UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P169

Oracle Label Security for Oracle8*i* Database Server Enterprise Edition

Release 8.1.7.3.0
running on Sun Solaris Version 8

Issue 1.0

March 2003

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

**ARRANGEMENT ON THE
MUTUAL 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 Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Trademarks:

CERTIFICATION STATEMENT

Oracle Label Security (OLS) Release 8.1.7.3.0 is a security option for Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0. Both products were developed by Oracle Corporation.

Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0 is an object-relational database management system which, when used with interoperable operating system platforms conforming to the CC Controlled Access Protection Profile (or equivalent security functionality), can be used to provide security for systems requiring TCSEC C2 (or equivalent security functionality) for databases.

OLS Release 8.1.7.3.0 enables application developers to add label-based access control to their Oracle8*i* applications, in addition to the discretionary access control provided by Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0. OLS Release 8.1.7.3.0 includes some of the TCSEC B1 security functionality for databases, without requiring the use of an underlying TCSEC B1 (or equivalent) operating system platform.

OLS Release 8.1.7.3.0, used with Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0, has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the CC Part 3 conformant requirements of Evaluation Assurance Level EAL4, for the specified CC Part 2 conformant functionality in the specified environment when running on the platforms specified in Annex A.

OLS Release 8.1.7.3.0, used with Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0, was evaluated on Sun Solaris Version 8 (which has previously been certified against the CC Controlled Access Protection Profile).

OLS Release 8.1.7.3.0, used with Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0, conforms to the CC Database Management System Protection Profile with the *Database Authentication* functional package (when running on Sun Solaris Version 8).

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body
Date authorised	7 March 2003

(This page is intentionally blank)

TABLE OF CONTENTS

(This page is intentionally 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
ETR	Evaluation Technical Report
OCI	Oracle Call Interface
OLS	Oracle Label Security
O-RDBMS	Object-Relational Database Management System
PGA	Program Global Area
PP	Protection Profile
SFR	Security Functional Requirement
SGA	System Global Area
SoF	Strength of Function
SQL	Structured Query Language
TOE	Target of Evaluation
TSF	TOE Security Functions
UKSP	United Kingdom Scheme Publication
VPD	Virtual Private Database

(This page is intentionally blank)

REFERENCES

a. OLS Security Target for Oracle8*i*, Release 3 (8.1.7),
Oracle Corporation,
Issue 0.9, April 2002.

b. Controlled Access Protection Profile,
National Security Agency,
Version 1.d, October 1999.

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

d. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 4.0, February 2000.

e. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

f. 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.

g. 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.

h. Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Requirements,
Common Criteria Interpretation Management Board,
CCIB-99-033, Version 2.1, August 1999.

i. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Evaluation Methodology Editorial Board,
Version 1.0, CEM-99/045, August 1999.

j. 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.

k. Task LFL/T147 Evaluation Technical Report 1,
Logica CLEF,
CLEF.28064.30.1, Issue 1.0, 27 November 2001.

l. Task LFL/T147 Evaluation Technical Report 2,
Logica CLEF,
CLEF.28064.30.2, Issue 1.0, 21 February 2002.

m. Task LFL/T147 Evaluation Technical Report 3,
Logica CLEF,
CLEF.28064.30.3, Issue 1.0, 1 May 2002.

n. Guidance Analysis For Oracle8*i* Database Server, Release 3 (8.1.7),
Oracle Corporation,
Issue 0.1, March 2001.

o. OLS Guidance Analysis for Oracle8*i*, Release 3 (8.1.7),
Oracle Corporation,
Issue 0.2, January 2002.

p. OLS Evaluated Configuration for Oracle8*i*, Release 3 (8.1.7),
Oracle Corporation,
Issue 0.4, April 2002.

q. Oracle Label Security Administrator's Guide, Release 8.1.7,
Oracle Corporation,
Part No. A87345-01, December 2000.

r. Oracle8*i* Administrator's Guide, Release 2 (8.1.6),
Oracle Corporation,
Part No. A76956-01, December 1999.

s. Oracle8*i* Reference, Release 2 (8.1.6),
Oracle Corporation,
Part No. A76961-01, December 1999.

t. Oracle8*i* Application Developer's Guide - Object Relational Features, Release 2 (8.1.6),
Oracle Corporation,
Part No. A76976-01, December 1999.

u. Oracle8*i* Concepts, Release 2 (8.1.6),
Oracle Corporation,
Part No. A76965-01, December 1999.

v. Oracle8*i* Administrator's Reference for SUN SPARC Solaris, Release 3 (8.1.7),
Oracle Corporation,

Part No. A85349-01, August 2000.

w. OCI Programmer’s Guide, Release 2 (8.1.6),
Oracle Corporation,
Part No. A76975-01, December 1999.

x. Oracle8*i* Error Messages, Release 2 (8.1.6),
Oracle Corporation,
Part No. A76999-01, December 1999.

y. Oracle Label Security Installation Notes, Release 8.1.7 for Sun SPARC Solaris,
Oracle Corporation,
Part No. A87348-01, December 2000.

z. Oracle8*i* Installation Guide, Release 3 (8.1.7) for Sun SPARC Solaris,
Oracle Corporation,
Part No. A85471-01, August 2000.

aa. Solaris 8.0 Security Release Notes - Common Criteria Certification,
Sun Microsystems, Inc,
Document No. s8.0_125, Version 1.0, December 2000.

(This page is intentionally blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the IT security evaluation of Oracle Label Security Release 8.1.7.3.0 (OLS) used in conjunction with Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0 (Oracle8*i*) to the Sponsor, Oracle Corporation. This report is intended to assist potential consumers when judging the suitability of the product for their particular requirements.

2. The prospective consumer is advised to read this report in conjunction with the Security Target [Reference a], which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

- Oracle Label Security Release 8.1.7.3.0, used with Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0

4. This product is also described in this report as the Target of Evaluation (TOE). The Developer was Oracle Corporation. Details of the evaluated configuration, including the product's supporting guidance documentation, are given in Annex A.

5. OLS provides label-based access control in addition to the discretionary access control provided by Oracle8*i*. OLS mediates the labels and privileges associated with each user session and controls access to rows in database tables based on the label or labels contained in the row. The product is used in conjunction with Oracle8*i* which can operate in standalone, client/server and distributed configurations. Oracle client products were not part of the scope of the evaluation.

6. The TOE provides the following security functionality:

- User identification and authentication
- Access controls on database objects
- Label-Based Access Control
- Granular privileges for the enforcement of least privilege
- User-configurable roles for privilege management
- Configurable auditing
- Secure access to remote Oracle databases
- Stored procedures and triggers for user-defined access controls and auditing

7. When used in conjunction with the operating system platform specified in Annex A, meeting the Common Criteria (CC) Controlled Access Protection Profile (CAPP) [b], Oracle8*i* can be used to provide security for systems that require TCSEC C2 or equivalent security functionality for databases. Details of the TOE's architecture can be found in Annex B to this report.

TOE Scope

8. The scope of the certification includes the following Oracle8*i* server products:

- Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0
- Oracle Server Manager 8.1.7.3.0
- Distributed Database Option 8.1.7.3.0
- Objects Option 8.1.7.3.0
- Oracle Label Security Release 8.1.7.3.0
- Net8 8.1.7.3.0

9. Access to the above server is provided via the Oracle Call Interface (OCI) Release 8.1.7.3.0 product, which constitutes the TOE Security Functions Interface (TSFI).

10. The TOE scope does not include any Oracle clients. Use of the TOE in a network connected to a potentially hostile network (such as the internet) is also outside the scope of this evaluation.

11. The scope of the certification applies to the TOE running on Sun Solaris Version 8. See Annex A for details of the platforms on which the TOE was tested.

12. The scope of the certification excludes the following options and features of Oracle8*i*, which were outside the scope of the evaluation:

- Advanced Security Option (ASO)
- Multi-Threaded Server (MTS)
- all integrity features

Protection Profile Conformance

13. The Security Target [a] claims conformance with the Database Management System Protection Profile (DBMS PP) [c] with the Database Authentication functional package. The Security Target introduces new Security Functional Requirements (SFRS) that are not in the DBMS PP. Those new SFRs cover the requirements associated with Label-Based Access Control.

Assurance Level

14. The Security Target [a] specifies the assurance requirements for the resultant evaluation. The assurance comprised pre-defined evaluation assurance level EAL4. CC Part 3 [h] describes the scale of assurance given by predefined evaluation assurance levels EAL1 to EAL7.

15. The Security Target [a] noted that the EAL4 assurance requirement exceeded the DBMS PP [c] claim of EAL3. EAL4 was also considered appropriate for the OLS Security Functionality claims, which were additional to the DBMS PP claims.

Strength of Function

16. The certified configuration of the TOE included the O-RDBMS authentication package.

17. The O-RDBMS authentication option included a one-way encryption algorithm (modified Data Encryption Standard) to encrypt passwords prior to storing them in the database. However, CESG, the UK national cryptographic security authority, makes no comment on the Strength of Function (SoF) of the encryption algorithm as it is publicly known. The Security Target [a] claims SoF-High for the password space provided by the TOE's password management function. The SoF-High claim applies to 2 different password profiles: a password of minimum length 8 characters with no lockout and a password of minimum length 6 characters with a 1 minute lockout after 3 consecutive logon failures.

Security Claims

18. The TOE's security objectives, the threats which these objectives counter and Organisational Security Policies which support the objectives are fully specified in DBMS PP [c] and referenced from the Security Target [a]. The functional requirements and security functions to elaborate the objectives are specified in the Security Target. All of the functional requirements were taken from CC Part 2 [g]; use of this standard facilitates comparison with other evaluated products. An overview of CC is given in CC Part 1 [f].

Threats countered by the TOE

19. The threats that the TOE is to counter are as follows:

- Unauthorised access to the database
- Unauthorised access to information
- Unauthorised access to labelled information
- Excessive consumption of resources
- Undetected attack
- Abuse of privileges

Threats countered by the TOE's environment

20. The threats that the TOE's environment must counter are as follows:

- Insecure configuration and operation
- Abrupt interruptions
- Physical attack

Organisational Security Policies

21. The Organisational Security Policies that the TOE is to satisfy are as follows:

a. Access to database objects is determined by the owner of the object, the identity of the database subject attempting access, the object access privileges of the database subject, the database administrative privileges of the database subject and the resources allocated to the subject.

b. Labels can be associated with subjects and with storage objects, which are rows within tables. A label is composed of a hierarchic level, a set of hierarchic groups and a set of non-hierarchic categories. A storage object label reflects the sensitivity of the information stored in the object. A subject label reflects the authorization of the subject to access the organization's labelled information subject to access rules. The flow of information from one entity to another shall only be permitted if it does not result in a subject observing labelled information that the subject is not authorized to see.

c. Database users are accountable for operations on objects configured by the owner of the object, and actions configured by database administrators.

Assumptions on the TOE

22. The TOE must also satisfy the following assumptions:

a. The TOE is installed, configured and managed in accordance with its evaluated configuration as specified in the Evaluated Configuration document [p]. (A.TOE.CONFIG)

b. Trusted users are required to use Oracle Server Manager for all privileged connections to the TOE. (A.TOE.DBA)

Environmental Assumptions and Dependencies

23. The TOE's environment must also satisfy the following assumptions:

a. The processing resources of the TOE and the underlying operating system are located within controlled access facilities which prevent unauthorised physical access by outsiders, system users and database users.

b. The underlying operating system is installed, configured and managed in accordance with its secure configuration.

c. The underlying operating system is configured such that only the approved group of individuals may obtain access to the system.

d. There will be one or more competent individuals assigned to manage the TOE and the underlying operating system and the security of the information that they contain who can be trusted not to abuse their privileges.

e. Any other IT components with which the TOE communicates are assumed to be under the same management control and operate under the same security policy.

f. When required by the TOE in a distributed database environment the underlying network services are assumed to be based on secure communications protocols which ensure the authenticity of users.

g. To ensure accountability in middle-tier environments, any middle tier(s) will pass the original client ID through to the TOE.

h. Label authorizations and policy privileges are assigned to users commensurate with the trust placed in them by the organization that owns or is responsible for the information processed or stored in the TOE.

24. The TOE has no hardware or firmware dependencies. The TOE has the following software dependencies:

a. Operating system support for the TOE's access control, auditing, resource management and backup and recovery mechanisms.

b. Reliance upon the operating system to protect the TOE from attack.

TOE Security Objectives

25. The TOE security objectives in the Security Target [a] are as follows:

a. The TOE must provide end users and administrators with the capability of controlling and limiting access. In particular:

i. The TOE must prevent unauthorised or undesired disclosure, entry, modification or destruction of data, database objects, database views and database control and audit data.

ii. The TOE must allow database users who own or are responsible for data to control access to that data by other authorised database users.

iii. The TOE shall prevent unauthorised access to residual data remaining in objects and resources following the use of those objects and resources.

b. The TOE must provide the means of controlling the consumption of database resources by authorised users of the TOE.

c. The TOE must provide the means of identifying and authenticating users of the TOE.

d. The TOE must provide the means of recording security relevant events in sufficient detail to help an administrator of the TOE to detect attempted security violations, or potential misconfiguration of the TOE security features that would leave the database open to compromise and to hold individual database users accountable for any actions they perform that are relevant to the security of the database in accordance with the accounting Organisational Security Policy.

e. The TOE, where necessary in conjunction with the underlying system, must provide functions to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized administrators can access such functionality

f. The TOE must provide the ability for labels to be associated with subjects and database objects. The TOE must use these labels to implement an information flow control policy that prevents the disclosure of labelled information to unauthorized entities.

Environmental Security Objectives

26. The environmental objectives in the Security Target [a], which are met by procedural or administrative measures in the TOE's environment, are as follows:

a. The TOE, where necessary in conjunction with the underlying system, must provide functions to enable an authorized administrator to effectively manage the TOE and its security functions, ensuring that only authorized administrators can access such functionality.

b. The underlying system must provide access control mechanisms by which all of the O-RDBMS related files and directories (including executables, run-time libraries, database files, export files, redo log files, control files, trace files, and dump files) may be protected from unauthorized access.

c. The underlying operating system must provide the means to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with. The TSF components are the files used by the O-RDBMS to store the database and the TOE processes managing the database.

d. Those responsible for the TOE must ensure that the TOE is delivered, installed, managed and operated in accordance with the operational documentation of the TOE, and that the underlying system is installed and operated in accordance with its operational documentation. If the system components are certified, they should be installed and operated in accordance with the appropriate certification documentation.

e. Those responsible for the TOE must ensure that those parts of the TOE that are critical to the security policy are protected from physical attack.

f. Administrators of the database must ensure that audit facilities are used and managed effectively. These procedures shall apply to the database audit trail and/or the audit trail for the underlying operating system and/or secure network services. In particular, appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs before audit trail exhaustion to ensure sufficient free space. Audit logs must be inspected on a regular basis and appropriate action should be taken on the detection of breaches of security or events that are likely to lead to a breach in the future. The system clocks must be protected from unauthorized modification (so that the integrity of the audit timestamps is not compromised).

g. Those responsible for the TOE must ensure that procedures and/or mechanisms are in place to ensure that, after system failure or other discontinuity, recovery without protection (i.e. security) compromise is obtained.

h. Administrators of the database must ensure that each user of the TOE is configured with appropriate quotas that are sufficiently permissive to allow the user to perform the operations for which the user has access and sufficiently restrictive that the user cannot abuse the access and thereby monopolise resources.

i. Those responsible for the TOE must ensure that only highly trusted users have the privilege which allows them to set or alter the audit trail configuration for the database, alter or delete any audit record in the database audit trail, create any user account or modify any user security attributes, or authorise use of administrative privileges.

j. Those responsible for the TOE must ensure that the authentication data for each user account for the TOE as well as the underlying system is held securely and not disclosed to persons not authorised to use that account. In particular, the media on which the authentication data for the underlying operating system and/or secure network services is stored shall not be physically removable from the underlying platform by unauthorised users, users shall not disclose their passwords to other individuals, and passwords generated by the system administrator shall be distributed in a secure manner.

k. Those responsible for the TOE must ensure that the confidentiality, integrity and availability of data held on storage media are adequately protected. In particular, the on-line and off-line storage media on which database and security related data (such as operating system backups, database backups and transaction logs, and audit trails) must not be physically removable from the underlying platform by unauthorised users. The on-line and off-line storage media must be properly stored and maintained and routinely checked to ensure the integrity and availability of the security related data. The media on which database-related files (including database files, export files, redo log files, control files, trace files and dump files) have been stored shall be purged prior to being re-used for any non-database purpose.

l. An additional OLS security objective is that those responsible for the TOE must ensure that users are assigned label authorizations and policy privileges commensurate with the degree of trust placed in them by the organization that owns, or is responsible for, the information processed by or stored in the TOE.

Security Functional Requirements

27. The TOE provides security functions to satisfy the following Security Functional Requirements relative to the DBMS PP [c]:

- Audit Data Generation (FAU_GEN.1)
- User Identity Association (FAU_GEN.2)
- Audit Review (FAU_SAR.1)
- Selectable Audit Review (FAU_SAR.3)
- Selective Audit (FAU_SEL.1)
- Protected Audit Trail Storage (FAU_STG.1)
- Prevention of Audit Data Loss (FAU_STG.4)
- Subset Access Control (FDP_ACC.1)
- Security Attribute Based Access Control (FDP_ACF.1)
- Full Residual Information Protection (FDP_RIP.2)
- Basic Authentication Failure Handling (FIA_AFL.1)
- Verification of Secrets (FIA_SOS.1)
- Timing of Authentication (FIA_UAU.1)
- Timing of Identification (FIA_UID.1)
- User Attribute Definition (FIA_ATD.1)
- User-Subject Binding (FIA_USB.1)
- Management of Security Attributes (FMT_MSA.1)
- Static Attribute Initialisation (FMT_MSA.3)
- Management of TSF Data (FMT_MTD.1)
- Revocation (FMT_REV.1)
- Security Roles (FMT_SMR.1)
- Non-bypassability of the TOE Security Policy (TSP) (FPT_RVM.1)
- TSF Domain Separation (FPT_SEP.1)
- Maximum Quotas (FRU_RSA.1)
- Basic Limitation on Multiple Concurrent Sessions (FTA_MCS.1)
- TOE Session Establishment (FTA_TSE.1)

28. The TOE provides security functions to satisfy the following Security Functional Requirements additional to the DBMS PP [c]:

- Information Flow Control subset (FDP_IFC.1).
- Hierarchical Security Attributes (FDP_IFF.2).
- Management of Security Functions Behaviour (FMT_MOF.1).

29. To cover requirements for the management of security attributes associated with Label-Based Access Control, SFR iterations FMT_MSA.1.1.2, FMT_MSA.3.1.2 and FMT_MSA.3.2.2 have been added. These iterations are not included in the DBMS PP [c].

30. The Security Target [a] also contains a security function for Discretionary Access Control (DAC) for database objects (F.DAC.OBA), which has been modified relative to the Security Target for Release 8.0.5.0.0 to include a new clause covering the application of security policies for fine-grained access control

Security Function Policy

31. The TOE has an explicit access control Security Function Policy defined in the FDP_ACC.1, FDP_ACF.1, FDP_IFC.1 and FDP_IFF.2 SFRs. See the Security Target [a] for further details.

Evaluation Conduct

32. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UKSP 01 [d] and UKSP 02 [e]. The Scheme has established a Certification Body which is managed by the Communications-Electronics Security Group (CESG) on behalf of Her Majesty's Government.

33. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a]. To ensure that the Security Target gave an appropriate baseline for a Common Criteria evaluation, it was first itself evaluated, as outlined by CC Part 3 [h].

34. The evaluation was performed against the EAL4 assurance package defined in CC Part 3 [h]. The CEM [i] was used as the methodology for the evaluation, although some results were reused from the CC evaluation of Oracle 8.1.7.0.0 [j] where this was valid for the TOE and complied with the CEM requirements.

35. The Evaluators conducted sampling during the evaluation, as required for the relevant work-units for EAL4. Guidance provided in CEM [i], Annex B, Section B.2, was followed. The Evaluators also confirmed the sample size and approach with the Certifier in all cases. For the testing, the Evaluators repeated 70% of the Developer's tests relevant to security. The Evaluators also checked that the tests covered all of the security functions of the TOE. Where the sampling related to gaining evidence that a process such as configuration control was being followed, the Evaluators sampled sufficient information to gain adequate confidence that this was the case.

36. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation was completed in May 2002 when the CLEF submitted the last of the Evaluation Technical Reports (ETRs) [k - m] to the Certification Body which, in turn, produced this Certification Report.

General Points

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

38. 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 completion of the evaluation. 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.

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

(This page is intentionally blank)

II. EVALUATION FINDINGS

40. The Evaluators examined the following assurance classes and components taken from CC Part 3 [h]:

Assurance class	Assurance components
Configuration management	Partial configuration management automation (ACM_AUT.1) Generation support and acceptance procedures (ACM_CAP.4) Problem tracking configuration management coverage (ACM_SCP.2)
Delivery and operation	Detection of modification (ADO_DEL.2) Installation, generation and startup procedures (ADO_IGS.1)
Development	Fully defined external interfaces (ADV_FSP.2) Security enforcing high-level design (ADV_HLD.2) Subset of the implementation of the TOE Security Functions (ADV_IMP.1) Descriptive low-level design (ADV_LLD.1) Informal correspondence demonstration (ADV_RCR.1) Informal TOE Security Policy (ADV_SPM.1)
Guidance documents	Administrator guidance (AGD_ADM.1) User guidance (AGD_USR.1)
Life cycle support	Identification of security measures (ALC_DVS.1) Developer defined life-cycle model (ALC_LCD.1) Well defined development tools (ALC_TAT.1)
Security Target	TOE description (ASE_DES) Security Environment (ASE_ENV) Security Target introduction (ASE_INT) Security objectives (ASE_OBJ) Protection Profile claims (ASE_PPC) IT security requirements (ASE_REQ) TOE summary specification (ASE_TSS)
Tests	Analysis of coverage (ATE_COV.2) Testing: high-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1) Independent testing – sample (ATE_IND.2)
Vulnerability Assessment	Misuse: validation of analysis (AVA_MSU.2) Strength of TOE security function evaluation (AVA_SOF.1) Independent vulnerability analysis (AVA_VLA.2)

41. All assurance classes were found to be satisfactory and were awarded an overall “pass” verdict.

42. There are a number of aspects of the evaluation that are relevant to consumers. These are summarised in the sections that follow.

Delivery and Installation

43. When a consumer orders the TOE the order number and invoice detailing the items ordered are provided to the consumer by Oracle. 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 have the names and addresses of the sender and recipient and are marked with the Oracle logo. The consumer receives the TOE as a package clearly labelled as 'Oracle8*i* Release 8.1.7.0.0 for Solaris 8'. The consumer should check that the order number of the delivery is the same as the order number on the invoice and that part numbers of all items supplied are the same as indicated on the invoice. These measures ensure that a third party could not masquerade as the Developer and supply potentially malicious software. Nevertheless, in general the consumer must rely on Oracle's own manufacturing procedures and the trust placed in the courier to counter the threat of interference to the TOE along the delivery path. The Evaluators have confirmed however that Oracle would use high security couriers or other measures if required by the consumer.

44. Consumers should download Patch Set Version 8.1.7.3.0 for Oracle8*i* Release 8.1.7.0.0 for Solaris 8 and Patch Set Version 8.1.7.3.0 for OLS 8.1.7.0.0 from http://metalink.oracle.com for existing customers or www.oracle.com for new customers. Customers can guard against spoofing by telephoning Oracle support and asking them to check their patch download audit log. An entry in the log would confirm that Oracle initiated the download.

45. Consumers should also be aware that if they apply additional patches to the TOE, the TOE will no longer be in its evaluated configuration. Oracle patches can only be delivered by download from the internet from http://metalink.oracle.com for existing customers or www.oracle.com for new customers.

46. When the consumer has received Release 8.1.7.0.0 of the TOE and has obtained the patch sets described in paragraph 45 above, they must perform a number of configuration steps in order to use the TOE in a secure state. These steps are described in the Evaluated Configuration document [p]. The Evaluators confirmed that the configuration of the TOE generated by the setup and installation procedure is secure when these steps are followed. The Evaluated Configuration document [p] is made available by Oracle to customers on request.

User Guidance

47. The referenced documentation relevant to the security of the TOE for the end user comprises [n-aa]. The procedures in the Evaluated Configuration document [p] are minimal for end users and are generally common sense measures (e.g. non-disclosure of passwords).

48. The referenced documentation relevant to the security of the TOE for administrators comprises [n-aa]. Those documents indicate how the TOE's environment can be secured. It is also anticipated that Oracle may make the Evaluated Configuration document [p] available to download from one of its web sites (e.g. via http://otn.oracle.com/docs/deploy/security/content.html).

Developer's Tests

49. The Developer's testing was designed to test the security mechanisms of the TOE which implement the security functionality identified in the Security Target [a] and their representations as identified in the high

and low level design and in the source code modules of the TOE. All testing was performed via the TOE's external interface, the OCI.

50. The Developer's testing consisted of an automated test suite and manual tests. The Evaluators confirmed that the actual test results were consistent with the expected test results and that any deviations were satisfactorily accounted for.

51. The configuration of the Developers' test environment is described in Annex A.

Evaluators' Tests

52. The Evaluators repeated 70% of the Developer's tests relevant to security and performed a series of independently devised functional tests to cover all of the TOE's Security Functions. The Evaluators' independent functional tests took the form of automated Structured Query Language (SQL) scripts.

53. The Evaluators also performed penetration testing of the TOE. The Evaluators conducted penetration tests based on samples of tests taken from previous Oracle evaluations and original tests for potential vulnerabilities introduced by new security features of the TOE. As a result of checking Internet sources, no publicly known vulnerabilities were found to be applicable to the TOE or to the TOE in its operating system environment.

54. The configuration of the Evaluators' test environment is described in Annex A.

(This page is intentionally blank)

III. EVALUATION OUTCOME

Certification Result

55. After due consideration of the ETR [k - m] 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 8.1.7.3.0, used with Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0 running on Sun Solaris Version 8 in the environment specified in Annex A, meets the specified CC Part 3 [h] conformant requirements for Evaluation Assurance Level EAL4 for the CC Part 2 [g] conformant functionality specified in the Security Target [a].

56. Oracle Label Security Release 8.1.7.3.0, used with Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0, conforms to DBMS PP [c] with the Database Authentication functional package when running on Sun Solaris Version 8.

57. The Strength of Function claim of SoF-High in the Security Target [a] is satisfied.

58. Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0, when used with the operating system platform specified in Annex A conforming to the CC CAPP, can be used to provide security for systems which require TCSEC C2 or equivalent security functionality for databases.

Recommendations

59. Prospective consumers of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. In particular, certification of the TOE does not apply to its use in a potentially hostile network environment.

60. The product provides some features that were not within the scope of the evaluation as identified in the “TOE Scope” section above. The secure use of these features has thus not been considered in the evaluation. These features should not be used if the TOE is to comply with the evaluated configuration.

61. Only the evaluated product configuration, specified in Annex A, should be installed. The evaluated configuration excludes any patches to OLS and Oracle8*i*. The product should be used in accordance with its guidance documentation [n - aa] and in accordance with the environmental considerations outlined in the Security Target [a] and the Evaluated Configuration document [p].

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

(This page is intentionally blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

- Oracle Label Security Release 8.1.7.3.0, used with Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0

2. The following installation options shall be selected during the installation of the database server in a custom installation:

- Oracle Enterprise Edition Release 8.1.7.0.0
- Oracle8*i* Server 8.1.7.0.0
- Development Tools 8.1.7.0.0
- OCI 8.1.7.0.0
- Oracle XML SQL Utility 2.0.0.0.0
- Oracle Installation Products 8.1.7.0.0
- Oracle Universal Installer 1.7.1.8.0
- Oracle Configuration Assistants 8.1.7.0.0
- Oracle Database Configuration Assistant 8.1.7.0.0
- Oracle Utilities 8.1.7.0.0
- SQL*Plus 8.1.7.0.0
- Oracle Database Utilities 8.1.7.0.0
- Net8 Products 8.1.7.0.0
- Net8 Client 8.1.7.0.0
- Net8 Server 8.1.7.0.0
- Oracle Names 8.1.7.0.0
- Oracle Connection Manager 8.1.7.0.0
- External Naming Network Information Services Plus
- Oracle Java products 8.1.7.0.0
- Oracle Java Database Connectivity (JDBC) Drivers 8.1.7.0.0
- Oracle JBDC/OCI Driver for the Java Development Kit (JDK) 1.1.8.1.7.0.0
- Oracle JBDC/OCI Driver for the JDK 1.2.8.1.7.0.0
- Oracle JDBC Thin Driver for JDK 1.1.8.1.7.0.0
- Oracle JDBC Thin Driver for JDK 1.2.8.1.7.0.0
- Oracle Java Tools 8.1.7.0.0
- Oracle8*i* Unix Documentation 8.1.7.0.0

3. The Oracle8*i* Patch Set Version 8.1.7.3.0 should then be installed

4. OLS 8.1.7.0.0 should then be installed with the OLS 8.1.7.3.0 patch.

5. The following installation options of the database client were in a custom installation in order to test the TOE:

- Oracle8*i* Client 8.1.7.0.0
- Net8 Protocols 8.1.7.0.0
- Net8 Client 8.1.7.0.0
- Oracle Protocol Support 8.1.7.0.0
- Oracle Utilities 8.1.7.0.0
- SQL*Plus 8.1.7.0.0

6. The supporting guidance documents evaluated that were relevant to security were:

- Guidance Analysis For Oracle 8*i* Database Server [n]
- OLS Guidance Analysis for Oracle 8*i* [o]
- OLS Evaluated Configuration for Oracle 8*i* [p]
- OLS Administrator's Guide [q]
- Oracle8*i* Administrator's Guide [r]
- Oracle8*i* Reference [s]
- Oracle8*i* Application Developer's Guide, Object Relational Features [t]
- Oracle8*i* Concepts [u]
- Oracle8*i* Administrator's Reference for SUN SPARC Solaris [v]
- OCI Programmer's Guide [w]
- Oracle 8*i* Error Messages [x]
- OLS Installation Notes [y]
- Oracle8*i* Installation Guide for Sun SPARC Solaris [z]
- Solaris 8.0 Security Release Notes [aa]

TOE Configuration

7. The TOE had a unique configuration when installed in its evaluated configuration. The TOE must be set up as documented in the Evaluated Configuration document [p]. The following are the types of steps that must be performed:

a. Installation of the operating system in its evaluated configuration (Sun Solaris Version 8).

b. Protection of the database files.

c. Miscellaneous steps to set up user accounts, access control and auditing. The Evaluated Configuration document requires that the TOE is set up for auditing.

d. General administration steps to ensure that the evaluated configuration is maintained.

Environmental Configuration

8. Testing was performed using Oracle8*i* Release 8.1.7.0.0 on client machines and OLS Release 8.1.7.3.0 with Oracle8*i* Database Server Enterprise Release 8.1.7.3.0 on server machines. The servers

were configured to support two database instances; the dual database configuration was used to test access to remote databases.

9. Developer testing was performed using Sun ULTRA60 machines, connected together using TCP/IP networking. The evaluators used the developer test configuration for repeating a sample of developer tests.

10. For additional functional testing and penetration testing, the evaluators used a Sun SPARCstation 20 client workstation and a Sun ULTRA1 server, connected together using TCP/IP networking.

11. The specification of the machines was as follows:

Machine Make	Sun	Sun	Sun
Machine Model	ULTRA60	ULTRA1	SPARCstation 20
Drive Specifications	36GB hard drive with Universal File System (UFS) DVD/CD-ROM drive	3GB hard drive with Universal File System (UFS) CD-ROM drive	3GB hard drive with Universal File System (UFS) CD-ROM drive
Operating Systems	Sun Solaris 8.0	Sun Solaris 8.0	Sun Solaris 8.0
Processor	SPARC	SPARC	SPARC
Physical Memory	512MB RAM	128MB RAM	160MB RAM
Network Cards	10/100BaseT network connection	10BaseT network connection	10BaseT network connection

(This page is intentionally blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. Oracle8*i* Database Server Enterprise Edition Release 8.1.7.3.0 is an Object-Relational Database Management System (O-RDBMS) that provides comprehensive, integrated and advanced security functionality for multi-user information management environments. An Oracle8*i* server consists of an Oracle8*i* database and an Oracle8*i* instance.

2. An Oracle8*i* database has separate physical and logical structures. 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.

3. The logical structure of an Oracle8*i* database is determined by its tablespaces, which are logical areas of storage, and its schemas 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 of an Oracle8*i* database is used. The schema objects and the relationships among them form the relational design of an Oracle8*i* database. Examples of logical structures include tablespaces, schema objects, data blocks, extents and segments.

4. An Oracle8*i* instance is the combination of background processes that are created and memory buffers that are allocated when an Oracle8*i* instance is started up. The background processes are of 2 types: user processes, which execute code of an application program or an Oracle tool or application, and Oracle processes, which are server processes that perform work on behalf of the user processes in addition to performing the work required to keep the Oracle8*i* server running. The memory buffers that are allocated during startup are collectively called the *System Global Area* (SGA).

5. Security functionality in the Oracle8*i* 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

6. Oracle8*i* supports client/server and standalone architectures. In both architectures, Oracle8*i* acts as a data server, providing access to the information stored in a database. Access requests are made via the Oracle8*i* interface products that provide connectivity to the database and submit SQL statements to the Oracle8*i* server. The Oracle8*i* interface products may be used on the same computer as the data server or on separate client machines which communicate with the Oracle8*i* server via underlying network services.

7. Net8 is the Oracle8*i* interface product that facilitates the proper transmission of information between Oracle client and server processes using standard communication protocols.

Anatomy

8. 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 a database is its data dictionary, which is a set of internal Oracle tables that contains all of the information the Oracle8*i* server needs to manage its database. A set of read-only views is provided to display the contents of these internal tables in a meaningful manner and also allows Oracle users to query the data dictionary without the need to access it directly.

9. All of the information about database objects is stored in the data dictionary and is 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. An Oracle8*i* database contains the data dictionary and 2 different types of database objects:

- Schema objects that belong to a specific user schema and contain user-defined information
- Non-schema objects that organise, monitor and control the database

10. 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

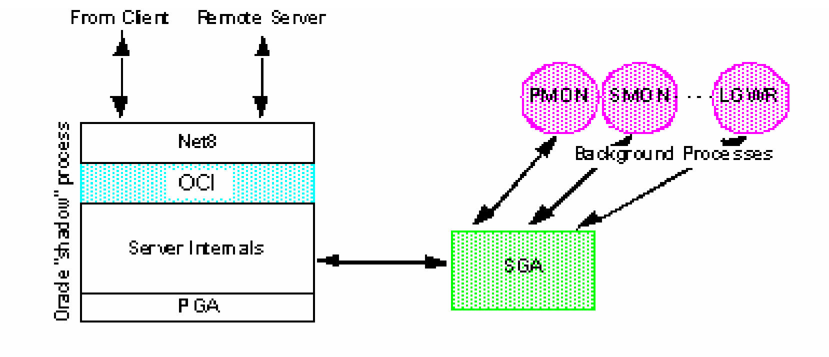
11. Within its database files, Oracle8*i* allocates storage for data in three hierarchical physical units: data blocks, extents and segments. When a user creates a schema object to store data (e.g. a table), a segment is created and the storage space for the segment is allocated to a specific tablespace.

12. An Oracle8*i* instance is made up of a number of distinct processes that form its core architecture. These processes are classified as background processes, which are comprised of user processes and server processes. A user background process is created and maintained to execute application software programs on behalf of a user (or client). Server background processes are created by the database during the creation of an instance of the database. These server processes handle requests from user processes and communicate with other server processes to consolidate functions on behalf of the database and user processes. 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.

13. Each 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 Oracle8*i* process architecture described above.



Key to Figure:

LGWR:	Log Writer, which writes to the redo logs.
OCI:	Oracle Call Interface.
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: Oracle8*i* Process Architecture

Configuration

15. The Oracle8*i* architecture supports 3 types of product configurations: standalone, client-server and distributed. A standalone configuration is one in which both the client application(s) and Oracle8*i* server run on a single operating system with at least one database. A client-server database configuration is one in which a client application runs on hardware physically separate from the Oracle8*i* server and its database(s) and must connect to the server and database(s) via a network. A distributed database configuration is one in which multiple client applications access multiple Oracle8*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 this environment any tier that communicates directly with the server is actually an Oracle client. Any lower tiers are outside the scope of this evaluation.

17. In all of its product configurations, however, Oracle8*i* enforces all its standard suite of security mechanisms.

Identification & Authentication

18. Oracle8*i* has 2 types of user: administrative users and normal users. Administrative users are those who are defined within an Oracle8*i* database as being authorised to perform administrative tasks such as

user maintenance, instance startup and shutdown and database backup and recovery. All other users defined within an Oracle8*i* database are normal users.

19. Oracle8*i* always identifies the user of its database 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:

- Directly by Oracle8*i* server using passwords managed by it.
- By relying on authentication mechanisms of the host operating system.
- By proxy authentication.
- Through an external authentication service or mechanism which depends on the use of the Oracle Advanced Security Option (an add-on product of the Oracle8*i* server).

20. In the evaluated configuration, external authentication services and host operating system based authentication are not used to authenticate authorised database users.

21. For Oracle authentication, a user must specify a user name and password in order to connect. The password is compared to the password for the user stored in the data dictionary and a database session is created if they match. The user's password is stored in the data dictionary in a one-way encrypted form.

22. 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.

23. Administrative users are authenticated to a database by virtue of having an entry in the Oracle8*i* password file or by having operating system-specific access rights. Operating system-specific access rights are normally established by being a member of a special operating system group. Such users connect to a database by the use of special keywords such as INTERNAL, AS SYSDBA or AS SYSOPER.

Access Controls

24. Oracle8*i* includes security features that control how a database is accessed and used. Associated with each database user is a schema identified by the user's name. By default, each database user creates and has access to all objects in the corresponding schema. Access to objects in other user schemas is governed by the Oracle8*i* Discretionary Access Control (DAC) mechanism.

25. DAC is a means of restricting access to information at the discretion of the owner of the information. The Oracle8*i* DAC mechanism can be used to selectively share database information with other users. The DAC mechanism can also be used to enforce need-to-know confidentiality and to control data disclosure, entry, modification and destruction.

26. Oracle8*i* DAC controls access to database objects based on the privileges enabled in an active database session. There are 2 types of privileges: *system privileges* and *object privileges*. System privileges allow users to perform a particular system-wide action or a particular action on a particular type of schema object. System privileges are typically available only to database administrators because these

privileges are very powerful. Object privileges allow database users to perform a particular action on a specific schema object.

27. Both object and system privileges may be directly granted to individual database 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 Oracle8*i* mechanisms that affect the set of privileges held by the session.

28. Fine-grained access control (also known as row-level access control) is available with the Virtual Private Database (VPD) technology that is a standard feature of Oracle8*i* Enterprise Edition. Fine-grained access control allows the administrator to associate policies with tables and views. These policies are implemented with Oracle's Procedural Language extension to Structured Query Language (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.

Oracle Label Security

29. Oracle Label Security (OLS) enables application developers to add label-based access control to their Oracle8*i* applications. If used, OLS mediates access to rows in database tables based on a label contained in each row, and the label and privileges associated with each user session. Oracle Label Security is built on the virtual private database technology of Oracle8*i* Enterprise Edition.

30. Oracle Label Security provides an out-of-the-box VPD policy which enables administrative users to create one or more custom security policies to be used for label access decisions without any 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, Oracle Label Security provides a straightforward and efficient way to implement fine-grained security policies using data label technology.

31. Figure B-2 (over page) illustrates the process by which data is accessed under Oracle Label Security. Within an application and Oracle8*i* session, a user issues a SQL request. Oracle8*i* checks the DAC privileges, making sure 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 Oracle Label Security and the SQL statement is modified on the fly to enforce the policy. Each data record has a label; Oracle Label Security is invoked for each row, to determine whether, based on the label, the user can or cannot access the row.

32. To create a customised Oracle Label Security policy, an administrative user defines a set of labels and a set of rules that govern data access, based on these labels. For example, assume that a user has SELECT privilege on an application table. Figure B-3 (over page) illustrates that, when the user executes a SELECT statement, Oracle Label Security evaluates each row selected and determines whether the user can access it based on the privileges and access labels assigned to the user by the security administrator.

Oracle Label Security can also be configured to perform security checks on UPDATE, DELETE, and INSERT statements.

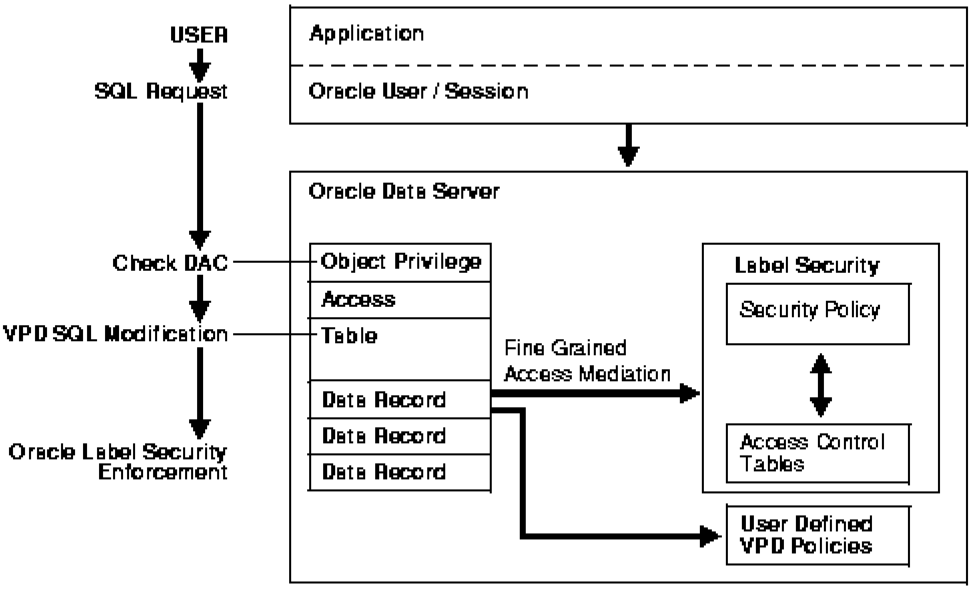
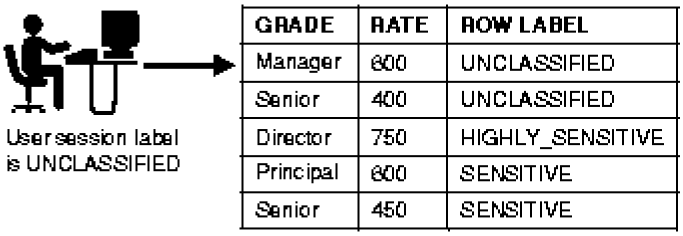


Figure B-2: Accessing Data Under OLS



User session label is UNCLASSIFIED

GRADE	RATE	ROW LABEL
Manager	600	UNCLASSIFIED
Senior	400	UNCLASSIFIED
Director	750	HIGHLY_SENSITIVE
Principal	600	SENSITIVE
Senior	450	SENSITIVE

Figure B-3: OLS Determines If The User Can Access Each Row Selected

33. Oracle Label Security 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 operation (such as SELECT) performed upon a row of data. When evaluating this access request by a user with the IN_CONFIDENCE label to a data row having the label IN_CONFIDENCE, Oracle Label Security determines that this access can, in fact, 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 use row labels to provide additional access control functionality where necessary.

34. 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 Oracle Label Security 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.

35. In Oracle Label Security, 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 typical government organisation might define levels UNCLASSIFIED, SENSITIVE, and HIGHLY_SENSITIVE. A commercial organisation might define a single level for 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 and ENGINEERING groups can be defined as children of the CEO group, creating an ownership relation. Labels can contain a single level component, a level combined with a set of either compartments or groups, or a level with both compartments and groups.

36. Users can be granted label authorisations for each OLS policy, which determine what kind of access (read or write) they have to the rows in the tables that have had that policy applied.

37. 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, authorising the procedure, rather than the user, to perform privileged operations.

38. In Oracle Label Security, administrators can apply different enforcement options for maximum flexibility in controlling the different Data Manipulation Language operations that users can perform. For each SELECT, INSERT, UPDATE and DELETE operation, administrators 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

39. Oracle8*i* ensures the accountability of its users' actions by the use of 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.

40. Audit categories offered by Oracle8*i* are: auditing by statement (auditing of specific types of SQL statements issued by all database users), by object (auditing specific actions on specific database objects for all users), by privilege (auditing the use of specific system privileges held by users), and by user (auditing actions of a specific user or a list of specified users).

41. When defining which actions are to be audited, Oracle8*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 by session (which results in a single record for an audited action for the duration of a session), or by access (which results in an audit record for every occurrence of an audited action).

42. Audit records can be written to the database audit trail, operating system audit trail or to a specified file in the operating system. Oracle8*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 be audited as well. If the audit records are directly sent to the host operating system, audit analysis may be performed using suitable audit analysis tools. Some operations such as connections as administrative users and instance startup and shutdown are always audited and are written directly to the host operating system.

43. In addition to the standard Oracle8*i* auditing features described above, application-specific auditing can be implemented using database triggers.

44. Oracle Label Security supplements the Oracle8*i* audit facility by tracking the use of its own OLS administrative operations and policy privileges. Under Oracle Label Security, 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.

Other Security Features

45. Oracle8*i* also provides other features that are related to its security mechanisms. These features provide significant security capabilities to support robust and reliable database applications. They include:

- Transaction integrity, concurrency and integrity constraints, to ensure the consistency and integrity of data held in a database

- Secure import and export of data, into the same or a different database (while maintaining data integrity and confidentiality)

- Backup and recovery of an Oracle8*i* database, using operating system-specific backup programs, or database import/export and recovery utilities

- Secure distributed processing using database links

- Oracle Policy Manager to facilitate the administration of Oracle Label Security policies.

46. All of those other security features, except for the database link functionality, were outside the scope of the evaluation.

47. 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 Oracle8*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

48. Add-on products of the Oracle8*i* server such as Oracle Advanced Security Option provide encryption of network traffic between clients and servers. Oracle Advanced Security Option also offers mechanisms to configure Oracle8*i* to use external third party authentication services. However, Oracle Advanced Security Option is not part of the evaluated configuration of the Oracle8*i* server.

49. Net8, the network transport and management product, forms part of the Oracle8*i* server and is included in the evaluated configuration. Net8 is Oracle's mechanism that interfaces with the communication protocols used by the underlying network services that facilitate distributed processing and distributed databases. Net8 supports communication over all major network protocols. It provides the transport infrastructure for client to server communication, hiding the underlying network protocols and associated programmatic interfaces from calling applications. Net8 can be administered either through manipulation of its configuration files or remotely through the Simple Network Management Protocol (SNMP), which is a standard feature of the Oracle8*i* server.

Operating System Administration

50. Oracle8*i* relies on the operating system for protection of its audit records (if written to the operating system instead of the database audit trail), import/export and backup and recovery files, and most importantly its database configuration and data files. Thus, security of the data managed by the Oracle8*i* server is dependent not only on the secure administration of Oracle8*i*, but also on the proper administration of the underlying operating system in any of the product configurations in which it is used.

(This page is intentionally blank)