122

CERTIFICATION REPORT No. CRP266

Oracle Identity Manager

Release 9.1.0.2

running on Red Hat Enterprise Linux AS Version 4 Update 5

Issue 1.0

January 2012

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

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 Manager Release 9.1.0.2		
Platform:	Red Hat Enterprise Linux AS Version 4 Update 5		
Description:	Oracle Identity Manager is an enterprise identity management system that centrally controls user accounts and access privileges to enterprise IT resources.		
CC Version:	Version 2.3		
CC Part 2:	Extended	CC Part 3:	Conformant
EAL:	EAL4 augmented by ALC_FLR.3		
SoF:	SoF-High		
CLEF:	Logica		
CC Certificate:	P266	Date Certified:	13 January 2012

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG 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 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 performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

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

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] 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 performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to this Agreement and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which carried out the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo **CC logo** **SOGIS MRA logo**

[1] All judgements contained in this Certification Report are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Oracle Identity Manager Release 9.1.0.2 to the Sponsor, Oracle Corporation, as summarised on page 2 'Certification Statement' of this report, 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 13 January 2012:

- **Oracle Identity Manager Release 9.1.0.2, running on Red Hat Enterprise Linux AS Version 4 Update 5**

4. The Developer was Oracle Corporation.

5. Oracle Identity Manager (OIM) is an enterprise identity management system that centrally controls user accounts and access privileges to enterprise IT resources.

6. The evaluated configuration of the 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' of this report.

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

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 (SFs) that refine the Objectives. Apart from FAU_GEN.1T.1 and FAU_GEN.1T.2, all of the remaining SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

9. There are no threats that have not been countered.

10. The TOE security policies are detailed in [ST].

11. The environmental assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Strength of Function Claims

12. The minimum Strength of Function (SoF) was claimed to be SoF-High. This was claimed for the *PWD* mechanism. The Evaluators have determined that these claims were met.

Evaluation Conduct

13. The CESG Certification Body monitored the evaluation, which was performed 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 January 2012, were reported in the Evaluation Technical Reports (ETRs) [ETR1], [ETR2], [ETR3] and [SUPP].

Conclusions and Recommendations

14. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

15. Prospective consumers of Oracle Identity Manager Release 9.1.0.2 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 [ECG] 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 [ECG]. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE. The CESG Certification Body also recommends that the TOE's consumers should assess the evaluated configuration [ECG] of the TOE with respect to the security policy of their operational environment and consider further improving security by:

a) increasing the *password length* from 6 to 8 or more, in line with current good practice; and

b) decreasing the *number of consecutive failed login attempts* from 10,000 to a value between 3 and 10, in line with current good practice.

17. The evaluators discovered a non-exploitable vulnerability whereby a user could identify resource request approval tasks assigned to other users. However the information disclosed was minimal, identifying the user and the date of the task, and its status (e.g. pending, completed). No details of the tasks themselves were disclosed (e.g. identity of the resource requested). Users should thus be aware that the existence of their resource provisioning approval tasks are not kept wholly private by the TOE. The evaluators recommend that this non-exploitable vulnerability, which does not prevent certification of the TOE, should be addressed in future versions of OIM.

Disclaimers

18. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

19. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

20. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the final ETR [ETR3] 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.

21. 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 under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

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

II. TOE SECURITY GUIDANCE

Introduction

23. The following sections provide guidance of particular relevance to purchasers of the TOE.

Delivery

24. On receipt of the TOE, the consumer should check that the evaluated version has been supplied and that the security of the TOE has not been compromised during delivery.

Installation and Guidance Documentation

25. The Installation and Secure Configuration documentation is as follows:

a) Evaluated Configuration Guide [ECG] – Provides guidance to administrators for securing the TOE and its environment. [ECG] refers to other guidance documents relevant to the TOE, namely:

- OIM Connector Guide for Database User Management [DBCG];
- Evaluated Configuration Guide for Oracle Database [ECGDB];
- Evaluated Configuration for Oracle Internet Directory [ECGOID];
- CC EAL4+ Evaluated Configuration Guide for Oracle Enterprise Linux 4 U4 and U5 [ECGOEL4];
- OIM Audit Report Developer’s Guide [ADG];
- OIM Connector Guide for Oracle Internet Directory [OCG].

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

a) OIM Admin and User Console Guide [AUCG].

III. EVALUATED CONFIGURATION

TOE Identification

27. The TOE is Oracle Identity Manager Release 9.1.0.2, which consists of the Oracle Identity Manager Server application, the Oracle Internet Directory Connector (Release 9.0.4.5) and the Database User Management Connector (Release 9.0.4.5).

TOE Documentation

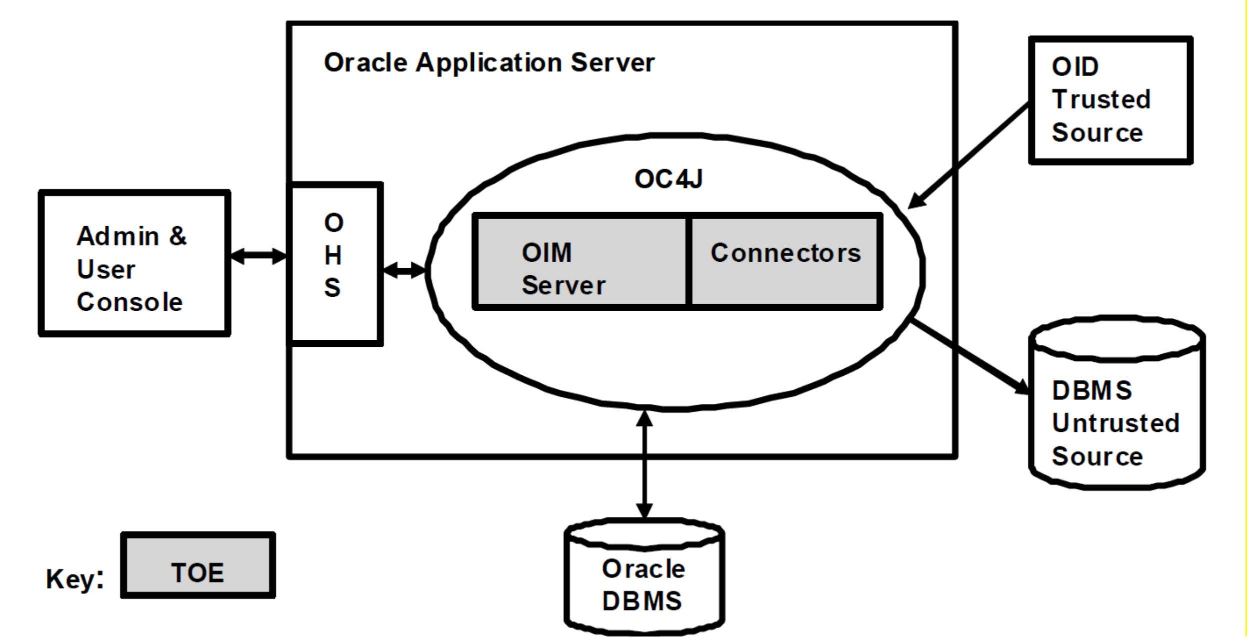
28. The relevant guidance for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

TOE Scope

29. The TOE Scope is defined in the Security Target [ST] Section 2. Functionality outside the TOE Scope is defined in [ST] Section 2 – "Other Oracle Identity Manager Security Features".

TOE Configuration

30. The TOE evaluated configuration is defined in [ECG] and summarised in Figure 1 below.



Oracle HTTP Server (OHS) is used to serve HTTPS requests from the Oracle Admin & User client to the OC4J container in which OIM operates.

Figure 1: TOE Configuration

Environmental Requirements

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

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

33. The environmental IT configuration is as follows:

a) The operating system and database server shall identify and authenticate users prior to providing access to the underlying system.

b) The operating system shall provide the discretionary access control mechanisms required to support the TOE and the IT environment in ensuring files can only be accessed by authorized users.

c) The operating system shall provide an auditing system to support the TOE and the IT environment by ensuring users can be held accountable for their access to IT assets other than via a TOE interface.

d) The system shall provide backup, restore and other secure recovery mechanisms. Such mechanisms are to be capable of archiving and restoring the TOE's audit trail.

Test Configuration

34. The Developers used the following configuration for their testing:

a) An OIM server installed on a Dell Rack Mounted Server, which hosted two virtual machines. Of the two virtual machines, one was a database (Oracle Database (ODB)) server and the other was a directory (Oracle Internet Directory (OID)) server. The configuration was similar to that specified in Section 2.1 of [ECG].

b) The client machine that was mainly used for testing was a Windows XP machine with Internet Explorer 7 (IE7).

c) The OIM machine had hostname *oim.oim-test.com* and IP address *172.20.16.139* assigned. The operating system was Red Hat Enterprise Linux AS Version 4 Update 5. The installed components were as follows (the last three were components of the TOE):

- Oracle Application Server 10g (10.1.3.3.0);
- Oracle Database 10g (10.2.0.2.0);
- Oracle Identity Manager 10g (9.1.0.2);
- Database User Management Connector (9.0.4.5);
- Oracle Internet Directory Connector (9.0.4.5).

35. The Evaluators used the same configuration as the Developers for their testing.

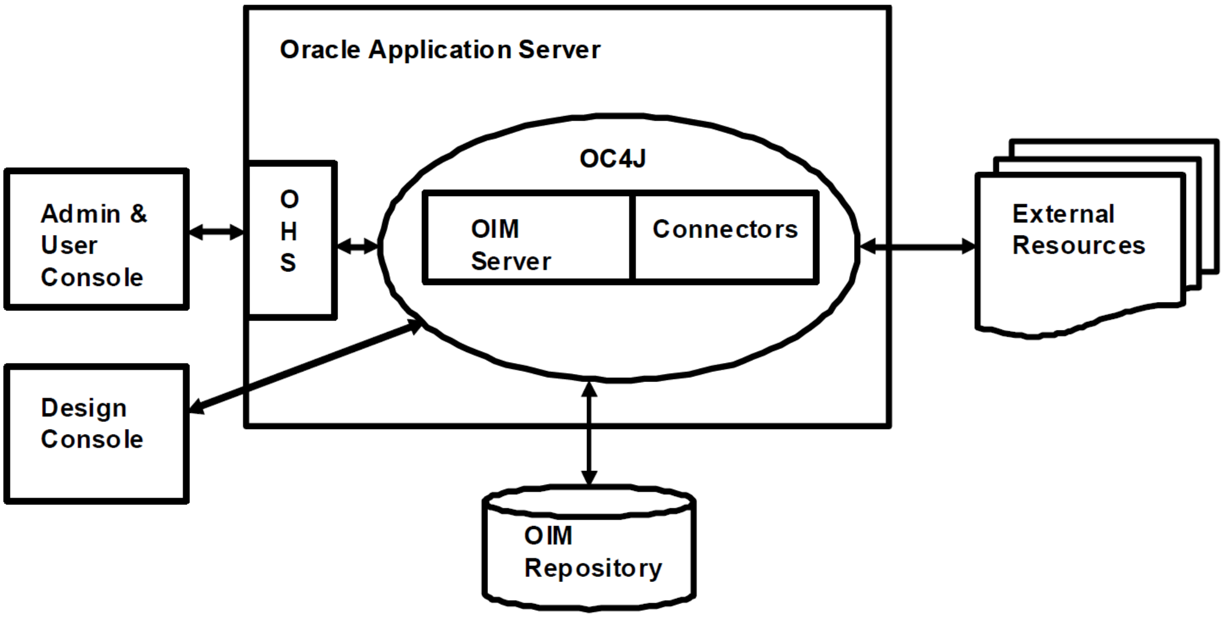
IV. PRODUCT ARCHITECTURE

Introduction

36. This Chapter gives an overview of the TOE’s main architectural features. Other details of the scope of evaluation are given in Chapter III ‘Evaluated Configuration’ of this report.

Product Description and Architecture

37. The TOE architecture (summarised in Figure 2 below) is that OIM is an enterprise identity management system that centrally controls user accounts and access privileges to enterprise IT resources. It provides the functionalities of identity administration, approval and request management, policy-based entitlement management, and audit and compliance automation. OIM automates user identity provisioning and de-provisioning and enables organizations to manage the entire life cycle of user identities across all resources in the organization.



Oracle HTTP Server (OHS) is used to serve HTTPS requests from the Oracle Admin & User client to the OC4J container in which OIM operates.

Figure 2: OIM Architecture

38. OIM is built on a Java 2 Enterprise Edition (J2EE)-based N-tier deployment architecture that separates the platform’s presentation, business logic and data tiers. OIM can provision Lightweight Directory Access Protocol (LDAP)-enabled and non-LDAP-enabled applications. OIM runs on leading J2EE-compliant application server platforms.

TOE Design Subsystems

39. The TOE consists of one subsystem (the OIM Server Application) which comprises:

a) **Administrative and User Console –** This provides a user interface that allows users access to OIM's self-service and delegated administration features that serve most of OIM's provisioning requirements. Users can access this interface via a Web browser.

b) **Authentication –** This leverages the Java Authentication and Authorisation Services (JAAS) provided by the Oracle Containers for Java (OC4J) application server to provide custom authentication functionality.

c) **Provisioning Server** – This provides functionality related to the execution of provisioning tasks and is the run-time engine for OIM.

d) **Provisioning Manager –** This is concerned with the creation of resources, processes and access policies. The provisioning manager is where provisioning transactions are assembled and modified.

e) **Password Management –** This includes methods for setting the Xellerate password for a specific user, setting passwords for users in the specified provisioned objects, and setting object and user password policies.

f) **Reconciliation Engine** – This ensures consistency between the provisioning environment of OIM and OIM-managed resources within the organization.

g) **Attestation Manager** – This provides a mechanism by which reviewers are periodically notified of a report, which they must review, that outlines the provisioned resources that certain users have.

h) **Integration Solutions (Connectors)** – OIM provides a three-tier integration solutions strategy for provisioning users to external IT systems. This strategy is designed to minimize custom development, maximize code re-use, and reduce deployment time.

i) **Services –** This supports the other OIM Server Application components via a set of services that provide commonly used functionality.

TOE Dependencies

40. The TOE has no hardware or firmware dependencies.

TOE Interfaces

41. The external TOE Security Functions Interface (TSFI) is described as follows:

- Java Server Pages, Version 2.0;
- Servlets, Version 2.4;

- Enterprise Java Beans (EJB), Version 2,1 and annotations;
- Java Message Service, Version 1.1;
- Java Authentication and Authorization Service (JAAS), Version 1.0;
- J2EE Connector Architecture, Version 1.5;
- Java Naming and Directory Interface (JNDI) 1.2.1.

V. TOE TESTING

TOE Testing

42. The Developer’s tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in ‘TOE Design Subsystems’) of this report;
- all SFs;
- the TSFI, as identified in Chapter IV (in ‘TOE Interfaces’) of this report.

43. The Developer’s tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly.

44. The test configuration used by the Developer and the Evaluators is identified in Chapter III of this report.

45. The Evaluators devised and ran a total of 13 independent functional tests, different from those performed by the Developer. No anomalies were found.

46. The Evaluators also devised and ran a total of 15 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

47. The Evaluators finished running their penetration tests on 30 November 2011.

Vulnerability Analysis

48. The Evaluators’ vulnerability analysis, which preceded penetration testing and was reported in [ETR1], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables, in particular the Developer’s vulnerability analysis.

Platform Issues

49. The Developer provided a Platform Rationale as to why the security of the TOE is not undermined by the underlying platforms. The Evaluators analysed that Platform Rationale, and performed various tests against the underlying OS and the database. The Evaluators confirmed that each underlying platform does not undermine the security of the TOE.

VI. REFERENCES

[ADG] Oracle Identity Manager Audit Report Developer's Guide,
Oracle Corporation,
E14045-03, Release 9.1.0.1, June 2010.

[AUCG] Oracle Identity Manager Admin and User Console Guide,
Oracle Corporation,
E14765-02, August 2009.

[CC] Common Criteria for Information Technology Security Evaluation
(comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[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.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

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

[DBCG] Oracle Identity Manager, Connector Guide for Database User Management,
Oracle Corporation,
E10425, Release 9.0.4, July 2009.

[ECG] Evaluated Configuration Guide for Oracle Identity Manager 10g (9.1.0.2),
Oracle Corporation,
Issue 1.0, 14 December 2011.

[ECGDB] Evaluated Configuration Guide for Oracle Database 10g Release 2 (10.2.0),
Oracle Corporation,
Issue 0.6, November 2007.

[ECGOEL4] CC EAL4+ Evaluated Configuration Guide for Oracle Enterprise Linux 4 U4 and U5,
Oracle Corporation,
Version 1.3, August 2007.

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

[ETR1] Evaluation Technical Report 1,
Logica CLEF,
LFL/T259/ETR1, Issue 1.0, October 2008.

[ETR2] Evaluation Technical Report 2,
Logica CLEF,
LFL/T259/ETR2, Issue 1.0, June 2011.

[ETR3] Evaluation Technical Report 3,
Logica CLEF,
LFL/T259/ETR3, Issue 1.1, 10 January 2012.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee,
Senior Officials Group – Information Systems Security (SOGIS),
Version 3.0, 8 January 2010 (effective April 2010).

[OCG] Oracle Identity Manager, Connector Guide for Oracle Internet Directory,
Oracle Corporation,
E10436-04, Release 9.0.4, December 2008.

[ST] Security Target for Oracle Identity Manager Release 9.1.0.2,
Oracle Corporation,
Issue 0.9, November 2011.

[SUPP] Supplement to LFL/T259 [ETR3],
CESG Certification Body,
CB/111214/LFL/T259, (final update) 12 January 2012.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.6, December 2009.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.3, December 2009.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.3, October 2010.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.4, December 2009.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC); standard Common Criteria abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]; and UK Scheme abbreviations (e.g. CESG, CLEF) covered in [UKSP00].

EJB	Enterprise Java Beans
JAAS	Java Authentication and Authorization Service
JNDI	Java Naming and Directory Interface
J2EE	Java 2 Enterprise Edition
LDAP	Lightweight Directory Access Protocol
OC4J	Oracle Containers for Java
ODB	Oracle Database
OHS	Oracle HTTP Server
OID	Oracle Internet Directory
OIM	Oracle Identity Manager
PWD	Password

This page is intentionally blank.