i.e. the bulk operations tools);
- `oidpasswd` (i.e. the OID database password utility);
- `oidstats` (i.e. the OID database statistics collection tool).

e. Oracle Process Management Notification 9.0.4.1.0.

f. Java Naming and Directory Interface Libraries 1.2.1.0.0.

13. The scope of the evaluation applies to the TOE:

a. when using Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) (identified in this report as ‘Oracle9*i*’), which has previously been certified to EAL4 augmented by ALC_FLR.3 [i]; and

b. when running on the Sun Solaris Version 8 2/02 operating system (identified in this report as ‘Solaris8’), which has previously been certified to EAL4 [k].

14. The Evaluated Configuration document [o] defines how the TOE must be installed in its evaluated configuration and defines the requirements for setting up the TOE environment. Attention is drawn to the configuration instructions in [o], particularly:

- [AS.POST-4] which prevents user access to certain administrative web pages
- [AS.CA-1] which seeks to prevent other applications running on client or server host machines with access to the network.

15. The section ‘Other Oracle Application Server Products’ in Chapter 2 of the Security Target [a] lists the main security-related products which are components of Oracle Application Server but lie outside the boundary of the TOE for this evaluation. These are:

- Oracle HTTP Server;
- Oracle Application Server Single Sign-on;
- Oracle Application Server Portal;
- Oracle Application Server Certification Authority.

16. The section ‘Other OC4J and OID Security Features’ in Chapter 2 of the Security Target [a] lists the features of OC4J and OID that lie outside the boundary of the TOE for this evaluation. These are:

a. The following OC4J features:

- Java Message Service;
- Remote Method Invocation;
- Data Sources;
- Java Transaction API;
- J2EE Connector Architecture;
- Java Object Cache;
- XML-based JAAS Provider;
- XMLUserManager;
- JAZN Admintool (but note that JAAS authorisation is outside the scope of the evaluation);

- Authentication other than via Basic Authentication (since Oracle Application Server Single Sign-on and Secure Sockets Layer (SSL) authentication environments are outside the scope of the evaluation).

b. The following OID components:

- Directory Replication Service;
- Directory Integration Platform;
- Server Side Plug-in Framework.

c. The following Directory Administration Tools:

- Oracle Directory Manager;
- Directory Replication Service Tools (i.e. the OID Reconciliation Tool and the Human Intervention Queue Manipulation Tool);
- Delegated Administration Service;
- Enterprise Manager Integration;
- the command-line tools which can be used to send LDAP messages to a host OID Server.

d. OID's use of SSL (since it is assumed that the OID Server and the clients used to access it are all within a secure network).

e. Facilities for enterprise users.

f. Guest user and proxy user (since the Evaluated Configuration document [o] requires that only the directory administrator knows the passwords for these users).

g. The OID C API and the OID Programming Language / Structured Query Language (PL/SQL) API.

h. The following Configuration Tools:

- Enterprise Manager;
- Distributed Configuration Management.

Protection Profile Conformance

17. The Security Target [a] did not claim conformance to any protection profile.

Assurance

18. The Security Target [a] specifies the assurance requirements for the evaluation. These comprise CC predefined Evaluation Assurance Level EAL4, augmented by ALC_FLR.3.

19. CC Part 1 [b] provides an overview of the Common Criteria. CC Part 3 [d] describes the scale of assurance given by predefined levels EAL1 to EAL7.

Strength of Function Claims

20. The Security Target [a] claims that the minimum Strength of Function (SOF) for the TOE is SOF-high.

21. That claim applies only to the user password mechanism. User authentication is required to ensure that a user has the required permissions to access a J2EE application.

22. OID implements four different levels of authentication when a connection is requested to the user repository's directory server (as detailed in the Security Target [a]):

a. Anonymous authentication (i.e. security function IA.ASESS).

b. Password-based (simple) authentication (i.e. security function IA.USESS). Note: OC4J refers to password-based authentication as Basic Authentication.

c. Certificate-based authentication, through SSL. (Note: This method of authentication is outside the scope of the evaluation.)

d. Indirect authentication (i.e. security function IA.PSESS, which is employed when a user repository session has been established using IA.USESS above).

23. The Security Target [a] identifies that the following security functions support the claimed SOF:

a. IA.AUTH and IA.USESS (SOF-High);

b. IA.PWDC, SAM.UATT and SAM.CHPWD (which all support IA.AUTH and IA.USESS by providing password management facilities).

Security Policy

24. The Security Target [a] identifies the following explicit security policy, with which the TOE must comply:

User Repository Access Control Security Policy, which the Security Target defines in the following Security Functional Requirements (SFRs) of the TOE:

- (user data protection): FDP_ACC.1 and FDP_ACF.1;
- (security management): FMT_MSA.1 and FMT_MSA.3.

25. In addition, the evaluators identified the following implicit security policies in the Security Target [a], with which the TOE must comply:

a. *Object Access Control Security Policy* (i.e. access is controlled to the user repository objects and to applications hosted by OC4J) – this is associated with objective O.ACCESS of the Security Target.

b. *Identification and Authentication Security Policy* (i.e. identification and authentication is required for access to the non-public user repository and to applications hosted by OC4J) – this is associated with objective O.I&A.TOE of the Security Target.

c. *Audit and Accountability Security Policy* (i.e. audit and accountability information is logged in detail for each security event, covering date, time, user, operation and characteristics) – this is associated with objective O.AUDIT of the Security Target.

d. *Security Management Security Policy* (i.e. only suitably authorised directory administrators can manage the TOE and its security functions) – this is associated with objective O.ADMIN.TOE of the Security Target.

26. The Security Target [a] identifies the following Organisational Security Policy (OSP), with which the TOE must comply:

P.ACCESS - Access to directory objects is determined by:

- the user identity and access control group memberships associated with the subject attempting the access;
- directory access control information directives that apply to the object.

Security Claims

27. The Security Target [a] fully specifies the TOE's security objectives, the threats that those objectives counter, the OSP that those objectives meet, and the SFRs and security functions to elaborate those objectives.

28. All of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products. The Security Target [a] extends two of those SFRs, relative to CC Part 2, as follows:

a. FAU_GEN.1 is extended to become:

   - (for the TOE): FAU_GEN.1T.1 and FAU_GEN.1T.2; and
   - (for the IT Environment): FAU_GEN.1E.1 and FAU_GEN.1E.2.

b. FPT_SEP.1 is extended to become:

   - (for the TOE): FPT_SEP.1T.1 and FPT_SEP.1T.2; and
   - (for the IT Environment): FPT_SEP.1E.1.

In both cases, the intent is that the TOE in combination with its IT environment collectively meets the requirements of FAU_GEN.1 and of FPT_SEP.1.

29. The Security Target [a] groups the specifications of the security functions as follows:

- Identification and Authentication;
- Application Access Control;
- Security Attribute Maintenance;
- User Repository Access Control;
- Audit and Accountability.

Evaluation Conduct

30. The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication (UKSP) 01 and 02 [f - h]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

31. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], which prospective consumers are advised to read.

32. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline.

33. The evaluation was performed in accordance with the following requirements:

- the EAL4 requirements specified in CC Part 3 [d];
- the Common Evaluation Methodology (CEM) [e];
- appropriate interpretations.

34. The Certification Body monitored the evaluation, which was performed by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation was completed in February 2006, when the CLEF submitted the last of its Evaluation Technical Reports (ETRs) [l - n] to the Certification Body. The Certification Body requested further details and, following the CLEF's satisfactory responses, the Certification Body produced this Certification Report.

General Points

35. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

36. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and what assurance exists for such patches.

37. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

38. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETRs [l - n] under the CC Part 3 [d] headings.

39. The following sections note considerations of particular relevance to consumers.

Delivery

40. When a consumer orders the TOE from the Vendor, Oracle provides the consumer with an order number and an invoice detailing the items ordered. The order is shipped via a trusted carrier to the consumer, who is informed separately of the carrier identity and the shipment details (e.g. waybill number). Packages are marked with the name and address of the sender (i.e. Oracle), name and address of the addressee (i.e. the consumer) and the Oracle logo.

41. The consumer receives the order as a package labelled as Oracle Application Server 10*g* (Release 9.0.4.0.0). The CD pack has part number “B15038-07 v5”, titled “Oracle Application Server 10*g* (9.0.4.0.0) for Solaris Operating System (SPARC), Release Date Jun-04”. Of those CDs, the sub-set required for the TOE has part numbers B13114-01, B13115-01 and B13116-01.

42. The consumer should check that the order number of the delivery is the same as the order number on the invoice, and that the part numbers of all items supplied are the same as those indicated on the invoice.

43. The above measures are intended to ensure that a third party could not masquerade as the Vendor and supply potentially malicious software. Nevertheless, the consumer must rely on Oracle’s manufacturing procedures and the trust placed in the carrier, to counter the threat of interference to the order along the delivery path. The Evaluators confirmed that Oracle would use a high security courier, or other measures, if required by the consumer.

44. To complete the set up of OC4J for its evaluated configuration, consumers must download Oracle Application Server 10*g* Patch Set 1 - July 2004 (i.e. Oracle Application Server 10*g* (9.0.4) Patch Set 1 (9.0.4.1.0) for Solaris Operating System (SPARC), Jul-04, patch number 3784229) from Oracle’s ‘MetaLink’ website (as outlined in paragraphs 52-53 below) and apply it to OC4J. This is described in the Evaluated Configuration document [o].

45. On receiving the TOE, the consumer should check that it is the evaluated version and should check that the security of the TOE has not been compromised during delivery.

46. Oracle also makes components of the TOE available for download from Oracle’s websites http://metalink.oracle.com (for existing consumers) and www.oracle.com (for new consumers), but does not provide digital signatures or checksums to enable consumers to verify the identity or integrity of the component. However the Certification Body recommends that, where the threat of spoofing of the Oracle websites, or the corruption or deliberate modification of TOE components in transit is considered relevant to the TOE’s operational environment, then consumers should obtain delivery of the TOE via physical media only (e.g. CD-ROMs for software, printed books for documentation).

Installation and Guidance Documentation

47. The only users of the TOE in its evaluated configuration are users and administrators. Administrators install the TOE, then set up and maintain the directory so that the Oracle Internet Directory Server is able to receive and respond to LDAP messages from users outside the scope of the TOE. Only administrators require direct interaction with the TOE.

48. Guidance to administrators regarding security of the TOE is provided in the Evaluated Configuration document [o], which also indicates how the TOE's environment can be secured.

49. The procedures in that document that are relevant to non-administrative users are generally limited to common-sense measures.

50. The Evaluated Configuration document [o] refers to other supporting documentation [a, p - y], as appropriate.

51. The Evaluated Configuration document [o] is released by Oracle to consumers on request. It is anticipated that Oracle may also make the document available for download from one of its websites (e.g. via http://www.oracle.com/technology/deploy/security).

Flaw Remediation

52. Oracle's flaw remediation information for consumers is available from two websites:

a. Oracle's 'MetaLink' website (http://metalink.oracle.com), which enables consumers with an Oracle support contract to:

   i. email details of flaws to Oracle, and receive technical support, by submitting a Technical Assistance Request;

   ii. receive email alerts from Oracle regarding flaws, fixes and workarounds;

   iii. read alerts and news posted on the MetaLink website by Oracle regarding flaws, fixes and workarounds;

   iv. download patches from Oracle via the MetaLink website.

b. Oracle's public website (http://www.oracle.com), which enables other consumers and the public to:

   i. email details of security flaws to Oracle, at secalert_us@oracle.com;

   ii. read alerts and news posted on the public website by Oracle regarding flaws, fixes and workarounds.

53. Oracle currently issues patches via the Internet only (at http://metalink.oracle.com), where they are available only to consumers with an Oracle support contract as noted above. Consumers can guard against spoofing by phoning Oracle support and asking them to check their patch download audit log; an entry in the log would confirm that Oracle initiated the download.

Strength of Function

54. The SOF claim for the TOE was as given above under “Strength of Function Claims”, namely the Security Target [a] claims SOF-high for the user password mechanism.

55. The Evaluated Configuration document [o] and the OID Evaluated Configuration document [s] specify the pre- and post-installation measures, and password controls that must be applied to the password profiles, in the evaluated configuration of the TOE.

56. The Evaluators found that the TOE’s password mechanism met the SOF-high claim of the Security Target [a].

57. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that the PWD mechanism is the only TOE mechanism that is probabilistic or permutational.

Vulnerability Analysis

58. The Evaluators searched for vulnerabilities regarding the TOE. They also searched for vulnerabilities regarding the TOE’s environment that could be used to compromise the TOE.

59. The Evaluators’ vulnerability analysis was based on public domain sources, Oracle’s Vulnerability Analysis document submitted to the evaluators, and on the visibility of the TOE given by the evaluation process.

Platform Issues

60. The TOE was evaluated on the database server platform, operating system platform and hardware platform specified in Table A-2.

61. The certified configuration is that running on those platforms only, i.e. it excludes all other platforms.

(This page is intentionally left blank)

III. EVALUATION OUTCOME

Certification Result

62. After due consideration of the ETRs [l - n] produced by the Evaluators, and the conduct of the evaluation as witnessed by the Certifier, the Certification Body has determined that Oracle Application Server 10*g* (Oracle Containers for J2EE and Oracle Internet Directory), Release 9.0.4.0.0, meets the CC Part 3 augmented requirements of Evaluation Assurance Level EAL4 (i.e. augmented with ALC_FLR.3) for the specified CC Part 2 extended functionality, in the specified environment, when running on the platforms specified in Annex A.

63. Oracle Application Server 10*g* (Oracle Containers for J2EE and Oracle Internet Directory), Release 9.0.4.0.0, was evaluated on a database server (Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0), which had previously been certified to EAL4 augmented by ALC_FLR.3 [i]), running on an operating system platform (Sun Solaris Version 8 2/02, which had previously been certified to EAL4 [k]).

64. The minimum Strength of Function (SOF) claim of SOF-high for the password management functions (i.e. the PWD mechanism) in the Security Target [a] is satisfied.

Recommendations

65. Prospective consumers of the TOE should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target. Note that the scope of the evaluation has only considered the use of the TOE in a secure physical environment isolated from other networks such as the Internet. Certification of the TOE does not apply to its use in an untrusted or potentially hostile network environment.

66. Only the evaluated TOE configuration should be installed. This is specified in Annex A, with further relevant information given above under the headings ‘TOE Scope’ and ‘Evaluation Findings’. Subsequent updates to the TOE are covered by Oracle’s flaw remediation process.

67. The above ‘Evaluation Findings’ include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

68. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration [a, o - y]. As stated elsewhere in this report, attention is drawn to the configuration instructions in the Evaluated Configuration document [o], particularly [AS.POST-4] and [AS.CA-1]. The Evaluated Configuration document also draws attention to the constraints of the network environment and the fact that the evaluation only refers to Basic Authentication and does not include the use of SSL and HTTPS (Hypertext Transfer Protocol over SSL).

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

   Oracle Application Server 10*g* (Oracle Containers for J2EE and Oracle Internet Directory), Release 9.0.4.0.0.

TOE Documentation

2. The relevant guidance documents, as evaluated for the TOE or referenced from the evaluated documents, were:

   - Oracle Application Server: Security Target [a];
   - Oracle Application Server: Evaluated Configuration document [o];
   - OC4J: Security Guide [p];
   - OC4J: User's Guide [q];
   - OID: Security Target [r];
   - OID: Evaluated Configuration document [s];
   - OID: Administrator's Guide [t];
   - Oracle Process Manager and Notification Server: Administrator's Guide [u];
   - Oracle9*i*: Evaluated Configuration document [v];
   - Solaris 8-2/02 Security Testing - Installation Procedure [w];
   - Oracle Application Server: Quick Installation/Upgrade Guide (9.0.4) for Solaris [x];
   - Oracle Application Server: Quick Installation/Upgrade Guide (10.1.2) for Solaris [y].

3. Further discussion of the guidance documents is given in Section II under the heading 'Installation and Guidance Documentation'.

TOE Configuration

4. The TOE should be installed, configured and maintained in accordance with the Evaluated Configuration document [o], which refers to other supporting documentation [a, p - y] as appropriate, as indicated above under the heading 'TOE Documentation'.

5. Annex A.2 of the Evaluated Configuration document [o] specifies exactly the software components that comprise the evaluated configuration of the TOE.

Environmental Configuration

6. OC4J has the following dependencies:

   - Java Naming and Directory Interface (JNDI);
   - Oracle Process Manager and Notification Server (OPMN) – used to start, stop and monitor OC4J processes.

7. OID has the following dependencies:

   - Oracle 9*i* Database Server Enterprise Edition 9.2.0 for the storage of directory data;
   - Oracle Net Services 9.2.0 for communications services.

8. The security of the TOE depends not only on secure administration of the TOE, but also on secure administration of the host operating systems, the database server and other services utilised under the J2EE specification.

9. The environmental configuration used by the Developer to test the TOE is summarised in Table A-1:

Machine	**Sun Ultra 60, used as the server and the client**
Processor	**360MHz CPU**
Memory	**1GB RAM**
Operating System	**Solaris 8 2/02**
Database Server	**Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0)**
Drives	**2 x 26GB hard drives, 3.5” floppy drive, CD drive**
Network Connection	**10/100BaseT network connection on the motherboard**

Table A-1: Environmental Configuration (Developer’s Tests)

10. The environmental configuration used by the Evaluators to test the TOE is summarised in Table A-2:

Machine	**Sun Ultra 60, used as the server for OID**
Processor	**450MHz Sun Ultra Sparc2**
Memory	**2GB RAM**
Operating System	**Solaris 8 2/02**
Database Server	**Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0)**
Drives	**40GB hard drive, 3.5" floppy drive, DVD drive**
Network Connection	**10/100BaseT network connection on the motherboard**
Machine	**Sun Ultra 60, used as the server for OC4J, OPMN and JNDI**
Processor	**450MHz Sun Ultra Sparc2**
Memory	**2GB RAM**
Operating System	**Solaris 8 2/02**
Database Server	**Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0)**
Drives	**40GB hard drive, 3.5" floppy drive, DVD drive**
Network Connection	**10/100BaseT network connection on the motherboard**
Machine	**Sun Ultra 60, used as the clients**
Processor	**450MHz Sun Ultra Sparc2**
Memory	**2GB RAM**
Operating System	**Solaris 8 2/02**
Database Server	**Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0)**
Drives	**40GB hard drive, 3.5" floppy drive, DVD drive**
Network Connection	**10/100BaseT network connection on the motherboard**

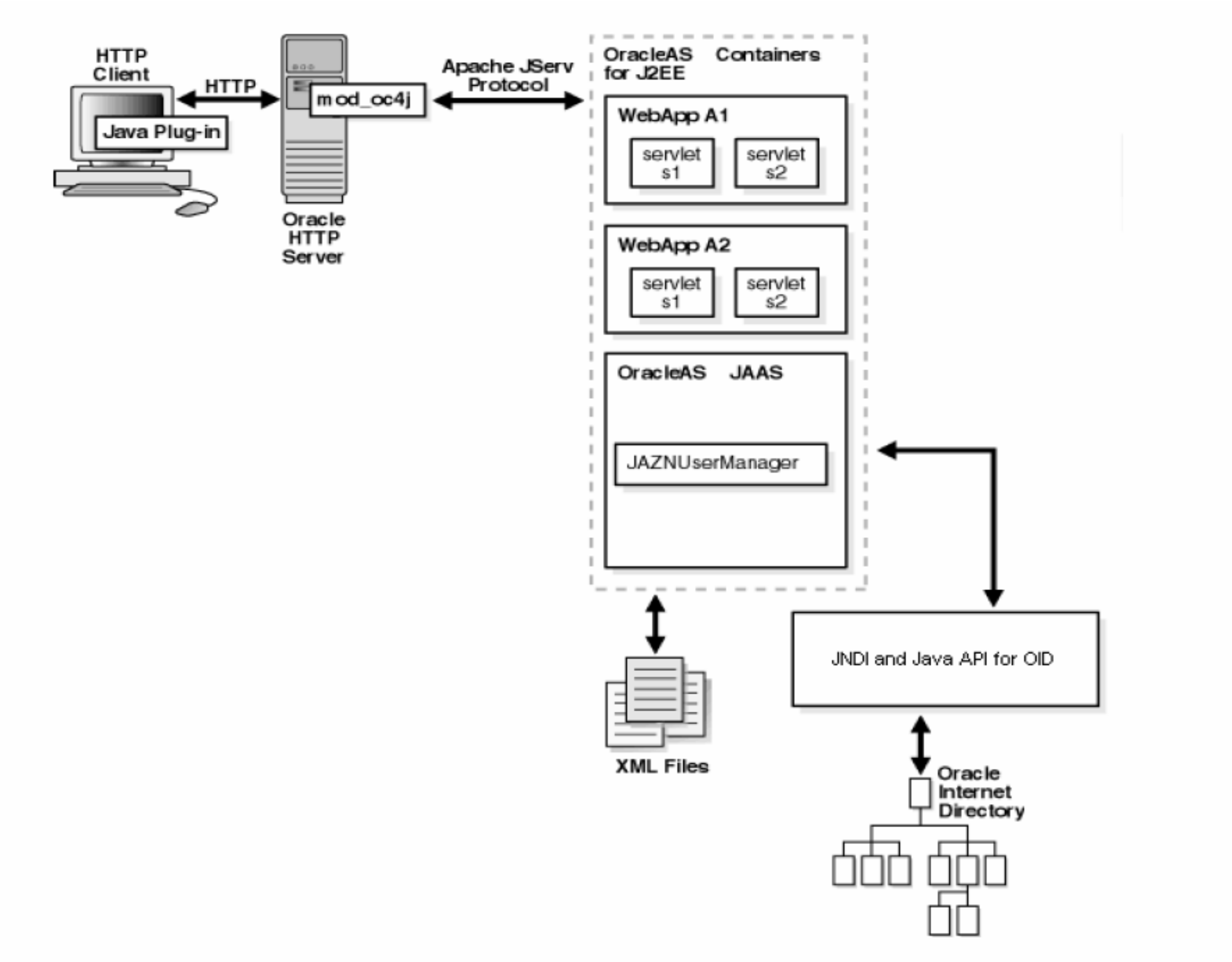
Table A-2: Environmental Configuration (Evaluators’ Tests)

11. Further details of the Developer’s testing and the Evaluators’ testing are given in Annex C.

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of this report and in Annex A.

Architectural Features



2. The diagram above represents a top-level view of the TOE architecture. Note that the HTTP Client and the Oracle HTTP Server are both part of the IT environment.

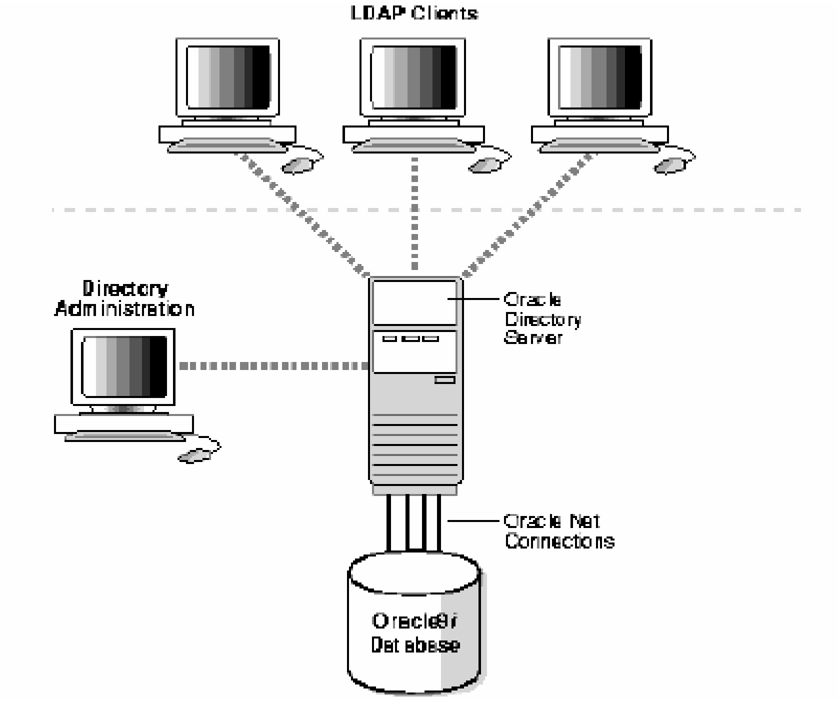
3. Oracle Internet Directory (OID) stores user entries in the directory; such entries include attributes for use in storing passwords. Different directory attributes can be used for the different types of passwords. In this context they are used for :

- authenticating users requesting access to the directory;
- authenticating users requesting access to an application;
- authenticating users requesting access to an Oracle database.

4. OID has a password policy facility that can be used to provide configurable controls on passwords to ensure a high Strength of Function for the OID password management function.

5. OID runs as an application on Oracle9*i* and uses its Oracle9*i* database to hold the directory data. The OID's audit log is used to record critical events on the Oracle Internet Directory Server that are important from both a security and an operational point of view.

6. The diagram below illustrates a typical configuration by which the directory administration client, and clients using the LDAP protocol, can connect to the Oracle Internet Directory Server. That server connects to the Oracle9*i* database using Oracle Net Services (ONS).



7. OID communicates with the database using ONS, which is Oracle's operating system-independent database connectivity solution.

Design Subsystems

8. The design subsystems of the TOE are:

   a. OC4J Server: This is described in Section I under the heading 'Evaluated Product'.

   b. Java Naming and Directory Interface (JNDI): This provides naming and directory functionality for Java applications. It enables Java applications to access different, possibly multiple, naming and directory services using a single API.

   c. Oracle Process Manager and Notification Server (OPMN): This is installed and configured with every Oracle Application Server installation type and is used to start, monitor and stop OC4J's processes in the TOE's evaluated configuration.

d. Java API for OID: An API is a set of exposed data structures and functions that an application can use to invoke services on a component. This API is used for communication with OID to access the user repository data.

   Note: This was not covered by the previous evaluation of OID [j]; it is covered by the present evaluation of Oracle Application Server, in respect of its use by OC4J.

e. Oracle Directory Server: This is the core system functionality that handles all of the LDAP protocol requests from external users and relays the data back in the correct format. It is also responsible for enforcing the Directory Information Model, handling all aspects of database operations, auditing, and security with respect to data (e.g. password policies, user information).

f. Oracle Directory Server Run-time Tools:

   i. OID Monitor (**`oidmon`**). This is responsible for initiating (i.e. re-starting failed server instances), monitoring and terminating the LDAP server process. It processes commands (initiated by **`oidctl`**) to start/stop the OID Server.

   ii. OID Control Utility (**`oidctl`**). This communicates with **`oidmon`**, by placing message data in database tables, causing **`oidmon`** to start/stop an OID Server.

g. Essential Directory Administration Tools: These tools directly access directory data stored in the database. They include **`catalog`**, **`bulkload`**, **`bulkdelete`**, **`bulkmodify`**, **`ldifwrite`**, **`oidpasswd`** and **`oidstats`**.

Hardware and Firmware Dependencies

9. The TOE has no hardware or firmware dependencies.

TSF Interfaces

10. The external interfaces of the TOE are as follows:

a. Apache JServ protocol: This is the run-time interface to OC4J. Users interact with the TOE (for authentication and authorisation purposes) through their browser, which communicates with Oracle HTTP Server (not part of the TOE), which in turn passes the request to OC4J. OC4J uses this protocol to request the browser to obtain a username and password from the user.

b. `oc4j.jar`: This is a command line interface to OC4J, used for start-up of OC4J. This interface is not normally used directly by administrators; instead OC4J is typically managed through OPMN (which uses this interface).

c. `admin.jar`: This is a command line interface to OC4J, used for shutdown of OC4J and for deploying applications to OC4J. This interface is not normally used directly by administrators; instead OC4J is typically managed through OPMN (which uses this interface).

d. JNDI: This is an API that provides directory and naming functionality to Java applications.

e. `opmnctl`: This is the command-line utility through which OPMN is invoked.

f. `JAZNConfigTool`: This is used for performing the directory-related configuration work for JAZN at installation time.

11. OID also provides an evaluated external interface to LDAP clients, through which user repository administration is performed.

ANNEX C: PRODUCT TESTING

Developer's Testing

1. The Developer installed and tested the TOE on the platform specified in Table A-1.

2. The Developer tested the security mechanisms, the security functions, the subsystems and the external interfaces of the TOE, using automated tests.

Evaluators' Testing

3. The Evaluators installed and tested the TOE on the platform specified in Table A-2.

4. Evaluator testing was carried out using a web browser via the Apache JServ protocol. Additional tests were carried out to exercise the OIDMON interface to OID. All of the Evaluators' testing was performed via these interfaces.

5. The Evaluators assessed the Developer's testing approach, coverage, depth and results. This included the following:

   a. the Evaluators checked that the Developer's testing approach covered the TOE's security mechanisms, security functions, subsystems and external interfaces;

   b. the Evaluators witnessed all of the Developer's tests;

   c. the Evaluators performed independently-devised functional tests to cover the security functions.

6. The Evaluators' findings confirmed that:

   a. the Developer's testing approach, depth, coverage and results were all adequate;

   b. the Developer's tests covered the TOE's security mechanisms, security functions, subsystems and external interfaces;

   c. (for the Developer's tests witnessed by the Evaluators): the actual test results were consistent with the expected test results and any deviations were satisfactorily accounted for;

   d. (for the Evaluators' independently-devised functional tests): the actual test results were consistent with the expected test results.

7. The Evaluators then performed penetration testing of the TOE. Those tests searched for potential vulnerabilities in the features of the TOE.

8. From checking various sources on the Internet, the Evaluators found no publicly known, exploitable vulnerabilities applicable to the TOE. Also, the evaluators found no publicly known, exploitable vulnerabilities regarding the TOE's environment that could be used to compromise the TOE.

9. The Evaluators found that all relevant, publicly known vulnerabilities had been resolved in the TOE and/or its guidance documentation (e.g. in the Evaluated Configuration document [o]), such that those vulnerabilities were not exploitable for the TOE.

10. The results of the Evaluators' penetration testing confirmed that:

    a. the claimed SOF in the Security Target [a], for the password space for the PWD mechanism (i.e. SOF-high), was satisfied;

    b. all identified potential vulnerabilities in the TOE have been addressed, i.e. the TOE in its intended environment has no exploitable vulnerabilities.