UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

COMMON CRITERIA CERTIFICATION REPORT No. P158

Oracle8*i* Database Server Enterprise Edition

**Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8**

Issue 1.0

August 2001

DBMS PP   **Release 8.1.7.0.0**
                          running on Microsoft Windows NT Version 4.0 with Service Pack 3
                                              and on Sun Solaris Version 8

**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.

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

CERTIFICATION STATEMENT

Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0 is a relational database management system developed by Oracle Corporation.

Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0 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 Common Criteria Part 2 conformant functionality in the specified environment when running on the platforms described in Annex A. Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0 conforms to the Database Management System Protection Profile with the Operating System Authentication and Database Authentication functional packages when running on Microsoft Windows NT 4.0 with Service Pack 3 and with the Database Authentication functional package when running on Sun Solaris Version 8.

When used in conjunction with operating system platforms described in Annex A which conform to the Common Criteria Controlled Access Protection Profile (or the equivalent ITSEC F-C2 functionality), Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0 can be used to provide security for systems which require TCSEC C2 or equivalent security functionality for databases. Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0 was evaluated on Sun Solaris Version 8 (which has been certified against the Controlled Access Protection Profile) and on Microsoft Windows NT 4.0 with Service Pack 3 (which has been certified against the ITSEC F-C2 functionality class).

Originator	**CESG**
	Certifier
Approval	**CESG**
	Technical Manager
	Certification Body
Authorisation	**CESG**
	Senior Executive
	UK IT Security Evaluation
	and Certification Scheme
Date authorised	3 August 2001

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

(This page is intentionally left blank)

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

TABLE OF CONTENTS

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

(This page is intentionally left blank)

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

ABBREVIATIONS

ASO	Advanced Security Option
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
*i*AS	Internet Application Server
IDE	Integrated Digital Electronics
LGWR	LoG WriteR
MTS	MultiThreaded Server
NTFS	NT File System
OCI	Oracle Call Interface
OPI	Oracle Programming Interface
O-RDBMS	Object-Relational DataBase Management System
PGA	Program Global Area
PMON	Process MONitor
PP	Protection Profile
SCSI	Small Computer System Interface
SFR	Security Functional Requirement
SGA	System Global Area
SMON	System MONitor
SNMP	Simple Network Management Protocol
SoF	Strength of Function
SQL	Structured Query Language
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UFS	Universal File System
UKSP	United Kingdom Scheme Publication
VPD	Virtual Private Database

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

(This page is intentionally left blank)

Release 8.1.7.0.0 **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

REFERENCES

a.   Oracle8*i* Security Target, Release 8.1.7,
       Oracle Corporation,
       Issue 0.9, April 2001.

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.   Scheme Information Notice No. 053, F-C2 Functionality Class,
       UK IT Security Evaluation and Certification Scheme,
       SIN No. 053, Issue 3.0, 1 May 1997.

e.   Description of the Scheme,
       UK IT Security Evaluation and Certification Scheme,
       UKSP 01, Issue 3.0, 2 December 1996.

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

g.   Evaluated Configuration for Oracle8*i* Database Server,
       Oracle Corporation,
       Issue 0.2, June 2001.

h.   Common Criteria Part 1,
       Common Criteria Implementation Board,
       CCIB-99-031, Version 2.1, August 1999.

i.   Common Criteria Part 2,
       Common Criteria Implementation Board,
       CCIB-99-032, Version 2.1, August 1999.

j.   Common Criteria Part 3,
       Common Criteria Implementation Board,
       CCIB-99-033, Version 2.1, August 1999.

k.   UK Interpretation 03: The usefulness of informal security policy models,
       UK IT Security Evaluation and Certification Scheme,
       UK/2.1/003, January 2000.

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

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

m.   Oracle8 Security Target, Release 8.0.5,
        Oracle Corporation,
        Issue 1.0, April 2000.

n.   Certification Report No. P106, Oracle8 Database Server Enterprise Edition,
        UK IT Security Evaluation and Certification Scheme,
        Issue 1.0, October 2000.

o.   Task LFL/T121 Evaluation Technical Report 1,
        Logica CLEF,
        CLEF.24888.30.1, Issue 1.0, 15 February 2000.

p.   Task LFL/T121 Evaluation Technical Report 2,
        Logica CLEF,
        CLEF.24888.30.1, Issue 1.0, 25 April 2001.

q.   Task LFL/T121 Evaluation Technical Report 3,
        Logica CLEF,
        CLEF.24888.30.1, Issue 1.0, 29 June 2001.

r.   Oracle8*i* Administrator's Guide,
        Oracle Corporation,
        A76956-01, Release 2 (8.1.6), December 1999.

s.   Oracle8*i* SQL Reference, Volumes 1 and 2,
        Oracle Corporation,
        A86006-01 & A86013-01, Release 3, September 2000.

t.   Oracle8*i* Reference,
        Oracle Corporation,
        A76961-01, December 1999.

u.   Oracle8*i* Application Developer's Guide, Object Relational Features,
        Oracle Corporation,
        A76976-01, December 1999.

v.   Oracle8*i* Concepts, Volumes 1 and 2,
        Oracle Corporation,
        A76963-01 & A76964-01, Release 2 (8.1.6), December 1999.

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

w.   Oracle8*i* Administrator's Guide for Windows NT,
        Oracle Corporation,
        A73001-01, January 2000.

x.   Oracle8*i* Administrator's Reference for SUN Solaris,
        Oracle Corporation,
        A85349-01, August 2000.

y.   Programmer's Guide to the OCI, Volumes 1 and 2,
        Oracle Corporation,
        A85349-01 & A76978-01, December 1999.

z.   Oracle 8 Error Messages, Volumes 1, 2 and 3,
        Oracle Corporation,
        A76998-01, A76996-01 & A76997-01, December 1999.

aa.   Certification Report No. P121, Microsoft Windows NT Workstation and Server Version 4.0
        (Build 1381) Service Pack 3,
        UK IT Security Evaluation and Certification Scheme,
        Issue 1.0, March 1999.

bb.   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.

cc.   UK Interpretation 05: SoF-Medium Rating for Passwords,
        UK IT Security Evaluation and Certification Scheme,
        UK/2.1/005, Version 1.0, 5 September 2000.

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

(This page is intentionally left blank)

Release 8.1.7.0.0 **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

I.   EXECUTIVE SUMMARY

Introduction

1.   This Certification Report states the outcome of the IT security evaluation of Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0 (also known as Oracle8*i* Release 3) to the Sponsor, Oracle Corporation, and 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 the 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:

Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0.

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.   Oracle8*i* is an Object-Relational Database Management System (O-RDBMS) that provides comprehensive security functionality for multi-user information management environments. The product can operate in standalone, client/server and distributed configurations, although 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
- •   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 platforms specified in Annex A meeting the Common Criteria Controlled Access Protection Profile (CAPP) [b] (or the equivalent ITSEC F-C2 functionality [d]), Oracle8*i* can be used to provide security for systems that require TCSEC C2 or equivalent security functionality for databases.

8.   Details of the TOE's architecture can be found in Annex B to this report.

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

TOE Scope

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

- Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0
- Distributed Database Option 8.1.7.0.0
- Objects Option 8.1.7.0.0
- Net8 8.1.7.0.0

10.   The TOE scope does not include any Oracle clients, including middle-tier or presentation-tier Oracle client products, such as Oracle Internet Application Server (*i*AS) or Oracle Portal. However, the Oracle8*i* Client 8.1.7.0.0 was used for testing the TOE. The use of the TOE in a network which is connected to a potentially hostile network (such as the internet) is also beyond the scope of this evaluation.

11.   The scope of the certification includes the following Oracle8*i* interface products:

- Oracle Server Manager 8.1.7.0.0
- Oracle Call Interface (OCI) 8.1.7.0.0
- SQL*Plus 8.1.7.0.0
- Net8 8.1.7.0.0

12.   The scope of the certification applies to the TOE running on Microsoft Windows NT 4.0 with Service Pack 3 and to the TOE running on Sun Solaris Version 8. See Annex A for details of the platforms on which the TOE was tested.

13.   The evaluation of Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0 **excludes** the following options and features, which have not been considered by the Evaluators:

- Advanced Security (ASO)
- Multithreaded Server (MTS)
- All integrity features

14.   The TOE includes the following new security features that were not present in the Oracle 8.0.5.0.0 TOE. Further details are provided in Annex B to this report.

- O-RDBMS authentication for users
- Proxy authentication on behalf of other users
- Fine-grained access control (also referred to as Virtual Private Database (VPD))

Protection Profile Conformance

15.   The Security Target [a] claims conformance with the Database Management System Protection Profile (DBMS PP) [c] with the Operating System Authentication and Database Authentication functional packages when running on Microsoft Windows NT 4.0 with Service Pack

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

3 and with the Database Authentication functional package when running on Sun Solaris Version 8. The Security Target does not introduce any Security Functional Requirements that are not in the DBMS PP, but it does augment the assurance package from EAL3 to EAL4 and customises the environmental assumptions (see assumptions A.TOE.CONFIG, A.TOE.DBA and A.MIDTIER below).

Assurance Level

16.   The Security Target [a] specifies the assurance requirements for the resultant evaluation. The assurance comprised predefined evaluation assurance level EAL4. Common Criteria (CC) Part 3 [j] describes the scale of assurance given by predefined evaluation assurance levels EAL1 to EAL7. EAL0 represents no assurance.

Strength of Function

17.   The certified configuration of the TOE included O-RDBMS authentication and operating system authentication packages when running on Microsoft Windows NT 4.0 with Service Pack 3 and O-RDBMS authentication when running on Sun Solaris Version 8.

18.   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.

19.   SoF-Medium is applicable to operating system authentication, for conformance to the Security Target and to the DBMS PP [c] requirement that the overall SoF of the operating system and the TOE are at least SoF-Medium.

Security Claims

20.   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 [i]; use of this standard facilitates comparison with other evaluated products. An overview of CC is given in CC Part 1 [h].

Threats countered by the TOE

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

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

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

Threats countered by the TOE's environment

22. The threats that the TOE's environment is to counter are as follows:

- Insecure configuration and operation
- Abrupt interruptions
- Physical attack

Organisational Security Policies

23. 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. 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

24. 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 Evaluation Configuration Document [g]. (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

25. 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.

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

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. (A.MIDTIER)

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

a.   Operating system support for the TOE's identification and authentication, 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

27.   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

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

resources by authorised users of the TOE.

c.   The TOE, with support from the underlying operating system, 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 authorised administrator to effectively manage the TOE and its security functions, ensuring that only authorised administrators can access such functionality.

Environmental Security Objectives

28.   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 authorised administrator to effectively manage the TOE and its security functions, ensuring that only authorised 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 unauthorised access.

c.   The underlying operating system must provide a means of identifying and authenticating users when required by the TOE to reliably identify authenticated users.

d.   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.

e.   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.

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

f.   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.

g.   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, eg 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 unauthorised modification (so that the integrity of the audit timestamps is not compromised).

h.   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 (ie security) compromise is obtained.

i.   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.

j.   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.

k.   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.

l.   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

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

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.

Security Functional Requirements

29. The TOE provides security functions to satisfy the following Security Functional Requirements:

- 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)
- 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 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)

30. The Security Target [a] contains 4 new security functions that were not present in the Security Target [m] for Oracle Release 8.0.5.0.0. These security functions are as follows:

- DBMS Identification and Authentication (F.IA.DBA)
- User password control (F.IA.PWD)
- Change of user passwords (F.IA.USE)
- Proxy connections for other users (F.PRI.PRX)

31. F.IA.DBA are mapped to the new FIA_UAU.1 Security Functional Requirement (SFR), F.IA.PWD and F.IA.USE are mapped to the new FIA_SOS.1 SFR, and F.PRI.PRX is mapped to the FIA_USB.1 SFR.

Release 8.1.7.0.0   DBMS PP
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

32.   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 [m] 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

33.   The TOE has an explicit access control Security Function Policy defined in the FDP_ACC.1 and FDP_ACF.1 SFRs. See the Security Target [a] for further details. The UK interpretation [k] of the Common Evaluation Methodology (CEM) [l] requirements for the informal security policy model were used for this evaluation, and no separate informal model for access control was provided.

Evaluation Conduct

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

35.   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 [j].

36.   The evaluation was performed against the EAL4 assurance package defined in CC Part 3 [j]. The CEM [l] was used as the methodology for the evaluation, although some results were reused from the Common Criteria evaluation of Oracle 8.0.5.0.0 where this was valid for the TOE and complied with the CEM requirements.

37.   The Evaluators conducted sampling during the evaluation, as required for the relevant work-units for EAL4. Guidance provided in CEM [l], 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 80% of the Developer's tests relevant to security and 100% of tests relating to features new in the TOE. 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.

38.   The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation was completed in June 2001 when the CLEF submitted the last of the Evaluation Technical Reports (ETRs) [o-q] to the Certification Body which, in turn, produced this Certification Report.

General Points

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

39.   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.

40.   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. Consumers are reminded of the security dangers inherent in downloading TOE components, hot-fixes and patches where these are available, and that the UK Certification Body provides no assurance whatsoever for patches obtained in this manner. More up to date information on known security vulnerabilities within individual certified products and systems can be found on the IT Security Evaluation and Certification Scheme web site www.itsec.gov.uk.

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

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

II.   EVALUATION FINDINGS

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

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)

43.   All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

44.   During this evaluation the Evaluators performed a site visit to examine the TOE development and production environment. Their site visit enabled them to confirm the application of procedures for the configuration management, delivery and operation and lifecycle support assurance classes.

45.   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

46.   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 (eg 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 Windows NT or Oracle8*i* 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.

47.   Consumers should be aware that Oracle makes components of the TOE available for download from metalink.oracle.com for existing customers or www.oracle.com for new customers, 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 web site or the corruption or deliberate modification of TOE components in transit is considered to be relevant to the operational environment of the TOE, consumers should obtain delivery of the TOE via physical media (eg CD-ROMs for software and printed books for documentation).

48.   Consumers should also be aware that if they apply 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 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.

49.   The TOE has a number of configuration steps that the consumer must perform in order to use the TOE. These steps are described in the Evaluated Configuration document [g]. The Evaluators confirmed that the configuration of the TOE generated by the setup and installation procedure was unique when the steps in the Evaluated Configuration document were followed.

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

User Guidance

50.   The documentation relevant to the security of the TOE for the end user comprise the referenced documents [g, s-z]. The procedures in the Evaluated Configuration document [g] are minimal for end users and are generally common sense measures (eg non-disclosure of passwords).

51.   The documentation relevant to the security of the TOE for administrators comprise the referenced documents [g, r-x]. The documents provided also indicate how the TOE's environment can be secured.

52.   The Evaluated Configuration document [g] is made available by Oracle to customers on request. It is also anticipated that the Evaluated Configuration document will also be made available for downloading from the Oracle web site, otn.oracle.com/deploy/security/seceval/listing.htm.

Developer's Tests

53.   The TOE was installed and tested on hardware platforms as specified in Annex A. The Oracle8*i* Release 8.1.7.0.0 client was installed on a Sun SPARCstation 20 running Sun Solaris Version 8 and on a Compaq Deskpro 4000 running Microsoft Windows NT 4.0 Workstation with Service Pack 3. Oracle8*i* Database Server Enterprise Release 8.1.7.0.0 was installed on a SUN ULTRA1 running Sun Solaris Version 8 and on a Compaq Proliant 4500 running Microsoft Windows NT 4.0 Server with Service Pack 3. The Sun Solaris Version 8 based client and server were used together as were the Microsoft Windows NT 4.0 client and server.

54.   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.

55.   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.

Evaluators' Tests

56.   The Evaluators repeated 80% of the Developer's tests relevant to security and 100% of tests relating to new features of the TOE 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.

57.   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.

DBMS PP

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

58.   The publicly known vulnerabilities that were found by the Evaluators related to Oracle *i*AS, Oracle Apache/Jserv, the Oracle Java Virtual machine and to Net8, the Oracle networking protocol. The first three of these are outside the evaluated configuration as defined in the Evaluated Configuration document [g]. The vulnerabilities in Net8 were countered by the assumption in the Security Target [a] A.TOE.CONFIG, that the TOE is installed, configured and managed in accordance with the Evaluated Configuration document. Requirement DB.CA-2 in the Evaluated Configuration document requires that no database applications shall be permitted to run on any host with access to the network unless they have been shown not to compromise the TOE's security objectives as stated in the Security Target [a] and in the DBMS PP [c]. Objective O.ACCESS.OBJECTS requires that the TOE must prevent unauthorised modification or destruction of database objects or data and environmental Objective O.SEP in DBMS PP requires that TSF components cannot be tampered with. In practice these requirements mean that the network on which the O-RDBMS and all its client applications run are under the control of a trusted administrator and that it is not connected to any untrusted or potentially hostile networks (such as the internet). In any case, the TOE's evaluated configuration cannot consider the threats on such untrusted networks since the underlying operating systems' evaluated configurations do not consider such threats.

59.   The configuration of the Evaluators' test environment is described in Annex A. The Evaluators' test environment was the same as the Developer's test environment.

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

III.   EVALUATION OUTCOME

Certification Result

60.   After due consideration of the ETR [o-q], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0, running on Microsoft Windows NT Version 4.0 with Service Pack 3 and on Sun Solaris Version 8 in the environment specified in Annex A, meets the specified CC Part 3 [j] conformant requirements for Evaluation Assurance Level EAL4 for the CC Part 2 [i] conformant functionality specified in the Security Target [a]. The TOE conforms to the DBMS PP [c] with the Operating System Authentication and Database Authentication functional packages when running on Microsoft Windows NT 4.0 with Service Pack 3 and with the Database Authentication functional package when running on Sun Solaris Version 8.

61.   When used in conjunction with the operating system platforms specified in Annex A conforming to the Common Criteria CAPP (or the equivalent ITSEC F-C2 functionality), Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0 can be used to provide security for systems which require TCSEC C2 or equivalent security functionality for databases.

62.   Oracle8*i* was evaluated on Microsoft Windows NT Version 4.0 with Service Pack 3 and on Sun Solaris Version 8. The Evaluators performed a vulnerability search for these operating system environments and found no vulnerabilities which could enable the TOE to be directly attacked, tampered with or bypassed.

63.   The certified configuration of the TOE included the operating system authentication and O-RDBMS authentication options when running on Microsoft Windows NT 4.0 with Service Pack 3 and O-RDBMS authentication when running on Sun Solaris Version 8. The Evaluators found that the password spaces provided by the O-RDBMS password profiles met the SoF-High claim in the Security Target [a]. As Microsoft Windows NT Version 4.0 with Service Pack 3 in its certified configuration has an ITSEC Strength of Mechanism of Medium (see Certification Report No. P121 [aa]), which the Certification Body has validated as equivalent to SoF-Medium using interpretation [cc], the requirement that the TOE's environment should meet the SoF-Medium requirement when operating system authentication is used is also met.

Recommendations

64.   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.

65.   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.

DBMS PP   **Release 8.1.7.0.0**
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

66.   Only the evaluated product configuration, specified in Annex A, should be installed. The evaluated configuration excludes any patches to Oracle 8.1.7.0.0. The product should be used in accordance with its guidance documentation [r-z] and in accordance with the environmental considerations outlined in the Security Target [a] and the Evaluated Configuration document [g].

67.   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.

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1.   The TOE is uniquely identified as:

- Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0

2.   The following installation options shall be selected during TOE 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 1.7.1.9.0 (Windows NT)
- Oracle Universal Installer 1.7.1.8.0 (Solaris)
- 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 (Solaris only)
- 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

3.   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

DBMS PP   **Release 8.1.7.0.0**
Annex A   running on Microsoft Windows NT Version 4.0 with Service Pack 3
                                                                      and on Sun Solaris Version 8

- Oracle Utilities 8.1.7.0.0
- SQL*Plus 8.1.7.0.0

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

- Oracle8*i* Evaluated Configuration document [g]
- Oracle8*i* Administrator's Guide [r]
- Oracle8*i* SQL Reference, Volumes 1 and 2 [s]
- Oracle8*i* Reference [t]
- Oracle8*i* Application Developer's Guide [u]
- Oracle8*i* Concepts, Volumes 1 and 2 [0]
- Oracle8*i* Administrator's Guide for Windows NT [w]
- Oracle8*i* Administrator's Guide for SUN Solaris [x]
- Programmer's Guide to the OCI, Volumes 1 and 2 [y]
- Oracle8*i* Error Messages, Volumes 1, 2 and 4 [z]

TOE Configuration

5.   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 [g]. The following are the types of steps that must be performed:

a.   Installation of the operating system in its evaluated configuration (Microsoft Windows NT Version 4 Service Pack 3 or 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

6.   The Developer's test environment consisted of a total of 4 systems, one Compaq DeskPro 4500 workstation, one Compaq Proliant 4500 server, one Sun SPARCstation 20 workstation and one Sun ULTRA1 server. The 2 Compaq machines were connected together using TCP/IP networking. The 2 Sun machines were connected together using TCP/IP networking. It is to be noted that for all of the testing, the Solaris machines and the Windows NT machines operated as separated networks except for the tests that required a remote connection.

7.   The Evaluators' test environment was the same as that of the Developer.

8.   The specification of the machines was as follows:

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3   **Annex A**
and on Sun Solaris Version 8

Machine Make	Compaq	Compaq	Sun	Sun
Machine Model	Proliant 4500	DeskPro 4000	ULTRA1	SPARCstation 20
Drive Specifications	2GB IDE hard drive with NTFS 4GB external SCSI hard drive with NTFS 3.5 inch floppy drive CD-ROM drive	2GB IDE hard drive with NTFS 3.5 inch floppy drive CD-ROM drive	3GB hard drive with UFS CD-ROM drive	3GB hard drive with UFS CD-ROM drive
Operating Systems	Microsoft Windows NT 4.0 Server (Build 1381 Service Pack 3)	Microsoft Windows NT 4.0 Workstation (Build 1381 Service Pack 3)	Sun Solaris 8.0	Sun Solaris 8.0
Processor	x86 Family 5 Model 2 Stepping 5	x86 Family 5 Model 2 Stepping 12	SPARC	SPARC
Physical Memory	128 MB	80 MB	128 MB	160 MB
Network Cards	Compaq Netelligent 10/100 TX PCI UTP network card	Compaq Netelligent 10/100 TX PCI UTP network card	10BaseT network connection	10BaseT network connection

DBMS PP
Annex A

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

(This page is intentionally left blank)

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3   **Annex B**
and on Sun Solaris Version 8

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1.   Oracle8*i* Database Server Enterprise Edition Release 8.1.7.0.0 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 Oracle8i 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 schema which are collections of database objects or logical structures that directly refer to the information stored in the database. The logical storage structures dictate how the physical space 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 both 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.

DBMS PP   **Release 8.1.7.0.0**
Annex B   running on Microsoft Windows NT Version 4.0 with Service Pack 3
                                                                                              and on Sun Solaris Version 8

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 (eg tables, views, etc). At the centre of 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 the 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 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 (eg 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 deallocated upon instance shutdown. Each process of the database accesses the SGA (of that particular instance) to

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3   **Annex B**
and on Sun Solaris Version 8

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 depicts the Oracle8*i* process architecture as described above.
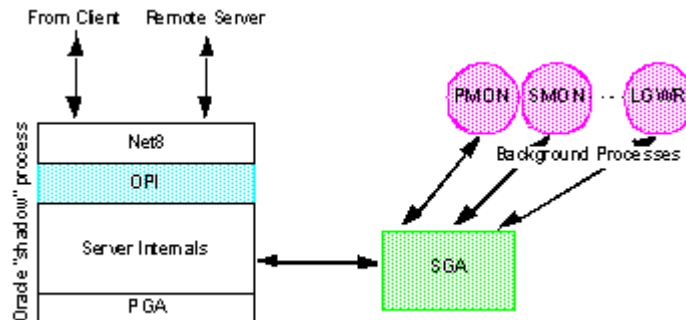
15.   The Process Monitor provides process recovery when a process fails. The System Monitor provides database instance recovery and the Log Writer writes to the redo logs.

Configuration

16.   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.

17.   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 (eg 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.

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

Identification & Authentication

19.   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.

DBMS PP   **Release 8.1.7.0.0**
Annex B   running on Microsoft Windows NT Version 4.0 with Service Pack 3
                                                        and on Sun Solaris Version 8

20.   Oracle8*i* always identifies users of its database prior to establishing a database session for a 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)

21.   In the evaluated configuration, external authentication services are not used to authenticate authorised database users.

22.   Host operating system based authentication allows a user to connect to the database without supplying a username or password. The database obtains the user's identity from the host operating system and compares it against an identity in its data dictionary. If a match is found, the user connects to the database if the user has the appropriate session privileges.

23.   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.

24.   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.

25.   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

26.   Oracle8*i* includes security features that control how a database is accessed and used. Associated with each database is a schema by the same name. By default, each database user creates and has access to all objects in the corresponding schema. Access to and security of objects in other user schemas is governed by the Oracle8*i* DAC mechanism.

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

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3   **Annex B**
and on Sun Solaris Version 8

28.   Oracle8*i* 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.

29.   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.

30.   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 PL/SQL functions and are always enforced on normal users no matter how data is accessed. Different policies can be applied for SELECT, INSERT, UPDATE and DELETE operations. It is also possible for more than one policy to be applied to a table, including building on top of base policies in packaged applications.

Audit

31.   Oracle8*i* ensures the accountability of its users' actions by the use of its auditing mechanisms which are designed to be as granular and flexible as possible to ensure that exactly what needs to be audited is properly recorded, but nothing more.

32.   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).

33.   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).

34.   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

DBMS PP   **Release 8.1.7.0.0**
Annex B   **running on Microsoft Windows NT Version 4.0 with Service Pack 3**
and on Sun Solaris Version 8

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.

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

Other Security Features

36.   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

37.   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 (ie the database to which they are directly connected) can access data in remote databases.

38.   Other than the database link functionality, these other security features were outside the scope of the evaluation. No claims regarding integrity were made in the Security Target [a] and import and export of data and backup and recovery are provided by separate Oracle products.

Network Management

39.   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.

40.   Net8, the network transport and management product forms part of the Oracle8*i* server and is included in the evaluated configuration. It 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

Release 8.1.7.0.0   **DBMS PP**
running on Microsoft Windows NT Version 4.0 with Service Pack 3   **Annex B**
and on Sun Solaris Version 8

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

41.   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.

DBMS PP
Annex B

Release 8.1.7.0.0
running on Microsoft Windows NT Version 4.0 with Service Pack 3
and on Sun Solaris Version 8

(This page is intentionally left blank)