



**UK IT SECURITY EVALUATION AND  
CERTIFICATION SCHEME**



122-B

**COMMON CRITERIA CERTIFICATION REPORT No. P210**

**Oracle Internet Directory 10g**

**Release 9.0.4.0.0**

**running on specified platforms**

Issue 1.0

February 2005

© Crown Copyright 2005

Reproduction is authorised provided the report  
is copied in its entirety

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:**

All product or company names are used for identification purposes only and may be trademarks of their respective owners.

## **CERTIFICATION STATEMENT**

Oracle Internet Directory 10g (Release 9.0.4.0.0) is a general purpose, Lightweight Directory Access Protocol (LDAP) Version 3-compliant, directory service. It uses an Oracle9i database to store its directory data and it communicates with the database using Oracle Net Services. It runs as an Oracle9i application.

Oracle Internet Directory 10g (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.

<b>Originator</b>	<b>CESG</b> Certifier
<b>Approval and Authorisation</b>	<b>CESG</b> Technical Manager of the Certification Body UK IT Security Evaluation and Certification Scheme
<b>Date authorised</b>	11 February 2005

(This page is intentionally left blank)

**TABLE OF CONTENTS**

**CERTIFICATION STATEMENT .....iii**

**TABLE OF CONTENTS..... v**

**ABBREVIATIONS .....vii**

**REFERENCES ..... ix**

**I. EXECUTIVE SUMMARY ..... 1**

    Introduction..... 1

    Evaluated Product..... 1

    TOE Scope..... 2

    Protection Profile Conformance ..... 3

    Assurance..... 3

    Strength of Function Claims ..... 3

    Security Policy..... 4

    Security Claims..... 5

    Evaluation Conduct..... 5

    General Points..... 6

**II. EVALUATION FINDINGS..... 7**

    Introduction..... 7

    Delivery ..... 7

    Installation and Guidance Documentation..... 7

    Flaw Remediation ..... 8

    Strength of Function ..... 8

    Vulnerability Analysis ..... 9

    Platform Issues..... 9

**III. EVALUATION OUTCOME ..... 11**

    Certification Result ..... 11

    Recommendations..... 11

**ANNEX A: EVALUATED CONFIGURATION ..... 13**

**ANNEX B: PRODUCT SECURITY ARCHITECTURE..... 15**

**ANNEX C: PRODUCT TESTING ..... 19**

(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
LDAP	Lightweight Directory Access Protocol
OID	Oracle Internet Directory
ONS	Oracle Net Services
OSP	Organisational Security Policy
PL/SQL	Programming Language / Structured Query Language
PP	Protection Profile
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
TSFI	TOE Security Functions Interface
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)



## **REFERENCES**

- a. Security Target for Oracle Internet Directory 10g (9.0.4),  
Oracle Corporation,  
Issue 1.0, November 2004.
- 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. P178:  
Oracle9i Database Enterprise Edition Release 9.2.0.1.0,  
UK IT Security Evaluation and Certification Scheme,  
Issue 1.0, September 2003.
- j. Common Criteria Certification Report No. P182:  
Sun Solaris Version 8 2/02,  
UK IT Security Evaluation and Certification Scheme,  
Issue 1.0, April 2003.

- k. Task LFL/T167 Evaluation Technical Report 1,  
LogicaCMG CLEF,  
310.EC200542:30.1, Issue 2.0, 25 May 2004.
- l. Task LFL/T167 Evaluation Technical Report 2,  
LogicaCMG CLEF,  
310.EC200489:005.001.ETR2, Issue 1.0, 5 July 2004.
- m. Task LFL/T167 Evaluation Technical Report 3,  
LogicaCMG CLEF,  
310.EC200489:005.001.ETR3, Issue 2.0, 16 November 2004.
- n. Evaluated Configuration for Oracle Internet Directory 10g (9.0.4),  
Oracle Corporation,  
Issue 0.4, November 2004.
- o. Oracle Internet Directory Administrator's Guide, 10g (9.0.4),  
Oracle Corporation,  
Part No. B12118-01, September 2003.
- p. Evaluated Configuration for Oracle9i, Release 2 (9.2.0),  
Oracle Corporation,  
Issue 0.7, March 2003.
- q. Solaris 8-2/02 Security Testing - Installation Procedure,  
Sun Microsystems,  
Issue 0.1, 5 November 2002.

## **I. EXECUTIVE SUMMARY**

### **Introduction**

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Oracle Internet Directory 10g (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 Internet Directory 10g (Release 9.0.4.0.0).

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

5. Oracle recommends that installations of Oracle Database Server and Oracle Application Server, within enterprises, should rely on OID for the centralised management of information about users and network resources.

6. OID is a general-purpose directory product, which runs as an Oracle9i application. It relies on the Oracle9i 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.

7. OID enables fast retrieval and centralised management of data about dispersed users and network resources, including security data such as user names and passwords for the Oracle9i product stack. It combines the Lightweight Directory Access Protocol (LDAP) Version 3 with the performance, scalability, robustness, and availability of the Oracle9i Database Server. (LDAP is a standard, extensible directory access protocol that is used by LDAP clients and servers to communicate.)

8. The security functionality in the TOE includes:

- a. user identification and authentication, with password management;
- b. security attribute maintenance;
- c. discretionary access controls - which use Access Control Items held in the directory to define users' authorisations for directory data access;
- d. audit and accountability.

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

## TOE Scope

10. The scope of the TOE includes the security features of the product in its capacity as an LDAP directory service. Thus the scope of the TOE comprises the following components:

- a. Oracle Internet Directory 9.0.4.0.0;
- b. Oracle Internet Directory Server 9.0.4.0.0;
- c. 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).

11. The scope of the certification applies to the TOE:

- a. when using Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0), 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 [j].

12. The Evaluated Configuration document [n] defines how the TOE must be installed in its evaluated configuration and defines the requirements for setting up the TOE environment.

13. The scope of the certification excludes various features of the product that are related to security but do not directly address any of the functional requirements identified in the Security Target [a]. Those excluded features, which are specified in the section 'Other OID Security Features' in Chapter 2 of the Security Target, are as follows:

- a. OID's use of Secure Sockets Layer (SSL) (as it is assumed that the OID Server and the clients used to access it are all within a secure network).
- b. The following OID components:
  - i. Directory Replication Service (which replicates LDAP data between Oracle Internet Directory Servers);
  - ii. Directory Integration Platform (which allows connectivity and synchronisation with other applications and directories, whether Oracle-built or not);

- iii. Server Side plug-in framework (which enables OID applications to make use of advanced capabilities such as referential integrity / cascading deletions of LDAP objects, external authentication of directory clients, brokered access, and synchronisation with external relational tables).
- c. The following Directory Administration Tools:
  - i. Oracle Directory Manager (which is OID's standalone, 100% Java on-line administration tool);
  - ii. Directory Replication Service Tools (which are two tools to help administer the directory replication service, i.e. the OID reconciliation tool and the human intervention queue manipulation tool);
  - iii. Delegated Administration Service (which allows delegated administrators, such as non-technical managers, to create and manage both users and groups, and it also allows end users to modify and manage their own passwords without needing to know how to run a command-line tool);
  - iv. Enterprise Manager Integration (which is used to start, stop, and monitor OID instances);
  - v. the command-line tools which can be used to send LDAP messages to a host OID Server.
- d. Facilities for enterprise users.
- e. Guest user and proxy user (since the Evaluated Configuration document [n] requires that only the directory administrator knows the passwords for these users).
- f. The OID C Application Programming Interface (API) and the OID Programming Language / Structured Query Language (PL/SQL) API.

### **Protection Profile Conformance**

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

### **Assurance**

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

16. 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**

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

18. That claim applies only to the TOE's authentication of users connecting to the directory, which employs a one-way hashing algorithm to encrypt passwords before storing them in the directory. The Security Target [a] refers to the TOE's password management functions collectively as the 'PWD' (i.e. Password) mechanism and claims SOF-high for the password space that they provide.

19. OID implements four different levels of authentication to validate the identity of users connecting to the directory (as detailed in the Security Target [a]):

- Anonymous authentication (i.e. security function IA.ASESS).
- Password-based (simple) authentication (i.e. security function IA.USESS).
- Certificate-based authentication, through SSL. (N.B. This method of authentication was not assessed during the evaluation).
- Indirect authentication (i.e. security function IA.PSESS, which is employed when a directory session has been established using IA.USESS above).

20. It was not necessary for the hashing algorithm to be evaluated, as the Evaluated Configuration document [n] specifies that the password attribute must be constrained, as follows:

- i. The directory administrator must ensure that access control settings for the super user password attribute are set to prevent users other than the super user from accessing this attribute.
- ii. Users must be instructed not to disclose their directory passwords to other individuals. This instruction must include the requirement that users must not change the access control settings for their user password attribute, to prevent other non-administrative users from accessing that attribute.

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

- a. IA.USESS (SOF-High);
- b. IA.PWDC, SAM.UATT and SAM.CHPWD (which all support IA.USESS by providing password management facilities).

### Security Policy

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

*Directory Object 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.

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

- a. *Identification and Authentication Security Policy* (i.e. identification and authentication is required for access to all non-public directory information), associated with objective O.I&A of the Security Target.
- b. *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), associated with objective O.AUDIT of the Security Target.

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

24. 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**

25. 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.

26. 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.

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

- Identification and Authentication;
- Directory Access Control;
- Security Attribute Maintenance;
- Audit and Accountability.

### **Evaluation Conduct**

28. 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.

29. 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.

30. 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.

31. 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.

32. The Certification Body monitored the evaluation, which was performed by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation was completed in November 2004, when the CLEF submitted the last of its Evaluation Technical Reports (ETRs) [k - m] 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**

33. 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.

34. 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.

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



## **II. EVALUATION FINDINGS**

### **Introduction**

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

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

### **Delivery**

38. 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.

39. The consumer receives the TOE as a package clearly labelled as Oracle Internet Directory 10g (Release 9.0.4.0.0). The CD pack has part number "B13219-01 v2"; it is titled "Oracle Application Server 10g (9.0.4.0.0) for Solaris Operating System (SPARC), Release Date Jan-04" and it contains 16 CDs. Of those CDs, the sub-set required for OID are part numbers B13114-01, B13115-01 and B13116-01.

40. 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.

41. 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 TOE along the delivery path. The Evaluators confirmed that Oracle would use a high security courier, or other measures, if required by the consumer.

42. 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.

43. 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](http://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**

44. The only users of the TOE in its evaluated configuration are 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.

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

46. The procedures in that document that are relevant to non-administrative users are generally limited to common-sense measures (e.g. *"the directory administrator shall instruct users not to disclose their directory passwords to other individuals"*).

47. The Evaluated Configuration document [n] refers to other supporting documentation [a, o - q], as appropriate.

48. The Evaluated Configuration document [n] 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

49. 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](mailto:secalert_us@oracle.com);
  - ii. read alerts and news posted on the public website by Oracle regarding flaws, fixes and workarounds.

50. 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

51. 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 password space provided by the TOE's password management functions (i.e. the 'PWD mechanism').

52. The Evaluated Configuration document [n] specifies the password controls that must be applied to the password profiles in the evaluated configuration of the TOE.

53. The Evaluators found that the TOE's password space met the SOF-high claim of the Security Target [a].

54. 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.

55. The Evaluators found that another probabilistic mechanism is used by the TOE, i.e. the TOE directory administration tools require the password for the **ods** (i.e. Oracle9i Database Server) database user, in order to authenticate that he/she is a directory administrator, as the tools work directly on the database using SQL (not via the directory using LDAP messages). This is sufficiently addressed for the TOE, as:

- a. the Evaluated Configuration document [n] requires that the Oracle9i Database Server used by the TOE, to hold its directory data, must be set up in its evaluated configuration as described in the Oracle9i Evaluated Configuration document [p];
- b. the Evaluated Configuration document also requires that the default profile for the database must be changed to Profile B as described in Annex A of the Oracle9i Evaluated Configuration document;
- c. the Oracle9i certification report [i] states that Oracle9i has a strength of SOF-high when it is set up in its evaluated configuration;
- d. hence the password mechanism in the Oracle9i database, when it is used by the TOE, has a strength of SOF-high

### **Vulnerability Analysis**

56. 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.

57. 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**

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

59. 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**

60. After due consideration of the ETRs [k - m] produced by the Evaluators, and the conduct of the evaluation as witnessed by the Certifier, the Certification Body has determined that Oracle Internet Directory 10g (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.

61. Oracle Internet Directory 10g (Release 9.0.4.0.0) was evaluated on a database server (i.e. Oracle9i 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 (i.e. Sun Solaris Version 8 2/02, which had previously been certified to EAL4 [j]).

62. 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**

63. 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. In particular, certification of the TOE does not apply to its use in an untrusted or potentially hostile network environment (such as the Internet).

64. 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.

65. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration [a, n - q].

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

(This page is intentionally left blank)

## **ANNEX A: EVALUATED CONFIGURATION**

### **TOE Identification**

1. The TOE is uniquely identified as:  
Oracle Internet Directory 10g (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:
  - OID Security Target [a];
  - OID Evaluated Configuration document [n];
  - OID Administrator's Guide [o];
  - Oracle9i Evaluated Configuration document [p]
  - Solaris 8-2/02 Security Testing - Installation Procedure [q].
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 [n], which refers to other supporting documentation [a, o - q] as appropriate, as indicated above under the heading 'TOE Documentation'.
5. Annex A.2 of the Evaluated Configuration document [n] specifies exactly the software components that comprise the evaluated configuration of the TOE.

### **Environmental Configuration**

6. The TOE has no hardware or firmware dependencies.
7. The TOE has software dependencies, in that it relies on the host operating system and database server to:
  - a. Protect the TOE's security features that are within the scope of its evaluation and certification, including its:
    - i. user identification and authentication, with password management;
    - ii. security attribute maintenance;
    - iii. discretionary access controls - which use Access Control Items held in the directory to define users' authorisations for directory data access;
    - iv. audit and accountability.
  - b. Protect the TOE from being bypassed, tampered with, misused or directly attacked.

8. Hence the security of the TOE depends not only on secure administration of the TOE, but also on secure administration of the host operating system and database server in configurations using the TOE.

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

<b>Machine</b>	<b>Sun Ultra Model 2170, used as the server and the client</b>
<b>Processor</b>	<b>2 x 168MHz CPUs</b>
<b>Memory</b>	<b>393MB RAM</b>
<b>Operating System</b>	<b>Solaris 8 2/02</b>
<b>Database Server</b>	<b>Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0)</b>
<b>Drives</b>	<b>5 hard drives (2.1GB, 2.3GB, 4.2GB, 9GB, 36.7GB), 3.5" floppy drive, CD drive</b>
<b>Network Connection</b>	<b>10/100BaseT network connection on the motherboard</b>

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

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

<b>Machine</b>	<b>Sun Ultra 60, used as the server and the client</b>
<b>Processor</b>	<b>450MHz Sun Ultra Sparc2</b>
<b>Memory</b>	<b>2GB RAM</b>
<b>Operating System</b>	<b>Solaris 8 2/02</b>
<b>Database Server</b>	<b>Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0)</b>
<b>Drives</b>	<b>40GB hard drive, 3.5" floppy drive, DVD drive</b>
<b>Network Connection</b>	<b>10/100BaseT network connection on the motherboard</b>

**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. Oracle Internet Directory (OID) is a general purpose directory service that enables fast retrieval and centralised management of information about dispersed users and network resources. It combines LDAP V3 with the high performance, scalability, robustness, and availability of the Oracle9i Database Server.

3. In a directory, a collection of information about an object is called an *entry*. Each entry is uniquely identified by a *distinguished name*, which defines exactly where that entry resides in the directory's hierarchy. Each entry contains information stored in *attributes*. Each directory has a *directory-specific entry* holding information regarding the whole directory (e.g. audit log).

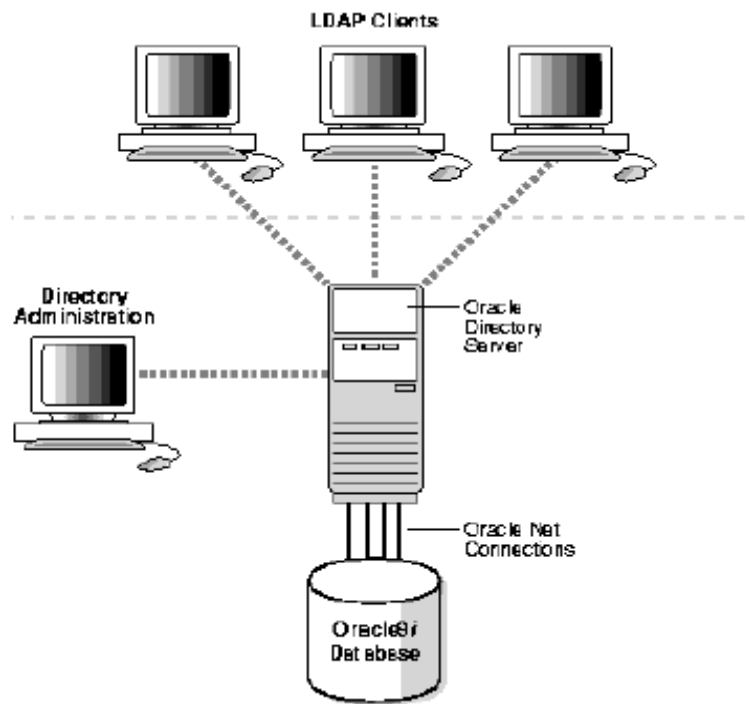
4. OID has facilities for storing user entries in the directory; such entries include attributes for use in storing passwords. Different directory attributes can be used for the different types of passwords. Passwords stored in the directory can be for:

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

5. 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. Such controls only apply to passwords used in authenticating users requesting access to the directory.

6. OID runs as an application on Oracle9i and uses its Oracle9i 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.

7. 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 Oracle9i database using Oracle Net Services (ONS).



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

### Design Subsystems

9. The design subsystems of the TOE are:
- Oracle Internet 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).
  - Run-Time Tool: OID Monitor (`oidmon`). This is responsible for initiating (i.e. restarting failed server instances), monitoring and terminating the LDAP server process. It processes commands to start/stop the Oracle Internet Directory Server which are initiated by `oidctl`.
  - Run-Time Tool: OID Control Utility (`oidctl`). This communicates with `oidmon`, by placing message data in Oracle Internet Directory Server tables, causing `oidmon` to start/stop an Oracle Internet Directory server.
  - Essential Administrating 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

10. The TOE has no hardware or firmware dependencies.

## TSF Interfaces

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

- a. The specified runtime tools (**oidmon** and **oidctl**).
- b. The specified directory administration tools:
  - i. the catalogue management tool (**catalog**);
  - ii. the bulk operations tools (**bulkload**, **bulkdelete**, **bulkmodify**, **ldifwrite**), which are used to perform operations on a large number (up to millions) of entries in a directory;
  - iii. the OID database password utility (**oidpasswd**);
  - iv. the OID database statistics collection tool (**oidstats**).

12. LDAP requests from users are also, in effect, an external interface of the TOE. This functionality is provided by the Oracle Internet Directory Server.

(This page is intentionally left blank)

## **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. All of the Evaluators' testing was performed via the external interfaces of the TOE (as specified in Annex B), using LDAP. All of those interfaces were tested.
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, using automated LDAP scripts, 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 [n]), 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.