UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P211

Oracle9*i* Database Enterprise Edition

Release 2 (9.2.0.1.0)

running on SuSE Linux Enterprise Server V8

Issue 1.0

February 2005

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

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

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

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

CERTIFICATION STATEMENT

Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) is an object-relational database management system developed by Oracle Corporation.

Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) 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.

Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) was evaluated on SuSE Linux Enterprise Server V8, which has previously been certified to EAL3 augmented by ALC_FLR.2.

When running on the operating system platform specified in Annex A, Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) conforms to the CC Database Management System Protection Profile with the *Database Authentication* functional package.

When used in conjunction with that operating system platform, which conforms to the CC Controlled Access Protection Profile, Oracle9*i* Database Enterprise Edition Release 9.2.0.1.0 can be used to provide security for systems that have historically required TCSEC C2 (or equivalent security functionality) for databases.

Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) has previously been certified to EAL4 augmented by ALC_FLR.3, when running on Sun Solaris Version 8 and on Microsoft Windows NT Version 4.0.

Originator	**N Whittaker-Axon** Certifier
Approval and Authorisation	**J C Longley** Technical Manager of the Certification Body
Date authorised	11 February 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
DAC	Discretionary Access Control
DBMS	Database Management System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
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
PP	Protection Profile
RC	Release Candidate
RDBMS	Relational Database Management System
SFP	Security Function Policy
SFR	Security Functional Requirement
SGA	System Global Area
SOF	Strength of Function
SP	Service Pack
SQL	Structured Query Language
SQLJ	Structured Query Language Java
TCSEC	Trusted Computer System Evaluation Criteria
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. 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.

k. Common Criteria Certification Report No. P158:
Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, August 2001.

l. Common Criteria Certification Report No. BSI-DSZ-CC-0234-2004:
SuSE Linux Enterprise Server V8 Service Pack 3, RC4 with
certification-sles-eal3 package,
Bundesamt für Sicherheit in der Informationstechnik, Germany,
14 January 2004.

TOE Evaluation Reports

m. Task LFL/T150 Evaluation Technical Report 1,
Logica CLEF,
CLEF.28286.T150.30.1, Issue 0.4, 17 May 2002.

n. Task LFL/T150 Evaluation Technical Report 2,
Logica CLEF,
336.EC28286.T150:30.2, Issue 0.9, 19 August 2002.

o. Task LFL/T150 Evaluation Technical Report 3,
Logica CLEF,
336.EC28286:T150.30.3, Issue 1.0, 9 June 2003.

p. Task LFL/T150 Evaluation Technical Report 4,
LogicaCMG CLEF,
310.EC28286.T150.30.4, Issue 0.9, 8 November 2004.

Evidence for Evaluation and Certification

q. Security Target for Oracle9*i*, Release 2 (9.2.0),
Oracle Corporation,
Issue 0.5, December 2003.

r. Evaluated Configuration for Oracle9*i*, Release 2 (9.2.0),
Oracle Corporation,
Issue 1.0, September 2004.

s. Oracle9*i* Database Administrator's Guide, Release 2 (9.2),
Oracle Corporation,
Part No. A96521-01, March 2002.

t. Oracle9*i* Database Concepts, Release 2 (9.2),
Oracle Corporation,
Part No. A96524-01, March 2002.

u. Oracle9*i* Database Error Messages, Release 2 (9.2),
Oracle Corporation,
Part No. A96525-01, March 2002.

v. Oracle9*i* Database Reference, Release 2 (9.2),
Oracle Corporation,
Part No. A96536-02, October 2002.

w. Oracle9*i* SQL Reference, Release 2 Release 2 (9.2) ,
Oracle Corporation,
Part No. A96540-02, October 2002.

x. How To Get Started,
Oracle Corporation,
Part No. A97375-01.

y. SLES Security Guide,
Klaus Weidner,
atsec GmbH and IBM Corporation,
Version 2.33, 4 December 2003.
Available from:
http://www.novell.com/linux/security/eal3/SLES8_EAL3_SecurityGuide.pdf

z. Installation Instructions for Oracle9*i* Release 2 (9.2) on SuSE Linux Enterprise Server 8 Powered by United Linux 1.0,
SuSE Inc., 2003.
Available from:
http://ftp.novell.com/partners/oracle/docs/920_sles8_install.pdf

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) IT security evaluation of Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0), running on SuSE Linux Enterprise Server V8, 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 q], which specifies the functional, environmental and assurance evaluation requirements.

3. Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) has previously been certified to EAL4 augmented by ALC_FLR.3, when running on Sun Solaris Version 8 ('Solaris8') and on Microsoft Windows NT Version 4.0 ('NT4.0'). See Certification Report P178 [j].

Evaluated Product

4. The version of the product evaluated was:

   Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0).

5. This report describes the product as the Target of Evaluation (TOE) and identifies it as 'Oracle9*i*'. The Developer was Oracle Corporation.

6. 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.

7. 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.

8. When used in conjunction with the operating system platform specified in Annex A, which conforms to the CC Controlled Access Protection Profile (CAPP) [f], Oracle9*i* can be used to provide security for systems that have historically required Trusted Computer System Evaluation Criteria (TCSEC) C2 (or equivalent security functionality) for databases.

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

TOE Scope

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

    Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0).

11. Access to the above product is provided via the Oracle Call Interface (OCI) Release 2 (9.2.0.1.0) product, which constitutes the TOE Security Functions Interface (TSFI).

12. OCI Release 2 (9.2.0.1.0) 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.

13. 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 Oracle9*i* Client Release 2 (9.2.0.1.0), but only for testing the TOE. Database links may be provided to connect different O-RDBMS servers over a network.

14. 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.

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

    SuSE Linux Enterprise Server V8 Service Pack (SP) 3, Release Candidate (RC) 4 with certification-sles-eal3 package (identified in this report as 'SLES8').

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

17. The previously evaluated version of the product was Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0, identified in this report as 'Oracle8*i*' (see its Certification Report [k]). The TOE includes the following new or modified security related features since Oracle8*i*:

- partitioned fine-grained access control, known as Virtual Private Database (VPD);
- secure application roles;
- fine-grained auditing;
- SYS auditing;
- global application context;
- flashback query;
- EXEMPT ACCESS POLICY system privilege;
- GRANT ANY OBJECT PRIVILEGE system privilege;
- synonyms for VPD policies.

18. 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.

19. 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 [q]. Those features, which are specified in the section 'Other Oracle9*i* 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

20. The Security Target [q] claims conformance with the CC Database Management System Protection Profile (DBMS PP) [e], with that profile's *Database Authentication* functional package, when running on SLES8.

21. The evaluated configuration of the TOE, running on SLES8, 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 Oracle9*i* server, using passwords managed directly by that server.

Assurance

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

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

24. 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

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

26. 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 [q] 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

27. 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.

28. See the Security Target [q] for further details.

Security Claims

29. The Security Target [q] claims conformance against DBMS PP [e]. In the Security Target:

a. The claimed threats are as per DBMS PP.

b. The claimed Organisational Security Policies are as per DBMS PP.

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

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

ii. A.MIDTIER is added.

d. The claimed TOE security objectives are as per DBMS PP.

e. The claimed environmental security objectives are as per DBMS PP.

f. The claimed SFRs are as per DBMS PP (which draws its SFRs from CC Part 2 [b]). Use of CC Part 2, as a standard, facilitates comparison with other evaluated products.

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

30. In the Security Target [q], the specifications of the security functions are grouped 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

31. 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.

32. 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.

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

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

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

- the EAL4 requirements specified in CC Part 3 [c];
- the CEM [d];
- appropriate interpretations.

36. 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 Solaris8 and NT4.0, to EAL4 augmented with ALC_FLR.3 (see Certification Report P178 [j]);

b. the evaluation of Oracle8*i* to EAL4 (see Certification Report P158 [k]).

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

38. The evaluation of Oracle9*i* running on Solaris8 and NT4.0 was completed in June 2003, when the CLEF submitted the last of its Evaluation Technical Reports (ETRs) [m - o] to the Certification Body, who then produced the Certification Report for that evaluation [j].

39. The evaluation of the TOE running on SLES8 was completed in November 2004, when the CLEF submitted its ETR for that evaluation [p] to the Certification Body. The Certification Body requested further details and, following the CLEF's satisfactory responses, the Certification Body produced this Certification Report.

General Points

40. The evaluation addressed the security functionality claimed in the Security Target [q], 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.

41. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and what assurance exists for such patches.

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

II. EVALUATION FINDINGS

Introduction

43. The evaluation addressed the requirements specified in the Security Target [q]. The results of this work were reported in the ETR [p] under the CC Part 3 [c] headings.

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

Delivery

45. 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.

46. The consumer receives the TOE as a package clearly labelled as:

> Oracle9*i* Database Release 2 (9.2.0.1.0) CD Pack for Linux Intel Release: NOV-02, Oracle Part Number A99637-01 v4.

The package contains six CDs.

47. 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.

48. 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.

49. 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.

50. Oracle makes components of the TOE available for download from Oracle's websites http://metalink.oracle.com (for existing consumers) and www.oracle.com (for new consumers), but does not provide digital signatures or checksums to enable consumers to verify the identity of the component or its integrity. The Evaluators and the Certification Body recommend that, where the threat of spoofing of the Oracle websites or the corruption or deliberate modification of TOE components in transit is considered relevant to the TOE's operational environment, then consumers should obtain delivery of the TOE via physical media (e.g. CD-ROMs for software, printed books for documentation).

Installation and Guidance Documentation

51. The Evaluated Configuration document [r] 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.

52. Guidance to administrators and end-users regarding security of the TOE is provided in the Evaluated Configuration document [r] and the Oracle9*i* Administrator's Guide [s]. 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).

53. The Evaluated Configuration document [r] and the Oracle9*i* Administrator's Guide [s] also refer to supporting documentation [q - z], as appropriate.

54. The Evaluated Configuration document [r] 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

55. 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.

56. Oracle currently issues patches via the Internet (at http://metalink.oracle.com), where they are available only to consumers with an Oracle support contract as noted above. Consumers can guard against spoofing by phoning Oracle support and asking them to check their patch download audit log; an entry in the log would confirm that Oracle initiated the download.

Strength of Function

57. Regarding the TOE's *Database Authentication*, the Security Target [q] 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.

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

59. The Evaluated Configuration document [r] 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 DBMS PP* [e] *and the Security Target* [q]". This counters the risk of automated login attacks from the client when no lockout is configured.

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

Vulnerability Analysis

61. 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. SLES8) that could be used to compromise the TOE, e.g. from client machines.

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

Platform Issues

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

64. 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

65. After due consideration of the ETR [m - p] produced by the Evaluators, and the conduct of the evaluation as witnessed by the Certifier, the Certification Body has determined that Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) 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.

66. Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) was evaluated on:

> SuSE Linux Enterprise Server V8 SP3, RC4 with certification-sles-eal3 package (which has been certified [l] against CC EAL3, augmented by ALC_FLR.2, with the CC Controlled Access Protection Profile (CAPP) [f]).

67. Oracle9*i* Database Enterprise Edition Release 2 (9.2.0.1.0) conforms to DBMS PP [e], with the *Database Authentication* functional package, when running on that operating system platform.

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

69. When used with the operating system platform specified in Annex A, which conforms to CAPP [f], Oracle9*i* Database Enterprise Edition Release 2(9.2.0.1.0) can be used to provide security for systems that have historically required TCSEC C2 (or equivalent security functionality) for databases.

70. 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. SLES8). Prospective consumers should be aware that:

a. SLES8 is not certified to that assurance level; it is certified to EAL3 augmented by ALC_FLR.2, see Certification Report BSI-DSZ-CC-0234-2004 [l];

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

Recommendations

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

72. 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.

73. 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.

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

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

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

75. As stated in DBMS PP [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.

76. 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:

   Oracle9*i* Enterprise Edition Release 2 (9.2.0.1.0).

TOE Documentation

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

- Oracle9*i* Security Target [q];
- Oracle9*i* Evaluated Configuration document [r];
- Oracle9*i* Database Administrator's Guide [s];
- Oracle9*i* Database Concepts [t];
- Oracle9*i* Database Error Messages [u];
- Oracle9*i* Database Reference [v];
- Oracle9*i* Structured Query Language (SQL) Reference [w];
- How To Get Started [x];
- SLES Security Guide [y];
- Installation Instructions for Oracle9*i* on SLES8 [z].

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 [r], which refers to supporting documentation [q - z] as appropriate, as indicated above under the heading 'TOE Documentation'.

5. Annex B.2 of the Evaluated Configuration document [r] specifies exactly the software components that comprise the evaluated configuration of the TOE. Those components are listed below for ease of reference:

- Assistant Common Files 9.2.0.1.0;
- Generic Connectivity Common Files 9.2.0.1.0;
- Generic Connectivity Using Open Database Connectivity (ODBC) 9.2.0.1.0;
- Oracle Net 9.2.0.1.0;
- Oracle Net Listener 9.2.0.1.0;
- Oracle Net Manager 9.2.0.1.0;
- Oracle Net Required Support Files 9.2.0.1.0;
- Oracle Net Services 9.2.0.1.0;
- Oracle Core Required Support Files 9.2.0.1.0;
- Oracle Call Interface 9.2.0.1.0;

- Oracle9*i* 9.2.0.1.0;
- Oracle9*i* Database 9.2.0.1.0;
- Oracle9*i* Development Kit 9.2.0.1.0;
- Parser Generator Required Support Files 9.2.0.1.0;
- Programming Language / Structured Query Language (PL/SQL) 9.2.0.1.0;
- PL/SQL Embedded Gateway 9.2.0.1.0;
- PL/SQL Required Support Files 9.2.0.1.0;
- Platform Required Support Files 9.2.0.1.0;
- Relational Database Management System (RDBMS) Required Support Files 9.2.0.1.0;
- Required Support Files 9.2.0.1.0.

Environmental Configuration

6. The TOE has no hardware or firmware dependencies.

7. The TOE has software dependencies, in that it relies on the host operating system 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 (N.B. the TOE does not use *OS Authentication* when running on SLES8);
      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.

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

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

Configuration Type	**Oracle9*i* on SLES8**
Machine	Compaq ProLiant DL360 *(used as the server and the client)*
Processor	Intel Pentium III 933MHz / Rev. A
Memory	2GB RAM
Operating System	SuSE Linux Enterprise Server V8 SP3, RC4 with certification-sles-eal3 package
Drives	9.1GB hard drive, 1.44MB floppy drive
Network Connection	Ethernet adapter with Ethernet connection

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

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

Configuration Type	Oracle9*i* on SLES8
Machine	IBM xSeries 335 *(used as the server)* [1]
Processor	Quad Intel Xeon 2.4GHz
Memory	2GB RAM
Operating System	SuSE Linux Enterprise Server V8 SP3, RC4 with certification-sles-eal3 package
Drives	2 x 25GB SCSI discs, IDE DVD drive
Network Connection	onboard Broadcom 1GB Ethernet adapter, Ethernet connection

[1] A Compaq Deskpro EN machine (with Intel Pentium III 866MHz processor, 256MB RAM and 12GB hard disc) was used as the client, running on SLES8, connected to the above server via a Local Area Network (LAN).

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

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

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

Introduction

1. The evaluated product was Oracle9*i*.

2. Oracle9*i* is an O-RDBMS that provides comprehe nsive, integrated and advanced security functionality for multi-user information management environments. An Oracle9*i* server consists of an Oracle9*i* database and an Oracle9*i* instance.

3. An Oracle9i database 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 Oracle9i instance is the combination of background processes that are created and memory buffers that are allocated when an Oracle9i 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 Oracle9*i* 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 Oracle9i database 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. Oracle9*i* supports both client/server and standalone architectures. In both architectures, Oracle9*i* acts as a data server, providing access to the information stored in a database. Access requests are made via the Oracle9*i* interface products that provide connectivity to the database and submit SQL statements to the Oracle9*i* server. The Oracle9*i* interface products may be used on the same computer as the data server, or on separate client machines which communicate with the Oracle9*i* server via underlying network services.

8. Oracle Net Services (ONS) is the Oracle9*i* 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 Oracle9*i* 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 Oracle9i database 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.

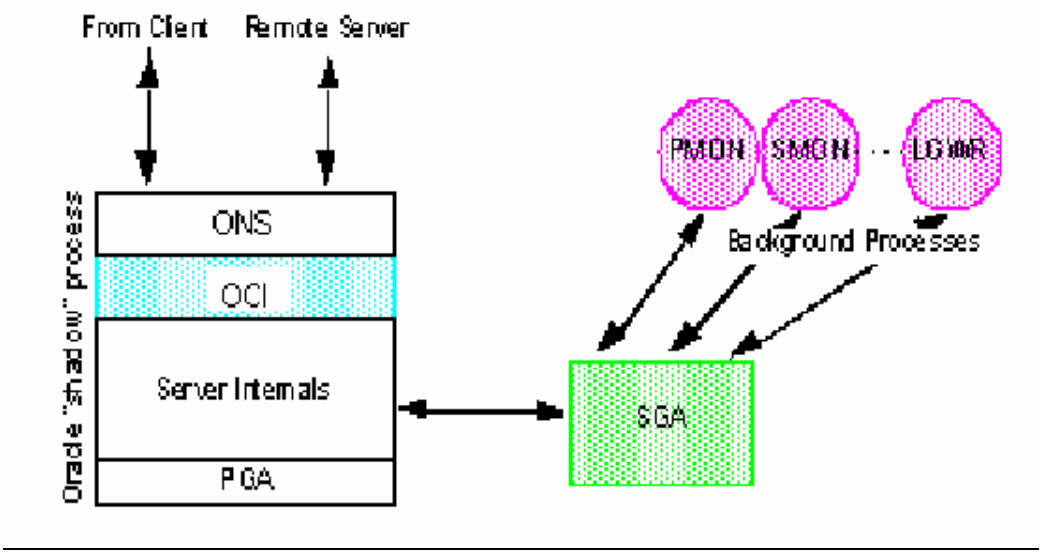
12. A schema is a collection of user-defined database objects that are owned by a single database user. The primary storage management database object is a tablespace. It is used to organise the logical storage of data. A suitably privileged user manages tablespaces to:

- 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, Oracle9*i* 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 Oracle9*i* process architecture described above :



Key to Figure:
LGWR: **Log Writer, which writes to the redo logs.**
OCI: **Oracle Call Interface.**
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: Oracle9*i* Process Architecture

Configuration

15. The Oracle9i 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 Oracle9*i* 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 Oracle9*i* 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 Oracle9*i* 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, Oracle9*i* enforces all its standard suite of security features.

Identification and Authentication

18. Oracle9*i* has 2 types of users:

a. administrative users, i.e. those who are defined within an Oracle9*i* database 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 Oracle9*i* database.

19. Administrative users are authenticated to the database by virtue of having an entry in the Oracle9*i* 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. INTERNAL, AS SYSDBA, AS SYSOPER.

20. Oracle9*i* 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 Oracle9*i* 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 (N.B. Oracle9*i* does not use *OS Authentication* when running on SLES8);

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 Oracle9*i* 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 Oracle9*i* 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. (N.B. Oracle9*i* does not use *OS Authentication* when running on SLES8.)

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. Oracle9*i* 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 Oracle9*i* DAC mechanism.

26. Oracle9*i* DAC is a means of restricting access to information at the discretion of the owner of the information. The Oracle9*i* DAC mechanisms can be used to enforce need-to-know confidentiality and to control data disclosure, entry, modification and destruction.

27. Oracle9*i* 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 Oracle9*i* 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 VPD technology, which is a standard feature of Oracle9*i* 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.

Audit

30. Oracle9*i* 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 Oracle9*i* 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, Oracle9*i* 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. Oracle9*i* 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 Oracle9*i* auditing features described above, application-specific auditing can be implemented using database triggers.

Other Security Features

35. Oracle9*i* 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 Oracle9*i* database, 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 Oracle9*i* 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 Oracle9*i*, such as Oracle Advanced Security Option, provide encryption of network traffic between clients and servers. Oracle Advanced Security Option also offers mechanisms to configure Oracle9*i* 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 Oracle9*i* 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 Oracle9*i* 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 [q] 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 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 two of the Developer's three general suites of tests;

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

   c. repeating 60% of the Developer's tests relevant to the security of the TOE;

   d. repeating all of the Developer's tests regarding new or modified features of the TOE since Oracle8*i*;

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

   f. 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 the sample of the Developer's tests repeated by the Evaluators): the actual test results were consistent with the expected test results and any deviations were satisfactorily accounted for ;

   d. (for the Evaluators' 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 Oracle8*i* evaluation [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 and its operating system environment (i.e. SLES8).

11. The publicly known vulnerabilities that the Evaluators found related to:

- ONS – which was within the scope of the evaluated configuration
- Oracle Internet Application Server) those 3 features were all
- Oracle Apache/Jserv) outside the scope of the
- Oracle Java Virtual machine) evaluated configuration

12. The ways by which the vulnerabilities relating to ONS 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).

13. 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. SLES 8) does not consider such threats.

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

a. the claimed SOF in the Security Target [q] 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.