UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P221

Oracle Database 10*g* Enterprise Edition

Release 1 (10.1.0.4)
with Critical Patch Update - July 2005
running on specified platforms

Issue 1.0

November 2005

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

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

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

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

Trademarks:

CERTIFICATION STATEMENT

Oracle Database 10*g* Enterprise Edition is an object-relational database management system developed by Oracle Corporation.

Oracle Database 10*g* Enterprise Edition Release 1 (10.1.0.4) with Critical Patch Update - July 2005 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the CC Part 3 augmented requirements of Evaluation Assurance Level EAL4 (i.e. augmented by ALC_FLR.3) for the specified CC Part 2 conformant functionality in the specified environment when running on the platforms specified in Annex A.

Oracle Database 10*g* Enterprise Edition Release 1 (10.1.0.4) with Critical Patch Update - July 2005 was evaluated on Red Hat Enterprise Linux AS Version 3 Update 2, which has previously been certified to EAL3 augmented by ALC_FLR.3.

When running on the operating system platform specified in Annex A, Oracle Database 10*g* Enterprise Edition, Release 1 (10.1.0.4) with Critical Patch Update - July 2005 conforms to the CC Database Management System Protection Profile with the *Database Authentication* functional package.

Originator	**N Whittaker-Axon** Certifier
Approval and Authorisation	**J C Longley** Technical Manager of the Certification Body
Date authorised	25 November 2005

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CAPP	Controlled Access Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CPU	Critical Patch Update
DAC	Discretionary Access Control
DBMS	Database Management System
DBMSPP	Database Management System Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
MLR	Merge Label Request
OCI	Oracle Call Interface
ONS	Oracle Net Services
O-RDBMS	Object-Relational Database Management System
OS	Operating System
PGA	Program Global Area
PL/SQL	Programming Language / Structured Query Language
RDBMS	Relational Database Management System
SFP	Security Function Policy
SFR	Security Functional Requirement
SGA	System Global Area
SOF	Strength of Function
SQL	Structured Query Language
SQLJ	Structured Query Language Java
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UKSP	United Kingdom Scheme Publication
VPD	Virtual Private Database

(This page is intentionally left blank)

REFERENCES

Standards and Criteria

a. 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.

b. 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.

c. 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.

d. 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.

e. Database Management System Protection Profile,
Oracle Corporation,
Issue 2.1, May 2000.

f. Controlled Access Protection Profile,
US National Security Agency,
Version 1.d, 8 October 1999.

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

h. CLEF Requirements: Part I – Startup and Operation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02 Part I, Issue 4.0, April 2003.

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

Previous Certification Reports

j. Common Criteria Certification Report No. P211:
Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0),
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, February 2005.

k. Common Criteria Certification Report No. P178:
Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0),
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, September 2003.

l. Common Criteria Certification Report No. BSI-DSZ-CC-0257-2004:
Red Hat Enterprise Linux AS Version 3, Update 2 with eal3-certification package,
Bundesamt für Sicherheit in der Informationstechnik, Germany,
2 August 2004.

TOE Evaluation Reports

m. Task LFL/T209 Evaluation Technical Report 1,
LogicaCMG CLEF,
310.EC201124:30.1, Issue 1.0, 14 October 2004.

n. Task LFL/T209 Evaluation Technical Report 2,
LogicaCMG CLEF,
Task209.EC201124:30.2.2, Issue 1.0, 9 June 2005.

o. Task LFL/T209 Evaluation Technical Report 3,
LogicaCMG CLEF,
Task209.EC201124:30.3.4, Issue 1.0, 8 September 2005.

p. Email from the Sponsor to the Certifier, 7 November 2005.

q. Emails from the Evaluators to the Certifier,
16 November 2005, 18 November 2005 and 21 November 2005.

Evidence for Evaluation and Certification

r. Security Target for Oracle Database 10*g* Release 1 (10.1.0),
Oracle Corporation,
Issue 1.1, November 2005.

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

t. Oracle Database Administrator's Guide, 10*g* Release 1 (10.1),
Oracle Corporation,
Part No. B10739-01, December 2003.

u. Oracle Database Installation Guide, 10*g* Release 1 (10.1.0.3) for Linux x86-64,
Oracle Corporation,
Part No. B14399-01, October 2004.

v. Oracle Database Security Guide, 10*g* Release 1 (10.1),
Oracle Corporation,
Part No. B10773-01, December 2003.

w. Oracle Database Concepts, 10*g* Release 1 (10.1),
Oracle Corporation,
Part No. B10743-01, December 2003.

x. Oracle Database Reference, 10*g* Release 1 (10.1),
Oracle Corporation,
Part No. B10755-01, December 2003.

y. Oracle Database Application Developer's Guide - Fundamentals, 10*g* Release 1 (10.1),
Oracle Corporation,
Part No. B10795-01, December 2003.

z. Oracle Database SQL Reference, 10*g* Release 1 (10.1),
Oracle Corporation,
Part No. B10759-01, December 2003.

aa. SQL *Plus User's Guide and Reference, Release 10.1,
Oracle Corporation,
Part No. B12170-01, December 2003.

bb. Oracle Call Interface Programmer's Guide, 10*g* Release 1 (10.1),
Oracle Corporation,
Part No. B10779-01, December 2003.

cc. Oracle Database Patch Set Notes, 10*g* Release 1 (10.1.0.4), Patch Set 2 for Linux x86,
Oracle Corporation
Available from Oracle MetaLink:
http://metalink.oracle.com

dd. Oracle Critical Patch Update - July 2005, Release Notes for Oracle Database Server
Version (10.1.0.4), README for Patch Number 4392423,
Oracle Corporation
Available from Oracle MetaLink:
http://metalink.oracle.com

ee. EAL3 Evaluated Configuration Guide for Red Hat Enterprise Linux,
Klaus Weidner,
Version 1.2, 29 June 2004
Available from:
ftp://www6.software.ibm.com/software/developer/library/os-ltc-security/RHEL-EAL3-Configuration-Guide.pdf

ff. Deploying Oracle9*i* Database on Red Hat Enterprise Linux,
Jennifer Lamb, Red Hat Inc,
March 2004
Available from:
http://www.redhat.com

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) IT security evaluation of Oracle Database 10g Enterprise Edition Release 1 (10.1.0.4) with Critical Patch Update - July 2005, running on specified platforms, to the Sponsor (Oracle Corporation) and is intended to assist prospective consumers when judging the suitability of the product for their particular requirements.

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

Evaluated Product

3. The version of the product evaluated was:

> Oracle Database 10*g* Enterprise Edition, Release 1 (10.1.0.4)
> with Critical Patch Update - July 2005.

4. This report describes the product as the Target of Evaluation (TOE) and identifies it as '*Oracle 10g*'. The Developer was Oracle Corporation.

5. The TOE is an Object-Relational Database Management System (O-RDBMS) that has been developed to provide comprehensive security functionality for multi-user distributed database environments.

6. The main security features provided by the TOE are:

- user identification and authentication, with password management options;
- Discretionary Access Control (DAC) on database objects;
- granular privileges for the enforcement of least privilege;
- user-configurable roles for privilege management;
- extensive and flexible auditing options;
- secure access to remote Oracle databases;
- stored procedures, triggers and security policies for user-defined access controls and auditing.

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

TOE Scope

8. The scope of the certification includes the following Oracle server product:

> Oracle Database 10*g* Enterprise Edition, Release 1 (10.1.0.4)
> with Critical Patch Update - July 2005.

9. Access to the above product is provided via the Oracle Call Interface (OCI) Release 1 (10.1.0.4) product, which constitutes the TOE Security Functions Interface (TSFI).

10. OCI Release 1 (10.1.0.4) is part of the evaluated configuration of the TOE. It provides a client-side, application programming interface (API) for developing database applications written in high level languages such as C.

11. The TOE can operate in standalone, client/server and distributed configurations. Oracle client products are outside the scope of the TOE's certification. (The Evaluators used Oracle Database 10*g* Client, Release 1 (10.1.0.3), but only for testing the TOE.) Database links may be provided to connect different O-RDBMS servers over a network.

12. The TOE can also operate in a multi-tier environment, but that is actually a particular type of client/server configuration in which the client application is located on a middle-tier, whilst the user interface is located on a separate 'thin' client (e.g. a web browser or a network terminal). In a multi-tier environment, any middle tier that communicates with the server is an Oracle client (which is outside the scope of the certification) and any lower tiers are also outside the scope of the certification.

13. The scope of the certification applies to the TOE running on the following operating system platform:

> Red Hat Enterprise Linux AS Version 3, Update 2 with eal3-certification package (identified in this report as 'Red Hat Linux AS 3').

14. Annex A summarises the platforms on which the TOE was evaluated.

15. The previously evaluated version of the product was Oracle 9*i* Database Server Enterprise Edition Release 2 (9.2.0.1.0), identified in this report as 'Oracle 9*i*' (see Certification Reports [j, k]). The TOE includes the following new or modified security related features since Oracle 9*i*:

- 'drop database' function;
- enhancements to standard auditing and fine grained auditing;
- uniform audit trail;
- Virtual Private Database (VPD) static and dynamic policies;
- column level VPD;
- shared VPD policy types;
- SYSAUX tablespace;
- enhancements to flashback (i.e. flashback database, flashback table, flashback version query, flashback drop, flashback transaction query);
- Structured Query Language (SQL) syntax.

16. The TOE should not be connected to any untrusted or potentially hostile network (such as the Internet), unless additional security measures are applied. Hence use of the TOE when connected to such a network is outside the scope of the certification.

17. The scope of the certification also excludes various features of the product which are related to security but do not directly address any of the functional requirements identified in the Security Target [r]. Those features, which are specified in the section 'Other Oracle Database 10*g* Security Features' in Chapter 2 of the Security Target, are as follows:

- data integrity;
- import/export;
- backup and recovery;
- Oracle Advanced Security;
- supplied packages;
- external authentication services;
- application-specific security;
- support for Structured Query Language Java (SQLJ).

Protection Profile Conformance

18. The Security Target [r] claims conformance with the DBMSPP [e], with that profile's *Database Authentication* functional package, when running on Red Hat Linux AS 3.

19. The evaluated configuration of the TOE (when running on Red Hat Linux AS 3) supports one mode of authentication in accordance with the above claim, namely *O-RDBMS Mode*. In that mode, *Database Authentication* is performed directly by the Oracle 10*g* server, using passwords managed directly by that server.

20. The claimed SFRs in the Security Target [r] were all included in the CC Database Management System Protection Profile (DBMSPP) [e], except that FMT_SMF.1 has been added to reflect a change to the CC after the DBMSPP was published. The Security Target claims that this change does not affect its conformance with the DBMSPP because FMT_SMF.1 only specifies the management functions for which the other families in the FMT class define usage restrictions.

Assurance

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

22. CC Part 1 [a] provides an overview of the CC.

23. CC Part 3 [c] describes the scale of assurance given by predefined levels EAL1 to EAL7, and provides details of ALC_FLR.3.

Strength of Function Claims

24. The Security Target [r] claims that the minimum Strength of Function (SOF) for the TOE is SOF-high. This exceeds the requirement in the DBMSPP [e], which requires at least SOF-medium overall for the TOE and the operating system.

25. The claim of SOF-high for the TOE is only applicable to its *Database Authentication*, which includes a one-way encryption algorithm (modified Data Encryption Standard (DES)) to encrypt passwords before storing them in the database. The Security Target [r] 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. However the modified DES encryption algorithm is publicly known and as such it is the policy of the UK national authority for cryptographic mechanisms, Communications-Electronics Security Group (CESG), not to comment on its appropriateness or strength.

Security Function Policy

26. The TOE has an explicit access control Security Function Policy (SFP), defined 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.

27. See the Security Target [r] for further details.

Security Claims

28. The Security Target [r] claims conformance against DBMSPP [e]. In the Security Target:

a. The claimed threats are as per the DBMSPP.

b. The claimed Organisational Security Policies are as per the DBMSPP.

c. The claimed assumptions are as per the DBMSPP, plus the following:

i. A.TOE.CONFIG is modified (to refer to the Evaluated Configuration document [s], but is otherwise unchanged);

ii. A.MIDTIER is added.

d. The claimed TOE security objectives are as per the DBMSPP.

e. The claimed environmental security objectives are as per the DBMSPP.

f. The claimed SFRs are as in the DBMSPP (which draws its SFRs from CC Part 2 [b]), except that the Security Target adds SFR FMT_SMF.1 to reflect a change to CC Part 2 after the DBMSPP was published. Use of CC Part 2, as a standard, facilitates comparison with other evaluated products.

g. The claimed assurance requirements are strengthened from those in the DBMSPP (i.e. the TOE's target assurance level is EAL4 augmented with ALC_FLR.3, which exceeds the DBMSPP assurance requirement of EAL3).

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

- identification and authentication (i.e. F.IA);
- access control: database resources (i.e. F.LIM);
- access control: discretionary access control (i.e. F.DAC);
- access control: roles and privileges (i.e. F.APR and F.PRI);
- audit and accountability (i.e. F.AUD).

Evaluation Conduct

30. The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme, as described in United Kingdom Scheme Publication (UKSP) 01 [g] and UKSP 02 [h, i]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

31. As stated on page ii of this report, the Certification Body is a member of the Common Criteria Mutual Recognition Arrangement. The evaluation was performed in accordance with the terms of that Arrangement.

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

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

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

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

35. Some results were re-used from the following previous evaluations, where such results complied with the above requirements and remained valid for the TOE:

a. the evaluation of Oracle9*i* (running on SUSE Linux Enterprise Server Version 8) to EAL4 augmented with ALC_FLR.3 (see Certification Report P211 [j]);

b. the evaluation of Oracle9*i* (running on Sun Solaris 8 Release 2/02 and Microsoft Windows NT Version 4.0) to EAL4 augmented with ALC_FLR.3 (see Certification Report P178 [k]).

36. The Certification Body monitored the evaluation, which was performed by the LogicaCMG Commercial Evaluation Facility (CLEF).

37. The evaluation of Oracle 10*g* (when running on Red Hat Linux AS 3) was completed in September 2005, when the CLEF submitted the last of its Evaluation Technical Reports (ETRs) [m - o] to the Certification Body. The Certification Body requested further clarification and, following satisfactory responses from the Sponsor [p] and the CLEF [q], the Certification Body produced this Certification Report.

General Points

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

39. 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 (September 2005). Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since then and, if appropriate, should check with the Vendor to see if any patches exist for the product and what assurance exists for such patches.

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

II. EVALUATION FINDINGS

Introduction

41. The evaluation addressed the requirements specified in the Security Target [r]. The results of this work were reported in the ETRs [m - o] under the CC Part 3 [c] headings.

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

Delivery

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

44. 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 indicated on the invoice.

45. 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 high security couriers, or other measures, if required by the consumer.

46. 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.

47. The TOE is delivered to the consumer as three separate components:

a. The appropriate CD pack, i.e. 10.1.0.3 (for Linux).

Note: The Evaluators and the Certification Body recommend that consumers should obtain delivery of this via physical media (e.g. CD-ROMs for software; printed documentation).

b. The patch set to make 10.1.0.4.

c. The critical patch update – July 2005.

Note: Oracle currently issues patches via the Internet only, i.e. at its MetaLink website (http://metalink.oracle.com). This includes checksums for recent patches and recent critical patch updates (including those in b. and c. above), for consumers to verify the identity and integrity of their downloaded patch files. MetaLink is available only to consumers with Oracle support contracts; it requires an account and a purchased licence, and this is valuable for providing an audit trail and accountability. A consumer can guard against spoofing of the Oracle website by phoning Oracle support and asking them to check their patch download audit log; a log entry would confirm that Oracle initiated the download and would identify the consumer's MetaLink account that downloaded the patch.

48. Those components are described in the Evaluated Configuration document [s] and summarised below, for the TOE running on Red Hat Linux AS 3:

a. The consumer orders and receives the CD pack from Oracle, which is labelled as:
'Oracle Database 10*g* Release 1 (10.1.0.3) CD/Media Pack v4 for Linux x86, Oracle Part Number B18736-01'.

b. The consumer downloads the 10.1.0.4 patch set from Oracle's MetaLink website:
'10.1.0.4 patch set for Oracle Database Server
Patch set 4163362
Linux x86'.

c. The consumer downloads the critical patch update from Oracle's MetaLink website:
'Patch Number 4392423
MLR ON TOP OF 10.1.0.4 FOR CPUJUL2005
RDBMS Server
Oracle 10.1.0.4
Linux x86
14-Jul-2005'.

Installation and Guidance Documentation

49. The Evaluated Configuration document [s] specifies the steps that a consumer must perform to ensure the secure installation and configuration of the TOE. The Evaluators confirmed that the TOE generated by the installation and configuration procedures is unique, if the steps in the Evaluated Configuration document are followed.

50. Guidance to administrators and end-users regarding security of the TOE is provided in the Evaluated Configuration document [s] and the Oracle 10*g* Administrator's Guide [t]. Those documents also indicate how the TOE's environment can be secured. The procedures in the Evaluated Configuration document that are relevant to end-users are generally limited to common-sense measures (e.g. non-disclosure of passwords).

51. The Evaluated Configuration document [s] and the Oracle 10*g* Administrator's Guide [t] also refer to supporting documentation [r - ff], as appropriate.

52. The Evaluated Configuration document [s] 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

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

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

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

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

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

iv. download patches from Oracle via the MetaLink website.

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

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

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

54. Oracle currently issues patches via the Internet only (at http://metalink.oracle.com, for consumers with Oracle support contracts only), as noted in paragraph 47 above.

Strength of Function

55. Regarding the TOE's *Database Authentication*, the Security Target [r] claims SOF-high for the password space provided by the TOE's password management functions (i.e. the 'PWD mechanism'). That claim applies to two different password profiles:

a. a password of minimum length 8 characters, with no lockout;

b. a password of minimum length 6 characters, with a 1 minute lockout after 3 consecutive failed login attempts.

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

57. The Evaluated Configuration document [s] also specifies a requirement that administrators of the TOE must ensure that *"no applications shall be permitted to run on any client or server machines which access the network, unless they have been shown not to compromise the TOE's security objectives stated in the DBMSPP* [e] *and the Security Target* [r]*"*. This counters the risk of automated login attacks from the client when no lockout is configured.

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

Vulnerability Analysis

59. The Evaluators searched for vulnerabilities regarding the TOE and its components. They also searched for vulnerabilities in the TOE's operating system environment (i.e. Red Hat Linux AS 3) that could be used to compromise the TOE, e.g. from client machines.

60. The Evaluators' vulnerability analysis was based on public domain sources and on the visibility of the TOE given by the evaluation process.

Platform Issues

61. The TOE was evaluated on the operating system platform and hardware platform specified in Annex A.

62. 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

63. After due consideration of the ETRs [m - o] produced by the Evaluators, and the conduct of the evaluation as witnessed by the Certifier, the Certification Body has determined that Oracle Database 10*g* Enterprise Edition Release 1 (10.1.0.4) with Critical Patch Update – July 2005 meets the CC Part 3 augmented requirements of Evaluation Assurance Level EAL4 (i.e. augmented by ALC_FLR.3), for the specified CC Part 2 conformant functionality in the specified environment when running on the platforms specified in Annex A.

64. Oracle Database 10*g* Enterprise Edition Release 1 (10.1.0.4) with Critical Patch Update – July 2005 was evaluated on Red Hat Enterprise Linux AS Version 3, Update 2 with eal3-certification package (which has previously been certified [l] against CC EAL3 augmented by ALC_FLR.3, with CAPP).

65. Oracle Database 10*g* Enterprise Edition Release 1 (10.1.0.4) with Critical Patch Update – July 2005 conforms to the DBMSPP [e], with the *Database Authentication* functional package, when running on that operating system platform.

66. The Strength of Function claim of SOF-high for *Database Authentication* in the Security Target [r] is satisfied.

67. This report certifies only the TOE to assurance level EAL4 augmented by ALC_FLR.3, when running on the operating system platform specified in Annex A (i.e. Red Hat Linux AS 3). Prospective consumers should be aware that:

a. Red Hat Linux AS 3 is not certified to that assurance level. (It has been certified to EAL3 augmented by ALC_FLR.3; see its Certification Report [l].)

b. The security functionality of the TOE relies on the security functionality of the operating system platform, as specified in Section 5.5 of the DBMSPP [e].

Recommendations

68. Prospective consumers of the TOE should understand the specific scope of the certification by reading this report in conjunction with the Security Target [r]. In particular, certification of the TOE does not apply to its use in an untrusted or potentially hostile network environment (such as the Internet).

69. The product provides some features that were not within the scope of the certification as identified in Chapter I under the heading 'TOE Scope'. Those features should therefore not be used if the TOE is to comply with its evaluated configuration.

70. Only the evaluated TOE configuration, as specified in Annex A, should be installed. Subsequent updates to the TOE are covered by Oracle's flaw remediation process.

71. The TOE should be administered and used in accordance with:

    a. the guidance documentation [s, t], which refers to supporting documentation [r - ff] as appropriate;

    b. the environmental considerations outlined in the Security Target [r] and the Evaluated Configuration document [s].

72. As stated in the DBMSPP [e], it is recommended that TOE administrators ensure that any audit records written to the underlying operating system do not result in space exhaustion on secondary storage devices. TOE administrators should use appropriate operating system tools to monitor the audit log size and to archive the oldest logs before the audit space is exhausted.

73. Further details are given in Chapter I under the heading 'TOE Scope' and in Chapter II.

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

   Oracle 10*g* Enterprise Edition, Release 1 (10.1.0.4) with Critical Patch Update – July 2005.

TOE Documentation

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

- Oracle 10*g* Security Target [r];
- Oracle 10*g* Evaluated Configuration document [s];
- Oracle 10*g* Administrator's Guide [t];
- Oracle 10*g* Installation Guide for Linux x86-64 [u];
- Oracle 10*g* Security Guide [v];
- Oracle 10*g* Concepts [w];
- Oracle 10*g* Reference [x];
- Oracle 10*g* Application Developer's Guide [y];
- Oracle 10*g* SQL Reference [z];
- SQL *Plus User's Guide and Reference [aa];
- OCI Programmer's Guide [bb];
- Oracle 10*g* Patch Set 2 Notes for Linux x86 [cc];
- Oracle 10*g* Critical Patch Update – July 2005, Release Notes [dd];
- EAL3 Evaluated Configuration Guide for Red Hat Linux [ee];
- Deploying Oracle 9*i* on Red Hat Linux [ff].

3. Further discussion of the guidance documents is provided in Chapter 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 [s], which refers to supporting documentation [r - ff] as appropriate, as indicated above under the heading 'TOE Documentation'.

Environmental Configuration

5. The TOE has no hardware or firmware dependencies.

6. The TOE has software dependencies, in that it relies on the host operating system to:

   a. Protect the TOE's security features that are within the scope of its evaluation and certification, including its:

      i. access control;

      ii. identification and authentication (Note: the TOE does not use *OS Authentication*, as no Microsoft Windows operating system platforms are used for the TOE);

      iii. auditing (including audit records, if written to the operating system rather than to the RDBMS audit trail);

      iv. security management;

      v. secured distributed processing.

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

7. 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 in configurations using the TOE.

8. The environmental configuration used by the Developer to test the TOE was as summarised in Table A-1. The environmental configuration used by the Evaluators to test the TOE was as summarised in Table A-2.

9. Further details of the TOE's environmental configuration are provided in Chapter I under the heading 'TOE Scope'.

Configuration Type	Oracle 10*g* on Red Hat Linux AS 3
Machine	Dell Power Edge 2650 *(used as the server and the client)*
Processor	dual Intel Xeon (2 x 3.06GHz)
Memory	6GB RAM
Operating System	Red Hat Enterprise Linux AS Version 3, Update 2 with eal3-certification package
Drives	290GB hard drive
Network Connection	10/100BaseT network connection on motherboard

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

Configuration Type	Oracle 10*g* on Red Hat Linux AS 3
Machine	IBM xSeries 335 *(used as the server*)*
Processor	Intel Xeon 2.86GHz
Memory	2.5GB RAM
Operating System	Red Hat Enterprise Linux AS Version 3, Update 2 with eal3-certification package
Drives	40GB hard drive; 3.5" floppy drive, CD-ROM
Network Connection	10/100/1000BaseT network connection on motherboard
* *A Compaq Deskpro EN machine (with Intel Pentium III processor 866MHz, 512MB RAM and 30GB hard disc) was used as the client, running on SUSE Linux 9, connected to the above server via a LAN.*	

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

ANNEX B: PRODUCT SECURITY ARCHITECTURE

Introduction

1. The evaluated product was Oracle 10*g*.

2. Oracle 10*g* is an O-RDBMS that provides comprehensive, integrated and advanced security functionality for multi-user information management environments. An Oracle 10*g* server consists of an Oracle Database 10*g* and an Oracle 10*g* instance.

3. An Oracle Database 10*g* has separate physical and logical structures:

   a. The physical structure of the database is determined by the operating system files that constitute the database. These files provide the actual physical storage for information. Examples of physical structures include data files, redo log files and control files.

   b. The logical structure of the database is determined by its tablespaces (which are logical areas of storage) and its schema (which are collections of database objects or logical structures that directly refer to the information stored in the database). The logical storage structures dictate how the physical space the database is used. The schema objects and the relationships among them form the relational design of the database. Examples of logical structures include tablespaces, schema objects, data blocks, extents and segments.

4. An Oracle 10*g* instance is the combination of background processes that are created and memory buffers that are allocated when an Oracle 10*g* instance is started up:

   a. The background processes are of 2 types:

      i. User processes. A user process is created and maintained to execute an application program (or Oracle tool or Oracle application) on behalf of a user (or client).

      ii. Server processes. A server process is created by the database during the creation of an instance of the database. Server processes handle requests from user processes, and communicate with other server processes to consolidate functions on behalf of the database and user processes, in addition to performing the work required to keep the Oracle 10*g* server running.

   b. The memory buffers that are allocated during startup are collectively called the System Global Area (SGA).

5. It should be noted that the same executable image is started and run, and that each process has available to it, the facilities of each of the other processes.

6. Security functionality in the Oracle Database 10*g* includes:

   - user identification and authentication;
   - access controls on database objects;

- granular privileges for the enforcement of least privilege;
- user-configurable roles for privilege management;
- extensive and flexible auditing options;
- secure access to remote Oracle databases;
- stored procedures and triggers for user-defined access controls and auditing.

7. Oracle 10*g* supports both client/server and standalone architectures. In both architectures, Oracle 10*g* acts as a data server, providing access to the information stored in a database. Access requests are made via the Oracle 10*g* interface products that provide connectivity to the database and submit SQL statements to the Oracle 10*g* server. The Oracle 10*g* interface products may be used on the same computer as the data server, or on separate client machines which communicate with the Oracle 10*g* server via underlying network services.

8. Oracle Net Services (ONS) is the Oracle 10*g* interface product that facilitates the proper transmission of information between Oracle client and server processes using standard communication protocols.

Anatomy

9. A database consists of a set of files that contain control data and other information stored within the database. Each database is an autonomous unit with its own data dictionary that defines the database objects it contains (e.g. tables, views, etc). At the centre of the database is its data dictionary, which is a set of internal Oracle tables that contains all of the information the Oracle 10*g* server needs to manage its database. A set of read-only views is provided to display the contents of the internal tables in a meaningful manner and also allows Oracle users to query the data dictionary without the need to access it directly.

10. All of the information about database objects is stored in the data dictionary and updated by the SQL commands that create, alter and drop database objects. Other SQL commands also insert, update and delete information in the data dictionary in the course of their processing.

11. An Oracle Database 10*g* contains the data dictionary and 2 different types of database objects:

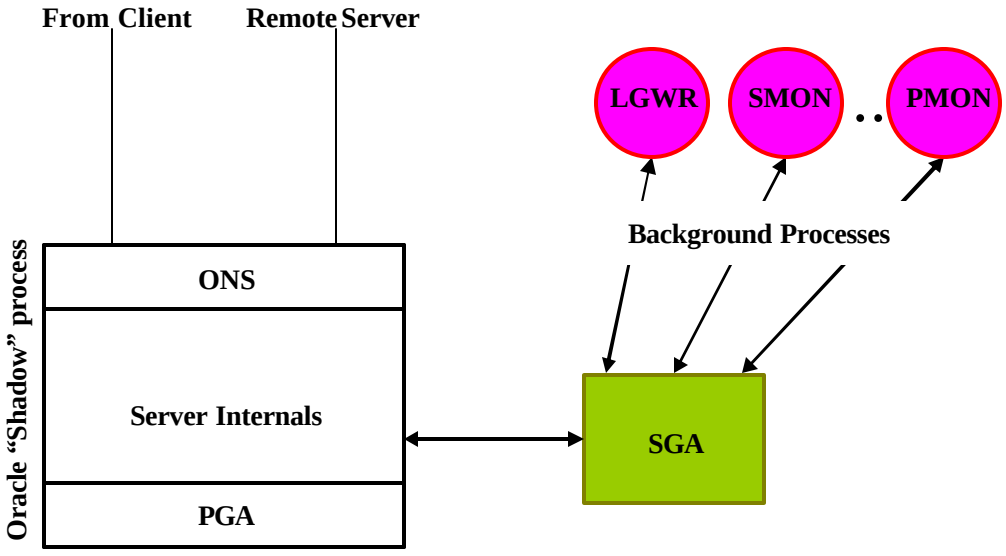
- schema objects: belong to a specific user schema and contain user-defined information;
- non-schema objects: organise, monitor and control the database.

12. A schema is a collection of user-defined database objects that are owned by a single database user. The primary storage management database object is a tablespace. It is used to organise the logical storage of data. A suitably privileged user manages tablespaces to:

- create new tablespaces and allocate database files to the tablespace;
- add database files to existing tablespaces to increase storage capacity;
- assign default tablespaces to users for data storage ;
- take tablespaces on-line and off-line for backup and recovery operations.

13. Within its database files, Oracle 10*g* allocates storage for data in three hierarchical physical units: data blocks, extents and segments. When a user creates a schema object to store data (e.g. a table), a segment is created and the storage space for the segment is allocated to a specific tablespace. Each process (i.e. user process or server process) has its own private area of memory called the Program Global Area (PGA). The PGA is a memory buffer that is allocated by the database when a server process is started. The System Global Area (SGA) is a shared memory region that is allocated when an instance of the database is started. Each instance of the database has its own SGA which is de-allocated upon instance shutdown. Each process of the database accesses the SGA (of that particular instance) to facilitate communication with the other processes. When a process starts, it examines its startup parameters and the contents of the SGA to determine what personality it should assume.

14. The diagram below (Figure B-1) depicts the Oracle 10*g* process architecture described above:



Key to Figure:

LGWR:	**Log Writer, which writes to the redo logs.**
ONS:	**Oracle Net Services**
PGA:	**Program Global Area.**
PMON:	**Process Monitor, which provides process recovery when a process fails.**
SGA:	**System Global Area.**
SMON:	**System Monitor, which provides database instance recovery.**

Figure B-1: Oracle 10*g* Process Architecture

Configuration

15. The Oracle 10*g* architecture supports 3 types of product configurations, i.e. standalone, client/server and distributed:

a. a standalone database configuration is one in which both the client application(s) and Oracle 10*g* server run on a single operating system with at least one database;

b. a client/server database configuration is one in which a client application runs on hardware that is physically separate from the Oracle 10*g* server and its database(s) and must connect to the server and database(s) via a network;

c. a distributed database configuration is one in which multiple client applications access multiple Oracle 10*g* servers and their databases, residing on physically different hardware, over networks.

16. A multi-tier configuration is a particular type of client/server configuration in which the client application is located on a middle-tier, whilst the user interface is located on a separate 'thin' client (e.g. a web browser or a network terminal). The middle-tier acts as an application server for client connections and can proxy on behalf of clients in the database. The model is an extension of the standard client/server configuration, as the database user is now at the middle tier. There is no Oracle software or interfaces on the 'thin' client. Proxy authentication is the mechanism by which this type of authentication works. In that environment, any tier that communicates directly with the server is actually an Oracle client and any lower tiers are outside the scope of the TOE's evaluation and certification.

17. In all of its product configurations, however, Oracle 10*g* enforces all its standard suite of security features.

Identification and Authentication

18. Oracle 10*g* has 2 types of users:

a. administrative users, i.e. those who are defined within an Oracle Database 10*g* as being authorised to perform administrative tasks (e.g. user maintenance, instance startup and shutdown, database backup and recovery);

b. normal users, i.e. all other users defined within an Oracle Database 10*g*.

19. Administrative users are authenticated to the database by virtue of having an entry in the Oracle 10*g* password file or by having operating system-specific access rights. Operating system-specific access rights are normally established by being a member of an operating system group; such users connect to the database by the use of special keywords, e.g. AS SYSDBA, AS SYSOPER.

20. Oracle 10*g* always identifies a user prior to establishing a database session for that user. Authentication of a user's claimed identity can be performed in one of the following ways, as detailed in the subsequent paragraphs respectively:

a. by *Database Authentication*, i.e. directly by the Oracle 10*g* server using passwords that are managed by that server;

b. by *OS Authentication*, i.e. relying on the authentication mechanisms of the host operating system (Note: the TOE does not use *OS Authentication*, as no Microsoft Windows operating system platforms are used for the TOE);

c. by proxy authentication;

d. through an external authentication service or mechanism that depends on the use of the Oracle Advanced Security Option (which is an add-on product for the Oracle 10*g* server and is not within the scope of the TOE's evaluation and certification).

21. For *Database Authentication*, a user must specify a user name and password in order to connect. The Oracle 10*g* server compares that password against that user's password stored in the data dictionary; if they match, a database session is created. The user's password is stored in the data dictionary in a one-way encrypted format.

22. *OS Authentication* allows a user to connect to the database without supplying a username or password. The database obtains the user's identity from the host operating system and compares it against an identity in its data dictionary. If a match is found, the user then connects to the database if he/she has the appropriate session privileges. (Note: the TOE does not use *OS Authentication*, as no Microsoft Windows operating system platforms are used for the TOE.)

23. In a multi-tier environment, Oracle controls the security of middle-tier applications by limiting privileges, preserving client identities through all tiers and auditing actions taken on behalf of clients. In order for the middle-tier to establish a proxy connection for another user, the middle-tier must authenticate itself in the normal manner to the database. Once a connection is made, the middle-tier may then establish a proxy connection for another user, provided that the middle-tier has been given the privilege to do this.

24. In the TOE's evaluated and certified configuration, external authentication services/ mechanisms are not used to authenticate authorised database users.

Access Control

25. Oracle 10*g* includes security features that control how a database is accessed and used. Associated with each database is a schema by the same name. By default, each database user creates and has access to all objects in the corresponding schema. Access to, and security of, objects in other user schemas is governed by the Oracle 10*g* DAC mechanism.

26. Oracle 10*g* DAC is a means of restricting access to information at the discretion of the owner of the information. The Oracle 10*g* DAC mechanisms can be used to enforce need-to-know confidentiality and to control data disclosure, entry, modification and destruction.

27. Oracle 10*g* controls access to database objects based on the privileges enabled in an active database session. There are 2 types of privileges, i.e. system privileges and object privileges:

a. System privileges allow users to perform particular system-wide actions or particular actions on particular types of schema objects. (As these privileges are very powerful, they are typically available only to database administrators.)

b. Object privileges allow users to perform particular actions on specific schema objects.

28. Both system privileges and object privileges may be granted directly to individual users, or granted indirectly by granting privileges to an Oracle role and then granting the role to a user. An Oracle role is a named group of privileges that is granted to a user or another role. In this

manner, a role facilitates easy, controlled and configurable privilege management. During a database session, the privileges enabled in that session may be changed using several Oracle 10*g* mechanisms that affect the set of privileges held by the session.

29. Fine-grained access control (also known as row-level access control) is provided by Virtual Private Database (VPD) technology, which is a standard feature of Oracle 10g Enterprise Edition. Fine-grained access control allows the administrator to associate policies with tables and views. These policies are implemented with PL/SQL functions and are always enforced on normal users no matter how data is accessed. Different policies can be applied for SELECT, INSERT, UPDATE and DELETE operations. It is also possible for more than one policy to be applied to a table, including building on top of base policies in packaged applications. Finally, using the column-level VPD feature, it is possible to ensure that policies are only applied if a particular column or columns are accessed by the user's query.

Audit

30. Oracle 10*g* ensures the accountability of its users' actions by the use of its auditing mechanisms which are designed to be as granular and flexible as possible to ensure that exactly what needs to be audited is properly recorded, but nothing more.

31. The audit categories offered by Oracle 10*g* are:

- by statement (i.e. auditing specific types of SQL statements by all users);
- by object (i.e. auditing specific actions on specific database objects by all users);
- by privilege (i.e. auditing specific system privileges by all users);
- by user (i.e. auditing actions of a specific user or a list of specified users).

32. When defining which actions are to be audited, Oracle 10*g* can be used to specify that only actions that are successful should be written in an audit record, or that only unsuccessful actions are recorded, or that the audit record should be written regardless. For most auditable operations, audit records can be created either by session (i.e. resulting in a single audit record for an audited action for the duration of a session) or by access (i.e. resulting in a separate audit record for each occurrence of an audited action).

33. Audit records can be written to the database audit trail or to the host operating system audit trail or to a specified file in the operating system. Oracle 10*g* provides a number of pre-defined views on the database audit trail to assist in the audit analysis of audit data. Only certain administrative users have the appropriate privileges to read and write all rows in the database audit trail. Normal users granted appropriate privileges may also access the database audit trail, but such access can also be audited. If the audit records are directly sent to the host operating system, audit analysis may be performed using suitable audit analysis tools. Some operations (e.g. connections as administrative users; instance startup and shutdown) are always audited and are written directly to the host operating system.

34. In addition to the standard Oracle 10*g* auditing features described above, application-specific auditing can be implemented using database triggers.

Other Security Features

35. Oracle 10*g* also provides other security features to support robust and reliable database applications. These include:

a. Secure distributed processing using database links. This is within the scope of the TOE's evaluation and certification. (See paragraph 36 of this Annex).

b. Transaction integrity, concurrency and integrity constraints, to ensure the consistency and integrity of data held in a database. This is outside the scope of the TOE's evaluation and certification.

c. Features provided by separate Oracle products which are outside the scope of the TOE's evaluation and certification, such as:

i. secure import and export of data, into the same or a different database, while maintaining data integrity and confidentiality;

ii. backup and recovery of an Oracle Database 10*g*, using operating system-specific backup programs, or database import/export and recovery utilities.

36. A database link is a named schema object that describes the connection path from one database to another. The databases referenced by database links may reside in a standalone, client-server, or distributed configuration. The information in a database link definition is used to provide identification and authentication information to the remote Oracle 10*g* server. By using database links to qualify schema objects, users in a local database (i.e. the database to which they are directly connected) can access data in remote databases.

Network Management

37. Add-on products for Oracle 10*g*, such as Oracle Advanced Security Option, provide encryption of network traffic between clients and servers. Oracle Advanced Security Option also offers mechanisms to configure Oracle 10*g* to use external third party authentication services. However, Oracle Advanced Security Option is not part of the evaluated configuration of the TOE.

38. Oracle Net Services (ONS) is a network transport and management product that forms part of the Oracle 10*g* server and is included in the TOE's evaluated and certified configuration. ONS interfaces with the communications protocols used by the underlying network services that facilitate distributed processing and distributed databases. ONS supports communication over all major network protocols. ONS provides the transport infrastructure for client-to-server communication, hiding the underlying network protocols and associated programmatic interfaces from calling applications. ONS can be administered either directly (i.e. through manipulation of its configuration files) or remotely (i.e. through the Simple Network Management Protocol (SNMP), which is a standard feature of the Oracle 10*g* server).

(This page is intentionally left blank)

ANNEX C: PRODUCT TESTING

Developer's Testing

1. The Developer installed and tested the TOE on the platforms as specified in Annex A.

2. The Developer's testing was designed to test the security mechanisms of the TOE, which implement the security functions identified in the Security Target [r] and their representations identified in the high level design, low level design and source code modules.

3. The Developer's testing consisted of an automated test suite and manual test suites.

Evaluators' Testing

4. The Evaluators installed and tested the TOE on the platforms as specified in Annex A.

5. All of the Evaluators' testing was performed via the TOE's external interface (i.e. OCI), using SQL.

6. For their testing, the Evaluators used sampling as required for the appropriate work-units for EAL4, following the guidance in the CEM [d], Section B.2. They confirmed sample sizes and methods in advance with the Certifier.

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

   a. witnessing the initiation of the Developer's suites of general tests;

   b. witnessing the initiation of the Developer's suite of TOE-specific tests;

   c. witnessing all of the Developer's tests relevant to the security of the TOE, including all of those tests regarding new or modified features of the TOE since Oracle9*i*;

   d. checking that the Developer's tests covered all of the TOE Security Functions (TSF), subsystems and TSFI;

   e. performing a series of independently devised functional tests, in the form of automated SQL scripts, to cover all of the TSF.

8. The Evaluators' findings confirmed that:

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

   b. the Developer's tests covered all of the TSF, subsystems and the TSFI;

   c. (for all of the Developer's tests relevant to the security of the TOE): the actual test results were consistent with the expected test results and any deviations were satisfactorily accounted for ;

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

9. The Evaluators then performed penetration testing of the TOE. Those tests were based on samples of previous tests (i.e. from the Oracle 9*i* evaluations [j, k]), supplemented by new tests to search for potential vulnerabilities introduced by new or modified features of the TOE.

10. From checking various sources on the Internet, the Evaluators found no publicly-known, exploitable vulnerabilities applicable to the TOE, its components or its operating system environment (i.e. Red Hat Linux AS 3).

11. The evaluators found publicly-known vulnerabilities regarding ONS (ONS was within the scope of the evaluated configuration), but those vulnerabilities were not exploitable. The ways by which those vulnerabilities were countered mean that, for the TOE's evaluated configuration, the network on which the O-RDBMS and all of its client applications run:

a. should be under the control of a trusted administrator;

b. should not be connected to any untrusted or potentially hostile networks (e.g. the Internet).

12. In any case, the TOE's evaluated configuration cannot consider the threats on untrusted or potentially hostile networks, since the evaluated configuration of the TOE's underlying operating system (i.e. Red Hat Linux AS 3) does not consider such threats.

13. The results of the Evaluators' penetration testing confirmed:

a. the claimed SOF in the Security Target [r] for the password space for *Database Authentication* (i.e. SOF-high);

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