UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

CERTIFICATION REPORT No. P106

Oracle8 Database Server Enterprise Edition

Release 8.0.5.0.0

running on Microsoft Windows NT Version 4.0 with Service Pack 3

Issue 1.0

October 2000

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 of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

CERTIFICATION STATEMENT

Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0 is a relational database management system developed by Oracle Corporation.

Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the 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 Database Server Enterprise Edition Release 8.0.5.0.0 conforms to the Database Management System Protection Profile using the Operating System Authentication functional package.

When used in conjunction with an operating system incorporating the Common Criteria Controlled Access Protection Profile (or the equivalent ITSEC F-C2 functionality), Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0 can be used to provide security for systems which require C2 security functionality for databases. Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0 was evaluated on Microsoft Windows NT Version 4.0 with Service Pack 3.

Originator	**CESG** Certifier
Approval	**CESG** Technical Manager Certification Body
Authorisation	**CESG** Senior Executive UK IT Security Evaluation and Certification Scheme
Date authorised	3 October 2000

(This page is intentionally left blank)

TABLE OF CONTENTS

CERTIFICATION STATEMENT iii

TABLE OF CONTENTS v

ABBREVIATIONS vii

REFERENCES ix

I. EXECUTIVE SUMMARY 1
Introduction 1
Evaluated Product 1
TOE Scope 1
Protection Profile Conformance 2
Assurance Level 2
Strength of Function 2
Security Claims 3
Threats countered by the TOE 3
Threats countered by the TOE's environment 3
Organisational Security Policies 3
Assumptions on the TOE 3
Environmental Assumptions and Dependencies 4
TOE Security Objectives 4
Environmental Security Objectives 5
Security Functional Requirements 7
Security Function Policy 7
Evaluation Conduct 8
Certification Result 8
General Points 8

II. EVALUATION FINDINGS 11
Delivery and Installation 12
User Guidance 13
Developer's Tests 13
Evaluators' Tests 13

III. EVALUATION OUTCOME 15
Certification Result 15
Recommendations 15

ANNEX A: EVALUATED CONFIGURATION 17

ANNEX B: PRODUCT SECURITY ARCHITECTURE 21

(This page is intentionally left blank)

ABBREVIATIONS

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
IDE	Integrated Digital Electronics
OCI	Oracle Call Interface
OPI	Oracle Program Interface
O-RDBMS	Object Relational DataBase Management System
PGA	Program Global Area
SFR	Security Functional Requirement
SGA	System Global Area
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
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

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

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

c. 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.

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

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

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

g. Evaluated Configuration for Oracle8 Database Server,
Oracle Corporation,
Issue 1.8, March 2000.

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.

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. UKSP 14 Addendum: EAL4 Delta Evaluation Work Programme, UK IT Security Evaluation and Certification Scheme, Version 2.0, 19 June 1998.

n. Certification Report No. 98/94, Oracle7 Release 7.2.2.4.13, UK IT Security Evaluation and Certification Scheme, Issue 1.0, February 1998.

o. Manual of Computer Security Evaluation, Part III, Evaluation Tools and Techniques, UK IT Security Evaluation and Certification Scheme, USKP 05, Version 2.0, 30 July 1997.

p. Task LFL/T076 Evaluation Technical Report 1, Logica CLEF, CLEF.24350.16.3, Issue 1.0, 12 February 1999.

q. Task LFL/T076 Evaluation Technical Report 2, Logica CLEF, CLEF.24350.16.4, Issue 1.0, 4 July 2000.

r. Task LFL/T076 Reply to ETR2 Comments, Logica CLEF, 31 August 2000.

s. Task LFL/T076 Response to letter CB/2220XV/LFL/T076 dated 8 September 2000, Logica CLEF, 15 September 2000.

t. Oracle8 Server Administrator's Guide, Oracle Corporation, A54641-01, Release 8.0, June 1997.

u. Oracle8 Server SQL Reference, Volumes 1 and 2, Oracle Corporation, A54648-01 & A54649-01, Release 8.0, June 1997.

v. Oracle8 Server Reference, Oracle Corporation, A54645-01, Release 8.0, June 1997.

w. Oracle8 Application Developer's Guide,
Oracle Corporation,
A54642-01, Release 8.0, June 1997.

x. Oracle8 Server Concepts, Volumes 1 and 2,
Oracle Corporation,
A54646-01 & A54644-01, Release 8.0, June 1997.

y. Oracle8 Enterprise Edition Getting Started, Release 8.0.5 for Windows NT,
Oracle Corporation,
A64416-01, Release 8.0.5, July 1998.

z. 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.

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the IT security evaluation of Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0 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 Database Server Enterprise Edition Release 8.0.5.0.0.

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.

4. Oracle8 is an Object-Relational Database Management System (O-RDBMS) that provides comprehensive security functionality for multi-user information management environments. The TOE can operate in standalone, client/server and distributed configurations.

5. The TOE provides the following security functionality:

- User identification
- 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

6. When used in conjunction with an operating system incorporating the Common Criteria Controlled Access Protection Profile [b] (or the equivalent ITSEC F-C2 functionality [c]), Oracle8 can be used to provide security for systems which require C2 security functionality for databases.

7. 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 server and clients products:

- Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0

- Distributed Database Option 8.0.5
- Oracle8 Objects Option 8.0.5.0.0
- Oracle8 Utilities 8.0.5.0.0
- Oracle8 Installer 3.3.0.1.3
- Net8 Client 8.0.5.0.0
- Net8 Server 8.0.5.0.0

9. The scope of the certification includes the following Oracle8 interface products:

- Oracle Server Manager 8.0.5
- Oracle Call Interface (OCI) 8.0.5.0.0
- Net8 Client 8.0.5.0.0
- Net8 Server 8.0.5.0.0
- TCP/IP Adapter 8.0.5
- Oracle Named Pipes Protocol Adapter 8.0.5.0.0

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

11. The evaluation of Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0 **excludes** the following options and features, which have not been considered by the Evaluators:

- O-RDBMS Authentication
- Oracle Advanced Networking Option

Protection Profile Conformance

12. The Security Target [a] claims conformance with the Database Management Protection Profile (DBMS PP) [f] using the Operating System Authentication functional package.

Assurance Level

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

Strength of Function

14. The TOE did not contain any permutational cryptographic functions. The certified configuration included only the operating system authentication option (ie with O-RDBMS Identification only). The O-RDBMS authentication option (ie with O-RDBMS Identification and Authentication) was not put forward for evaluation. No Strength of Function (SoF) was therefore claimed by the TOE. However, the Security Target [a] and DBMS PP [f] require that the overall SoF of the operating system and the TOE must be SoF-Medium.

Security Claims

15. The TOE's security objectives, and the threats and Organisational Security Policies which counter these objectives, are fully specified in DBMS PP [f] 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 Common Criteria (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

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

- 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

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

- Insecure configuration and operation
- Abrupt interruptions
- Physical attack

Organisational Security Policies

18. 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

19. 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].

b. The TOE is configured to use operating system authentication.

c. There are one or more competent individuals assigned to manage the TOE and the security information that it contains and who can be trusted not to abuse their

privileges. These trusted users must use the Oracle Server Manager for all privileged connections to the TOE.

Environmental Assumptions and Dependencies

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

a. The TOE processing resources of the TOE and the underlying operating system are controlled access facilities which prevents 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.

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

- Operating system support for the TOE's identification and authentication, access control, auditing, resource management and backup and recovery mechanisms
- Reliance upon the operating system to protect the TOE from attack

TOE Security Objectives

22. 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, 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 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

23. 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 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.

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 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

24. 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)
- User Attribute Definition (FIA_ATD.1)
- Timing of Identification (FIA_UID.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)

Security Function Policy

25. 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 CEM requirements for the informal security policy model were used for this evaluation, and no separate informal model for access control was provided.

Evaluation Conduct

26. 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 [d, e]. The Scheme has established a Certification Body which is jointly managed by CESG and the Department of Trade and Industry on behalf of Her Majesty's Government.

27. 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].

28. The evaluation was performed against the EAL4 assurance package defined in CC Part 3 [j]. The Common Evaluation Methodology (CEM) [l] was used as the methodology for the evaluation, although the EAL4 Delta Evaluation Work Programme [m] was used where work was reused from the previously performed ITSEC E3 evaluation of Oracle7 Release 7.2.2.4.13 (see Certification Report 98/94 [n]). The use of UK specific guidance (viz the EAL4 Delta Evaluation Work Programme) was appropriate because the Oracle8 evaluation commenced in 1998 before the publication of the formal issue of CEM.

29. The Evaluators conducted sampling during the evaluation, as required for the relevant work-units for EAL4. Guidance provided in the EAL4 Delta Evaluation Work Programme [m] and 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 all of the Developer's tests and 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.

30. The Evaluators used software tools during independent testing. The Evaluators used these tools in accordance with guidance from the Certification Body and from UKSP 05 Part III [o] Chapter 12.

31. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation was completed in September 2000 when the CLEF submitted the final Evaluation Technical Report (ETR) [p-s] to the Certification Body which, in turn, produced this Certification Report.

Certification Result

32. For the evaluation result see the "Evaluation Outcome" section.

General Points

33. 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 system and whether such patches have been evaluated and certified. Consumers are reminded of the security dangers inherent in downloading 'hot-fixes' 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.

34. 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.

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

(This page is intentionally left blank)

II. EVALUATION FINDINGS

36. 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)

Assurance class	Assurance components
	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)

37. Where no changes were identified between the TOE and Oracle7 Release 7.2.2.4.13, some reuse was made of the results of the Oracle7 Release 7.2.2.4.13 evaluation using the EAL4 Delta Evaluation Work Programme [m] for the following assurance classes :

- 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)
- Analysis of coverage (ATE_COV.2)
- Testing: high-level design (ATE_DPT.1)
- Functional testing (ATE_FUN.1)
- Independent testing - sample (ATE_IND.2)
- Partial configuration management automation (ACM_AUT.1)
- Generation support and acceptance procedures (ACM_CAP.4)
- Detection of modification (ADO_DEL.2)
- Installation, generation and startup procedures (ADO_IGS.1)
- Identification of security measures (ALC_DVS.1)

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

39. 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

40. The consumer receives the TOE as a shrink-wrapped package clearly labelled as Oracle8 Release 8.0.5.0.0 for Windows NT. The CD-ROM is identified by its part number, A65262-01, and the shrink-wrapped cardboard box has part number A65263-01. Shrink-wrapping ensures that interference with the TOE will be detectable.

41. The TOE is sent by a mutually known carrier to the consumer. Packages have the names and addresses of the sender and recipient and are marked with the Oracle logo. These measures ensure that a third party could not masquerade as the Developer and supply potentially malicious software.

42. The TOE has a number of configuration steps which the consumer must perform in order to use the TOE. These steps are described in the Evaluated Configuration document [g]. The

Evaluators were satisfied that all values of parameters selected in configuration steps within the evaluated configuration lead to a secure installation of the TOE.

User Guidance

43. The documentation relevant to the security of the TOE for the end user comprise the referenced documents [g, u-y]. The procedures in the Evaluated Configuration document [g] are minimal for end users and are generally common sense measures (eg non-disclosure of passwords). The requirement for the operating system to perform user authentication is covered in the Getting Started Guide [y].

44. The documentation relevant to the security of the TOE for administrators comprise the referenced documents [g, t-v]. The documents provided also indicate how the TOE's environment can be secured.

Developer's Tests

45. The TOE was installed and tested on 3 hardware platforms as specified in Annex A. The Oracle8 Release 8.0.5.0.0 client was installed on one computer and the TOE was installed on the other 2 computers, which acted as database servers. All 3 platforms were used in the testing.

46. 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.

47. 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

48. The Evaluators repeated all 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.

49. 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 the Certification Body's vulnerability database and Internet sources, no publicly known vulnerabilities were found to be applicable to the TOE. The Evaluators also used the ISS Database Scanner 3.0.1 automated tool to check for vulnerabilities, but no vulnerabilities were identified by the tool.

50. 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.

III. EVALUATION OUTCOME

Certification Result

51. After due consideration of the ETR [p], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0 , running on Microsoft Windows NT Version 4.0 with Service Pack 3 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 [f] using the Operating System Authentication functional package.

52. When used in conjunction with an operating system incorporating the Common Criteria Controlled Access Protection Profile (or the equivalent ITSEC F-C2 functionality), Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0 can be used to provide security for systems which require C2 security functionality for databases. Oracle8 was evaluated on Microsoft Windows NT Version 4.0 with Service Pack 3.

53. The TOE did not contain any permutational cryptographic functions. The certified configuration included only the operating system authentication option (ie with O-RDBMS Identification only). The O-RDBMS authentication option (ie with O-RDBMS Identification and Authentication) was not included in the scope of the evaluation. No SoF was therefore relevant to the TOE. However, However, the Security Target [a] and DBMS PP [f] require that the overall SoF of the operating system and the TOE must be SoF-Medium. 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 [z]), this requirement is met.

Recommendations

54. Prospective consumers of the product should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a].

55. The TOE 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. It is recommended that these features should not be used if the TOE is to comply with the evaluated configuration.

56. Only the evaluated product configuration, specified in Annex A, should be installed. The product should be used in accordance with its guidance documentation [t-y].

57. The product should only be used in accordance with the environmental considerations outlined in the Security Target [a] and the Evaluated Configuration document [g].

58. Consumers should consider the threats not countered by the TOE when devising their Organisational Security Policy, especially if the TOE is being used on a network which is connected to potentially hostile networks (which is outside of its evaluated configuration- see the networking connectivity assumptions in DBMS PP [f], reproduced in the “Executive Summary” section above.)

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

   Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0

2. The following components shall be selected during TOE installation:

   - Oracle Database Server Enterprise Edition Release 8.0.5.0.0
   - Oracle8 Objects Option 8.0.5.0.0
   - Oracle8 Utilities 8.0.5.0.0
   - Oracle8 Installer 3.3.0.1.3
   - Oracle Call Interface 8.0.5.0.0
   - SQL*Plus 8.0.5.0.0
   - Net8 Client 8.0.5.0.0
   - Net8 Server 8.0.5.0.0

3. The following components are installed automatically during TOE installation:

   - Required Support Files 8.0.5.0.0
   - Oracle Named Pipes Adapter 8.0.5.0.0
   - Oracle TCP/IP Adapter 8.0.5
   - Oracle Names Server 8.0.5.0.0
   - Oracle Database Assistant 2.0.0.0.0
   - Java Runtime Environment 1.1.1.0
   - Oracle Trace Collection Services 8.0.5.0.0
   - Oracle8 Enterprise Release Notes 8.0.5.0.0
   - Oracle Net8 Assistant 8.0.5.0.0
   - Oracle8 JDBC Drivers 8.0.5.0.0
   - Assistant Common Files 1.0.1.0.0

4. The TOE contains the following components:

   - Oracle Database Server Enterprise Edition Release 8.0.5.0.0
   - Distributed Database Option 8.0.5
   - Oracle8 Objects Option 8.0.5.0.0
   - Oracle8 Utilities 8.0.5.0.0
   - Oracle8 Installer 3.3.0.1.3
   - Net8 Client 8.0.5.0.0
   - Net8 Server 8.0.5.0.0
   - Oracle Named Pipes Adapter 8.0.5.0.0
   - Oracle TCP/IP Adapter 8.0.5
   - Required Support Files 8.0.5.0.0
   - Oracle Call Interface 8.0.5.0.0

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

- Oracle8 Server Administrator's Guide [t]
- Oracle8 Server SQL Reference, Volumes 1 and 2 [u]
- Oracle8 Server Reference [v]
- Oracle8 Application Developer's Guide [w]
- Oracle8 Server Concepts, Volumes 1 and 2 [x]
- Oracle8 Enterprise Edition Getting Started, Release 8.0.5 for Windows NT [y]
- Evaluated Configuration document [g]

TOE Configuration

6. The TOE had the following configuration options as documented in the Evaluated Configuration document [g]:

a. Installation of Microsoft Windows NT Version 4.0 operating system.

b. Installation of Microsoft Windows NT Version 4.0 Y2K and Eurofix patches.

c. Enabling of operating system authentication.

d. Disabling of the password file.

e. Protection of the database files.

f. Miscellaneous steps to set up user accounts, access control and auditing.

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

7. The Evaluators concluded that no TOE configuration options affected the security of the TOE.

Environmental Configuration

8. The Developer's test environment consisted of a total of 3 systems, one Compaq DeskPro 4500 workstation and 2 Compaq Proliant 4500 servers.

9. The servers' specification was as follows:

- Microsoft Windows NT Server Version 4.0 (Build 1381 Service Pack 3)
- x86 Family 5 Model 2 Stepping 5 processor with 128 MB RAM
- Hard drives including Small Computer System Interface (SCSI) and Integrated Drive Electronics (IDE) adapters, with total capacity ranging from 4 GB to 6 GB
- CD-ROM
- 3.5 diskette drive

- Monitor
- Keyboard
- Compaq Netelligent 10/100 TX PCI UTP network cards

10. The workstation's specification was as follows:

- Microsoft Windows NT Workstation Version 4.0 (Build 1381 Service Pack 3)
- x86 Family 5 Model 2 Stepping 12 processor with 80 MB RAM
- 2GB hard drive including IDE adapter
- CD-ROM
- 3.5 diskette drive
- Monitor
- Keyboard
- Compaq Netelligent 10/100 TX PCI UTP network cards

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. Oracle8 Database Server Enterprise Edition Release 8.0.5.0.0 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 server consists of an Oracle8 database and an Oracle8 instance.

2. An Oracle8 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 datafiles, redo log files and control files.

3. The logical structure of an Oracle8 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 database is used. The schema objects and the relationships among them form the relational design of an Oracle8 database. Examples of logical structures include tablespaces, schema objects, data blocks, extents and segments.

4. An Oracle8 instance is the combination of background processes that are created and memory buffers that are allocated when an Oracle8 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 server running. The memory buffers that are allocated during startup are collectively called the *System Global Area*.

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

7. Net8 is the Oracle8 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 which 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 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 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 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.

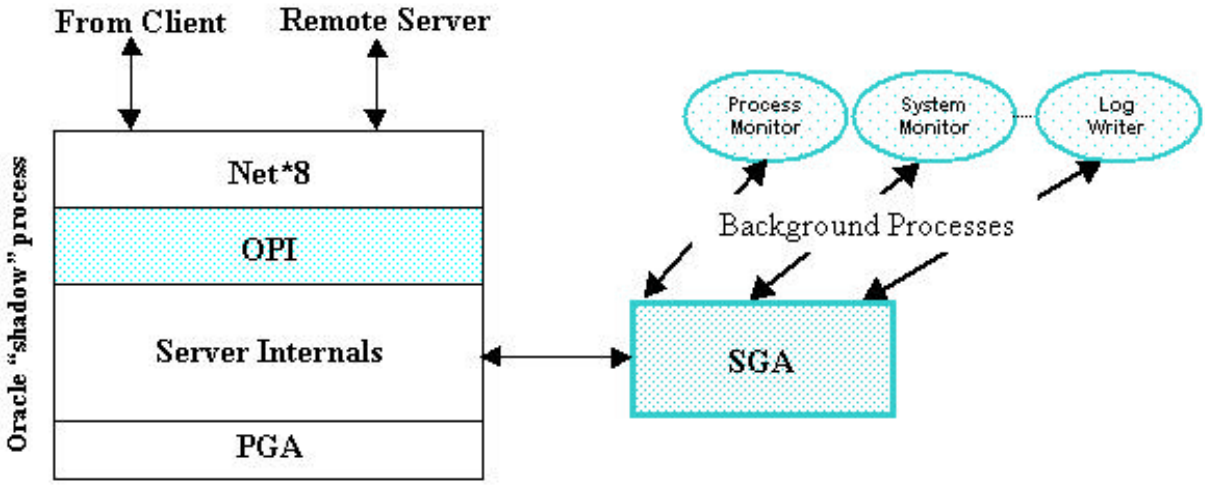
12. An Oracle8 instance is made up of a number of distinct processes that form its core architecture. These processes are classified as background processes which are comprised of user processes and server processes. A user background process is created and maintained to execute application software 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 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 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 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 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 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 servers and their databases, residing on physically different hardware, over networks.

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

18. Oracle8 has 2 types of user; administrative users and normal users. Administrative users are those who are defined within an Oracle8 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 database are normal users.

19. Oracle8 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 directly by the Oracle8 server using passwords managed by it, or by relying on the authentication mechanisms of the host operating system, or through an external authentication service or mechanism which depends on the use of the

Oracle Advanced Networking Option (an add-on product of the Oracle8 server). In the evaluated configuration, only the host operating system authenticates authorised database users. In this scenario, a user connects 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.

20. Administrative users are authenticated to a database by virtue of having an entry in the Oracle8 password file or by having operating system-specific access rights. In the evaluated configuration, administrative users are only authenticated through their 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

21. Oracle8 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 Discretionary Access Control (DAC) mechanism.

22. Oracle8 provides DAC, which is a means of restricting access to information at the discretion of the owner of the information. The Oracle8 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.

23. Oracle8 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. 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 mechanisms that affect the set of privileges held by the session.

Audit

24. Oracle8 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.

25. Audit categories offered by Oracle8 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).

26. When defining which actions are to be audited, Oracle8 can be used to specify that only actions which 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).

27. Audit records can be written to the database audit trail, operating system audit trail or to a specified file in the operating system. Oracle8 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.

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

Security Features

29. Oracle8 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 database, using operating system-specific backup programs, or database import/export and recovery utilities
- secure distributed processing using database links

30. 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 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.

Network Management

31. Add-on products of the Oracle8 server such as Oracle Advanced Networking Option provide encryption of network traffic between clients and servers. Oracle Advanced Networking Option also

offers mechanisms to configure Oracle8 to use external third party authentication services. However, Oracle Advanced Networking Option is not part of the evaluated configuration of the Oracle8 server.

32. Net8, the network transport and management product forms part of the Oracle8 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 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 server.

Operating System Administration

33. Oracle8 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 server is dependent not only on the secure administration of Oracle8, but also on the proper administration of the underlying operating system in any of the product configurations in which it is used.