



**UK IT SECURITY EVALUATION AND  
CERTIFICATION SCHEME**



122-B

**COMMON CRITERIA CERTIFICATION REPORT No. P179**

**Oracle Label Security for Oracle9i Database Enterprise Edition**

**Release 2 (9.2.0.1.0)  
running on Sun Solaris Version 8 and on  
Microsoft Windows NT Version 4.0 with Service Pack 6a**

Issue 1.0

September 2003

© Crown Copyright 2003

Reproduction is authorised provided the report  
is copied in its entirety

UK IT Security Evaluation and Certification Scheme  
Certification Body, PO Box 152  
Cheltenham, Glos GL52 5UF  
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. \*

\* Whilst the Arrangement has not yet been extended to address ALC\_FLR.3, a working agreement exists amongst Parties to the Arrangement to recognise the Common Evaluation Methodology ALC\_FLR supplement (reference [e] in this report) and the resultant inclusion of ALC\_FLR.3 elements in certificates issued by a Qualified Certification Body.

**Trademarks:**

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

## **CERTIFICATION STATEMENT**

Oracle Label Security (OLS) Release 2 (9.2.0.1.0) is a security option for Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0). Both products were developed by Oracle Corporation.

Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0) is an object-relational database management system.

OLS Release 2 (9.2.0.1.0) enables application developers to add label-based access control to their Oracle9i applications, in addition to the discretionary access control provided by Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0).

OLS Release 2 (9.2.0.1.0), used with Oracle9i 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.

OLS Release 2 (9.2.0.1.0), used with Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0), was evaluated on Sun Microsystems Solaris Version 8 (which has previously been certified against the CC Controlled Access Protection Profile) and on Microsoft Windows NT Version 4.0 with Service Pack 6a configured to C2 specification (which has previously been rated to TCSEC Class C2).

OLS Release 2 (9.2.0.1.0), used with Oracle9i 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 running on Sun Microsystems Solaris Version 8) and with the *Operating System Authentication* and *Database Authentication* functional packages (when running on Microsoft Windows NT Version 4.0 with Service Pack 6a configured to C2 specification).

When used in conjunction with the operating system platforms specified in Annex A, which conform to the CC Controlled Access Protection Profile (or equivalent functionality), OLS Release 2 (9.2.0.1.0) used with Oracle9i 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.

<b>Originator</b>	<b>N Whittaker-Axon</b> Certifier
<b>Approval and Authorisation</b>	<b>J C Longley</b> Technical Manager of the Certification Body
<b>Date authorised</b>	30 September 2003

(This page is intentionally left blank)

## TABLE OF CONTENTS

<b>CERTIFICATION STATEMENT .....</b>	<b>iii</b>
<b>TABLE OF CONTENTS .....</b>	<b>v</b>
<b>ABBREVIATIONS .....</b>	<b>vii</b>
<b>REFERENCES .....</b>	<b>ix</b>
<b>I. EXECUTIVE SUMMARY .....</b>	<b>1</b>
Introduction.....	1
Evaluated Product.....	1
TOE Scope .....	2
Protection Profile Conformance .....	3
Assurance.....	4
Strength of Function Claims .....	4
Security Function Policy.....	4
Security Claims.....	5
Evaluation Conduct .....	5
General Points.....	6
<b>II. EVALUATION FINDINGS.....</b>	<b>7</b>
Introduction.....	7
Delivery .....	7
Installation and Guidance Documentation.....	8
Flaw Remediation.....	8
Strength of Function .....	9
Vulnerability Analysis .....	9
Platform Issues.....	9
<b>III. EVALUATION OUTCOME.....</b>	<b>11</b>
Certification Result .....	11
Recommendations .....	11
<b>ANNEX A: EVALUATED CONFIGURATION .....</b>	<b>13</b>
<b>ANNEX B: PRODUCT SECURITY ARCHITECTURE .....</b>	<b>17</b>
<b>ANNEX C: PRODUCT TESTING.....</b>	<b>21</b>

(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
DML	Data Manipulation Language
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEC	IT Security Evaluation Criteria
LBAC	Label-Based Access Control
OCI	Oracle Call Interface
OLS	Oracle Label Security
ONS	Oracle Net Services
O-RDBMS	Object-Relational Database Management System
OS	operating system
PL/SQL	Programming Language/Structured Query Language
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SP	Service Pack
SQL	Structured Query Language
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UFS	Unix File System
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 Interpretation Management Board, CCIMB-99-031, Version 2.1, August 1999.
- b. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Common Criteria Interpretation Management Board, CCIMB-99-032, Version 2.1, August 1999.
- c. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Common Criteria Interpretation Management Board, CCIMB-99-033, Version 2.1, August 1999.
- d. Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Common Evaluation Methodology Editorial Board, CEM-99/045, Version 1.0, August 1999.
- e. Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Supplement: ALC\_FLR - Flaw Remediation, Common Evaluation Methodology Editorial Board, CEM-2001/0015R, Version 1.1, February 2002.
- f. Database Management System Protection Profile, Oracle Corporation, Issue 2.1, May 2000.
- g. Controlled Access Protection Profile, US National Security Agency, Version 1.d, 8 October 1999.
- h. Description of the Scheme, UK IT Security Evaluation and Certification Scheme, UKSP 01, Issue 4.0, February 2000.
- i. The Appointment of Commercial Evaluation Facilities, UK IT Security Evaluation and Certification Scheme, UKSP 02, Issue 3.0, 3 February 1997.

### **Previous Evaluation and Certification Reports**

- j. Common Criteria Certification Report No. P178:  
Oracle9i Database Enterprise Edition Release 9.2.0.1.0,  
UK IT Security Evaluation and Certification Scheme,  
Issue 1.0, September 2003.
- k. Common Criteria Certification Report No. P169:  
Oracle Label Security for Oracle8i Database Server Enterprise Edition Release 8.1.7.3.0,  
UK IT Security Evaluation and Certification Scheme,  
Issue 1.0, March 2003.
- l. Common Criteria Certification Report No. P148:  
Sun Solaris Version 8 with AdminSuite Version 3.0.1,  
UK IT Security Evaluation and Certification Scheme,  
Issue 1.0, November 2000.
- m. Final Evaluation Report:  
Microsoft Corporation Windows NT Workstation and Server, Version 4.0, Service Pack 6a  
With C2 Update,  
Science Applications International Corporation, Center for Information Security  
(Trust Technology Assessment Program - Evaluation Laboratory),  
15 December 1999.

### **TOE Evaluation Reports**

- n. Task LFL/T151 Evaluation Technical Report 1,  
Logica CLEF,  
CLEF.28286.T151.30.1, Issue 0.4, 17 May 2002.
- o. Task LFL/T151 Evaluation Technical Report 2,  
Logica CLEF,  
336.EC28286.T151:30.2, Issue 0.9, 23 August 2002.
- p. Task LFL/T151 Evaluation Technical Report 3,  
Logica CLEF,  
336.EC28286:T151.30.3, Issue 1.0, 9 June 2003.

### **Evidence for Evaluation and Certification**

- q. OLS Security Target for Oracle9i, Release 2 (9.2.0),  
Oracle Corporation,  
Issue 0.7, November 2002.
- r. OLS Evaluated Configuration for Oracle9i, Release 2 (9.2.0),  
Oracle Corporation,  
Issue 0.7, March 2003.

- s. Oracle9i Database Getting Started, Release 2 (9.2) for Windows, Oracle Corporation, Part No. A95490-01, March 2002.
- t. Oracle9i Database Installation Guide, Release 2 (9.2.0.1.0) for Windows, Oracle Corporation, Part No. A95493-01, May 2002.
- u. Oracle9i Installation Guide, Release 2 (9.2.0.1.0) for UNIX Systems: AIX-based Systems, Compaq Tru64 UNIX, HP 9000 Series HP-UX, Linux Intel and Sun Solaris, Oracle Corporation, Part No. A96167-01, May 2002.
- v. Oracle9i Database Administrator's Guide, Release 2 (9.2), Oracle Corporation, Part No. A96521-01, March 2002.
- w. Oracle9i Database Concepts, Release 2 (9.2), Oracle Corporation, Part No. A96524-01, March 2002.
- x. Oracle9i Database Error Messages, Release 2 (9.2), Oracle Corporation, Part No. A96525-01, March 2002.
- y. Oracle9i Database Reference, Release 2 (9.2), Oracle Corporation, Part No. A96536-01, March 2002.
- z. Oracle9i SQL Reference, Release 2 Release 2 (9.2), Oracle Corporation, Part No. A96540-01, March 2002.
- aa. Oracle Label Security Administrator's Guide, Release 2 (9.2), Oracle Corporation, Part No. A96578-01, March 2002.
- bb. Oracle9i Application Developer's Guide - Fundamentals, Release 2 (9.2), Oracle Corporation, Part No. A96590-01, March 2002.
- cc. Solaris 8.0 Security Release Notes - Common Criteria Certification, Sun Microsystems, Inc, Version 1.0, December 2000.
- dd. Microsoft Windows NT 4.0: C2 Configuration Checklist, Microsoft Corporation, (no reference), last updated 5 April 2000.

(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 Oracle Label Security Release 2 (9.2.0.1.0) ('OLS'), used with Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0) ('Oracle9i'), 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.

### **Evaluated Product**

3. The version of the product evaluated was:

- Oracle Label Security Release 2 (9.2.0.1.0), used with Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0)

4. This report describes the product as the Target of Evaluation (TOE) and identifies it as 'Oracle9iOLS'. The Developer was Oracle Corporation.

5. Oracle9i 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. OLS provides label-based access control (LBAC), in addition to the discretionary access control (DAC) provided by Oracle9i. OLS mediates the labels and privileges associated with each user session and it controls access to rows in database tables, based on the label(s) contained in each row.

7. The main security features provided by the TOE are as follows:

- user identification and authentication, with password management options
- DAC on database objects
- LBAC
- 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 platforms specified in Annex A, which conform to the CC Controlled Access Protection Profile [g] (or equivalent functionality), Oracle9iOLS 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.
10. Annex B summarises the security architecture.

### **TOE Scope**

11. The scope of the certification includes the following Oracle server products:
  - Oracle Label Security Release 2 (9.2.0.1.0)
  - Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0)
12. Access to the above products is provided via the Oracle Call Interface (OCI) Release 2 (9.2.0.1.0) product, which constitutes the TOE Security Functions Interface (TSFI).
13. 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.
14. 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 Oracle9i 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.
15. 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.
16. The scope of the certification applies to the TOE running on the following operating system platforms:
  - a. Sun Microsystems Solaris Version 8 (identified in this report as 'Solaris 8'); and
  - b. Microsoft Windows NT Version 4.0 (Build 1381) with Service Pack (SP) 6a, configured to C2 specification (identified in this report as 'NT4.0 SP6a-C2').
17. Annex A summarises the platforms on which the TOE was evaluated.

18. The previously evaluated product was OLS Release 8.1.7.3.0 used with Oracle8i Database Server Enterprise Edition Release 8.1.7.0.0, identified in this report as 'Oracle8iOLS'; see its Certification Report [k]. The TOE includes the following new or modified security related features since Oracle8iOLS (the OLS specific feature is indicated by \*, otherwise the features are provided by Oracle9i):

- 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
- OLS - releasabilities (also known as nationality caveats) \*

19. 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.

20. 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 Oracle9i Security Features' in Chapter 2 of the Security Target, are as follows:

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

### **Protection Profile Conformance**

21. The Security Target [q] claims conformance with the CC Database Management System Protection Profile (DBMS PP) [f], with that profile's following authentication packages:

- a. (When running on Solaris 8): the *Database Authentication* functional package.
- b. (When running on NT4.0 SP6a-C2): the *Operating System (OS) Authentication* functional package and the *Database Authentication* functional package.

22. The evaluated configuration of the TOE supports two modes of authentication, in accordance with the above claims, namely:

- a. *O-RDBMS Mode* (when the TOE is running on Solaris 8 or on NT4.0 SP6a-C2), i.e. in which *Database Authentication* is performed directly by the Oracle9i server, using passwords managed directly by that server.
- b. *OS Mode* (when the TOE is running on NT4.0 SP6a-C2), i.e. in which the Oracle9i server relies on *OS Authentication* performed by that underlying operating system.

### **Assurance**

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

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

25. CC Part 3 [c] describes the scale of assurance given by predefined levels EAL1 to EAL7.

26. The Common Evaluation Methodology (CEM) Part 2 Supplement on Flaw Remediation [e] provides details of ALC\_FLR.3.

### **Strength of Function Claims**

27. 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 [f], which requires at least SOF-medium overall for the TOE and the operating system.

28. 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.

29. For its *OS Authentication*, the TOE relies on the authentication provided by the underlying operating system, i.e. NT4.0 SP6a-C2 as noted in paragraph 22.b above.

### **Security Function Policy**

30. 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, FDP\_ACF.1, FDP\_IFC.1 and FDP\_IFF.2
- (security management): FMT\_MSA.1 and FMT\_MSA.3

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



## Security Claims

32. The Security Target [q] claims conformance against DBMS PP [f]. In the Security Target:
- a. The claimed threats are as per DBMS PP, plus T.LBAC.
  - b. The claimed Organisational Security Policies are as per DBMS PP, plus P.LABEL and P.INFOFLOW.
  - 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); and
    - ii. A.MIDTIER and A.USERS are added.
  - d. The claimed TOE security objectives are as per DBMS PP, plus O.ACCESS.LBAC.
  - e. The claimed environmental security objectives are as per DBMS PP, plus O.USERS.
  - f. The claimed SFRs are as per DBMS PP (which draws its SFRs from CC Part 2 [b]), plus additional SFRs (i.e. FDP\_IFC.1.1, FDP\_IFF.2.1 - 2.7, FMT\_MOF.1.1, FMT\_MSA.1.1.2, FMT\_MSA.3.1.2 and FMT\_MSA.3.2.2) taken directly from CC Part 2. 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).
33. 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: object access control (i.e. F.ACCESS)
  - access control: discretionary access control (i.e. F.DAC)
  - access control: label-based access control (i.e. F.LBAC)
  - access control: roles and privileges (i.e. F.APR and F.PRI)
  - audit and accountability (i.e. F.AUD)

## Evaluation Conduct

34. 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 [h] and UKSP 02 [i]. The Scheme has established a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

35. 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.

36. 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.

37. 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.

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

- the EAL4 requirements specified in CC Part 3 [c]
- the CEM [d]
- the CEM supplement on Flaw Remediation [e]
- the appropriate interpretations

39. Some results were reused from the following previous evaluations, where such results were still valid for the TOE:

- Oracle9i evaluation to EAL4 with ALC\_FLR.3 (see Certification Report P178 [j])
- Oracle8iOLS evaluation to EAL4 (see Certification Report P169 [k])

40. The Certification Body monitored the evaluation, which was performed by the Logica Commercial Evaluation Facility (CLEF). The evaluation was completed in June 2003, when the CLEF submitted the last of its Evaluation Technical Reports (ETRs) [n - p] to the Certification Body. The Certification Body requested further details and, following the CLEF's satisfactory responses, produced this Certification Report.

### **General Points**

41. 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.

42. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) 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 whether such patches have been evaluated and certified.

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

## **II. EVALUATION FINDINGS**

### **Introduction**

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

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

### **Delivery**

46. 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.

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

- a. Oracle9i Database Release 2 (9.2.0.1.0) (CD Pack v1) for Sun SPARC Solaris, Oracle Part Number A91783-01; or
- b. Oracle9i Database Release 2 (9.2.0.1.0) (CD Pack v1) for Microsoft Windows, Oracle Part Number A91809-01.

Note that 'OLS' is not specifically identified on the product packaging, as OLS is delivered as part of Oracle9i as a configurable option.

48. 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.

49. 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.

50. 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.

51. Oracle makes components of the TOE available for download from Oracle's websites <http://metalink.oracle.com> (for existing consumers) and [www.oracle.com](http://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**

52. 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.

53. Guidance to administrators and end-users regarding security of the TOE is provided in the Evaluated Configuration document [r], the OLS Administrator's Guide [aa] and the Oracle9i Administrator's Guide [v]. 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).

54. The Evaluated Configuration document [r], the OLS Administrator's Guide [aa] and the Oracle9i Administrator's Guide [v] refer to supporting documentation [q - dd] as appropriate.

55. The Evaluated Configuration document [r] is released by Oracle to consumers on request. It is anticipated that Oracle may also make that document available for download from one of its web sites (e.g. <http://otn.oracle.com/docs/deploy/security/content.html>).

## **Flaw Remediation**

56. 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; and
  - 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](mailto:secalert_us@oracle.com); and
  - ii. read alerts and news posted on the public website by Oracle regarding flaws, fixes and workarounds.

57. 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**

58. 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; and
- b. a password of minimum length 6 characters, with a 1 minute lockout after 3 consecutive failed logon attempts.

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

60. 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 [f] and the Security Target [q]". This counters the risk of automated logon attacks from the client when no lockout is configured.

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

62. Regarding the TOE's *OS Authentication*, the TCSEC Class C2 evaluation of NT4.0 SP6a-C2 [m] did not specifically incorporate a CC SOF analysis, but is regarded as a reputable evaluation of that operating system and the Evaluators of the TOE checked the latest public sources for any known weaknesses in its authentication mechanism.

## **Vulnerability Analysis**

63. The Evaluators searched for vulnerabilities regarding the TOE and its components. They also searched for vulnerabilities in the TOE's operating system environments (i.e. Solaris 8 and NT4.0 SP6a-C2) that could be used to compromise the TOE, e.g. from client machines.

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

## **Platform Issues**

65. The TOE was evaluated on the operating system platforms and hardware platforms specified in Annex A.

66. 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**

67. After due consideration of the ETRs [n - p] produced by the Evaluators, and the conduct of the evaluation as witnessed by the Certifier, the Certification Body has determined that Oracle Label Security Release 2 (9.2.0.1.0), used with Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0), meets the CC Part 3 [c] augmented requirements of Evaluation Assurance Level EAL4 (i.e. augmented by ALC\_FLR.3), for the CC Part 2 [b] conformant functionality specified in the Security Target [q] in the specified environment when running on the platforms specified in Annex A.

68. Oracle Label Security Release 2 (9.2.0.1.0), used with Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0), was evaluated on:

- a. Sun Microsystems Solaris Version 8 (which has previously been certified [l] against the CC Controlled Access Protection Profile (CAPP) [g]); and
- b. Microsoft Windows NT Version 4.0 (Build 1381) with Service Pack 6a, configured to C2 specification (which has previously been rated [m] to TCSEC Class C2).

69. Oracle Label Security Release 2 (9.2.0.1.0), used with Oracle9i Database Enterprise Edition Release 2 (9.2.0.1.0), conforms to DBMS PP [f] with the *Database Authentication* functional package (when running on Sun Microsystems Solaris Version 8) and with the *OS Authentication* and *Database Authentication* functional packages (when running on Microsoft Windows NT Version 4.0 (Build 1381) with Service Pack 6a, configured to C2 specification).

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

71. When used with the operating system platforms specified in Annex A, which conform to CAPP [g] (or equivalent functionality), Oracle Label Security Release 2 (9.2.0.1.0) used with Oracle9i 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.

#### **Recommendations**

72. 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).

73. 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.

74. 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.

75. The TOE should be administered and used in accordance with:
- a. the guidance documentation [r, aa, v], which refers to supporting documentation [q - dd] as appropriate; and
  - b. the environmental considerations outlined in the Security Target [q] and the Evaluated Configuration document [r].
76. As stated in DBMS PP [f], 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.
77. 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 Label Security Release 2 (9.2.0.1.0), used with Oracle9i Database 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:

- Oracle9iOLS Security Target [q]
- Oracle9iOLS Evaluated Configuration document [r]
- Oracle9iOLS Administrator's Guide [aa]
- Oracle9i Database Getting Started for Windows [s]
- Oracle9i Database Installation Guide for Windows [t]
- Oracle9i Installation Guide for UNIX Systems [u]
- Oracle9i Database Administrator's Guide [v]
- Oracle9i Database Concepts [w]
- Oracle9i Database Error Messages [x]
- Oracle9i Database Reference [y]
- Oracle9i SQL Reference [z]
- Oracle9i Application Developer's Guide - Fundamentals [bb]
- Solaris 8.0 Security Release Notes - CC Certification [cc]
- Microsoft Windows NT 4.0: C2 Configuration Checklist [dd]

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 - dd] 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 (the OLS specific component is indicated by \*, otherwise the components are provided by Oracle9i):

- 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
- Oracle9i 9.2.0.1.0
- Oracle9i Database 9.2.0.1.0
- Oracle9i Development Kit 9.2.0.1.0
- Oracle Label Security 9.2.0.1.0 \*
- Oracle9i Windows Documentation 9.2.0.1.0 (Windows only)
- 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;
    - iii. auditing (including audit records, if written to the operating system rather than to the database audit trail);
    - iv. security management; and
    - 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	Oracle9iOLS on NT4.0 SP6a-C2	Oracle9iOLS on Solaris 8
Machine	Compaq DeskPro EN (used as a server)	Sun Ultra 60 (used as a server)
Processor	Dual 600MHz Intel Pentium III	600MHz Sun UltraSPARC
Memory	512MB RAM	512MB RAM
Operating System	NT4.0 Server (Build 1381) SP6a-C2	Solaris 8
Drives	2 x 18GB hard drives, 3.5" floppy drive, CD-ROM drive	36GB hard drive with Unix File System (UFS), 3.5" floppy drive, DVD/CD-ROM drive
Network Connection	Intel Pro 100 VM network card	10/100BaseT network connection on motherboard

**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	Oracle9iOLS on NT4.0 SP6a-C2	Oracle9iOLS on Solaris 8
Machine	Compaq DeskPro EN (used as a server) <sup>1</sup>	Sun Ultra 60 (used as a server) <sup>2</sup>
Processor	866MHz Intel Pentium III	Identical to configuration used by the Developer (i.e. see 'Oracle9iOLS on Solaris 8' column in Table A-1 above)
Memory	512MB RAM	
Operating System	NT4.0 Server (Build 1381) SP6a-C2	
Drives	15GB hard drive, 3.5" floppy drive, CD-ROM drive	
Network Connection	Intel Pro 100 VM network card	

<sup>1</sup> An equivalent machine was used as a client (running on NT4.0 Workstation (Build 1381) SP6a-C2) for the Evaluators' testing.

<sup>2</sup> An equivalent machine was used as a client (running on Solaris 8) for the Evaluators' testing

**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)

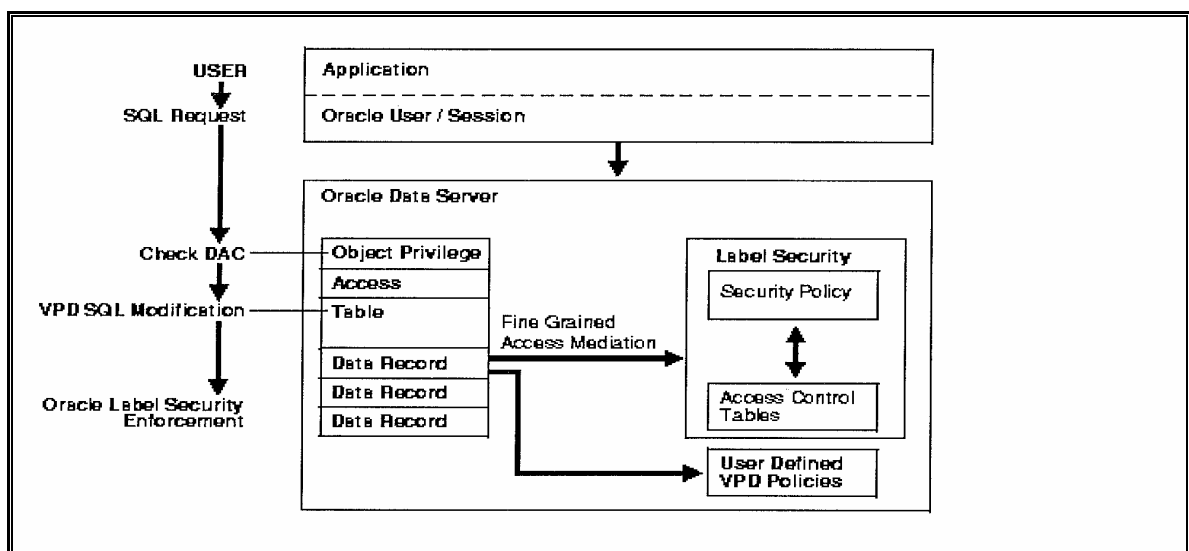
## ANNEX B: PRODUCT SECURITY ARCHITECTURE

### Introduction

1. The evaluated product was Oracle9iOLS.
2. OLS builds upon the VPD technology of Oracle9i.
3. The Oracle9i security architecture is summarised in Annex B of the Oracle9i Certification Report [j]. The OLS specific security architecture is summarised in the following two sections.

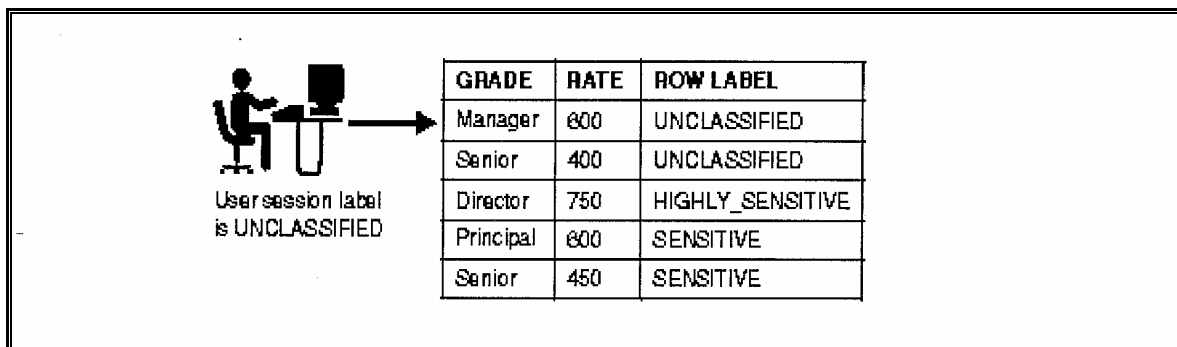
### OLS Label-Based Access Control

4. OLS enables application developers to add LBAC to their applications for Oracle9i. If used, OLS mediates access to rows in database tables, based on a label contained in each row and based on the label and privileges associated with each user session.
5. OLS provides an out-of-the-box VPD policy that enables administrative users to create one or more custom security policies for label access decisions, without knowledge of a programming language. There is no need to write the additional code that is normally required for direct use of VPD, because in a single step a security policy can be applied to a given table. In this way, OLS provides a straightforward and efficient way to implement fine-grained security policies using data label technology.
6. Figure B-1 illustrates the process of accessing data under OLS. Within an application and an Oracle9i session, a user issues a SQL request. Oracle9i checks the DAC privileges, checking that the user has SELECT privileges on the table. Then it checks to see if a VPD policy has been attached to the table. It finds that the table is protected by OLS, so the SQL statement is modified on the fly to enforce the policy. Each data record has a label; OLS is invoked for each row to determine whether, based on the label, the user can or cannot access the row.



**Figure B-1: Accessing Data Under OLS**

7. To create a customised OLS policy, an administrative user defines a set of labels and a set of rules that govern data access, based on those labels. For example, assume that a user has SELECT privilege on an application table. Figure B-2 illustrates that, when the user executes a SELECT statement, OLS assesses each row selected and determines whether the user can access it (i.e. based on the privileges and access labels assigned to the user by the administrative user). OLS can also be configured to perform security checks on UPDATE, DELETE, and INSERT statements.



**Figure B-2: OLS Determines If The User Can Access Each Row Selected**

8. OLS mediates access to data in a table according to the label associated with each row of data, the label associated with the user session, the policy privileges associated with the user session, and the policy enforcement options associated with the table. Consider, for example, a standard Data Manipulation Language (DML) operation (such as SELECT) performed upon a row of data. OLS assesses a request by a user with the IN\_CONFIDENCE label to access a data row with the IN\_CONFIDENCE label; OLS determines that this access can be achieved. In this way, data of different sensitivities, or belonging to different companies, can be stored and managed on a single system, while preserving data security through standard Oracle access controls. Likewise, applications from a broad range of industries can each use row labels to provide additional access control functionality where necessary.

9. Individual application tables can be protected, and not all of the tables in the application need to be protected by an OLS policy. Lookup tables such as zip codes, for example, do not need to be protected. Multiple OLS policies can be created. For example, a human resources policy could co-exist with a defence policy in the same database. Each of the policies can be independently configured and can have its own unique label definitions.

10. In OLS, each row of a table can be labelled as to its level of confidentiality. The label contains three components: a single level or sensitivity ranking; one or more horizontal compartments or categories; and one or more hierarchical groups. The level specifies the sensitivity of the data. A government organisation might define levels UNCLASSIFIED, IN\_CONFIDENCE, SENSITIVE and HIGHLY\_SENSITIVE. A commercial organisation might define levels PUBLIC and COMPANY\_IN\_CONFIDENCE data. The compartment component is non-hierarchical; compartments are typically defined to segregate data, such as data related to an ongoing strategic initiative. Finally, groups are used to record ownership and can be used hierarchically. For example, FINANCE, SALES and ENGINEERING groups can be defined as children of a CORPORATION group, creating an ownership relation. Labels can

contain a single level component, or a level combined with a set of either compartments or groups, or a level with both compartments and groups.

11. Users can be granted label authorisations for each OLS policy, which determine the kind of access (read or write) they have to the rows in tables to which that policy has been applied.
12. Policy privileges enable a user or stored program unit to bypass aspects of the label-based access control policy. In addition, the administrator can authorise the user or program unit to perform specific actions, such as the ability of one user to assume the authorisations of a different user. Privileges can be granted to program units, i.e. authorising the procedure (rather than the user) to perform privileged operations.
13. In OLS, administrators can apply different enforcement options for maximum flexibility in controlling the different DML operations that users can perform. For each SELECT, INSERT, UPDATE and DELETE operation, administrative users can specify a particular type of enforcement of the security policy on a per-table basis. In this way, the label-based access controls can be customised for each table.

#### **Audit**

14. OLS supplements the Oracle9i audit facility, by tracking the use of its own OLS administrative operations and policy privileges. Under OLS, audit trail records contain a label associated with the session that generated the audit, so that the relationship between operations, data labels and the label of the user performing the operation can be seen.

(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 (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;
  - e. checking that the Developer's tests covered all of the TOE Security Functions (TSF), subsystems and TSFI; and
  - 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' found 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; and
  - d. (for the Evaluators' functional tests): the actual test results were consistent with the expected test results.

9. The Evaluators then performed penetration testing on the TOE. Those tests were based on samples of tests from the previous Oracle8iOLS 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 environments (i.e. Solaris 8 and NT4.0 SP6a-C2).

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; and
- 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 configurations of the TOE's underlying operating systems (i.e. Solaris 8 and NT4.0 SP6a-C2) do 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); and
- b. that all identified potential vulnerabilities in the TOE have been addressed, i.e. the TOE in its intended environment has no exploitable vulnerabilities.