UK ITSEC SCHEME CERTIFICATION REPORT No. P103

Oracle7

Release 7.2.2.4.13

Issue 1.0

October 1998

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

AGREEMENT 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 Agreement Group and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement.

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

Trademarks:

Oracle7 and PL/SQL are trademarks of Oracle Corporation.

CERTIFICATION STATEMENT

Oracle7 Release 7.2.2.4.13 is a relational database management system developed by the Oracle Corporation.

As detailed in this report, Oracle7 Release 7.2.2.4.13 has been evaluated under the terms of the UK ITSEC Scheme and has met the CC Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified CC Part 2 functionality. The Security Target conforms with the registered Protection Profile for Commercial Database Management Systems, PP C.DBMS.

When used in conjunction with an operating system incorporating the Common Criteria Protection Profile for Controlled Access (or the equivalent ITSEC F-C2 functionality), Oracle7 can be used to provide security for systems which require C2 security functionality for databases.

Originator	**H R Uzzell** Certifier
Approval	**Dr. R Pizer** Head of the Certification Body
Authorisation	**P M Seeviour** Senior Executive UK ITSEC Scheme
Date authorised	7 October 1998

(This page is intentionally left blank)

TABLE OF CONTENTS

CERTIFICATION STATEMENT iii

TABLE OF CONTENTS v

ABBREVIATIONS vii

REFERENCES ix

I. EVALUATION SUMMARY 1
Introduction 1
Evaluated Product 1
Product Environment 1
PP Conformance 2
Evaluation 2
General Points 3

II. EVALUATION OUTCOME 5
Certification Result 5
Unresolved Issues 5
Recommendations 5

ANNEX A: PRODUCT SECURITY FUNCTIONALITY 7

ANNEX B: PRODUCT ENVIRONMENTAL CONSIDERATIONS 11

ANNEX C: PRODUCT SECURITY ARCHITECTURE 13

ANNEX D: EVALUATED CONFIGURATION 15

(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
ETR	Evaluation Technical Report
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
LAN	Local Area Network
OCI	Oracle Call Interface
OCILIB	Oracle Call Interface Library
OPI	Oracle Programming Interface
OSP	Organisational Security Policies
PP	Protection Profile
RDBMS	Relational Database Management System
SFP	Security Function Policy
SQL	Structured Query Language
TOE	Target of Evaluation
TSF	TOE Security Functions
UKSP	United Kingdom Scheme Publication
UPI	User Programming Interface

(This page is intentionally left blank)

REFERENCES

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

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

c. Common Criteria Part 1,
CCIB-97/081R, Version 2.0 Draft 19 December 1997.

d. Common Criteria Part 2,
CCIB-97/082R, Version 2.0 Draft 19 December 1997.

e. Common Criteria Part 3,
CCIB-97/083R, Version 2.0 Draft 19 December 1997.

f. Common Evaluation Methodology
UK Support Group
UKSP 14 Addendum: EAL4 Delta Evaluation, 19 June 1998.

g. Common Evaluation Methodology
Interim Common Criteria Evaluation Manual
ICCEM UKSP05.CCINT, 19 June 1998.

h. Harmonised Information Technology Security Evaluation Criteria,
Commission of the European Communities,
CD-71-91-502-EN-C, Version 1.2, June 1991.

i. Information Technology Security Evaluation Manual,
Commission of the European Communities,
Version 1.0, 10 September 1993.

j. Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 2.0, 30 July 1997.

k. Security Target for Oracle7 Database Server Release 7.2,
Oracle Corporation,
Issue 0.5, August 1998

l. Security Target for Oracle7 Database Server Release 7.2,

Oracle Corporation,
Issue 0.3, April 1997

m. Common Criteria Protection Profile,
Commercial Database Management System (PP C.DBMS)
Issue 1.0, March 1998.

n. LFL/T088 Evaluation Technical Report,
Logica CLEF,
CLEF 23400.16.2, Issue 1.0, 12 August 1998

o. LFL/T088 Evaluation Technical Report 1 Addendum,
Logica CLEF,
CLEF 23400.16.2, Issue 1.0, 17 September 1998

p. LFL/T088 Protection Profile Evaluation Technical Report,
Logica CLEF,
CLEF 23400.16.1, Issue 1.0, 14 October 1998.

q. Certification Report No 98/94,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, February 1998.

r. Certification Report No 96/71,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, February 1997.

s. Common Criteria
Controlled Access Protection Profile
Issued by Information System Security Organisation
Version 1.8 (draft), September 1998

t. Oracle7 Server for Windows NT Release Notes,
Oracle Corporation,
A56068-01, Release 7.2.2.4.13, June 1997.

u. Oracle7 Server for Windows NT Release Notes Addendum,
Oracle Corporation,
Issue 1, June 1997.

v. Oracle7 Server SQL Reference,
Oracle Corporation,
A20325-2, Release 7.2, April 1995.

w. Oracle7 Server Documentation Addendum,
Oracle Corporation,

A12042-3, Release 7.1, 19 June 1994.

x. Oracle7 Server Distributed Systems Volume 1: Distributed Data,
Oracle Corporation,
A19488-2, Release 7.2, April 1995.

y. Oracle7 Server Reference,
Oracle Corporation,
A20327, Release 7.2, April 1995.

z. Oracle Application Developer's Guide,
Oracle Corporation,
A20323-2, Release 7.2, March 1995.

aa. PL/SQL User's Guide and Reference,
Oracle Corporation,
A19486-2, Release 2.2, March 1995.

bb. Oracle7 Server Messages,
Oracle Corporation,
A19483-2, Release 7.2, April 1995.

cc. Oracle7 Server Concepts,
Oracle Corporation,
A20321, Release 7.2, March 1995.

dd. Oracle7 Server Migration,
Oracle Corporation,
A19484-2, Release 7.2, March 1995.

ee. Oracle7 Server Tuning,
Oracle Corporation,
A25421-1, Release 7.2, April 1995.

ff. Oracle7 Server Oracle Network Products for Windows NT User's Guide,
Oracle Corporation,
A36290-1, Release 2.2, January 1995.

gg. Oracle7 Server Products for Windows NT Release Notes,
Oracle Corporation,
A25653-2, Release 7.2.2.4.0, January 1995.

hh. Oracle TCP/IP Protocol Adapter for Windows Installation and User's Guide,
Oracle Corporation,

A31938-1, Release 2.2, April 1995.

ii. Oracle TCP/IP Protocol Adapter for Windows Release Notes,
Oracle Corporation,
A31939-2, Release 2.2.2.0.2C, July 1995.

jj. SQL*NET for Windows User's Guide,
Oracle Corporation,
A31936-1, Release 2.2, April 1995.

kk. SQL*NET for Windows Release Notes,
Oracle Corporation,
A31937-1, Version 2.2.2.1.0, May 1995.

ll. Oracle7 Server Administrators Guide,
Oracle Corporation,
A20322-2, Release 7.2, April 1995.

mm. Oracle7 Server Utilities**,**
Oracle Corporation,
A19485-2, Release 7.2, March 1995.

nn. Oracle7 Server Release 7.2 for Windows NT User's Guide,
Oracle Corporation,
A31934-2, Release 7.2, January 1995.

oo. SQL*NET Administrator's Guide
Oracle Corporation,
A11325-1, Version 2.0, July 1993.

pp. Oracle7 Server Roadmap for Windows NT,
Release 7.2 A40655-1, January 1995

qq. Programmers Guide to Oracle call Interface
Release 7.2 A19489-2, April 1995

I. EVALUATION SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria IT security evaluation of Oracle7 Release 7.2.2.4.13 to the Sponsor, Oracle Corporation. This report is intended to assist potential users when judging the suitability of the product for their particular requirements.

2. The prospective user is advised to read the report in conjunction with the Security Target [k], which defines the functional, environmental and assurance requirements.

Evaluated Product

3. The version of the product evaluated was: Oracle7 Release 7.2.2.4.13, developed by the Oracle Corporation.

4. The evaluated configuration is detailed in Annex D. This product is also described in this report as the Target of Evaluation (TOE).

5. Oracle7 is a Relational Database Management System (RDBMS). The TOE can operate in standalone, client/server and server/server configurations. The standalone and client/server configurations allow one or more users to access a database stored on a single platform. In standalone configuration the application software is stored and run on the same platform as the database server, while in a client/server configuration the application software and the database server are stored on different platforms connected via a network. A server/server configuration supports distributed databases by the use of database links to access data on a remote database.

6. Annex A outlines the security objectives of the TOE, the threats and Organisational Security Policies (OSP) together with the functional requirements in support of the security objectives. All of the functional requirements are taken from CC Part 2 Reference [d]; use of this standard facilitates comparison with other evaluated products.

7. The security architecture of the product is outlined in Annex C.

Product Environment

8. The TOE relies on the underlying operating system to provide user authentication. The TOE can be configured to write audit events to the audit trail of the underlying operating system, but can also be configured to use the audit trail within the database. However, certain events (startup, shutdown, connect internal) are always written to the audit trail within the operating system because they are operating system events rather than RDBMS events.

9. When used in conjunction with an operating system incorporating the Common Criteria Protection Profile for Controlled Access [s] (or the equivalent ITSEC F-C2 functionality), Oracle7

can be used to provide security for systems which require C2 security functionality for databases. Annex B outlines the secure usage assumptions relating to use of the underlying operating system.

10. To demonstrate the required assurance, the TOE was evaluated on a Compaq NT Version 3.51 distributed processing operating system - refer to Annex D for the rational behind using this configuration for NT.

PP Conformance

11. The Security Target [k] conforms with the registered Protection Profile for Commercial Database Management Systems [m]. This PP has been successfully evaluated under Common Criteria, reference Evaluation Technical Report [p].

Evaluation

12. The TOE was submitted for evaluation under the predefined evaluation assurance level EAL4 as described in CC Part 3 [e].

13. The TOE has previously been certified to ITSEC E3 as specified in the Certification Report 98/94 [q]. Appropriate reuse of the E3 evaluation work packages was made in accordance with the evaluation methodology specified in [f], with additional evaluation activity being performed to fully comply with CC requirements. The additional activity was based on identifying differences between the mapping of security functions within the ITSEC Security Target [l] and the CC Security Target [k].

14. The evaluation was carried out in accordance with the rules of the UK IT Security Evaluation and Certification Schemes which is described in United Kingdom Scheme Publication (UKSP) 01 and UKSP 02 [a, b]. 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.

15. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [k]. The Evaluators first confirmed that the Security Target conformed to the CC requirements and thus formed a suitable baseline for evaluation.

16. The Evaluators then confirmed that the TOE met the CC Part 3 [e] conformant assurance requirements of EAL4. CC Part 3 describes the scale of assurance given by predefined evaluation assurance levels EAL0 to EAL7, where EAL0 represents no assurance.

17. A claim is not made for a strength of function as the TOE does not contain any critical mechanisms. The evaluated configuration included only the operating system authentication option (ie with RDBMS Identification only). The RDBMS authentication option (ie with RDBMS Identification and Authentication) was not put forward for evaluation.

18. The evaluation was performed prior to the finalisation of the Common Evaluation Methodology (CEM). Therefore, the evaluation was performed using the methodology contained within the following documents:

a. Common Criteria Part 1 [c];

b. Common Criteria Part 2 [d];

c. Common Criteria Part 3 [e];

d. Common Evaluation Methodology (CEM) [f];

e. UK Interim CC Evaluation Manual - ICCEM [g];

f. Harmonised Information Technology Security Evaluation Criteria [h].

g. Information Technology Security Evaluation Manual [i]; and

h. Manual of Computer Security Evaluation part III [j].

19. The Certification Body asserts that the methodology defined by the above documents is sufficient to demonstrate that the evaluation criteria for EAL4 has been met.

20. The Certification Body monitored the evaluation which was carried out by the Logica Commercial Evaluation Facility (CLEF). The evaluation was completed in September 1998 when the CLEF submitted the Evaluation Technical Reports (ETR) [n, o] to the Certification Body, resulting in the production of this Certification Report.

General Points

21. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities remain undiscovered.

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

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

(This page is intentionally left blank)

II. EVALUATION OUTCOME

Certification Result

24. After due consideration of the ETRs [n, o], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Oracle7 Version 7.2.2.4.13 meets the CC Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified CC Part 2 functionality. It was also determined that the requirements specified within the Protection Profile - C.DBMS [m] were met.

Unresolved Issues

25. There are no unresolved issues.

Recommendations

26. Prospective users of the product should understand the specific scope of the Certification by reading this report in conjunction with the Security Target [k] and the Protection Profile [m].

27. Only the evaluated configuration of the product should be installed as specified in Annex D. The evaluated configuration includes guidance documentation issued by Oracle [t - qq]; the product should be used in accordance with this guidance documentation.

28. The product should be used in conjunction with an underlying operating system incorporating the Common Criteria Protection Profile for Controlled Access [s] (or the equivalent ITSEC F-C2 functionality). Annex B outlines the secure usage assumptions relating to use of the underlying operating system.

29. The customer should ensure that the assurance and strength of function within the underlying operating systems is sufficient to meet his requirements.

30. The product should be used in accordance with the environmental considerations as outlined in Annex B.

(This page is intentionally left blank)

ANNEX A: PRODUCT SECURITY FUNCTIONALITY

1. A full specification of the security requirements, including originating OSPs, threats and objectives, any TOE-specific operations, and security functions, is given in the Security Target [k]. The Security Target has drawn on the Protection Profile for C.DBMS [m] for all of the requirements.

Organisational Security Policies

P.ACCESS	Access rights to specific data objects are determined by: the owner of the object; and the identity of the subject attempting the access; and the implicit and explicit access rights to the object granted to the subject by the object owner.

Threats

T.ACCESS	Unauthorised access to the database.
T.DATA	Unauthorised access to information.
T.RESOURCE	Excessive consumption of resources.
T.ATTACK	Undetected compromise of IT assets occurs as a result of an attack.
T.ABUSE	Abuse of authorised privileges.

Objectives

O.I&A	The TOE must provide the means of identification and authentication of users (the Evaluators noted that for the purpose of this evaluation, authentication of users was undertaken the operating system).
O.ACCESS	The TOE must provide end-users and administrators with the capability of controlling and limiting access, by identified individuals, to the data or resources they own or are responsible for.
O.AUDIT	The TOE must provide the means of recording security relevant events in sufficient detail to help an administrator to detect security violations and to hold individuals accountable for their actions.
O.RESOURCE	The TOE must provide the means of controlling the consumption of global resources by specified users of the TOE, including the number of concurrent sessions.

O.ADMIN The TOE, where necessary in conjunction with the underlying operating system, must provide functionality to support authorised administrators in managing the TOE and its security functions.

TOE Security Functional Requirements

2. The following security functional requirements are based on CC Part 2 [d]:

Identification and Authentication

FIA_UID.1.1 The TSF shall allow users to perform certain actions before being identified - see [k] for specific assignments.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_ATD.1.1 The TSF shall maintain a set of privileges, roles, resource limits belonging to individual users - see [k] for specific assignments.

FIA_USB.1.1 The TSF shall associate user security attributes with subjects acting on behalf of that user.

Security Attribute Based Access Control

FDP_ACC.1.1 The TSF shall enforce database object access control SFP on subjects, named objects and all permitted operations on named objects by a subject.

FDP_ACF.1.1 The TSF shall enforce database object access control SFP to objects based on user and owner identity.

FDP_ACF.1.2 The TSF shall enforce specified rules to determine if an operation among controlled subjects and objects is allowed.

FDP_RIP.1.1 The TSF shall ensure that upon the allocation of a resource to schema and non-schema objects any previous information content is unavailable.

Security Management

FMT_MSA.1.1 The TSF shall enforce the database object access control SFP to restrict modification of user attributes to authorised administrators and provide authorised users with the ability to modify object privileges.

FMT_MSA.3.1 The TSF shall enforce the database object access control SFP to provide restrictive default values for object security attributes that are used to enforce the database object access control SFP.

FMT_MSA.3.2	The TSF shall allow no users to specify alternate initial values to override the default values when an object is created.
FMT_MTD.1.1	The TSF shall restrict access to the audit trail.
FMT_REV.1.1	The TSF shall manage the group of roles that can invoke revocation of security attributes.
FMT_REV.1.2	The TSF shall enforce specified revocation rules.
FMT_SMR.1.1	The TSF shall maintain SYSDBA, SYSOPER roles.
FMT_SMR.1.2	The TSF shall associate users with roles.

Resource Utilisation

FRU_RSA.1.1	The TSF shall enforce quotas limiting the maximum quantity of resources to users and subjects - see [k] for specific assignments.

TOE Access

FTA_MCS.1.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.
FTA_MCS.1.2	The TSF shall enforce, by default, a limit of a single session per user.

Security Audit

FAU_GEN.1.1	The TSF shall generate an audit record of specified auditable events - see [k] for specific assignments.
FAU_GEN.1.2	The TSF shall record within each audit record a set of specified information.
FAU_GEN.2.1	The TSF shall associate auditable events with the identity of the user who caused the event.
FAU_SAR.1.1	The TSF shall provide authorised users with the capability to read audit data.
FAU_SAR.1.2	The TSF shall provide audit records in a manner suitable for the user to interpret the information.
FAU_SAR.3.1	The TSF shall provide audit review tools with the ability to search and sort on specified database fields - see [k] for specific assignments.

FAU_SEL.1.1 The TSF shall include or exclude auditable events based on attributes - see [k] for specific assignments.

FAU_SEL.1.2 The TSF shall provide only the authorised administrator with the ability to select which events are to be audited.

FAU_STG.1.1 The TSF shall store generated audit records in a permanent audit trail.

TOE IT Security Functions

3. To ensure equivalent functionality, the transition from ITSEC to CC resulted in the creation of 4 additional TSFs and the amalgamation of 3 ITSEC SEFs into one TSF. This avoided unnecessary repetition and ensured completeness of mapping to a corresponding CC component. The effect of these changes has been evaluated, with a traceability analysis and additional functional testing being carried out in compliance with CC assurance requirements.

ANNEX B: PRODUCT ENVIRONMENTAL CONSIDERATIONS

Except where indicated, all environmental considerations are taken from the Protection Profile for C.DBMS [m].

Threats Countered by the Operating Environment

T.OPERATE	Insecure operation of the system compromising IT assets.
T.CRASH	Abrupt interruption to the operation of the TOE.
T.BADMEDIA	Corruption of storage media.
T.PHYSICAL	Physical attack on the TOE or underlying operating system/network services.
T.TRUSTED	Abuse of privileges by Trusted Users.

Environmental Objectives

O.INSTALL	Installation and management procedures for the TOE and underlying systems are operated in accordance with the relevant operational documentation.
O.PHYSICAL	Those parts of the TOE which are critical to security policy must be protected from physical attack.
O.AUDITLOG	Administrators of the database must ensure effective management of audit facilities.
O.RECOVERY	Procedures and mechanisms must be in place to ensure that secure recovery can be undertaken after a system failure has occurred.
O.QUOTA	System administrators must ensure that each user of the TOE is configured with sufficient quotas to permit authorised operations without monopolising resources.
O.TRUST	Only highly trusted users have the privilege to set or modify audit trail configuration, and to create or modify users and roles.
O.AUTHDATA	Authentication data for each user account on the underlying operating systems and/or network services must be held securely.
O.MEDIA	Data held on storage media is physically protected, periodically checked and prevented from re-use for any non-database purpose.
O.CONFIGURE	Administrators of the database must ensure that the TOE is configured in accordance with this additional objective specified in [k].

Secure Usage Assumptions

Connectivity Assumptions

A.OS	The TOE relies on an underlying operating system that is installed and operated in a secure manner.
A.NETWORK	Underlying network services in a distributed environment must be based on secure communications protocols which ensure the authenticity of users.
A.PEER	All systems which communicate with the TOE are assumed to be under the same management control and security policy constraints.
A.FILES	All database files and directories are protected from unauthorised access by the operating system DAC mechanism.
A.APPLICATIONS	All executables which may be activated alongside the TOE are assumed to maintain the security policy constraint. This is specified in [k] as an additional assumption to those listed in the Protection Profile C.DBMS [m].

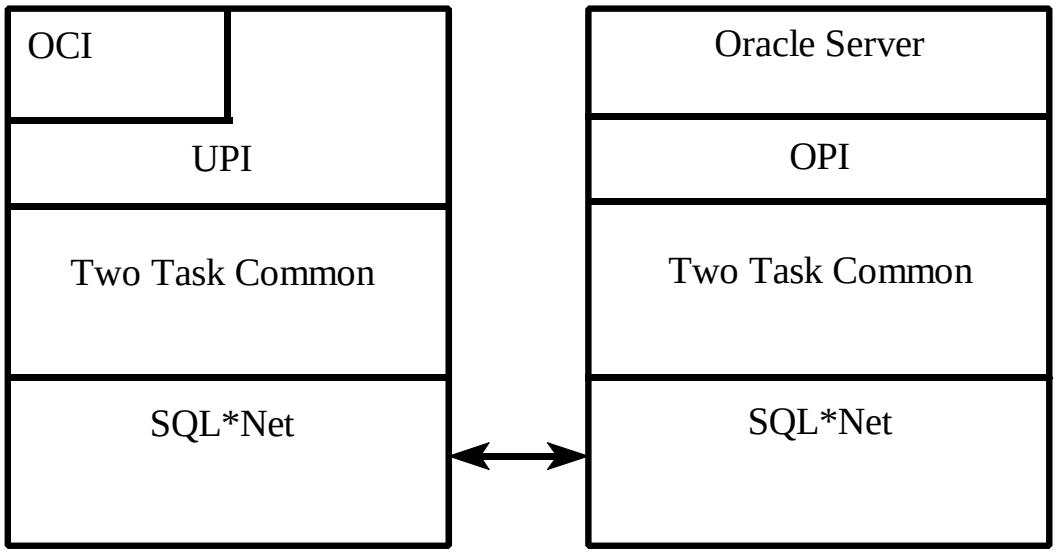
Physical Assumptions

A.LOCATE	Processing resources of the TOE, underlying operating system and network services are located within physically controlled access facilities.
A.PROTECT	Hardware and software critical to security policy enforcement is physically protected from unauthorised modification by potentially hostile outsiders.

Personnel Assumptions

A.ACCESS	The underlying operating systems and secure network services are configured so that only the approved user group has access to the system.
A.MANAGE	There will be competent individuals assigned to manage the TOE who can be trusted not to abuse privileges.

ANNEX C: PRODUCT SECURITY ARCHITECTURE



1. The evaluated configuration includes all of the components in the above diagram. OCI, SQL*DBA and SQL*Plus are the evaluated interfaces. All other Oracle Applications (whether using OCI or UPI) were outside the scope of the evaluation.

2. The components identified in this diagram are:

   a. Oracle Server and the Oracle Programming Interface (OPI): The Oracle Server is the main Oracle executable which maintains and controls access to the database. All security decisions are made within this component. The way in which the Oracle server communicates with other processes is through the OPI. The OPI cannot be called directly from the application code. The only way applications can send requests and receive data from the Oracle Server is via the OCI (Oracle Call Interface) or UPI (User programming Interface).

   b. OCI and UPI are the public and private interfaces, respectively, which allow application programs to communicate with the Oracle Server. OCI is a public interface which is described within the Oracle Documentation Set. Third Party applications would use this interface to access the database. UPI is an interface for which no publicly available documentation is available. Oracle Applications such as SQL*DBA, SQL*Plus and Oracle Forms use the UPI interface.

   c. Two Task Common and SQL*Net: UPI and OPI communicate with each other via SQL*Net and Two Task Common routines. The Two Task Common routines simply convert the output from UPI and OPI into a format suitable for transmission over

SQL*Net. SQL*Net provides the required communication services which consist of Session Establishment, Communications and Network Management.

3. The Oracle Server High level Component is split into several layers, one of which is responsible for security. All operations which require security checking of the user or database objects use the functionality within the layer to perform that checking.

4. All operations performed by the Oracle Server are driven by SQL (or equivalent OCI) requests by users. When an operation is submitted by a user, various checks are performed to ensure that the operation is valid and allowed. Security checking within Oracle happens as early as possible within any operation that is requested by a user. Therefore, some operations will be rejected during the parse phase of an operations processing. Others may however, not be prevented until the execute phase. No operation will complete unless the user has the required privilege.

5. The Operating System dependent code is restricted to a very thin layer. Consequently, the differences between different ports of Oracle are minimal. In particular, the security functionality would be largely unaffected by any such port.

Client Server Architecture

6. Oracle has 2 major architectural concepts: *instance* and *database*. An *instance* consists of a set of DBMS server processes, which do the work of the DBMS by executing the Oracle7 Database Server software, and a set of shared memory segments. A *database* consists of a set of files which contain the information stored in the database.

7. Each database is an autonomous unit with its own data dictionary that defines the database objects it contains (eg tables, valid users and their privileges, etc). In a distributed system there can be many databases, each can contain many database objects, but every database object is stored only within one database.

8. An *instance* is therefore an active entity, and a *database* is passive. In order for users to access the database, the instance must be started. If the user is defined as a valid user and has the appropriate access rights, then the instance will create a database session for that user.

9. A user connects directly to a local instance and database. Subsequently a user may connect indirectly to a remote instance and database, through the local instance. Access to a remote database is achieved using database links with appropriate access rights defined in the remote database. As each instance is autonomous, the remote instance enforces security based on the access rights of the user.

ANNEX D: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as: Oracle7 Release 7.2.2.4.13.

2. The evaluated configuration includes guidance documentation issued by Oracle [t - qq].

TOE Configuration

3. The TOE comprises the following components:

- Oracle Named Pipes Adapter 2.2.2.1.0
- Oracle SPX Adapter 2.2.2.1.0
- Oracle TCP/IP Adapter 2.2.2.1.0
- Oracle Distributed Option 7.2.2.4.0
- Oracle7 Server 7.2.2.4.13
- Oracle7 Utilities 7.2.2.4.6
- Required Support Files 7.2.2.4.12D
- SQL*Net Client 2.2.2.1.0
- SQL*Net Server 2.2.2.1.0
- SQL*DBA (line mode only) 7.2.2.4

4. The above Oracle Software was installed using the Oracle Installer Version 3.1.2.1.3 using the Selective Product Install Option.

5. Oracle7 Release 7.2.2.4.13 is a patch which is installed over Oracle 7.2.2.4.0. The patch replaces the "Oracle7 Server" and "Oracle7 Utilities" and "Required Support Files" components of the product. The other components are unchanged.

6. The TOE can operate in standalone, client/server and server/server configurations. The standalone and client/server configurations allow one or more users to access a database stored on a single platform. In standalone configuration the application software is stored and run on the same platform as the database server, while in the client/server configuration the application software and the database server are stored on different platforms connected via a network. The server/server

configuration supports distributed databases, ie the use of database links to access data on a remote database.

7. The products, components and options which were not evaluated but which were used for evaluation testing were:

- SQL*Plus 3.2.2.0.1
- OCILIB 7.2.2.4

Environmental Configuration

8. Evaluation testing was performed on 2 Compaq Proliant 4500 x86 (Family 5 Model 2 Stepping 5) machines connected by a LAN. Each machine had 65600 KB of physical memory.

9. The evaluation was carried out using COMPAQ NT Version 3.51 distributed processing operating system (build 1057) as the underlying operating system. It was originally intended to evaluate the TOE on the Microsoft Windows NT Version 3.51 distributed processing operating system as specified in the Certification Report No 96/71 [r]. However, because the Evaluators were unable to obtain build 1057 of Microsoft Windows NT Version 3.51 from Microsoft, all the Evaluator testing was performed on Compaq NT Version 3.51 (build 1057). The TOE is largely operating system independent and the Evaluators expect any differences that exist between Compaq NT 3.51 and Microsoft Windows NT 3.51 to have no effect on the operation of the TOE. It is therefore also assumed for the purposes of this evaluation that the operating system has provided the correct information to the Oracle7 RDBMS.