122-B

CERTIFICATION REPORT No. CRP244

Oracle Internet Directory 10*g*
Release 10.1.0.4.1
running on Red Hat Enterprise Linux AS Release 4 Update 5

Issue 1.0

June 2008

UK 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[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them 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.

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	Oracle Corporation
Developer	Oracle Corporation
Product and Version	Oracle Internet Directory 10*g* (10.1.4.0.1)
Platform	Red Hat Enterprise Linux AS Release 4 Update 5
Description	Oracle Internet Directory 10*g* (10.1.4.0.1) is a general purpose, Lightweight Directory Access Protocol (LDAP) Version 3-compliant, directory service. It uses an Oracle10*g* database to store its directory data and it communicates with the database using Oracle Net Services. It runs as an Oracle10*g* application.
CC Part 2	Extended
CC Part 3	Conformant
EAL	EAL4 augmented by ALC_FLR.3
SoF	SoF-High
PP Conformance	N/A
CLEF	Logica UK Limited
Date Certified	27 June 2008

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 [UKSP01] and 02 [UKSP02P1, UKSP02P2]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. 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. Both parts of the evaluation were performed in accordance[1] with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

Trademarks:

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

[1] All judgements contained in this Certification Report are covered by the Recognition Arrangement.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Oracle Internet Directory 10g (Release 10.1.4.0.1) to the Sponsor, Oracle, as summarised in the Certification Statement, 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 [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC EAL4 augmented by ALC_FLR.3 on 11 April 2008:

- **Oracle Internet Directory 10g (release 10.1.4.0.1)**

4. The Developer was Oracle Corporation.

5. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration'.

6. An overview of the TOE and its security architecture can be found in Chapter IV 'Product Architecture'. Configuration requirements are specified in Section 2 of [ST].

Protection Profile Conformance

7. The Security Target [ST] does not claim conformance to any protection profile.

Security Claims

8. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats that these Objectives counter and the Security Functional Requirements (SFRs) and Security Functions that define the TOE implementation of the Objectives. All of the SFRs are taken from CC Part 2 [CC2]; the following SFRs have been extended:

- FAU_GEN.1T Audit Data Generation,
- FPT_SEP.1T TSF Domain Separation

9. The TOE security policies are detailed in ST [ST]. The OSPs that must be met are specified in [ST] Section 5.

10. The environmental assumptions related to the operating environment are detailed in Chapter III under 'Environmental Requirements'.

Strength of Function Claims

11. The Security Target [ST] claims that the minimum Strength of Function (SOF) for the TOE is SOF-High.

12. 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 [ST] 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.

Evaluation Conduct

13. The TOE SFRs and the security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of Oracle Internet Directory 10g (release 9.0.4.0.0), which had previously been certified [CRP210] by the UK IT Security Evaluation and Certification Scheme to the CC EAL4 assurance level. For the evaluation of Oracle Internet Directory 10*g* (release 10.1.4.0.1), the Evaluators made reuse of the previous evaluation results where appropriate.

14. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in April 2008, were reported in the Evaluation Technical Reports [ETR1], [ETR2] and [ETR3].

Conclusions and Recommendations

15. The conclusions of the Certification Body are summarised in the Certification Statement on page 2.

16. Prospective consumers of Oracle Internet Directory 10*g* (release 10.1.4.0.1) should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

17. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE

Disclaimers

18. This Certification Report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration'.

19. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (which is smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. 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 the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered by a Scheme-approved Assurance Continuity process.

II. TOE SECURITY GUIDANCE

Introduction

20. The following sections provide guidance that is of particular relevance to purchasers of the TOE.

Delivery

21. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised during delivery.

22. Section 2 of [ECD] lists all components that constitute the TOE, including specific CD part numbers.

Installation and Guidance Documentation

23. The Installation and Configuration documentation is as follows:

- [ECD] Evaluated Configuration Document – Provides guidance to administrators for securing the TOE and its environment. [ECD] references other TOE specific documents namely: [OIDIG] and [DBECD].

24. Procedures in the above documents 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"*).

25. The Evaluated Configuration Documents [ECD], [OIDIG] and [DBECD] are 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, for example via:

http://www.oracle.com/technology/deploy/security/seceval/oracle-common-criteria-evaluated.html

26. The User Guide and Administration Guide documentation is as follows:

- [AG] – OID Administrator's Guide;
- [UR] – Oracle Identity Management User Reference;
- [ECD] – OID Evaluated Configuration Document.

III. EVALUATED CONFIGURATION

TOE Identification

27. The TOE is Oracle Internet Directory 10*g* (Release 10.1.4.0.1).

TOE Documentation

28. The relevant guidance documentation for the evaluated configuration is identified above under 'Installation and Guidance Documentation'.

TOE Scope

29. The TOE Scope is defined in [ST] Section 2. Functionality that is outside the scope of the TOE is defined in [ST] Section 2 – "Other OID Security Features".

TOE Configuration

30. The evaluated configuration of the TOE is defined in [ECD] Annex A.

Environmental Requirements

31. The environmental assumptions for the TOE are stated in [ST] Section 3.

32. The TOE was evaluated running on Red Hat Linux AS Version 4 Update 5.

33. 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.

34. 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 secure configurations using the TOE.

Test Configuration

35. Developer tests were run at Oracle's data centre in Austin, Texas, from a remote machine at Oracle offices in Redwood Shores, California. Tests were run on Linux machines with Red Hat.

36. Tests were performed on machines that satisfied the minimum installation requirements for the TOE (e.g. memory, hard disk capacity and CPU).

37. The following configuration was used by the Evaluators for testing

Machine	Dell PowerEdge 1950
Processor	2 x Intel Xeon Dual Core Processors
Memory	16 GB Memory
Operating System	Red Hat Enterprise Linux AS Release 4 Update 5
Database Server	Oracle Database 10*g* (10.1.0.5.0)
Drives	160 GB
Network Connection	10/100/1000 Ethernet Card

Table 1 – Environmental Configuration (Evaluators' tests)

38. Further details of the Developer's testing and Evaluators' testing are given in Chapter V.

IV. PRODUCT ARCHITECTURE

Introduction

39. This Chapter gives an overview of the main TOE architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

40. 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 Lightweight Directory Access Protocol (LDAP) Version 3 with the high performance, scalability, robustness, and availability of Oracle Database.

41. 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. An example of this information would be the audit log for the directory.

42. OID has facilities for storing user entries in the directory; such entries include attributes for 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; and
- authenticating users requesting access to an Oracle database.

43. 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.

44. OID runs as an application on Oracle Database and uses its database to hold the directory data. The OID 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.

45. 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 Oracle Database using Oracle Net Services (ONS).

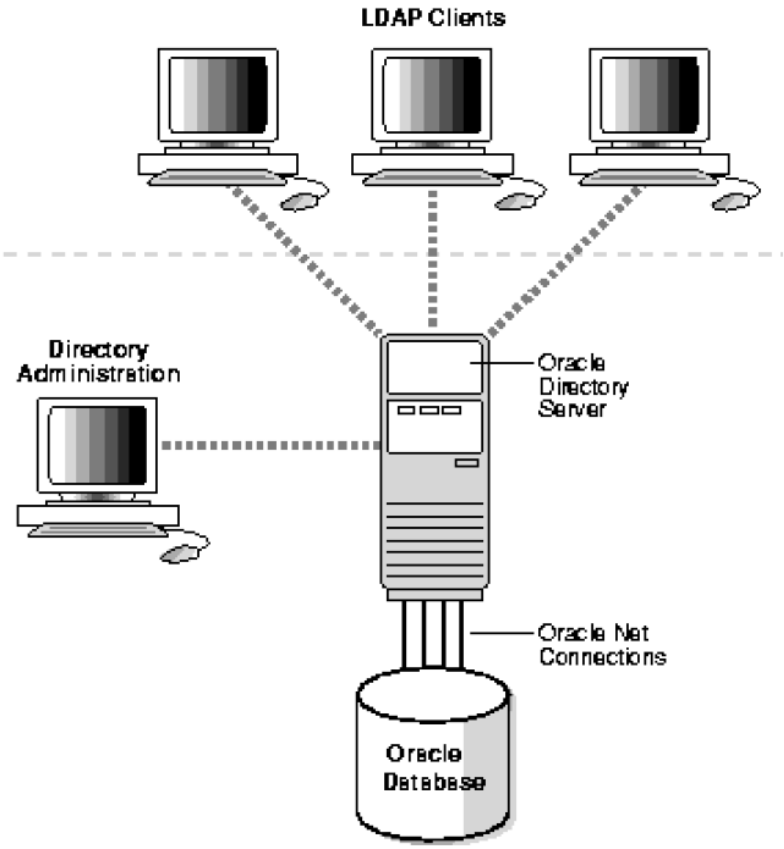

Figure 1 - Oracle Internet Directory Architecture

TOE Design Subsystems

46. The TOE subsystems, and their security features/functionality, are as follows:

- *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, monitoring, re-starting and terminating the directory server processes. It processes commands to start/stop the Oracle Internet Directory Server that are issued 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 Administration Tools. These tools directly access directory data stored in the database. They include `catalog`, `bulkload`, `bulkdelete`, `bulkmodify`, `ldifwrite`, `oidpasswd` and `oidstats`.

TOE Dependencies

47. The TOE has no hardware or firmware dependencies.

TOE Interfaces

48. The external TSFI is described as follows:

- The specified run-time tools (`oidmon` and `oidctl`).

- The specified directory administration tools: the catalogue management tool (`catalog`); the bulk operations tools (`bulkload`, `bulkdelete`, `bulkmodify`, `ldifwrite`), which are used to perform operations on a large number of entries in a directory; the OID database password utility (`oidpasswd`); and the OID database statistics collection tool (`oidstats`).

- LDAP requests from users are also, in effect, an external interface of the TOE. The functionality to process these requests is provided by the Oracle Internet Directory Server.

V. TOE TESTING

TOE Testing

49. The Developer's tests covered all SFRs, all TOE high-level subsystems (as identified under 'TOE Design Subsystems'), all SFRs and the TSFI (as identified under 'TOE Interfaces' in Chapter IV). The tests included those TOE interfaces which are internal to the product and thus had to be exercised indirectly.

50. The Evaluators installed and tested the TOE on the platform specified in Table 1, in accordance with the logical configuration as shown in Figure 1.

51. The Evaluators devised and ran independent functional tests, different from those performed by the Developer. No anomalies were found. The Evaluators also devised penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected. The Evaluators used various tools during testing of the TOE including: Jxplorer, Nmap and the Protos LDAP testing suite.

Vulnerability Analysis

52. The Evaluators' vulnerability analysis, which preceded penetration testing, was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Issues

53. The Developers provided a Platform Rationale which provided reasoning as to why the security of the TOE is not undermined by the underlying platforms. The Evaluators analysed the Rationale and performed various tests against the underlying OS and the database. The Evaluators confirm that each underlying platform does not undermine the security of the TOE.

VI. REFERENCES

[AG] Oracle Internet Directory Administrator's Guide 10g (10.1.4.0.1), Part no. B15991-01, July 2006, Oracle Corporation.

[A&R] Abbreviations and References, UK IT Security Evaluation and Certification Scheme, Issue 1.4, January 2008.

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1, Introduction and General Model, Common Criteria Maintenance Board, CCMB-2005-08-001, Version 2.3, August 2005.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2, Security Functional Requirements, Common Criteria Maintenance Board, CCMB-2005-08-002, Version 2.3, August 2005.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3, Security Assurance Requirements, Common Criteria Maintenance Board, CCMB-2005-08-003, Version 2.3, August 2005.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2005-08-004, Version 2.3, August 2005.

[CRP210] Certification Report for Oracle Internet Directory 10*g* (release 9.0.4.0.0), UK IT Security Evaluation and Certification Scheme, Issue 1.0, February 2005.

[DBECD] Evaluated Configuration for Oracle Database 10*g* Release 1 (10.1.0), November 2005, Issue 0.5, Oracle Corporation.

[ECD] Evaluated Configuration for Oracle Internet Directory 10g (10.1.4.0.1), March 2008, Issue 0.3, Oracle Corporation.

[ETR1] LFL/T244 Evaluation Technical Report 1, Evaluation of Oracle Internet Directory 10*g* (10.1.4.0.1), Issue 1.0, 23 August 2007, Logica CLEF.

[ETR2] LFL/T244 Evaluation Technical Report 2, Evaluation of Oracle Internet Directory 10*g* (10.1.4.0.1), Issue 1.1, 10 April 2008, Logica CLEF.

[ETR3] LFL/T244 Evaluation Technical Report 3,
Evaluation of Oracle Internet Directory 10*g* (10.1.4.0.1),
Issue 1.0, 11 April 2008, Logica CLEF.

[OIDIG] Evaluated Configuration for Oracle Identity and Access Management 10*g* (10.1.4.0.1): Oracle Internet Directory Installation,
January 2008, Issue 0.1, Oracle Corporation.

[ST] Security Target for Oracle Internet Directory 10*g* (10.1.4.0.1),
Issue 0.9, May 2008, Oracle Corporation.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

[UR] Oracle Identity Management User Reference 10g (10.1.4.0.1),
Part no. B15998-01, July 2006, Oracle Corporation.

VII. ABBREVIATIONS

This list does not include well known IT terms (such as GUI, HTML, LAN, PC) or standard Common Criteria abbreviations (such as TOE, TSF; see Common Criteria Part 1 [CC1]) or Scheme abbreviations (such as CESG, CLEF; see [A&R]).

ECD	Evaluated Configuration Document
LDAP	Lightweight Directory Access Protocol
OID	Oracle Internet Directory
ONS	Oracle Net Services
PWD	Password