122-B

CERTIFICATION REPORT No. CRP245

Oracle Identity and Access Management 10*g*
Release 10.1.4.0.1
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 Identity and Access Management 10*g* (10.1.4.0.1)
Platform	Red Hat Enterprise Linux AS Release 4 Update 5
Description	Oracle Identity and Access Management (Oracle IAM) is a suite consisting of Oracle Access Manager, Oracle Virtual Directory and Oracle Internet Directory. It allows enterprises to manage and automate the end-to-end lifecycle of user identities, and provides users with secure, fine-grained access to enterprise resources and assets.
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 Identity & Access Management 10*g* (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 18 April 2008:

- Oracle Identity & Access Management 10*g* (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 'TOE Security 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 which 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,
- FAU_SAR.1T Audit Review,
- FAU_SAR.3T Selectable Audit Review,
- FAU_STG.1T Protected Audit Trail Storage.

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 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

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

15. Prospective consumers of Oracle Identity & Access Management 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.

16. 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

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

18. 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

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

Delivery

20. 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 in delivery.

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

Installation and Guidance Documentation

22. 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: [OIDECD], [DBECD], [OVDIG], [OHSIG] and [OAMIG].

23. The Evaluated Configuration Documents [OIDECD], [DBECD], [OVDIG], [OHSIG] and [OAMIG] 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

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

- [ECD] – OIAM Evaluated Configuration Document
- [OAMAG] – OAM Administration Guide
- [OAMICAG] – OAM Identity Common Administration Guide
- [OIDAG] – OID Administrator's Guide
- [OVDPM] – OVD Product Manual
- [UR] – Oracle Identity Management User Reference

III. EVALUATED CONFIGURATION

TOE Identification

25. The TOE is Oracle Identity & Access Management 10*g* (release 10.1.4.0.1), which consists of:

- Oracle Internet Directory Server 10.1.4.0.1
- Oracle Internet Directory Tools 10.1.4.0.1
- Oracle Virtual Directory Server 10.1.4.0.1
- OracleAS Identity Management aaa 10.1.4
- OracleAS Identity Management Identity 10.1.4
- OracleAS Identity Management WebPass 10.1.4
- OracleAS Identity Management WebGate 10.1.4

TOE Documentation

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

TOE Scope

27. 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 OIAM Security Features".

TOE Configuration

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

Environmental Requirements

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

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

31. The TOE has software dependencies, in that it relies on the host operating system, database server and web 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. resource access control;

iii. security attribute maintenance;

iv. audit and accountability.

b. Protect the TOE from being bypassed, tampered with, misused or directly attacked.

32. 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, database server and web server in secure configurations using the TOE.

Test Configuration

33. The following configuration was used by the Developers for testing

	Server 1	Server 2
Machine name	Dell PowerEdge 1950	Dell PowerEdge 1950
Processor	2 x Intel Xeon Dual Core Processor	2 x Intel Xeon Dual Core Processor
Memory	16GB Memory	16GB Memory
Operating System	Red Hat Enterprise Linux AS Release 4 Update 5	Red Hat Enterprise Linux AS Release 4 Update 5
Drives	160 GB	160 GB
Products	**Oracle Identity Manager Infrastructure 10.1.4.0.1** Oracle Internet Directory 10.1.4.0.1 (includes Oracle Database 10.1.0.5.0) Virtual Directory 10.1.4.0.1 HTTP Server 10.1.3.1.0 WebGate 10.1.4.0.1 WebPass 10.1.4.0.1 Policy Manager 10.1.4.0.1 Access Manager Patch 5912931	**Oracle Identity Manager Infrastructure 10.1.4.0.1** Oracle Internet Directory 10.1.4.0.1 (includes Oracle Database 10.1.0.5.0) Identity Server 10.1.4.0.1 Access Server 10.1.4.0.1 Access Manager Patch 5912931

Table 1 – Environmental Configuration (Developer's tests)

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

	Server 1	Server 2
Machine name	Dell PowerEdge 1950	Dell PowerEdge 1950
Processor	2 x Intel Xeon Dual Core Processor	2 x Intel Xeon Dual Core Processor
Memory	16GB Memory	16GB Memory
Operating System	Red Hat Enterprise Linux AS Release 4 Update 5	Red Hat Enterprise Linux AS Release 4 Update 5
Drives	160 GB	160 GB
Products	**Oracle Identity Manager Infrastructure 10.1.4.0.1** Oracle Internet Directory 10.1.4.0.1 (includes Oracle Database 10.1.0.5.0)	**Oracle Identity Manager Infrastructure 10.1.4.0.1** Oracle Internet Directory 10.1.4.0.1 (includes Oracle Database 10.1.0.5.0)

	Server 1	Server 2
	Virtual Directory 10.1.4.0.1 HTTP Server 10.1.3.1.0 WebGate 10.1.4.0.1 WebPass 10.1.4.0.1 Policy Manager 10.1.4.0.1 Access Manager Patch 5912931	Identity Server 10.1.4.0.1 Access Server 10.1.4.0.1 Access Manager Patch 5912931

Table 2 – Environmental Configuration (Evaluators' tests)

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

IV. PRODUCT ARCHITECTURE

Introduction

36. 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

37. Oracle Identity and Access Management is a suite of products that allows enterprises to manage and automate the end-to-end lifecycle of user identities, and provides users with secure, fine-grained access to enterprise resources and assets. For this evaluation of Oracle Identity and Access Management the products that constitute the Target of Evaluation are Oracle Access Manager, Oracle Internet Directory and Oracle Virtual Directory. Thus the TOE is a resource access control system that uses LDAP directories to hold its security credentials.

38. In its operational mode, the TOE receives requests that have originated from an access client, queries the LDAP directories for authentication, authorization and auditing rules, validates credentials, authorizes users to access resources, and manages user sessions. The use of Oracle Identity and Access Management administration tools to set up the LDAP directories to hold the authentication, authorization and auditing rules and credentials is outside the scope of the TOE.

TOE Design Subsystems

39. The TOE subsystems are contained within the products of the Oracle Identity and Access Management suite as follows:

- Oracle Access Manager provides Web-based identity administration, as well as access control to Web applications and resources running in a heterogeneous environment. It provides the user and group management, delegated administration, password management and self-service functions necessary to manage large user populations in complex, directory-centric environments. Access Manager supports all popular authentication methods including browser forms, digital certificates and smart cards, and integrates seamlessly with most application servers and portals. User identities and credentials can be accessed from a number of LDAP-based repositories including Oracle Internet Directory, Microsoft Active Directory and Sun Java System Directory. With Access Manager, user access policies can be defined and enforced with a high degree of granularity through centralised management. Please note that only the limited set of authentication methods that are relevant to the secure network in the TOE's evaluated configuration are included in the TOE scope and that Oracle Virtual Directory is used as the LDAP-based repository for user security attributes in the evaluated configuration.

  The TOE subsystems that are within Oracle Access Manager are the Identity Server, the Access Server, WebPass and WebGate. Oracle Access Manager's administration tools are outside the scope of the TOE.

- Oracle Internet Directory 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. In the TOE, OID is used to store the policy data and configuration data required by Oracle Access Manager.

  The TOE subsystems that are within Oracle Internet Directory are the Oracle Internet Directory Server, the Oracle Directory Server Run-Time Tools (oidmon and oidctl) and the Essential Directory Administration Tools.

- Oracle Virtual Directory is an LDAPv3-enabled service that provides virtualised abstraction of one or more enterprise data sources into a single directory view. Oracle Virtual Directory provides the ability to integrate LDAP-aware applications into diverse directory environments while minimizing or eliminating the need to change either the infrastructure or the applications. In the TOE, Oracle Virtual Directory combines the user data required by OAM from multiple data sources to create an aggregated, virtual directory. From the point of view of OAM, the virtual directory looks and behaves just like any other LDAP directory.

  The TOE subsystem that is within Oracle Virtual Directory is the Oracle Virtual Directory Server. Oracle Virtual Directory's administration tools are outside of the TOE.

40. The diagram below illustrates the configuration of the TOE. Under normal circumstances, the TOE is entered when a user has clicked on a link in a Web page to a resource. WebGate is the Web server plug-in that intercepts the HTTP request from the user's browser for access to the resource. WebGate forwards the request to the Access Server for authentication and authorization. The dotted line in the diagram indicates the mechanism whereby Identity Server can be entered via WebPass to enforce the TOE's password policy. This happens, for example, when the user's password has expired and the user has to supply a new one before the access request can be processed. The Oracle Directory Server instances that are outside of the TOE Boundary in the diagram are part of the test configuration for the TOE and are used to hold TOE user security credentials.

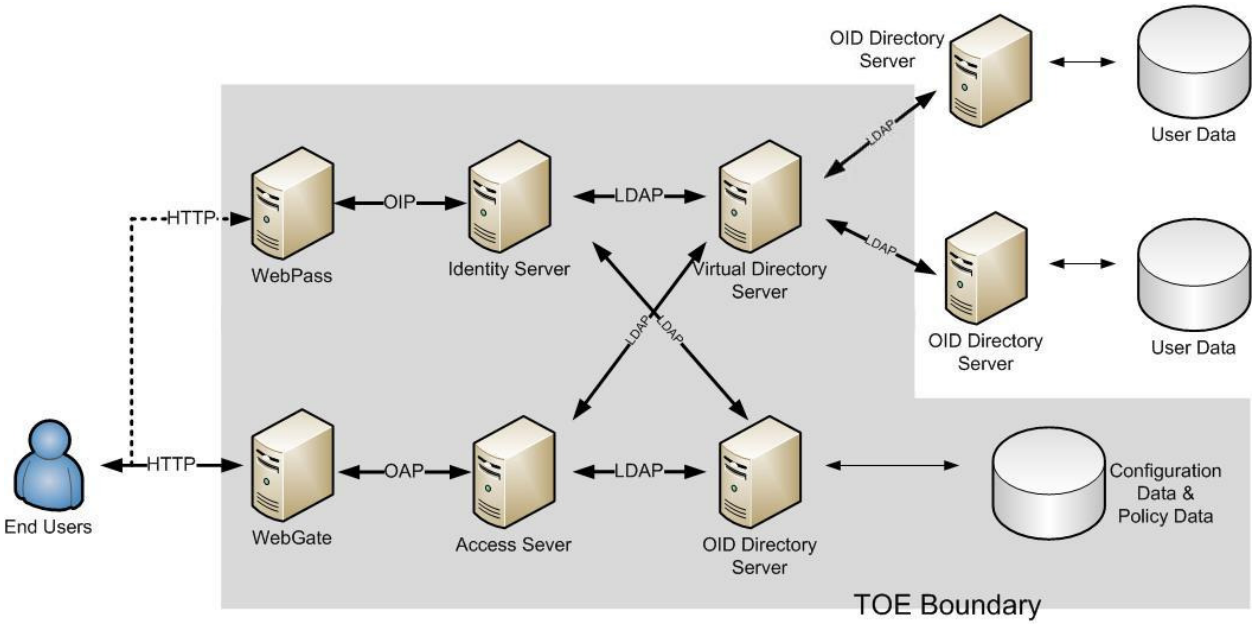

Figure 1 - Oracle Identity and Access Management Architecture

TOE Dependencies

41. The TOE has no hardware or firmware dependencies.

TOE Interfaces

42. The external TSFI is described as follows:

- The call to the WebGate module from the Oracle HTTP Server `httpd` daemon.
- The call to the WebPass module from the Oracle HTTP Server `httpd` daemon to enforce the TOE's password policy when an end user has requested access to a resource.
- Access via the operating system command line to the directory administration tools that are essential for the OID directory to be maintained and administered securely.

V. TOE TESTING

TOE Testing

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

44. 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.

45. The Evaluators installed and tested the TOE on the platform specified in Table 2, in accordance with the logical configuration specified in Figure 1.

46. 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: Microsoft Internet Explorer, Mozilla Firefox, EditCookies (Firefox extension), WebScarab, Nmap and the Protos LDAP testing suite.

Vulnerability Analysis

47. 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

48. The Developer's 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, Part 2: Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2005-08-004, Version 2.3, August 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 Identity & Access Manager 10*g* (10.1.4.0.1), March 2008, Issue 0.3, Oracle Corporation.

[ETR1] LFL/T245 Evaluation Technical Report 1, Evaluation of Oracle Identity & Access Manager 10*g* (10.1.4.0.1), Issue 1.0, 23 August 2007, Logica CLEF.

[ETR2] LFL/T245 Evaluation Technical Report 2, Evaluation of Oracle Identity & Access Manager 10*g* (10.1.4.0.1), Issue 1.1, 16 April 2008, Logica CLEF.

[ETR3] LFL/T245 Evaluation Technical Report 3, Evaluation of Oracle Internet Directory 10*g* (10.1.4.0.1), Issue 1.0, 18 April 2008, Logica CLEF.

[OAMAG] Oracle Access Manager Access Administration Guide 10*g* (10.1.4.0.1), Part No. B25990-01, July 2006, Oracle Corporation.

[OAMICAG] Oracle Access Manager Identity & Common Administration Guide 10*g* (10.1.4.0.1), Part No. B25343-01, July 2006, Oracle Corporation.

[OAMIG] Evaluated Configuration for OIAM 10*g* (10.1.4.0.1): Oracle Access Manager Installation, February 2008, Issue 0.2, Oracle Corporation.

[OHSIG] Evaluated Configuration for OIAM 10*g* (10.1.4.0.1): Oracle HTTP Server Installation, January 2008, Issue 0.1, Oracle Corporation.

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

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

[OVDIG] Evaluated Configuration for OIAM 10*g* (10.1.4.0.1): Oracle Virtual Directory Installation, February 2008, Issue 0.2, Oracle Corporation.

[OVDPM] Oracle Virtual Directory Product Manual 10*g* (10.1.4.0.1), Part No. B28833-01, June 2006, Oracle Corporation.

[ST] Security Target for Oracle Identity & Access Manager 10*g* (10.1.4.0.1), Issue 0.9, March 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
OAM	Oracle Access Manager
OIAM	Oracle Identity and Access Manager
OID	Oracle Internet Directory
ONS	Oracle Net Services
OVD	Oracle Virtual Directory
PWD	Password

(This page is intentionally blank.)