Oracle8 Security Target
Release 8.0.5

April 2000

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Common Criteria Security Target for Oracle8™ Database Server
Release 8.0.5

April 2000

Author: Seve Pannifer

Contributors: Duncan Harris, Lydia Frew, Howard Smith, Hugh Griffin and John Morrissey

Contents

CHAPTER

1 Introduction

This document is the security target for the Common Criteria evaluation of the Oracle8 Database Server, Release 8.0.5.

Identification and CC Conformance

Title: Oracle8 Security Target

Target of Evaluation (TOE): Oracle8 Server Enterprise Edition, with the Distributed Database Option and the Objects Option.

Release: 8.0.5

Operating System Platform: Microsoft Windows NT 4.0.

CC Conformance: Database Management System Protection Profile (DBMS PP) [DPP]. The authentication package claimed for this Security Target is DBMS in Operating System Authentication Mode. This Security Target conforms to [CC, Part 2] and [CC, Part 3]. No new SFRs have been introduced and no augmented assurance criteria have been specified.

Assurance: EAL4.

Keywords: Oracle8, O-RDBMS, database, security target, EAL4

Version of Common Criteria [CC] used to produce this document: 2.1

TOE Overview

Oracle8 is an object-relational database management system (O-RDBMS), providing advanced security functionality for multi-user distributed database environments. The security functionality in Oracle8 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, and
- stored procedures and triggers for user-defined access controls and auditing.

Oracle8 supports both client/server and standalone architectures. In both architectures, the Oracle8 Server acts as a *data server*, providing access to the information stored in a database. Access requests are made via Oracle8 *interface products* that provide connectivity to the database and submit Structured Query Language (SQL) statements to the Oracle8 data server. The Oracle8 interface products may be used on the same computer as the data server, or they may run on separate client machines and communicate with the data server via network interfaces.

TOE Product Components

The Oracle8 Server Enterprise Edition includes the products identified in Table 1. Access to the Oracle8 server is provided by the interface products identified in Table 2. Features of the TOE products that cannot be used in configurations that comply with the DBMS PP and this Security Target are identified in Table 3.

Table 1: TOE Server Products

TOE Server Products
Oracle8™ Server Enterprise Edition 8.0.5
Distributed Database Option 8.0.5
Objects Option 8.0.5
Net8™ 8.0.5
TCP/IP Adapter 8.0.5

Table 2: TOE Interface Products

TOE Interface Products
Oracle Server Manager 8.0.5
Oracle Call Interface 8.0.5
SQL*Plus 8.0.5
Net8™ 8.0.5
TCP/IP Adapter 8.0.5

Table 3: Excluded Product Features

Product	Excluded Features
Oracle8 Server	Multithreaded Server Option 8.0.5

Document Overview

Chapter 2 of this security target provides a high-level overview of the security features of the Oracle8 data server. Chapter 3 identifies the assumptions, threats, and security policies of the Oracle8 TOE environment. Chapter 4 describes the security objectives for the TOE and for the environment needed to address the assumptions, threats, and security policies identified in Chapter 3. Chapter 5 identifies the Security Functional Requirements (SFRs), the Security Assurance Requirements (SARs) and the security requirements for the Oracle8 TOE environment. Chapter 6 summarises each TOE Security Function (TSF) provided by Oracle8 to meet the security requirements. Chapter 7 describes how the Oracle8 TOE conforms to the requirements of the DBMS Protection Profile and Chapter 8 provides the rationale for the security claims made within this security target.

Appendix A contains a list of references and Appendix B provides a glossary of the terms.

This Page Intentionally Blank

CHAPTER

2 TOE Description

This section describes the Oracle8 product features that provide security mechanisms and contribute to the security of a system configured with the Oracle8 TOE. The security features of the product are explained primarily in part IV of *Oracle8 Server Administrator's Guide* [SAD] and in part VII of *Oracle8 Server Concepts* [SCN]. In general, these descriptions correspond to the specifications of IT security functions provided in chapter 6 of this Security Target.

This chapter describes the major elements of the Oracle8 architecture, the types of database objects supported by Oracle8, the access control mechanisms used to protect those objects, controls on user resource consumption, the accountability and auditing mechanisms, and the security management features provided by Oracle8. Additional Oracle8 security features that are not addressed by the security functional requirements of Chapter 3 are also briefly discussed.

Oracle8 Architecture

The Oracle8 architectural components are described in detail in [SCN, parts I, II, and III].

Database

A *database* consists of a set of files which contain, in addition to some control data, the information which is said to be stored in the database. Each database is an autonomous unit with its own *data dictionary* that defines the *database objects* it contains (e.g. tables, views, etc.). In a distributed system there can be many databases: each database can contain many database objects, but each database object is stored within a single database.

Instance

An *instance* consists of a set of Oracle *background processes*, which do the work of the DBMS by executing Oracle8 software, and a shared memory area. 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 and must mount and open the database for use. A database is persistent: it has an indefinite lifetime from the time it is created, and the database files and contents exist independently of whether the database is mounted to

an instance and whether the underlying platform is running. The lifetime of an instance can be indefinite, from when it is started to when it is shut down, and is dependent on whether the underlying platform is running.

Database Connections and Sessions

Each database user employs Oracle8 interface products to establish a *database connection* to an Oracle8 *server process* for a particular database instance. If the user is defined as a valid user for the database and has the required *privileges*, then the server will create a *database session* for the user. While connected, the user can make requests to the Oracle8 server to read and write information in the database. The server handles each request, performing the read and write accesses to database objects and returning data and results to the user, in accordance with the user's privileges to database objects and other constraints configured by a *database administrative user*.

Distributed Databases

In a distributed environment, a user may access database objects from multiple databases. After establishing an initial database session on one instance, the user can transparently establish database sessions on other (remote) database instances using *database links*. A database link identifies a remote database and provides authentication information. By qualifying references to database objects with the name of a database link, a user can access remote database objects. However, each Oracle8 database instance is autonomous with respect to security — a remote server enforces security based on the privileges of the user as defined in that remote database.

Structured Query Language (SQL)

The Oracle8 server supports the ANSI/ISO SQL standard [SQL92] at the entry level of compliance and provides Oracle-specific SQL language extensions. All operations performed by the Oracle8 server are executed in response to an SQL statement that specifies a valid SQL command.

- Data Definition Language (DDL) statements are statements which create, alter, drop, and rename database objects, grant and revoke privileges and roles, configure audit options; add comments to the data dictionary; and obtain statistical information about the database and its use;
- Data Manipulation Language (DML) statements are statements which manipulate the data controlled by database objects in one of four ways: by querying the data held in a database object; by row insertions; by row deletion; by column update. They include the command to lock a database object.
- Transaction Control statements are statements which manage changes made by DML statements and help to ensure the integrity of the database. They include commits and rollbacks for individual transactions, and checkpoints for the database;
- Session Control statements dynamically manage the properties of a user's database session.
- System Control statements dynamically manage the processes and parameters of an Oracle8 database instance.

Programming Language/SQL (PL/SQL) is a procedural language supported by Oracle8 that provides program flow control statements as well as SQL statements [PLS]. *Program units* written in PL/SQL can be stored in a database and executed during the processing of a user's SQL command.

An Oracle8 Database

An Oracle8 database contains the data dictionary and two different types of database objects:

- schema objects that belong to a specific user *schema* and contain user-defined information [SCN part IV], and
- non-schema objects to organise, monitor, and control the database [SCN part II, SAD]

In an Oracle8 database there are two kinds of user:

- normal users. Note that this includes SYS and SYSTEM. [SAD, 1-2]
- Database Administrator Roles SYSOPER and SYSDBA, which allow users to perform administrative tasks such as database startup and shutdown, and ALTER DATABASE commands. [SAD, 1-8]

Note that connecting to a database via the CONNECT INTERNAL command is supported for backward compatibility reasons only. [SAD, 1-8]

Data Dictionary

At the centre of an Oracle8 database is the data dictionary — a set of internal Oracle tables that contain all of the information the Oracle8 server needs to manage the database. The data dictionary tables are owned by the user SYS and can only be modified by highly privileged users. [SCN] advises that no Oracle user should **ever** alter any object contained in the SYS schema and the security administrator should keep strict control of this central account. A set of read-only views is provided to display the contents of the internal tables in a meaningful way and also allow Oracle users to query the data dictionary without the need to access it directly.

All of the information about database objects is stored in the data dictionary and updated by the SQL DDL 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.

Schema Objects

A *schema* is a collection of user-defined database objects that are owned by a single database user. Oracle8 with the Objects and Distributed Database Options supports the schema object types identified in [SQL, 2-2].

A special schema PUBLIC is provided by Oracle8 to contain objects that are to be accessible to all users of the database. Typically, the kinds of objects that are created in the PUBLIC schema are:

- Public database links that define access to remote databases,
- Public synonyms which point to objects which all users may need to access.

Non-Schema Objects

[SQL, 2-3] lists object types can be created and manipulated with SQL, but are not contained within a schema. These include tablespaces, roles, profiles and users.

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, and

•take tablespaces on-line and off-line for backup and recovery operations.

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

Database Users

Oracle8 contains two kinds of user: normal users and the special database administrative roles (SYSDBA and SYSOPER). Throughout this document the following terms are used to describe these users:

- Normal User/Database Subject: A user who is explicitly authorised to access the database by virtue of being explicitly defined and identified to an instance of the Oracle8 Database Server. The pre-defined users SYS and SYSTEM are normal users;
- Specially Authorised User: A user who is authorised to access the database by virtue of having platform specific DBA or OPER access rights;
- Database Administrative User/Administrative User: Any user (either a normal or a specially authorised user) who is authorised to perform a particular administrative task. This authorisation may be granted via a database privilege or via the DBA/OPER roles.

Note that the word *authorised* is used (e.g. “an authorised administrative user”) to indicate the specified user type has the specific authorisation (e.g. via a privilege) for the operation under consideration.

Database security is managed by privileged users through the maintenance of users, roles, and profiles.

•USERS identify distinct database user names and their authentication method.
•ROLES provide a grouping mechanism for a set of privileges.
•PROFILES provide a set of properties (e.g., resource limits, password management options) that can be assigned to individual users.

These security topics are discussed in detail in subsequent sections of this chapter.

Access Controls

Oracle8 access controls can be used to selectively share database information with other users. The access control mechanisms can be used to enforce need-to-know style confidentiality as well as control data disclosure, entry, modification, and destruction. In addition to the access controls enforced by the Oracle8 server, application-specific access controls can be implemented using views and triggers to mediate a user’s access to application data.

Oracle8 controls access to database objects based on the privileges enabled in the database session. There are two types of Oracle8 privileges: *object privileges* and *system privileges.* Both object and system privileges may be granted directly to individual users, or granted indirectly by granting the privilege to an Oracle *role* and then granting the role to the user. Privileges and roles may also be granted to PUBLIC, authorizing all database users for the privilege. During a database session, the privileges enabled in the session may be changed using several Oracle8 mechanisms that affect the set of privileges held by the session.

System Privileges

Oracle8 provides over 80 distinct system privileges to support the concept of least privilege — each database user can be granted only those system privileges that are needed to perform his or her job function. Often end-users would only need a minimal set of system privileges to connect to the database. Some administrative users may be granted more powerful system privileges to authorise them to manage administrative objects, bypass particular server access controls, or perform specialised operations. A user may grant a system privilege to additional database users only if he or she holds that privilege with an administrative option (WITH ADMIN OPTION).

Object Privileges

An object privilege is permission to access a schema object in a prescribed manner (e.g., to INSERT rows into a table or EXECUTE a stored procedure). The owner of the schema containing the object may grant object privileges to other database users or roles. In addition, the owner may grant other users the right to grant those object privileges to additional database users (WITH GRANT OPTION).

Because object privileges are granted to users at the discretion of other users, this type of security is termed discretionary. Oracle8 ensures that users who attempt to gain access to objects have been granted the necessary object privileges for the specific operation, or have an overriding system privilege or role. The owner of an object always has total access to that object.

Roles

Oracle8 facilitates correct privilege administration by enabling privileges to be grouped together into database roles. The benefits of Oracle database roles include:

- Reduced privilege administration,
- Dynamic privilege management,
- Least privilege,
- Privilege bracketing, and
- Consistency.

Reduced privilege administration

Rather than explicitly granting the same set of privileges to several users, the privileges for a group of related users can be granted to a role, and then only the role needs to be granted to each member of the group. Roles permit numerous Oracle privileges to be granted or revoked with a single SQL statement.

Dynamic privilege management

If the privileges of a group of users must change, only the privileges of the role(s) need to be modified instead of the privileges granted to every user. The security domains of all users granted the group's role automatically reflect the changes made to the role.

Least privilege

The roles granted to a user can be selectively enabled (available for use) or disabled (not available for use). This helps a user to control use of those privileges which could result in unintended disclosure, entry, modification, or destruction of data.

Privilege Bracketing

Because the Oracle data dictionary records which roles have been granted to the current user, database applications can be designed to query the dictionary and automatically enable and disable selective roles when a user attempts to execute applications.

System Security Policy

To enable centralised implementation of privilege management in a system of which Oracle may be only one component, Oracle also provides for linking database roles to platform-specific group access controls. In this way, database roles can only be enabled by users if they are a current member of the appropriate group in the underlying platform. This helps to ensure a correct and consistent implementation of a system-wide security policy.

DDL Restriction

Privileges held via roles cannot be used with DDL statements that require access to database objects. For example, to create a view, a user requires access to the tables referenced by the view. The user must have *directly granted privileges* authorizing the access to the underlying tables. Privileges held via a role are not applicable when the server performs the object access checking on DDL statements.

Pre-defined Roles

By default Oracle8 databases contain several pre-defined roles including.:

- CONNECT — containing the system privileges to connect and create basic schema objects,
- RESOURCE — containing the system privileges necessary to create PL/SQL program units and triggers, and
- DBA — containing all system privileges WITH ADMIN OPTION.

These roles are provided for backward compatibility [SAG, 21-13] and can be modified or removed by suitably privileged users.

Session Privileges

During the database session, the privileges held by the session can vary. When a database session is initially established, it has all of the system and object privileges directly granted to the user or to PUBLIC. In addition, the session has all of the privileges granted to any default roles associated with the user. The set of privileges can be changed by

- Enabling and disabling roles,
- Accessing a view,
- Executing a stored program unit, or
- Firing a trigger as the result of a DML statement.

Enabling Roles

During a database session, a user can enable and disable any granted role. Consequently, the privileges of the database subject can be modified to reflect different requirements for access to database objects.

Views

When a user creates a view, that user must have directly granted privileges that authorise access to all of the tables (or views) referenced in the view's query. In addition, if the user holds the necessary privileges WITH GRANT option or WITH ADMIN option, then the user may grant access to the view to other database users, authorizing them for indirect access to the tables in the view. In this way, views can be used to restrict access to information based on complex SQL queries that select only the authorised data from the tables.

Stored Program Units

In order to use a stored program unit (procedure, function, or package), a user must have the privilege to EXECUTE the program unit. However, when the program unit runs, the privileges for its execution are set to the owner's directly granted privileges, not the invoker's privileges. This allows access privileges to be encapsulated with the database operations being performed by the program unit. Any user with EXECUTE privilege for the program unit is authorised to indirectly access any database objects accessible to the program unit's owner.

Triggers

The security context for the execution of triggers is similar to that of stored program units. When a trigger fires as a result of a table access, the execution privileges for the trigger are set to the trigger owner's directly granted privileges rather than the privileges of the user who initiated the table update.

Quotas

Using Oracle8 profiles, an administrative user can set quotas on the amount of processing resources a user can consume during a databases session. Limits can be specified for the following:

- enabled roles per session (via an init.ora parameter)
- database sessions per user,
- CPU time per session,
- CPU time per SQL call,
- connect time per session,
- idle time per session,
- database reads per session,
- database reads per SQL command, and
- a composite limit (based on CPU time, connect time, and database reads).

Once a profile has been created, it can be assigned to one or more users, depending on their need for processing resources. When a user exceeds the resource limit, the Oracle8 server will abort the operation, and, in some cases, terminate the user's session, or, in other cases, simply terminate current SQL statement or rollback the current transaction.

An administrative user may also set quotas on the amount of storage space that can be allocated for each user's schema objects in any specific tablespace.

Identification and Authentication

Oracle8 always identifies authorised users of an Oracle8 database prior to establishing a database session for the user. Authentication can be performed directly by the Oracle8 server using passwords managed by the server, or the server can rely on the authentication done by the underlying OS platform. The TOE covers authentication done by the underlying OS platform, in DBMS PP terms this implies that the TOE operates in OS Authentication mode.

For OS authentication, the database user connects to the Oracle8 server without specifying a user name or password. The server obtains the user's identity from the OS, and if the user is an authorised database user, a database session is created.

Special Authentication

Specially authorised users may connect to the database to perform functions such as starting up or shutting down an Oracle8 instance. These users can be authorised by either the use of a password file, or by having platform-specific access rights.

Platform-specific access rights are normally established by being a member of a special operating system group. On a UNIX platform, the group defaults to the 'dba' group but can be changed. On an NT platform, the fixed group is ORA<SID>_OPER or ORA<SID>_DBA.

When a specially authorised user wants to undertake special operations, he or she connects to the database through a special keyword: INTERNAL, AS SYSDBA or AS SYSOPER. When connected using the INTERNAL or AS SYSDBA keywords the database session then runs as the user SYS. When connected using the AS SYSOPER keyword the database session then runs as the user PUBLIC.

Auditing

Oracle8 ensures that relevant information about operations performed by users can be recorded so that the consequences of those operations can later be linked to the user in question, and the user held accountable for his or her actions. Oracle8 does this by providing auditing options which are designed to be as granular and flexible as possible to ensure that exactly what needs to be audited, as dictated by the application or system security policy, is recorded, but nothing more. This helps to ensure that the size of audit trails remain manageable and the important records easily accessible. Oracle8 provides capabilities to permit auditing plans to be quickly enabled to implement crisis responses. In addition to the standard Oracle8 auditing features described here, application-specific audit trails can be implemented using triggers to capture auditing details about the changes made to the information in the database.

Audit Categories

An administrative user can request auditing of a number of actions in each of three categories:

- *By Statement*
  Auditing specific types of SQL statements including database connections and disconnections. Statement auditing can be set to audit one, several, or all users.
- *By Object*
  Auditing specific statements on specific database objects for all users.
- *By Privilege*
  Auditing use of specific system privileges. Privilege auditing can be set to audit one, several, or all users.

Audit Options

Administrative users can further focus each auditing request by specifying auditing for only successful, only unsuccessful, or both successful and unsuccessful attempts. Such users can also specify, for most audit events, that audit records be created *by session* or *by access*: by session results in only a single record for an audited action for the duration of a database session; by access results in a record for every occurrence of an audited action.

Oracle also permits administrative users to assign default object auditing options which will automatically be used for any new schema objects which are created.

Audit Records

Oracle8 auditing permits audit information to be written to a database audit trail or to the audit trail of the underlying operating system. The Oracle8 audit records always includes the following elements when they are meaningful for the audited event:

- User;
- Session Identifier;
- Terminal Identifier;
- Name of Object Accessed;
- Operation Performed;
- Completion Code of Operation;
- Date and Timestamp;
- System Privilege Used.

Audit Analysis

If Oracle writes to the database audit trail, then the powerful SQL data manipulation facilities of the DBMS can be used by administrative users to perform selective audit

analysis of relevant database operations, user actions, uses of privilege, and object accesses in a secure manner. Oracle provides a number of pre-defined views on the database audit trail to assist in such audit analysis.

If Oracle is configured to write to an operating system audit trail, then platform services can be used to consolidate and analyse the database audit trail with audit trails from other system components to provide a comprehensive auditing portrait for the system. Alternatively, the audit data in the operating system or network services audit trail could be loaded securely into an Oracle database for comprehensive audit analysis using the SQL data manipulation facilities of the DBMS.

Auditing of SYS

No information about actions performed by users connected as the special user SYS (through the special keywords INTERNAL, AS SYSDBA and AS SYSOPER) are recorded in the Oracle8 audit trail. However, attempts to make these special connections, to startup an instance, and to shutdown an instance are always recorded. These specific audit records are written to the OS platform audit trail because they are OS events and because the database may not be available to be written into.

Since the special database user SYS owns the database audit trail table, users connected as SYS may read and write all rows in the audit trail table. Any normal user granted appropriate object privileges on the database audit trail, or appropriate system privileges, may also access the database audit trail to perform audit trail analysis and clear out old audit records, but such accesses can be audited.

Security Management

Oracle8 provides a number of mechanisms to support the management of database security. This section discusses the administrative system privileges, the importance of the initialization file, the use of CONNECT INTERNAL, AS SYSOPER and AS SYSDBA, and Oracle8 server dependencies on the administration of the underlying OS platform.

Administrative Privileges

Oracle8 contains over 80 distinct system privileges. Each system privilege allows a user to perform a particular database operation or class of database operations. If a user has no privileges then they cannot perform any operations, including connecting to the database.

Normally, ordinary users would be given a minimal set of privileges allowing them to connect to the database and access the necessary data. Other users may be given the ability to perform specific administrative functions by being granted specific system privileges.

Oracle8 security management can be delegated, therefore, to any number of users. Site-specific roles can be defined to delegate administrative responsibilities based on organisational structures.

Initialization File

When an Oracle8 instance is started, the parameters specified in an initialisation file specify operational characteristics of Oracle8 server functionality, including security functionality. It is critical that the security parameters specified in the initialization file for the instance be set to the values which conform to the evaluated configuration. The parameter values required by this security target are identified in *Oracle8 Evaluated Configuration* [EC].

SYSDBA and SYSOPER

When a user is connected as INTERNAL, AS SYSOPER or AS SYSDBA, the user is authorised to perform special database operations. Authorisation to connect as INTERNAL, AS SYSDBA or AS SYSOPER is made via OS mechanisms (i.e., membership in an OS-defined group) and requires that a user be authenticated by the OS.

A user connected AS SYSOPER is authorised to perform database startup, shutdown, and backup operations. A user connected as INTERNAL or AS SYSDBA has the same authorizations as SYSOPER with the additional capabilities to create databases and perform the operations allowed by all system privileges WITH ADMIN option. Users who connect as INTERNAL, AS SYSOPER and AS SYSDBA have access to all of the data dictionary tables (which are owned by the user SYS).

OS Administration

The security of the data managed by the Oracle8 data server is dependent not only on the secure administration of Oracle8, but also on the correct administration of the underlying OS platform and any other nodes connected in a distributed environment. The requirements on OS and network configuration for this security target are identified in *Oracle8 Evaluated Configuration* [EC]. Guidance for the correct configuration of Oracle8 for a specific OS platform is contained in the *Oracle8 Installation and Configuration Guide* [ICG] for that platform.

Other Oracle8 Security Features

In addition to the security features described above, Oracle8 provides features which are related to security but do not directly address any of the functional requirements identified in this Oracle8 Security Target. However, they provide significant security capabilities to support robust and reliable database applications:

Data Integrity

Oracle8 provides mechanisms to ensure that the consistency and integrity of data held in a database can be maintained. These mechanisms are transactions, concurrency controls, and integrity constraints. Transactions ensure that updates to the database occur in well-defined steps that move the database from one consistent state to another. Transactions and concurrency controls together ensure that multiple users can have shared access to the database with consistent and predictable results: each user sees a consistent state of the database and can make updates without interfering with other users. Integrity constraints ensure that the values of individual data items are of the defined type and within defined limits, and that defined relationships between database tables are properly maintained.

Import/Export

It is important to ensure that data can be moved out of one database and re-inserted into the same or a different database while maintaining the data integrity and confidentiality. Oracle enables secure exporting of information from a database into an operating system file. Only appropriately privileged users may export information to which they do not normally have read access. Similarly, Oracle enables secure importing of information into a database from Oracle-generated operating system export files. Only appropriately privileged users may import information into database tables to which they do not normally have write access.

When a database object is exported, the list of users having object privileges to access the object can also be exported and then imported into the new database with the database object.

Backup and Recovery

Backup of an Oracle8 database can be performed using platform-specific backup programs, the Oracle8 import/export utilities, or the Oracle8 recovery manager. The choice of mechanism depends upon the application needs, but all approaches can provide secure, reliable backup and recovery of the database.

The Oracle8 transaction integrity mechanisms also provide the basis for secure recovery following the failure of an Oracle8 instance or platform operating system. Whenever an Oracle8 instance is started, any transactions that were not committed prior to the failure are rolled back. This returns all of the information in the database, including the data dictionary tables, to a consistent and secure state.

Secure Distributed Processing

The basic distributed features included in the Oracle8 server make use of database links to define a connection path to a remote Oracle database. When a connection is made to a remote database, the information in the database link definition is used to provide identification and authentication information to the remote Oracle server. The remote server creates a database session for the user specified by the database link (if the user is authorised for access to the remote database) and then makes its access control decisions based on that identity and its privileges *in the remote database*.

By using database links to qualify schema object names, a user in a local database can

- select (e.g., join) data from tables in any number of remote Oracle databases,
- use DML statements to update tables in remote Oracle databases (Oracle8 automatically implements a two-phase commit protocol), and
- execute stored program units in remote Oracle databases.

Access to the remote database is transparent; however careful administration and control of the distributed environment is essential [SD1].

Oracle add-on products include the Advanced Networking Option and the Oracle Security Server. The Advanced Networking Option provides encryption of the Oracle network traffic between clients and servers and between two communicating servers and adaptors for various external authentication services and certificate authorities. The Oracle Security Server supports global authentication and global management of Oracle roles.

Supplied Packages

A number of standard packages are available to install in an Oracle8 database. These provide supportive functionality that can be invoked by other users and applications. They provide the following types of functions:

- Access to SQL features from PL/SQL programs, including dynamic SQL,
- Alert mechanisms for asynchronous notification of database events,
- File access functions to read and write OS files,
- Job queues for scheduling repeating administrative procedures,
- Lock management functions for user-defined locks,
- Oracle pipes for communication among database sessions,
- Output operations for procedure debugging,
- Functions to manipulate LOBs,
- Queues for asynchronous message generation and delivery (Advanced Queuing),
- Administration of distributed transactions and snapshots, and
- HTTP callouts to access Web services.

External Authentication Services

In addition to the standard Oracle8 database authentication and OS authentication methods described above, Oracle8 can be configured to use an external third party authentication service.

CHAPTER

3 Security Environment

Threats

As per [DPP, 3.2].

Organisational Security Policies

As per [DPP, 3.3];

Assumptions

The TOE operates in OS Authentication mode as per [DPP, 1.2]

As per [DPP, 3.4] with the following modifications and additions:

A.TOE.CONFIG The TOE is installed, configured and managed in accordance with [ECD], its evaluated configuration.

A.OSA All database user accounts are configured to use OS Authentication (by using the *identified externally* SQL clause).

A.TOE.DBA In accordance with A.MANAGE [DPP, 3.4.2.2], there will be one or more competent (or “trusted) individuals assigned to manage the TOE and the security of the information it contains who can be trusted not to abuse their privileges. In accordance with A.TOE.CONFIG and A.OSA, these trusted users are required to use Oracle Server Manager for all privileged connections to the TOE.

This Page Intentionally Blank

CHAPTER

4 Security Objectives

TOE Security Objectives

As per [DPP, 4.1].

Environmental Security Objectives

As per [DPP, 4.2].

This Page Intentionally Blank

CHAPTER

5 IT Security Requirements

TOE Security Functional Requirements

Table 4 below lists each Security Functional Requirement (SFR) included in this Security Target and identifies which Common Criteria operations (assignment (A), selection (S), refinement(R),and/or iteration (I)) have been applied to the requirement relative to the DBMS Protection Profile [DPP] in OS Authentication mode.

The remainder of this section details the functional requirements as completed for this Security Target. The text for completed operations is highlighted with *ITALICISED CAPITAL LETTERS* within each requirement. Annex B provides definitions for various terms used in the functional requirements.

Table 4: List of Security Functional Requirements

Component	Name	A	S	R	I
FAU_GEN.1	Audit Data Generation	X		X	
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit Review				
FAU_SAR.3	Selectable Audit Review	X			
FAU_SEL.1	Selective Audit	X			
FAU_STG.1	Protected Audit Trail Storage				
FAU_STG.4	Prevention of Audit Data Loss	X	X		
FDP_ACC.1	Subset Access Control				
FDP_ACF.1	Securitiy Attribute Based Access Control	X			
FDP_RIP.2	Full Residual Information Protection				

Component	Name	A	S	R	I
FIA_ATD.1	User Attribute Definition	X			
FIA_UID.1	Timing of Identification	X		X	
FIA_USB.1	User-Subject Binding				
FMT_MSA.1	Management of Security Attributes	X			
FMT_MSA.3	Static Attribute Initialisation	X			
FMT_MTD.1	Management of TSF Data	X		X	
FMT_REV.1	Revocation	X			
FMT_SMR.1	Security Roles	X			
FPT_RVM.1	Non-Bypassability of the TSP				
FPT_SEP.1	TSF Domain Separation				
FRU_RSA.1	Maximum Quotas	X			
FTA_MCS.1	Basic Limitation on Multiple Concurrent Sessions	X			
FTA_TSE.1	TOE Session Establishment	X			

Security Audit

FAU.GEN.1.1 The TSF shall be able to generate a database audit record of the following auditable events:

a) Start-up and shutdown of the database audit functions;
b) All auditable events for the basic level of audit as identified in Table 4 of [DPP]; and
c) *NO ADDITIONAL EVENTS.*

FAU.GEN.1.2 The TSF shall record within each database audit record at least the following information:

a) Date and time of the database event, type of database event, database subject identity, and the outcome (success or failure) of the event; and
b) For each database audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *OTHER RELEVANT INFORMATION AS IDENTIFIED IN TABLE 4 OF [DPP].*

FAU.GEN.2.1 The TSF shall be able to associate each auditable database event with the identity of the database user that caused the event.

FAU.SAR.1.1 The TSF shall provide authorised database users with the capability to read all database audit information from the database audit records.

FAU.SAR.1.2 The TSF shall provide the database audit records in a manner suitable for the database user to interpret the information.

FAU.SAR.3.1 The TSF shall provide the ability to perform searches and sorting of database audit data based on *THE VALUES OF AUDIT DATA FIELDS*.

FAU.SEL.1.1 The TSF shall be able to include or exclude auditable database events from the set of audited database events based on the following attributes:

a) event type;
b) database subject identity;
c) database object identity;
d) *DATABASE SYSTEM PRIVILEGE*.

FAU.STG.1.1 The TSF shall protect the stored database audit records from unauthorised deletion.

FAU.STG.1.2 The TSF shall be able to prevent modifications to the database audit records.

FAU.STG.4.1 *THE TSF SHALL PREVENT DATABASE AUDIT EVENTS, EXCEPT THOSE TAKEN BY THE AUTHORIZED DATABASE USER WITH SPECIAL RIGHTS, IF THE AUDIT TRAIL IS FULL.*

User Data Protection

FDP.ACC.1.1 The TSF shall enforce the database object access control SFP on:

a) database subjects;
b) database objects;
c) all permitted operations on database objects by database subjects covered by the SFP.

FDP.ACF.1.1 The TSF shall enforce the database object access control SFP to database objects based on:

a) the identity of the owner of the database object; and
b) the object access privileges to the database object held by the database subject; and
c) the database administrative privileges of the database subject.

FDP.ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled database subjects and controlled database objects is allowed:

a) if the user associated with the database subject is the owner of the database object, then the requested access is allowed; or
b) if the database subject has the database object access privilege for the requested access to the database object, then the requested access is allowed; or
c) otherwise access is denied, unless access is explicitly authorised in accordance with the rules specified in FDP.ACF.1.3.

FDP.ACF.1.3 The TSF shall explicitly authorise access of database subjects to database objects based on the following additional rules:

a) if the database subject has a database administrative privilege to override the database object access controls for the requested access to the database object, then the requested access is allowed;
b) *IF THE SUBJECT IS CONNECTED AS INTERNAL OR AS SYSBDA THEN THE REQUESTED ACCESS IS ALLOWED; OR*
c) *IF THE SUBJECT IS CONNECTED AS SYSOPER AND THE REQUESTED ACTION IS ONE OF OPERATIONS*

PERMITTED FOR THE SYSOPER USER SPECIFIED IN [SAG, 1-8], THEN THE REQUESTED ACCESS IS ALLOWED.

FDP.ACF.1.4 The TSF shall explicitly deny access of database subjects to database objects based on the following additional rules: NONE.

FDP.RIP.2.1 The TSF shall ensure that any previous information content of a database resource is made unavailable upon the allocation of a resource to all database objects.

Identification and Authentication

Note that user authentication is provided by the OS as database authentication is beyond the scope of this evaluation. Assumption A.I&A ensures that users are identified and authenticated prior to any interaction with the TOE.

FIA.ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual database users:

a) database user identity;
b) database object access privileges;
c) database administrative privileges;
d) *ORACLE ROLES*.

FIA.UID.1.1 The TSF shall allow *THE FOLLOWING LIST OF ACTIONS* on behalf of the database user before the database user is identified:

a) OBTAIN THE CURRENT ORACLE VERSION STRING AND NUMBER;
b) ESTABLISH A DATABASE CONNECTION; AND
c) RECEIVE ERROR MESSAGES UPON ERROR..

FIA.UID.1.2 The TSF shall require each database user to be successfully identifed before allowing any other TSF-mediated actions on behalf of that database user.

FIA.USB.1.1 The TSF shall associate the appropriate database user security attributes with database subjects acting on behalf of that database user.

Security Management

FMT.MSA.1.1 The TSF shall enforce the database object access control SFP to restrict the ability to modify the database object security attributes:

a) *DATABASE OBJECT ACCESS PRIVILEGES* to *THE OBJECT'S OWNER AND OTHER DATABASE USERS AUTHORIZED BY THE OWNER.*
b) *DATABASE SYSTEM PRIVILEGES* to *USERS WHO HAVE BEEN GRANTED THAT PRIVILEGE WITH ADMIN OPTION OR USERS WHO CONNECT INTERNAL OR AS SYSDBA*.
c) *DATABASE ROLES* to *DATABASE USERS AUTHORIZED TO MODIFY ROLES*.

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

FMT.MSA.3.2 The TSF shall allow *NO DATABASE USERS* to specify alternative initial values to override the default values when a database object is created.

FMT.MTD.1.1 The TSF shall according to table 5 OF [DPP] restrict the ability to perform operations on TSF data to database administrative users.

FMT.REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the database users and database objects within the TSC to:

a) authorised database administrators (for users and objects);
b) authorised database users (only for the database objects they own or database objects for which they have been granted database object access privileges allowing them to revoke security attributes);
c) *NO OTHER ROLES.*

FMT.REV.1.2 The TSF shall enforce the *FOLLOWING* rules:

a) revocation of database object access privileges shall take effect prior to all subsequent attempts to establish access to the database object;
b) revocation of database administrative privileges shall take effect prior to when the user begins the next database session;
c) *NO ADDITIONAL REVOCATION RULES.*

FMT.SMR.1.1 The TSF shall maintain the database roles:

a) database administrative user;
b) database user;
c) *DATABASE ROLES DEFINED BY SUITABLY PRIVILEGED DATABASE ADMINISTRATIVE USERS*.

Note that due a difference in terminology between the CC and the Oracle8 product the two occurrences of the word "role" in FMT.SMR.1.1 have different meanings. The first occurrence, which is part of the required CC wording, is general term meaning any kind of user that can be created within the TSF. The second occurrence, which is part of a completed assignment in [DPP], is a specific term refering to Oracle8 database roles that can be configured and granted to users of the Oracle8 product.

FMT.SMR.1.2 The TSF shall be able to associate database users with database roles.

Protection of the TOE Security Functions

FPT.RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within theTSC is allowed to proceed.

FPT.SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted database subjects.

FPT.SEP.1.2 The TSF shall enforce separation between the security domains of database subjects in the TSC.

Resource Utilisation

FRU.RSA.1.1 The TSF shall enforce maximum quotas of the following resources:
a) CPU_TIME;
b) ELAPSED TIME;
c) LOGICAL DATA BLOCKS READ; AND
d) DATABASE STORAGE ALLOCATED.

that an individual database user can use over a specified period of time:

TOE Access

FTA.MCS.1.1 The TSF shall restrict the maximum number of concurrent database sessions that belong to the same database user.

FTA.MCS.1.2 The TSF shall enforce, by default, a limit of *A NUMBER, CONFIGURED BY AN AUTHORIZED ADMINISTRATIVE USER,* sessions per database user.

FTA.TSE.1.1 The TSF shall be able to deny database session establishment based on *USER IDENTITY*.

Note that the DBA and OPER users can always connect to the database.

TOE Security Assurance Requirements

The target assurance level is EAL4 as defined in Part 3 of the CC. No augmented assurance requirements are defined.

Security Requirements for the IT Environment

As per [DPP 5.3 & 5.6].

Minimum Strength of Function

There are no TOE security functional requirements or IT security functions for which a Strength of Function claim is appropriate, however the Strength of Function claim for the composite system is *SOF-Medium.*

CHAPTER

6 TOE Summary Specification

TOE Security Functionality

This section contains a high-level specification of each TOE Security Function (TSF) that contributes to satisfaction of the Security Functional Requirements of chapter 5. The specifications cover five major areas: identification and authentication, object access controls, resource quotas, privileges and roles, and auditing. Table 5 below shows that all the SFRs are satisfied by at least one TSF and that every TSF is used to satisfy at least one SFR.

Table 5: Mapping of TSFs to SFRs

	FIA				FDP						FMT								FPT			FRU	FTA			FAU									
	ATD.1.1	UID.1.1	UID.1.2	USB.1.1	ACC.1.1	ACF.1.1	ACF.1.2	ACF.1.3	ACF.1.4	RIP.2.1	MSA.1.1	MSA.3.1	MSA.3.2	MTD.1.1	REV.1.1	REV.1.2	SMR.1.1	SMR.1.2	RVM.1.1	SEP.1.1	SEP.1.2	RSA.1.1	MCS.1.1	MCS.1.2	TSE.1.1	GEN.1.1	GEN.1.2	GEN.2.1	SAR.1.1	SAR.1.2	SAR.3.1	SEL.1.1	STG.1.1	STG.1.2	STG.4.1
F.IA.PRE		Y	Y																															
F.IA.UID			Y														Y																	
F.IA.OSA			Y																															
F.IA.CNF							Y																											
F.IA.IDE			Y																Y	Y	Y													
F.IA.CSA			Y														Y	Y						Y										
F.IA.CSN			Y														Y							Y										
F.IA.ATT	Y			Y										Y																				
F.LIM.CNF														Y	Y						Y													
F.LIM.POL																					Y		Y											
F.LIM.NSESS																					Y	Y	Y											
F.LIM.TIME																					Y													
F.LIM.RSESS																					Y													
F.LIM.RCALL																					Y													
F.DAC.OBID					Y	Y	Y																											
F.DAC.OBREF					Y	Y	Y																											
F.DAC.SUA					Y	Y																												
F.DAC.OBA					Y	Y							Y																					
F.DAC.POL						Y	Y	Y				Y	Y						Y															
F.DAC.SEP																				Y	Y													
F.DAC.OR										Y																								
F.APR.GOP											Y		Y	Y																				
F.APR.ROP											Y			Y	Y																			
F.APR.GRSP											Y		Y	Y	Y																			
F.APR.GRR											Y		Y	Y	Y		Y																	
F.APR.DER																		Y																
F.APR.EDR				Y														Y																
F.PRI.SPRIV				Y		Y	Y	Y				Y				Y																		
F.PRI.XVP				Y																														
F.AUD.SOM																									Y						Y			
F.AUD.SEV																									Y						Y			
F.AUD.ALW																									Y						Y			
F.AUD.CNF							Y	Y																							Y			
F.AUD.ACC														Y														Y		Y				
F.AUD.DEL														Y																		Y	Y	
F.AUD.INF																										Y	Y							
F.AUD.VIEW																														Y	Y			
F.AUD.FULL																																		Y

Identification and Authentication

F.IA.PRE Oracle shall only allow users to:

a) obtain the current Oracle version string and version number;

b) establish a connection;

c) receive error messages upon error.

before identifying and authenticating the user.

F.IA.UID Each database user is uniquely identified.

F.IA.OSA <u>OS Identification and Authentication:</u>

If a user is configured in the TOE as being *identified externally* then the TOE will identify and authenticate the user by confirming that the requesting subject's OS user identifier,

prefixed by the value of the OS_AUTHENT_PREFIX initialisation parameter, matches a database user identifier.

Note that in F.IA.OSA the TOE is not performing any authentication, per se. Rather the TOE is dependent on the OS to correctly authenticate the user.

F.IA.CSN The TOE will create a database session as a normal user only if the CREATE SESSION privilege is held by the database user and the TOE has identified and authenticated the user as a valid database user (by OS identification and authentication).

F.IA.IDE For each interaction between a user and the TOE following the successful creation of a database session, the TOE is able to establish the identity of the user. A subject can only submit requests to a Server and receive responses (information) from a Server while the subject is establishing a connection or connected to an instance during the course of a database session.

F.IA.CSA The TOE will create a database session as a SYSDBA user or SYSOPER user only if the user is authenticated using OS authentication and the requesting subject has the platform-specific access rights for OSDBA and OSOPER, respectively, as defined in [SAG, 1-6].

F.IA.CNF The TOE will allow only a suitably authorised user to create a database user.

F.IA.ATT The data dictionary contains a unique set of security attributes for each user including their username, privileges, roles and resource limits that can be displayed and modified by suitably privileged users using standard SQL commands.

Access Control

Database Resources

F.LIM.CNF The TOE will allow only a suitably authorised user to:

a) alter the default Resource Profile for a database;

b) create and alter specific Resource Profiles and assign and reassign them to each individual database users.

F.LIM.POL When a user attempts to use a database resource that is subject to controls specified by Resource Profiles, the TOE will enforce the limits specified by the resource profile (if any) explicitly assigned to the user, otherwise it enforces the limits specified by the default Resource Profile for the database.

F.LIM.NSESS The TOE prevents a user from creating more than the maximum number of concurrent sessions specified for that user for an instance of the TOE.

F.LIM.TIME If a user exceeds the specified CONNECT_TIME or IDLE_TIME resource limits by the (OS specific) amount for a single session then the TOE will terminate the session when the user attempts an operation.

F.LIM.RSESS If a user attempts to perform an operation that exceeds the specified resource limits for a single session then the TOE will:

a) terminate the operation;

b) force the termination of the session.

F.LIM.RCALL If a user attempts to perform an operation that exceeds the specified resource limits for a single SQL statement then the TOE will terminate the operation.

Object Access Control

F.DAC.OBID The TOE ensures that every object created in a database is uniquely identified in that database. Specifically, each schema object owned by a normal user is uniquely identified within the user's schema[1].

F.DAC.OBREF The TOE correctly resolves every reference to a database object that conforms to the Object naming rules specified in [SQL, chapter 2], including references via database links[2].

F.DAC.SUA For normal users, the TOE enforces DAC on database objects based on the following subject attributes:

a) the identity of the user associated with the database session;

b) the system privileges and object privileges which are effective for the database session.

F.DAC.OBA For normal users, the TOE enforces DAC on database objects based on the following object attributes:

a) the identity of the owner of the object;

b) the object privileges which have been granted on the object.

F.DAC.POL The TOE enforces the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) If the user is the owner of the object then the requested access is allowed.

b) If the database session has the necessary object privileges effective for the object then the requested access is allowed. The object privileges relevant to different types of objects are specified in [SAG, Chapter 21 Object Privileges], and provide the ability to restrict a user's access to an object to those operations which do not modify the object.

c) If the database session has the necessary system privileges effective then the requested access is allowed. The system privileges relevant to different types of database-wide and

1. The owner of an object is the owner of the schema containing the object, not necessarily the user who created the object. More precisely, unique identification is by object type as well as object name within a schema.

2. A reference to a database link (e.g. CONNECT /@otherdb or SELECT * FROM TBL@otherdb) will be correctly resolved to the referenced database. A database object can be uniquely identified in a distributed system, because it is uniquely identified in the database, and the database is unique in the system. The threat is that failure to uniquely identify objects and user accounts could result in reading, creating, modifying or destroying the wrong object (or copy of an object) if the user has the same access rights in each database.

schema-specific operations are specified in [O7_SAG] Chapter 13 System Privileges, and provide the ability to restrict a user's use of operations to those operations which do not modify objects.

d) If the user is the DBA user (the database session has the privilege to override the access controls) then the requested access is allowed.

e) If the user is the OPER user and the operation is one of those specified in [SAG, Chapter 1 OSOPER and OSDBA], for the OSOPER role then the requested access is allowed.

F.DAC.SEP The TOE does not allow interference between concurrent database sessions.

F.DAC.OR Upon allocation of a resource to schema and non-schema objects, any previous information is unavailable. In Oracle, there is no way to access an object once it has been deleted, i.e. the resources have been returned to the TOE. This is because any references to it no longer exist and, even if they were recreated, they would never be associated with the previous, non-existent object.

All objects have a unique ID. Even if a deleted object is recreated using the same name, the object ID would be different.

Schema and non-schema objects are defined in [SQL, 2]. Every object in the TOE is categorised as either a schema or non-schema object.

Privileges and Roles

Granting and Revoking Privileges and Roles

F.APR.GOP A normal user (the grantor) can grant an object privilege to another user, role or PUBLIC (the grantee) only if:

a) the grantor is the owner of the object; *or*

b) the grantor has been granted that object privilege with the GRANT OPTION.

F.APR.ROP A normal user (the revoker) can revoke an object privilege from another user, role or PUBLIC (the revokee), and any further propagation of that object privilege started by the revokee, only if the revoker is the original grantor of the object privilege.

F.APR.GRSP A user (the grantor) can grant a system privilege to another user, role or PUBLIC (the grantee), and revoke a system privilege from the grantee, only if:

a) the grantor (or revoker) is the DBA user; *or*

b) the database session of the grantor (or revoker) has the GRANT ANY PRIVILEGE privilege effective; *or*

c) the grantor (or revoker) has been granted that system privilege directly with the ADMIN OPTION.

F.APR.GRR A user (the grantor) can grant a role to another user, role or PUBLIC (the grantee), and revoke a role from the grantee, only if:

a) the grantor is the DBA user; *or*

b) the database session of the grantor (or revoker) has the GRANT ANY ROLE privilege effective; *or*

c) the grantor (or revoker) has been granted that role with the ADMIN OPTION[1].

Enabling and Disabling Roles

F.APR.DER A role can be granted to a user in one of the following ways:

a) As a non-default role, in which case the user must explicitly enable the role during a database session in order for any other roles within that role to be enabled and any privileges within that role to become effective for that user.

b) As a default role, in which case the role will be enabled automatically for each database session created by that user.

F.APR.EDR During a database session the user can control which roles are effective at any time during the course of the database session by enabling and disabling the roles which have been granted to that user (where the role may have been granted directly to the user or granted indirectly to the user through other roles[2]), subject to the following restrictions which apply to implicit remote sessions:

a) The non-default roles granted to a user in a remote database cannot be enabled while the user is connected to the remote database.

b) The default roles granted to a user in a remote database cannot be disabled while the user is connected to the remote database.

Effective Privileges

F.PRI.SPRIV A privilege will be effective in a user session only if:

a) the privilege was granted to the user directly and has not been revoked from the user; *or*

b) the privilege was granted indirectly via the PUBLIC user group and has not been revoked from PUBLIC; *or*

c) the privilege was granted to the user indirectly via a role, and has not been revoked from that role and the role is effective in the current session.

F.PRI.XVP A suitably authorised user can provide other users with access to proxy mechanisms (namely Views and Program Units) which will act on behalf of the owning user (by executing with the privileges of the owning user) to allow other users to have controlled access to specified aggregations of data.

---

1. This includes the case where the grantor is the user who created the role - see [OR_SAG] p.12-16: "When a user creates a role, the role is automatically granted to the creator with the ADMIN OPTION." and the warning on p.12-12 (Set Default Roles) which adds the fact that a role is automatically granted to its creator as a default role.

2. When a role that contains other roles is enabled all the indirectly granted roles are implicitly enabled.

Audit and Accountability

F.AUD.SOM When standard auditing is enabled (as DBMS or OS Auditing) for an instance, the TOE will:

a) write an audit record for every occurrence of an auditable event other than CONNECT and DISCONNECT; and

b) write an audit record for every pair of CONNECT/ DISCONNECT events.

F.AUD.SEV The TOE will allow a suitably authorised user to specify which events for a database are auditable, as follows:

a) by use of DDL statements, for all users or for specified users;

b) by use of DML statements;

i. for specified Object Privilege Objects;

ii. for all Object Privilege Objects subsequently created, by default;

c) by use of system privileges, for all users or for specified users;

d) for each event of type b) by session or by access, i.e. only one audit record written for each auditable event that occurs in the same session or one audit record written for each auditable event. For events of type c) by session or by access, unless a DDL statement when always by access;

e) for each event of type a), b) and c) by outcome, i.e. success, failure, or both.

F.AUD.ALW If an operating system audit trail is provided and is enabled, and irrespective of the TOE's audit configuration, the TOE will audit every successful occurrence of the following events to the operating system audit trail:

a) start-up;

b) shut-down;

c) successful connection through the keywords INTERNAL, AS SYSDBA or AS SYSOPER.

F.AUD.CNF The TOE will allow only a suitably authorised[1] user to set or alter the audit configuration for a database.

F.AUD.ACC The TOE will allow suitably authorised users to select by criteria audit information from the database audit trail, as follows:

a) any suitably privileged user can view all audit records;

b) the owner of an object can view the audit records relating to that object.

1. By default (after installation), the TOE allows only the DBA user, SYS and SYSTEM (who are granted the DBA role during installation) to set and alter the audit configuration. It is possible for these users to grant the relevant privileges to other users, but it is assumed that they will not do this in practice.

F.AUD.DEL The TOE will allow only a suitably authorised[1] user to delete or update audit records from the Database Audit Trail.

F.AUD.INF The TOE will record the following information into each Database Audit Trail record, provided that the information is meaningful to the particular audited event:

Date and time of event; username; instance ID for the Oracle instance where the user is accessing the database; session identifier; terminal identifier of the user's terminal; name of object accessed; operation performed or attempted; outcome of the operation; system privileges used.

In particular:

a) when a user attempts a connections to a database, whether successful or not, at least the following information is recorded when the TOE is configured to audit connection attempts: date and time of event, username, instance ID for the Oracle instance where the user is accessing the database, session identifier, terminal identifier of the user's terminal, outcome of the connection attempt;

b) when a user attempts to access any database object, whether successful or not, at least the following information is recorded when the TOE is configured to audit such access attempts: date and time of event, username, name of object accessed, operation performed or attempted, outcome of the operation;

c) when a user attempts to create or drop any database object, whether successful or not, at least the following information is recorded when the TOE is configured to audit such create or drop actions: date and time of event, username, name of object to be created or dropped, operation performed or attempted, outcome of the operation;

d) when a user attempts to affect the security of the TOE, by, for example, startup up and shutting down an instance of the TOE, creating new, modifying existing or dropping old user accounts, tablespaces, databases, rollback segments, etc. as the TOE permits at least the following information is recorded when the TOE is configured to audit such actions: date and time of event, username, name of object accessed, operation performed or attempted, outcome of the operation.

F.AUD.VIEW Oracle provides both the SQL language and built-in views, based on the underlying audit trail table SYS.AUD$, with the ability to both view and search the audit data.

1. By default, the TOE allows only the DBA user, SYS and SYSTEM (who are granted the DBA role during installation) to delete or update rows from SYS.AUD$. It is possible for these users to grant the relevant privileges to other users, but it is assumed that they will not do this in practice.

F.AUD.FULL With DBMS auditing, if the tablespace containing the audit trail table becomes full, no further auditable actions can occur until space is made available.

Security Mechanisms and Techniques

No specific security mechanisms or techniques are claimed or required for this TOE.

Assurance Measures

The target assurance level is EAL4, which exceeds the assurance requirement of EAL3 as stated in [DPP]. No specific assurance measures are claimed. The following table identifies the Oracle8 documentation that supports each security assurance requirement for EAL4.

Table 6: Oracle8 Assurance Measures

Component	Name	Documents
ACM_AUT.1	Partial CM Automation	[CM]
ACM_CAP.4	Generation Support and Acceptance Procs	[CM]
ACM_SCP.2	Problem Tracking CM Coverage	[CM]
ADO_DEL.2	Detection of Modification	[OSQM]
ADO_IGS.1	Installation, Generation, and Startup	[ICG]
ADV_FSP.2	Fully Defined External Interfaces	[ADG] [ERR] [FS] [SQL]
ADV_HLD.2	Security Enforcing High-level Design	[AD] [OSD]
ADV_IMP.1	Subset of the TSF Implementation	[SRC]
ADV_LLD.1	Descriptive Low-level Design	[DD]
ADV_RCR.1	Informal Correspondence Demonstration	[AD] [DD] [FS] [SRC]
ADV_SPM.1	Informal TOE Security Policy Model	[SPM]
AGD_ADM.1	Administrator Guidance	[EC] [GA] [ICG] [SAD] [SRB]
AGD_USR.1	User Guidance	[GA]
ALC_DVS.1	Identification of Security Measures	[SODE]

Component	Name	Documents
ALC_LCD.1	Developer Defined Life Cycle Model	[PRP]
ALC_TAT.1	Well Defined Development Tools	[CM]
ATE_COV.2	Analysis of Coverage	[TP]
ATE_DPT.1	Testing - High-level Design	[TP]
ATE_FUN.1	Functional Testing	[TP]
ATE_IND.2	Independent testing - sample	[TP]
AVA_MSU.2	Validation of Analysis	[GA]
AVA_SOF.1	Strength of TOE Security Functions	[SOFA]
AVA_VLA.2	Independent Vulnerability Analysis	[VA]

CHAPTER

7 Protection Profile Claims

PP Reference

The TOE conforms to the Database Management System Protection Profile (DBMS PP) [DPP] and operates in OS Authentication Mode.

PP Tailoring

Table 4 in chapter 5 identifies each Security Functional Requirement for this Security Target and the tailoring operations performed relative to the DBMS Protection Profile. The tailoring is identified in *ITALICISED CAPITAL LETTERS* within the text of each Security Functional Requirement in chapter 5. All of the tailoring operations are in conformance with the assignments and selections in the DBMS PP.

PP Additions

There are no additional threats, organisational security policies, assumptions or objectives included in this security target.

A reference to [ECD] has been added to the assumption A.TOE.CONFIG. This does not change the meaning of the assumption. Rather it merely points to a specific document where the evaluated configuration, which is refered to in the assumption is defined.

Assumption A.OSA has been added to ensure that all users of the TOE are configured to use OS authentication. The addition of this assumption ensures that the Security Target is consistent with the TOE security objective O.I&A [DPP, 4.1]. This objective states that the TOE must provide a means of identifying and authenticating users with or without the support of the underlying system. For this evaluation, identification and authentication of users is performed with the support of the underlying OS. Therefore, the inclusion of this assumption maintains PP compliance.

Security Functional Requirement FAU_SAR.3.1 in [DPP, 5.1.1] stipulates that searching and sorting of the database audit trail shall be provided on the basis of user

identity. FAU_SAR.3.1 in this security target extends this to allow searching and sorting on the basis of the values of the audit data fields, thus implictly covering the requirement of [DPP, 5.1.1].

The assurance requirement specified in this security target is EAL4. This includes all assurance requirements in the DBMS PP (which mandates EAL3).

CHAPTER

8 Rationale

Security Objectives Rationale

As per [DPP, 6.1].

Security Requirements Rationale

Security Requirements Satisfy the Security Objectives

There are no additional IT security objectives. Therefore, the ST complies fully with the DBMS PP; see [DPP, 6.2, 6.3, and 6.4] for further information.

Strength of Function Validity

The minimum strength of function for the TOE as a composite system is *SOF-medium* to ensure compliance with [DPP, 5.5, 5.8 and 6.6]. The DBMS component uses the OS authentication and therefore in itself, has no critical security enforcing mechanisms which are open to direct attack. Therefore, no security function exists which has a vulnerability in the concept of its underlying mechanisms. Therefore, no claims are made for a minimum strength of function for the DBMS.

Assurance Measures Compliant with Requirements

The target assurance level is EAL4, which exceeds the assurance requirement of EAL3 as stated in [DPP]. No augmented assurance requirements are defined. See [DPP] for further information.

TOE Summary Specification Rationale

This section demonstrates that the TOE Security Functions and Assurance Measures are suitable to meet the TOE security requirements.

TOE Security Functions Satisfy Requirements

Table 5 of chapter 6 identifies the Oracle8 TOE Security Functions that address each of the SFRs in chapter 5.

Table 8 demonstrates for each SFR, the TOE security functions are suitable to meet

the SFR and the combination of TOE security functions work together so as to satisfy the SFR:

SFR	TOE Security Functions	Rationale
FIA.ATD.1.1	F.IA.ATT	The data dictionary stores the required security attributes
FIA.UID.1.1	F.IA.PRE	F.IA.PRE satisfies FIA.UID.1.1 directly.
FIA.UID.1.2	F.IA.PRE F.IA.UID F.IA.OSA F.IA.IDE F.IA.CSA F.IA.CSN	F.IA.CSN and F.IA.CSA state the conditions for being able to establish a database session and hence perform TSF-mediated actions. These security functions depend directly on F.IA.OSA. F.IA.PRE is relevant as one of the actions allowed prior to session creation is attempting to establish a session. F.IA.PRE ensures that the identity of the user is known for the duration of the session, once created.
FIA.USB.1.1	F.IA.ATT F.APR.EDR F.PRI.SPRIV F.PRI.XVP	F.IA.ATT provides the security attributes for each user. The effective security attributes for a database session are controlled by F.APR.EDR and F.PRI.SPRIV. In addition the TSF provides support for views and program units which act on behalf of the owning user. F.PRI.XVP defines the security attributes associated with these items.
FDP.ACC.1.1	F.DAC.OBID F.DAC.OBREF F.DAC.SUA F.DAC.OBA	F.DAC.OBID and F.DAC.OBREF ensures that all objects (which are subject to DAC) can be uniquely identified. F.DAC.SUA and F.DAC.OBA state that the DAC policy extends to all subjects and objects.
FDP.ACF.1.1	F.DAC.OBID F.DAC.OBREF F.DAC.SUA F.DAC.OBA F.DAC.POL F.PRI.SPRIV	F.DAC.OBID and F.DAC.OBREF ensures that all objects (which are subject to DAC) can be uniquely identified. F.DAC.SUA includes the subject and their enabled privileges (as specified in F.PRI.SPRIV) in the DAC policy. F.DAC.OBA states that the object and any associated object privileges are considered by the DAC policy. F.DAC.POL is a statement of the DAC policy.
FDP.ACF.1.2	F.IA.CNF F.DAC.OBID F.DAC.OBREF F.DAC.POL F.PRI.SPRIV F.AUD.CNF	F.DAC.POL a) and b) specifies access to objects based on ownership or object privileges. F.DAC.OBID and F.DAC.OBREF are relevant as they define object ownership which is the basis of the DAC policy. FPRI.SPRIV is relevant as it defines which privileges are enabled for any user. F.IA.CNF and F.AUD.CNF are relevant I&A data and the audit trail are subject to the DAC policy.
FDP.ACF.1.3	F.DAC.POL F.PRI.SPRIV F.AUD.CNF	F.DAC.POL c) specifies access to objects based on enabled system privileges. F.DAC.POL d) and e) cover access as the special users SYSDBA and SYSOPER. F.SPRIV is relevant as it defines which privileges are enabled for any user. F.AUD.CNF is relevant as the audit trail is subject to the DAC policy
FDP.ACF.1.4	N/A	This SFR does not claim any functionality. It is included for compliancy with the CC.
FDP.RIP.2.1	F.DAC.OR	F.DAC.OR satisfies FDP.RIP.2.1 directly.

Table 7: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FMT.MSA.1.1	F.APR.GOP F.APR.ROP F.APR.GRSP F.APR.GRR	F.APR.GOP and F.APR.ROP cover FMT.MSA.1.1 a) which is concerned with modifying object privileges. F.APR.GRSP covers FMT.MSA.1.1 b) which is concerned with modifying system privileges. F.APR.GRR covers FMT.MSA.1.1 c) which is concerned with modifying roles.
FMT.MSA.3.1	F.DAC.POL F.PRI.SPRIV	F.DAC.POL and F.PRI.SPRIV implicitly include restrictive default values. If a user has not been explicitly granted the necessary privlege or a role containing the required privilege then the requested action will not succeed.
FMT.MSA.3.2	F.DAC.SUA F.DAC.OBA F.DAC.POL F.APR.GOP F.APR.ROP F.APR.GRR	As no database users can specify alternative initial values, there is no direct mapping to a corresponding TSF. On object creation no object privileges are granted and it is not possible to configure this to be the case. Unless access to an object has been explicitly granted, as described in F.DAC.OBA, F.APR.GOP, F.APR.ROP and F.APR.GRR, no access will be allowed. Access to an object is enforced by F.DAC.SUA, F.DAC.OBA, and F.DAC.POL.
FMT.MTD.1.1	F.IA.ATT F.LIM.CNF F.APR.GOP F.APR.ROP F.APR.GRSP F.APR.GRR F.AUD.ACC F.AUD.DEL	These TOE security functions are concerned with the modification of TSF data (security attributes and audit data). This data is stored in the data dictionary and is protected from unauthorised access by the same mechanism as all other data in the database. F.IA.ATT and F.LIM.CNF cover identification and authentication, and resource limit attributes. F.APR.* cover privilege and role TSF data. F.AUD.* cover audit data.
FMT.REV.1.1	F.LIM.CNF F.APR.ROP F.APR.GRSP F.APR.GRR	Only suitably privileged users can revoke (or modify) the following attributes: resource limits (F.LIM.CNF), object privieleges (F.APR.ROP), system privileges (F.APR.GRSP) and roles (F.APR.GRR).
FMT.REV.1.2	F.PRI.SPRIV	Directly granted privileges and roles are revoked immediately. This is more rigorous than SFR FMT.REV.1.2. Revocation of roles takes effect when a role is re-enabled in the current session or a new user session is created.
FMT.SMR.1.1	F.IA.UID F.IA.CSA F.IA.CSN F.APR.GRR	F.IA.UID, F.IA.CSA and F.IA.CSN in combination ensure that the TSF maintains normal database users and database administrative users. F.APR.GRR covers database roles defined by a suitably privileged user.
FMT.SMR.1.2	F.IA.CSA F.APR.DER F.APR.EDR	F.APR.DER and F.APR.EDR covers granting database roles to database users. F.IA.CSA is relevant specifies how to allow a user to connect as one of the special administrative users SYSDBA and SYSOPER.
FPT.RVM.1.1	F.IA.IDE F.DAC.POL	F.IA.IDE ensures that the TOE always knows who the current user is. F.DAC.POL ensures then that the database access control policy is upheld for this user.

Table 7: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FPT.SEP.1.1	F.IA.IDE F.DAC.SEP	F.IA.IDE ensures that the identity of the user associated with each interaction with the TOE is clear. F.DAC.SEP ensures that the interactions between different users and the TOE cannot interfere with each other. Additionally there is no way to access the TOE except through the evaluated interfaces described by the TOE security functions.
FPT.SEP.1.2	F.IA.IDE F.DAC.SEP	F.IA.IDE ensures that the identity of the user associated with each interaction with the TOE is clear. F.DAC.SEP ensures that the interactions between different users and the TOE cannot interfere with each other.
FRU.RSA.1.1	F.LIM.CNF F.LIM.POL F.LIM.NSESS F.LIM.TIME F.LIM.RSESS F.LIM.RCALL	F.LIM.CNF covers configuration of the resource quotas. F.LIM.POL, F.LIM.NSESS, F.LIM.TIME, F.LIM.RSESS and F.LIM.RCALL enforces the resource quotas configured.
FTA.MCS.1.1	F.LIM.NSESS	F.LIM.NSESS directly satisfies FTA.MCS.1.2
FTA.MCS.1.2	F.LIM.NSESS F.LIM.POL	As with FTA.MCS.1.1 except that F.LIM.POL ensures that the default number of concurrent sessions allowed is enforced if a user specific configuration has not been specified.
FTA.TSE.1.1	F.IA.CSN F.IA.CSA	F.IA.CSN and F.IA.CSA define the pre-requisites for session establishment, including possession of the CREATE SESSION privilege and being identified as a SYSDBA/SYSOPER, respectively. These are configured on the basis of individual user identity. Therefore, it is possible to deny access based on user identity.
FAU.GEN.1.1	F.AUD.SOM F.AUD.SEV F.AUD.ALW	The database audit functionality is always active. Whether or not, auditing is actually performed is dependent on configuration of a parameter in the init.ora file which is controlled by the OS. F.AUD.SOM, F.AUD.SEV and F.AUD.ALW ensure all actions configured to be audited are audited.
FAU.GEN.1.2	F.AUD.INF	F.AUD.INF directly satisfies FAU.GEN.1.2
FAU.GEN.2.1	F.AUD.INF	F.AUD.INF directly satisfies FAU.GEN.2.1
FAU.SAR.1.1	F.AUD.ACC	F.AUD.ACC directly satisfies FAU.SAR.1.1
FAU.SAR.1.2	F.AUD.VIEW	F.AUD.VIEW directly satisfies FAU.SAR.1.2
FAU.SAR.3.1	F.AUD.VIEW F.AUD.ACC	F.AUD.VIEW directly satisfies FAU.SAR.3.1, additionally F.AUD.ACC determines which records are available to the user for selection.

Table 7: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FAU.SEL.1.1	F.AUD.SOM F.AUD.SEV F.AUD.ALW F.AUD.CNF	F.AUD.SEV and F.AUD.CNF allow a suitably privileged user to configure exactly which events should be audited. F.AUD.SOM and F.AUD.ALW specify events that are always audited. Note that for audit records database subjects are always the database users, so that for example an audit record generated by a stored procedure will be generated with the username of the invoker, not that of the procedure or the procedure owner.
FAU.STG.1.1	F.AUD.DEL	F.AUD.DEL directly satisfied FAU.STG.1.1.
FAU.STG.1.2	F.AUD.DEL	F.AUD.DEL protects audit records from unauthorised modification or deletion.
FAU.STG.4.1	F.AUD.FULL	F.AUD.FULL directly satisfies FAU.STG.4.1

Table 7: TOE Security Function Suitability and Binding

PP Claims Rationale

Chapter 5 lists all of the SFRs included in this security target; this list includes all of the SFRs identified in the DBMS PP. All of the operations applied to the SFRs are in accordance with the requirements of the DBMS PP.

This Page Intentionally Blank

ANNEX

A References

[ADG] *Oracle8 Application Developer's Guide,* Release 8.0.5, Oracle Corporation.

[CC] *Common Criteria for Information Technology Security Evaluation,* Version 2.1, ISO/IEC 15408, CCIB-99-031, 032, & 033, August 1999.

[CM] *Oracle8 Configuration Management Plan,* Oracle Corporation.

[DD] *Oracle8 Detailed Design Admendments,* Oracle Corporation.

[ECD] *Oracle8 Release 8.0.5 Evaluated Configuration Document,* Oracle Corporation.

[ERR] *Oracle8 Error Messages,* Oracle Corporation.

[FS] *Oracle8 Functional Specification,* Oracle Corporation.

[GA] *Oracle8 Administrator and User Guidance Analysis,* Oracle Corporation.

[DPP] *DBMS Protection Profile (DBMS PP),* Issue 2.0, Oracle Corporation, April 2000.

[ICG] *Oracle8 Installation and Configuration Guide,* Oracle Corporation.

[ITSEC] *Information Technology Security Evaluation Criteria,* Issue 1.2, Commission of the European Communities, 28 June 1991.

[MEMO 1] *CESG Computer Security Memorandum No. 1 - Glossary of Computer Security Terms,* Issue 2.0, November 1989.

[OSD] *Oracle8 Operating System Dependencies,* Release 8.0.5, Oracle Corporation.

[OSQM] *Oracle UK Ltd Shipping Quality Manual,* Oracle Corporation.

[PLS] *PL/SQL User's Guide and Reference,* Release 8.0, Oracle Corporation, A54654-01, June 1997.

[PRP] *Oracle8 Product Release Process,* Oracle Corporation.

[SAD] *Oracle8 Server Administrator's Guide,* Release 8.0.5, Oracle Corporation.

[SCN] *Oracle8 Server Concepts,* Release 8.0.5, Oracle Corporation.

[SD1] *Oracle8 Server Distributed Database Systems,* Release 8.0.5, Oracle Corporation.

[SODE] *Security of the Oracle Development Environment,* Oracle Corporation.

[SOFA] *Strength of Functions Analysis,* Oracle Corporation.

[SPM] *Oracle8 Security Policy Model,* Oracle Corporation.

[SQL] *Oracle8 Server SQL Reference,* Release 8.0.5, Oracle Corporation.

[SQL92] *Database Language SQL, ISO/IEC 9075:1992 and ANSI X3.135-1992,*

[SRB] *Oracle8 System Release Bulletin,* Oracle Corporation.

[SRC] *Oracle8 Source Code,* Oracle Corporation.

[SRF] *Oracle8 Server Reference,* Release 8.0.5, Oracle Corporation.

[TCSEC] *Trusted Computer Security Evaluation Criteria,* Department of Defense, United States of America, DoD 5200.28-STD, December 1985.

[TP] *Oracle8 Test Plan, Procedures, Results, and Analysis,* Oracle Corporation.

[VA] *Oracle8 Vulnerability Analysis,* Oracle Corporation.

ANNEX

B Glossary

Acronyms

DAC	Discretionary Access Control
DDL	Data Definnition Language
DES	Data Encryption Standard
DML	Data Manipulation Language
ORDBMS	Object-Relational Database Management System
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SQL	Structured Query Language
TOE	Target Of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface

TSP	TOE Security Policy

Terms

Data Definnition Language (DDL)	The SQL statements used to define the schema and schema objects in a database [SQL]
Data dictionary	A set of internal Oracle tables that contain information about the logical and physical structure of the database. [SCN]
Data Encryption Standard (DES)	A standard for encryption, FIPS PUB 46-2 and FIPS PUB 81. []
Data Manipulation Language (DML)	The SQL statements used to query and manipulate data in schema objects [SQL]
Data server	A component of a DBMS that supports concurrent access to a database by multiple users, possibly at different nodes in a distributed environment. [ST]
Database	A collection of data that is treated as a unit; the general purpose of a database is to store and retrieve related information []
Database administrative user	A database user to whom one or more administrative privileges have been granted. An administrative privilege is any system privilege which is not CREATE SESSION. [DPP],[ST]
Database connection	A communication pathway between a user and a DBMS. [DPP]
Database link	A definition of a one-way communication path from an Oracle database to another database. [SCN]
Database non-administrative user	A database user who only has privileges to perform operations in accordance with the TSP. [DPP]
Database object	An object contained within a database. [DPP]
Database session	A connection of an identified and authenticated user to a specific database; the session lasts from the time the user connects (and is identified and authenticated) until the time the user disconnects. [DPP]
Database subject	A subject that causes database operations to be perfomed. [DPP]
Database user	A user who interacts with a DBMS and performs operations on objects stored within the database. [DPP]
Discretionary Access Control	Access control based on access rights granted by users other than the System Security Officer. [MEMO 1]

Instance	The combination of a set of Oracle background processes and memory that is shared among the processes. A database instance must be started (the shared memory allocated and the background processes created) by an authorised administrative user before the database managed by the instance can be accessed. [SCN]
Interface product	A TOE component that resides in a user process and can be used to communicate with an Oracle database server in a secure manner. [ST]
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations. Objects are visible through the TSFI and are composed of one or more TOE resources encapsulated with security attributes. [CC], [SQL]
Object-Relational Database Management System (ORDBMS)	A DBMS that supports object-oriented technology as well as relational databases. [SCN]
Owner	The owner of a named database object is the database user who is responsible for the object and may grant other database users access to the object on a discretionary basis. [DPP]
Normal User	A database user who was created using the CREATE USER command. This includes the users SYS and SYSTEM but excludes the SYSOPER and SYSDBA users.
Platform	The combination of software and hardware underlying the DBMS. [ST]
Privilege	A right to access objects and/or perform operations that can be granted to some users and not to others. [DPP]
Privilege, database administrative	A privilege authorising a subject to perform operations that may bypass, alter, or indirectly affect the enforcement of the TSP. [DPP]
Privilege, database object access	A privilege authorising a subject to access a named database object. [DPP]
Privilege, directly granted	An Oracle system or object privilege that has been explicitly granted to a user. Privileges granted to any roles the user has been granted are not included in the set of directly granted privileges. [SCN]
Privilege, object	An Oracle privilege that allows users to perform a particular action on a specific schema object. Oracle object privileges are database object access privileges. [SCN]
Privilege, system	An Oracle privilege that allows users to perform a particular systemwide action or a particular action on a particular type of object. Some Oracle system privileges are database administrative privileges. [SCN]
Program unit	A PL/SQL program; a procedure, function, or package. [PLS]
Role (CC)	A predefined set of rules establishing the allowed interactions between a user and the TOE. [CC]
Role (Oracle)	A named group of related system and/or object privileges that can be granted to users or to other roles. [SCN]

Schema	A collection of logical structures of data (schema objects), owned by a specific database user. [SQL]
Security attribute	Information associated with subjects, users, and/or objects which is used for the enforcement of the TSP. [CC]
Security domain	The set of objects that a subject has the ability to access. [TCSEC]
Security Function (SF)	A part or parts of the TOE which have to be relied upon for enforcing a closely related subset of the rules from the TSP. [CC]
Security Function Policy (SFP)	The security policy enforced by a SF. [CC]
Security Runctional Requirement (SFR)	A security functional requirement defined in a protection profile or security target. [CC]
Server process	An Oracle process that services requests for access to an Oracle database from connected user processes. [SCN]
SOF-medium	A level of TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possession a moderate attack potential. [CC]
SQL statement	A string of SQL text containing a command and supporting clauses. All access to an Oracle database is via SQL statements. [SCN]
Strength of function (SOF)	A qualificatioin of a TOD security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms. [CC]
Structured Query Language (SQL)	A standardised database access lanaguage; Oracle8 SQL is a superset of the ANSI/ISO SQL92 standard at entry level conformance. [SQL]
Subject	An entity within the TSC that causes operations to be performed. [CC]
System	A specific IT installatioin, with a particular purpos and operational environment [CC]
Target Of Evaluation (TOE)	The product or system being evaluated. [CC]
TOE resource	Anything usable or consumable in the TOE. [CC]
TOE Scope of Control (TSC)	The set of interactions which can occur with or within a TOE and are subject to the rules of the TSP. [CC]
TOE Security Function (TSF)	A part of the TOE that either directly enforces or contributes to the enforcement of the TSP. [CC]
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE. [CC]
TSF Interface (TSFI)	A set of interfaces, whether interactive (man-machine interface) or programmatic (ap-

	plication programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF. [CC]
User	Any entity (human or machine) outside the TOE that interacts with the TOE. [CC]
User process	A process that requests services, on behalf of a user or application, from an Oracle server process. [SCN]

This Page Intentionally Blank