OLS Security Target for
Oracle Database 10*g* Release 2 (10.2.0)

October 2007

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

OLS Security Target for Oracle Database 10*g*
Release 2 (10.2.0)

Issue 2.0 Version 11

October 2007

Author: Saad Syed, modifications made by Helmut Kurth

Contributors: Peter Goatly, Shaun Lee, Petra Manche

Contents

1 Introduction....1

Identification and CC Conformance 1
TOE Overview 2
TOE Product Components 3
Document Overview 4

2 TOE Description 5

Oracle Database 10g Architecture....5
An Oracle Database....7
Access Controls....11
Quotas....18
Identification and Authentication....19
Auditing....20
Security Management....23
Consistency of Replicated TSF Data 24
Secure Distributed Processing....24
Other Oracle Database 10g Security Features....25

3 Security Environment 27

Threats....27
Organisational Security Policies 27
Assumptions....28

4 Security Objectives 29

TOE Security Objectives 29
Environmental Security Objectives 29

5 IT Security Requirements 31

TOE Security Functional Requirements 31
TOE Security Assurance Requirements 48
Security Requirements for the IT Environment 48
Minimum Strength of Function 49

6 TOE Summary Specification 51

TOE Security Functionality 51
Security Mechanisms and Techniques 68
Assurance Measures 69

7 Protection Profile Claims 71

PP Reference 71
PP Tailoring 71
PP Additions 71

8 Rationale 75

Security Objectives Rationale 75
Security Requirements Rationale 76
TOE Summary Specification Rationale 83
PP Claims Rationale 89
Assurance Measures Rationale 89

A Glossary 91

Acronyms 91
Terms 92

B References 97

CHAPTER

1 Introduction

This document is the security target for the Common Criteria evaluation of Oracle Database 10*g*, Release 2 (10.2.0.3) with Oracle Label Security for Enterprise Edition.

Identification and CC Conformance

Title: OLS Security Target for Oracle Database 10*g*, Issue 2.0 Version 11

Target of Evaluation (TOE): Oracle Database 10*g* Enterprise Edition, with Oracle Label Security.

Release: 10.2.0.3 with all critical patch updates up to and including July 2007

Note: This includes the guidance documentation which consists of [OLS_ECD] and the Oracle Database 10*g* Release 2 documentation library (Part No. B19306-01).

Note: Oracle's release numbers are of the form a.b.c.d where

- a is the major release number
- b is the maintenance release number
- c is the application server release number
- d is the component release number

In some cases there may be an additional number at the end which then defines a platform-specific release number (usually a patch set). In the case of the TOE, all components have the release number 10.2.0.3 with no platform.

Operating System Platforms: Red Hat Enterprise Linux AS (version 4 Update 2) for which [CCEVS-VR-06-0020] is the Common Criteria certification report;
SuSE Linux Enterprise Server 9
for which [DSZ0256] is the Common Criteria Certification Report;

CC Conformance: U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.1. ([BR-DBMSPP])

The CC conformance claim is: part 2 extended and part 3 conformant
This Security Target conforms to [CC, Part 2] and [CC, Part 3]. [BR-DBMSPP] contains extended SFRs which are included in this Security Target. All other SFRs in this Security Target are conformant to [CC, Part 2]. ALC_FLR.3 is the only augmented assurance criterion specified in addition to the ones in the EAL4 assurance package.

Assurance: EAL4 augmented with ALC_FLR.3[1].

Keywords: Oracle Database 10*g*, O-RDBMS, database, Oracle Label Security, OLS, security target, EAL4

Version of the Common Criteria [CC] used to produce this document: 2.3 .

TOE Overview

Oracle Database 10*g* is an object-relational database management system (O-RDBMS), providing advanced security functionality for multi-user distributed database environments. The security functionality in Oracle Database 10*g* includes:

- user identification and authentication, with password management options and support for enterprise users (password option only). In the case of Enterprise Users (defined later) this function is partly provided by the IT-environment. Note that [BR-DBMSPP] defines identification and authentication as a function of the IT environment. This is the case for a DBMS that relies on the underlying operating system for the identification and authentication of the user. In the case of the Oracle DBMS the identification and authentication is either performed by the TOE in total (in the case of users that are not Enterprise Users) or performed with the assistance of an authentication server in the IT environment (in the case of Enterprise Users). In both cases it is the TOE that mediates the identification and authentication of the user;
- discretionary access controls on database objects, which controls access to objects based on the identity of the subjects or groups to which the subjects and objects belong, and which allows authorized users to specify how the objects that they control are protected;
- granular privileges for the enforcement of least privilege;
- user-configurable roles for privilege management, including an authorized administration role to allow authorized administrators to configure the policies for discretionary access control, identification and authentication, and auditing. The TOE must enforce the authorized administration role;
- quotas on the amount of processing resources a user can consume during a database session;
- audit capture is the function that creates information on all auditable events;
- extensive and flexible auditing options;
- secure access to remote Oracle databases; *and*
- stored procedures, triggers and security policies for user-defined access controls

1. ALC_FLR.3 provides assurance at the highest defined component level that there are flaw remediation procedures for the TOE by which discovered security flaws can be reported to, tracked and corrected by the developer, and by which corrective actions can be issued to TOE users in a timely fashion.

and auditing.

Those functions are a superset of the security functions defined in [BR-DBMSPP], chapter 2.3.

Oracle Database 10*g* relies on the IT-environment for the non-bypassibility and domain separation properties. Those properties need to be provided by the underlying operating systems in co-operation with the hardware platform. The operating system platforms listed above have all been evaluated for conformance to the Controlled Access Protection Profile [CAPP] which requires to enforce those properties. In addition Oracle Database 10*g* enforces its own separation between different users based on the functions provided by the underlying operating system.

Oracle Database 10*g* supports both client/server and standalone architectures. In addition, Oracle Database 10*g* supports multi-tier architectures, however in this environment any tier (middle-tier) that communicates directly with the server is actually an Oracle client and any lower tiers are outside of the scope of this ST. In all architectures, the Oracle Database 10*g* Server acts as a *data server*, providing access to the information stored in a database. Access requests are made via Oracle Database 10*g interface products* that provide connectivity to the database and submit Structured Query Language (SQL) statements to the Oracle Database 10*g* data server. The Oracle Database 10*g* 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.

Oracle Label Security (OLS) enables application developers to add label-based access control (LBAC) to their Oracle Database 10*g* applications. In addition to discretionary access control (DAC) that is provided by Oracle Database 10*g*, it mediates access to rows in database tables based on a label (or labels) contained in each row, and the labels and privileges associated with each user session. Such labels quantify the sensitivity of data and the clearance of users to access sensitive data.

TOE Product Components

The Oracle Database 10*g* with Oracle Label Security includes the products identified in Table 1. Access to the Oracle Database 10*g* server is provided via the interface products identified in Table 2.

[OLS_ECD] defines which TOE products must be installed in the evaluated configuration and defines the requirements for setting up the TOE environment.

Table 1: TOE Server Products

TOE Server Products
Oracle Database 10*g* Enterprise Edition 10.2.0.3
Oracle Label Security 10*g* 10.2.0.3

Table 2: TOE Interface Products

TOE Interface Products
SQL*Plus 10.2.0.3
Oracle Call Interface 10.2.0.3
Oracle Net Services 10.2.0.3

Document Overview

This document consists of an update to Issue 1.2 of the OLS Security Target for the Oracle Database 10g Release 1 (10.1.0), [OLS_ST10gR1], which was used in the most recent Common Criteria evaluation of Oracle10*g* with OLS. Changes made relative to [OLS_ST10gR1] are mainly introduced by the change in the Protection Profile for which conformance is claimed. Other chnages inlcude the change to the TOE's name, changes to the operating system platforms, additional functions considers in the evaluation (mainly support for Enterprise Users, Partitioning and Real Application Clusters) and changed references to information in technical publications.

Chapter 2 of this security target provides a high-level overview of the security features of the Oracle Database 10*g* data server and Oracle Label Security. Chapter 3 identifies the assumptions, threats, and security policies of the 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 IT environment. Chapter 6 summarises each Security Function (SF) provided by Oracle Database 10*g* and Oracle Label Security to meet the security requirements. Chapter 7 describes how the 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.

CHAPTER

2 TOE Description

This section describes the product features that provide security mechanisms and contribute to the security of a system configured using Oracle Database 10*g* with Oracle Label Security. For a detailed description of the security features of Oracle Database 10*g* the reader is referred to [SG, Part II] and [DAG, part V]. A detailed description of the additional security features provided by Oracle Label Security can be found in [OLSAG, Part I]. 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 Oracle Database 10*g* architecture, the types of database objects supported by Oracle Database 10*g*, 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 Oracle Database 10*g*. The access control mechanisms consist of the discretionary access control supplied in Oracle Database 10*g* together with the label-based access control supplied by Oracle Label Security. Additional Oracle Database 10*g* security features that are not addressed by the security functional requirements of Chapter 5 are also briefly discussed.

Oracle Database 10*g* Architecture

The Oracle Database 10*g* architectural components are described in detail in [CON]. The additional components provided for Oracle Label Security are described in [OLSAG].

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 Oracle Database 10*g* 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 Oracle Database 10*g* interface products to establish a *database connection* to an Oracle Database 10*g 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 Oracle Database 10*g* 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 Oracle Database 10*g* 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 Oracle Database 10*g* 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 Oracle Database 10*g* 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 Oracle Database 10*g* instance.

- Embedded SQL statements incorporate DDL, DML, and transaction control statements within a procedural language program.

Programming Language/SQL (PL/SQL) is a procedural language supported by Oracle Database 10*g* 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.

The flashback query feature allows data to be queried from a point in the past. Once a user has set the date and time that they would like to view, any SQL query that they execute will operate on data as it existed at that point in time. This can allow suitably authorised users to correct their own mistakes. SQL operations can be used to view the change history in order to identify the error. The error can then be backed out of by restoring data as it existed before the error.

Note that the Flashback functionality does not reverse certain DDL statements such as TRUNCATE, although it can provide a way to restore accidentally dropped tables. It also does not apply to packages, procedures, or functions.

Client side interfaces

The Oracle Call Interface (OCI - described in [OCI]) provides an application programming interface (API) for developing database applications written in high level languages such as C.

An Oracle Database

An Oracle 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 [CON part II]; *and*
- non-schema objects to organise, monitor, and control the database [CON part II], [DAG].

In an Oracle database there are two types of connections for users of the database:

- Administrator connection.
  This covers users who connect to the database via AS SYSOPER or AS SYSDBA by virtue of possessing either the SYSOPER or SYSDBA system privilege (see [DAG, 1]). Users making a connection AS SYSOPER are allowed to perform operator administrative tasks (e.g. database startup and shutdown, and ALTER DATABASE commands). Users making a connection AS SYSDBA are allowed to perform all administrative tasks (including granting and/or revoking object privileges on other users' objects);
- Normal connection (note that this includes users SYS and SYSTEM. [DAG, 1]).
  This covers users who are authorised to access the database by virtue of being explicitly defined and identified to an instance of the Oracle database server.

Data Dictionary

At the centre of an Oracle database is the data dictionary - a set of internal Oracle tables that contain all of the information the Oracle database 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. [SG, 10: System Privileges] cautions that

extreme care must be taken when granting roles which provide privileged access to the data dictionary. 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 is 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. Oracle Database 10*g* supports the schema object types identified in [SQL, 2] and contains the following objects

- Clusters
- Constraints
- Database links
- Database triggers
- Dimensions
- External procedure libraries
- Index-organized tables
- Indexes
- Indextypes
- Java classes, Java resources, Java sources
- Materialized views
- Materialized view logs
- Object tables
- Object types
- Object views
- Operators
- Packages
- Sequences
- Stored functions, stored procedures
- Synonyms
- Tables
- Views.

A special schema PUBLIC is provided by Oracle Database 10*g* 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] lists object types that can be created and manipulated with SQL, but are not contained within a schema. These include:

- Contexts
- Directories
- Parameter files (PFILEs) and server parameter files (SPFILEs)
- Profiles
- Roles
- Rollback segments
- Tablespaces
- 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*
- alter tablespaces for backup and recovery operations.

Within the database files, Oracle Database 10*g* 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

Oracle Database 10*g* has two kinds of user connection: administrative connection (connecting AS SYSDBA or AS SYSOPER) and normal connection. Throughout this document the following terms are used to classify the types of database users:

- Normal User/Database Subject:
  A user who is connected via a normal connection. Note that the pre-defined users SYS and SYSTEM can be normal users.
- Database Administrative User/Administrative User:
  Any user who is authorised to perform administrative tasks. This term covers:
  - A Normal User who is authorised to perform an administrative task via the possession of an administrative privilege which permits the operation of the task.
  - A user who connects to the database via an administrative connection. Users making an administrative connection are authorised to access the database by virtue of having the SYSDBA or SYSOPER system privilege (i.e. they possess OS platform specific access rights, or are listed in the Oracle Database 10*g* password file as a SYSDBA or SYSOPER user).

Note that the word *authorised* is used (e.g. “an authorised administrative user”) to indicate that the user 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.

Additional security can be provided via customised OLS security policies, each of which defines a set of labels and a set of rules that govern data access, based on these labels.

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

Enterprise Users

In addition to the two types of users mentioned above the TOE also allows users to managed either locally or centrally within a directory. Users managed within a directory are called Enterpsise users. Each enterprise user has a unique identity across the enterprise. Users defined locally in the database are called local users.

Single password authentication lets users authenticate to multiple databases with a single global password although each connection requires a unique authentication. A password verifier, which is the hash of the password is securely stored in the centrally located, LDAP-compliant directory. In addition the directory also stores a user's global roles.

The password policy for Enterprise users is enforced by the directory, not by the TOE. Passwords need to be set and changed via functions of the directory. The directory server will then generate the password verifier (the hash value of the password).

Enterprise User Security requires Oracle Internet Directory 10g (9.0.4) or higher. Other LDAP-compliant directory services are supported by using Oracle Internet Directory Integration Platform to synchronize them with Oracle Internet Directory. The evaluated configuration however is restricted to use Orcale Internet Directory. Note that the Oracle Internet Directory is not part of the TOE but a part of the TOE environment.

Although Enterprise User Security also offers user authentication using public key certificates or using Kerberos, only password based authentication is supported in the evaluated configuration.

Partitioning

Partitioning addresses key issues in supporting very large tables and indexes by letting you decompose them into smaller and more manageable pieces called partitions. SQL queries and DML statements do not need to be modified in order to access partitioned tables. However, after partitions are defined, DDL statements can access and manipulate individual partitions rather than entire tables or indexes. This is how partitioning can simplify the manageability of large database objects. Also, partitioning is entirely transparent to applications.

Partitioning is useful for many different types of applications, particularly applications that manage large volumes of data. OLTP systems often benefit from improvements in manageability and availability, while data warehousing systems benefit from performance and manageability.

Partitioning is a feature now included in the evaluated configuration. All the security functions used to protect elements of an Oracle database defined in this Security Tar-

get work transparently with Partitioning.

Real Application Clusters

Real Application Clusters (RAC) comprises several Oracle instances running on multiple clustered computers, which communicate with each other by means of a so-called interconnect. RAC uses cluster software to access a shared database that resides on shared disk. RAC combines the processing power of these multiple interconnected computers to provide system redundancy, near linear scalability, and high availability. RAC also offers significant advantages for both OLTP and data warehouse systems and all systems and applications can efficiently exploit clustered environments.

Real Application Clusters is a feature now included in the evaluated configuration. All the security functions used to protect elements of an Oracle database defined in this Security Target work transparently with Real Application Clusters.

Data Integrity

Oracle Database 10*g* 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.

With RAC installed each instance of RAC mantains its own copy of the system global area and the database cache, which are synchronized over the interconnect. In addition global locks on the RAC environment ensure that concurrent updates are synchronized. Those mechanism together with the mechanisms mentioned above for transcation management and concurrency control for the database ensure the consistency and integrity of both user and TSF data in a RAC environment.

Access Controls

Access control is the process of defining a user's ability to read or write information. Oracle Database 10*g* always provides *discretionary access control* (DAC). When the Oracle Label Security (OLS) product has been installed, *label-based access control* (LBAC) can be applied in addition to DAC.

Discretionary Access Control

DAC can be used to selectively share database information with other users. This access control mechanism can be used to enforce need-to-know style confidentiality as well as control data disclosure, entry, modification, and destruction. In addition to the DAC controls enforced by the Oracle Database 10*g* server, application-specific access controls can be implemented using views and triggers to mediate a user's access to application data.

The DAC mechanism controls access to database objects based on the privileges enabled in the database session. There are two types of DAC 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, authorising all database users for the privilege. During a database session,

the privileges enabled in the session may be changed using several Oracle Database 10*g* mechanisms that affect the set of privileges held by the session.

System Privileges

Oracle Database 10*g* 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 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. Oracle Database 10*g* 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

Oracle Database 10*g* 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. Note that this feature is not used to implement any security functional requirement of this Security Target.

Secure Application Roles

A secure application role is a role which is enabled by a PL/SQL package. A database administrative user can grant a secure application role all the privileges necessary to run a particular application. The role will then only be enabled if the application's check of the relevant conditions is successful. This means that the use of such a role can be based on information about the user's session, such as the IP address of a user who has connected through a proxy.

Global Roles

Global roles are roles assigned to an Enterprise User within the user schema in the directory server. Assigning privilges to global roles is still done within each database. This allows to have the privileges associated with a global role to be defined and managed individually for each database. When an Enterprise user successfully logs into a database, the database will get the user's global roles from the directory and than assigns the user's privileges in accordance with the privileges assigned to the local and global roles the user has.

DDL Restriction

Privileges held via roles cannot be used to perform a DML operation that is required to issue a DDL statements. For example a user who receives the SELECT ANY TABLE system privilege or the SELECT object privilege for a table through a role can use neither privilege to create a view on a table that belongs to another user. The user must have *directly granted privileges* authorising the access to the underlying tables.

Pre-defined Roles

By default Oracle 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 and can be modified or removed by suitably privileged users [SG, 5].

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 in addition to those granted to PUBLIC. The session also 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.

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, authorising 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 may be set to the owner's directly granted privileges (definers rights), or the invoker's privileges (invokers rights) depending on options set when the program unit is created. 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.

Information about stored program units which have policy privileges for Label-Based Access Control is given in the section on "Trusted Stored Program Units" below.

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.

Information about labels and policy privileges for Label-Based Access Control for triggers is given in the section on "LBAC and Triggers" below.

Fine-grained Access Control

Fine-grained (or row-level) access control is available with the virtual private database (VPD) technology which is a standard feature of the Oracle Database 10*g* Enterprise Edition. Fine-grained access control allows a database administrative user to associate security policies with tables, views and synonyms. These policies are implemented by PL/SQL functions and are enforced on a normal user no matter how the data is accessed (unless the user is authorised by the possession of the system privilege EXEMPT ACCESS POLICY). Such security policies can be defined to be enforced when a query references particular columns.

Different policies can be applied for SELECT, INSERT, UPDATE and DELETE operations. Note that the use of the Oracle Database 10*g* MERGE SQL command causes SELECT and INSERT or UPDATE operations to be performed. Note also that it is possible for more than one policy to be applied to a table, including building on top of base policies in packaged applications.

Application Context

An application context allows an application to make security decisions based on additional attributes attached to a user's session information. An application context provides a protected session persistent storage area for additional user attributes defined by the application.

To support application managed session pooling by middle tier applications, the DBMS_SESSION interface for managing application context is enhanced for Oracle Database 10*g*. This interface now has a client identifier for each application context so

that the application context can be managed globally while each client will see only their assigned application context.

Partitioned Fine-grained Access Control

Oracle Database 10*g* provides the ability to partition security policy enforcement by application. This enables different security policies to be applied, depending upon which application is accessing the data. Oracle Database 10*g* enables partitioning of fine-grained access control through policy groups and a driving application context. The driving application context securely determines which application is accessing the data, and policy groups facilitate the management of policies which apply by application.

A database administrative user specifies which policy group the policy falls into when adding a policy to a table/view using the ADD_GROUPED_POLICY interface. The driving context is defined using the ADD_POLICY_CONTEXT interface.

This feature is not used to implement the access control policy defined in chapters 5 of this document.

Label-Based Access Control

OLS provides label-based access control, which builds on VPD to mediate access to data at a row level without any code having to be written. Each data row is given one or more labels, each of which is used to store information about data sensitivity.

To be allowed access to a row, a user must satisfy both OLS label-based access control (LBAC) and Oracle Database 10*g* DAC requirements which are based on the user's system-level privileges and database object privileges. Thus, to gain access to a row, a user must first be authenticated to the Oracle database. Second, the user must have the DAC object and system privileges required for the operation. Finally, the user must meet the criteria enforced by LBAC, which are based on the labels of the user and the data row.

In most applications, a relatively small number of application tables will require label-based access controls, while the protection provided by standard DAC will suffice for the majority of tables.

Data Labels

In OLS, each row of a table can be labelled as to its level of confidentiality. Each label contains three components:

- a single hierarchical level or sensitivity ranking,
- one or more horizontal compartments or categories, and
- one or more hierarchical groups.

The level specifies the sensitivity of the data. A typical organisation might define levels UNCLASSIFIED, CONFIDENTIAL, SENSITIVE, and HIGHLY_SENSITIVE. Alternatively, a commercial organisation might define levels only for PUBLIC and COMPANY_CONFIDENTIAL data.

The compartment component is non-hierarchical; compartments are typically defined to segregate data - such as data related to a particular ongoing strategic initiative. For example, a commercial organisation might define compartments for FINANCIAL, OPERATIONAL, SECURITY and PERSONNEL data.

Finally, groups are used to record ownership and can be used hierarchically. For example, FINANCE, SALES and ENGINEERING groups can be defined as children of a CORPORATION group, creating an ownership relation. In this example, the FINANCE, SALES and ENGINEERING groups are conceptually part of the CORPO-

RATION group and any user authorised to access data which has a label that contains the CORPORATION group will also be authorised to access data which has a label containing one or more of the FINANCE, SALES or ENGINEERING groups.

Labels can contain a single level component, a level combined with a set of either compartments or groups, or a level and both compartments and groups.

OLS Administrators

There are two main roles for users involved in administering Oracle Label Security for a database: the LBAC Administrator role and OLS Policy Administrator roles. Throughout this document the following terms are used to describe these users:

- LBAC Administrator: A user who is able to create, alter and drop OLS policies in the database by virtue of possessing the LBAC_DBA role and EXECUTE privilege on the SA_SYSDBA package;
- OLS Policy Administrator / Policy administrator: A user who is able to execute the administrative packages for the OLS policy for which they possess the corresponding *policy*_DBA role. This user should be granted the EXECUTE privilege only on the OLS administrative packages that they require for their role.

Each OLS policy must have at least one OLS policy administrator. The same person could be the administrator for more than one policy.

Label Authorisations

A Policy Administrator can grant to users label authorisations which determine what kind of access (read or write) they have to the rows that are labelled. These authorisations are explained further in the sections below.

Session Label

Each OLS user has *user label authorisations* which are stored in the data dictionary or, for enterprise users, in the external directory server. They include:

- a maximum and minimum level,
- a set of authorised compartments,
- a set of authorised groups, and
- for each compartment and group, a specification of read-only access, or read-write access.

When the Policy Administrator sets up the user label authorisations for the user, he or she also specifies the user's initial session label.

The session label is the particular combination of level, compartments, and groups at which a user works at any given time. The user can change the session label provided that it remains within the user's label authorisations.

Row Label

When the Policy Administrator sets up a user's label authorisations, he or she also specifies an initial default row label which is used when a session is started up.

The row label is the particular default label assigned to data which a user enters during a session (if the user is not permitted to define the label explicitly). It can be changed by the user to any level, from the one specified in the user's current session label, down to the user's minimum level. It can include only compartments and groups contained in the current session label, and for which the user has write access.

OLS Policies

OLS policies are established to specify how label-based access control is to be enforced on a database. Each OLS policy is created by an LBAC Administrator and the Policy Administrator then defines a set of labels and a set of enforcement options to govern LBAC access to data. These enforcement options provide for maximum flexibility in controlling the different Data Manipulation Language operations that users

can perform. For each operation - SELECT, INSERT, UPDATE, and DELETE - administrators can specify a particular type of enforcement of the security policy. Note that the use of the Oracle Database 10*g* MERGE SQL command causes SELECT and INSERT or UPDATE operations to be performed.

One or more policies can be applied to each table. A policy can also be applied to a schema. This has the effect of applying the policy to each table contained within the schema. Each row in each table in the database has a label column for each policy that applies to the table. For each OLS policy, Policy Administrators give user label authorisations to users and assign policy privileges to users and stored program units to permit access to data in tables controlled by the policy.

Policy Privileges

Policy privileges enable a user or stored program unit to bypass aspects of the label-based access control policy. In addition, the Policy Administrator can authorise the user or program unit to perform specific actions, such as the ability of one user to assume the authorisations of a different user.

Policy privileges can be granted to program units to authorise the procedure rather than the user to perform privileged operations. When only stored program units, and not individual users, have policy privileges, the system is most secure. Further, such program units encapsulate the OLS policy, which minimises the amount of application code that needs to be reviewed for security.

OLS Administration Tools

OLS provides administrative interfaces via packages supplied with OLS to define and manage OLS policies for a database. Initially, an LBAC Administrator must create a policy and then a Policy Administrator defines the levels, compartments, and groups that compose the labels, and then she or he can define the set of valid data labels for the policy.

The Policy Administrator can then use the administrative interfaces to:

- set the policy enforcement options,
- apply the policy to tables and schemas,
- authorise users,
- assign privileges to users and stored program units, and
- configure auditing.

The Oracle Policy Manager is a graphical user interface which can be used to call the OLS packages to perform the administrative functions for OLS policies. This GUI tool is not part of the TOE.

Relationships between Labels

When checking whether a user can read labelled data, OLS uses the dominance relationship between two labels. Provided that the policy enforcement option INVERSE_GROUPS is not in operation, if Label1 and Label2 are such that:

- Label1’s level is greater than or equal to Label2’s level, and
- Label2 contains one or more groups and Label1 contains at least one of the groups which belong to Label2 (or the parent group of one such subgroup), and
- Label1 contains all the compartments which belong to Label2,

then Label1 is said to "dominate" Label2.

If the policy enforcement option INVERSE_GROUPS is in operation, then [OLSAG, 14] defines a different dominance relationship for labels.

If a user's label dominates the label of a data item, then OLS allows the user to read that item (provided that the DAC rules also permit the user to access the data item).

Label Functions

OLS provides functions and procedures to manipulate labels. These include:

- functions to determine whether, given two labels, one label dominates the other or the labels are not comparable,
- functions to find the least upper bound and the greatest lower bound of two or more labels,
- a function to merge two labels together,
- a procedure to set the label of the current database session,
- a procedure to set the default row value for the current database session,
- a procedure to restore the label and the default row value for the current database session,
- a function to return the security attributes of the current database session.

Trusted Stored Program Units

Stored program units can become "trusted" when a Policy Administrator assigns them policy privileges. A stored program unit can be run with its own autonomous policy privileges, rather than those of the user who invokes it. For example, if a user possess no policy privileges, but executes a stored program unit which has the WRITEDOWN privilege, the user can update labels. In this case, the policy privileges used are those of the stored program unit, and not the user's. Trusted program units can encapsulate privileged operations in a controlled manner. By using procedures, packages, and/or functions that have been assigned policy privileges, a user may be able to access data that his or her own labels and policy privileges would not authorise. For example, to perform aggregate functions over all of the data in a table, not just the data visible to the user, a user could make use of a trusted program unit set up by an administrator. Program units can thus perform operations on behalf of users, without the need to grant policy privileges directly to users.

LBAC and Triggers

When a trigger fires, it is executed with the session label and with the policy privileges of the user that invoked the trigger.

Quotas

Using Oracle Database 10*g* profiles, a database administrative user can set quotas on the amount of processing resources a user can consume during a database 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 Oracle Database 10*g* server will abort the operation, and, in some cases, terminate the user's session, or, in other cases, simply terminate the current SQL statement or rollback the current transaction.

A database 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.

Resumable statements are a feature in Oracle Database 10*g* which allows an administrator to temporarily suspend a large operation, such as a batch update data load. This might be necessary when space has run out. Suspending the operation gives the database administrator an opportunity to take corrective steps to resolve the error condition. After the error has been corrected, the suspended operation automatically resumes execution. A suspended resumable operation is aborted automatically if the error is not fixed within a set time period.

Users must have the RESUMABLE system privilege before they can execute resumable operations. An ALTER SESSION ENABLE RESUMABLE statement is provided to enable SQL statements to be resumable when they are invoked within the session. Resumable operations are suspended under one of the conditions: Out of space, Space limit error, or Space quota error.

Identification and Authentication

Oracle Database 10*g* always identifies authorised users of an Oracle database prior to establishing a database session for the user. Authentication can be performed directly by the Oracle Database 10*g* server using passwords managed by the server, or the server can rely on the authentication done by the underlying OS platform.

For OS authentication, the database user connects to the Oracle Database 10*g* 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. This form of authentication is appropriate for Oracle Database 10*g* only if it is running on a Microsoft Windows operating system. Since no Microsoft Windows operating system platforms are to be used for this evaluation, the TOE does not use this form of authentication.

As an option the TOE can authenticate users via a TOE-external LDAP compliant directory server (e. g. Oracle Internet Directory). This function (named "Enterprise Users") is included as an option for authenticating users in the TOE but restricted to password based authentication only. Other authentication options (e. g. using digital certificates) are not supported in the evaluated configuration.

For Oracle authentication, a user must specify a user name and password in order to connect. For local authentication the password is compared to the password for the user stored in the data dictionary and if they match, a database session is created. The user's password is stored in the data dictionary in a one-way encrypted form, so before the comparison is made, the password specified by the user is also one-way encrypted. For enterprise user authentication using passwords the database server requests the user password verifier from the directory and performs the comparison. When successful, the database gets the user's global roles from the diectory.

Password Management

A user may change his or her password at any time. Oracle Database 10*g* provides the facility for suitably privileged users to create password complexity check functions that can screen new passwords of local users for certain criteria, e.g.:

- a minimum number of characters in length;
- not equal to the user name;
- includes a minimum number of alphabetic, numeric, or punctuation characters;
- does not match any word on an internal list of words;
- differs from the previous password by a certain number of characters.

A suitably authorised user can also set password lifetime, a failed logon count leading to account lockout, expiration options, and password reuse requirements in an Oracle Database 10*g* profile. By assigning different profiles to different groups of users, the password management parameters can vary among users.

By default the database does not enforce any password profile limits, however it is critical that certain password controls are used in all profiles such that the TOE achieves a *high* strength of function for the password mechanism (see the Minimum Strength of Function section in chapter 5). Guidance covering the different password controls, and instructions for modifying profiles to achieve SOF-*high*, is provided in the TOE's Evaluated Configuration Document [OLS_ECD].

For Enterprise Users the password management is performed by the external LDAP server and is therefore a function of the IT-environment.

Special Authentication

Database administrative users may connect to the database to perform functions such as starting up or shutting down an Oracle Database 10*g* 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. For example, on a UNIX platform, the group defaults to the 'dba' group, but can be changed.

When a database administrative user wants to undertake special operations, he or she connects to the database through a special keyword: AS SYSDBA or AS SYSOPER. When connected using the 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

Oracle Database 10*g* 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. Oracle Database 10*g* 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. Oracle Database 10*g* provides capabilities to permit auditing plans to be quickly enabled to implement crisis responses. In addition to the standard Oracle Database 10*g* 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

A database 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

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

Fine-Grained Auditing

Database administrative users can request fine-grained auditing to monitor query access based on content and can also request that DML operations be monitored. Whenever the policy conditions are met for returning a row from a query block, the query is audited. These policies are implemented by PL/SQL functions.

Audit Records

Oracle auditing permits audit information to be written to a database audit trail or to the audit trail of the underlying operating system. Audit records always include 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 database 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

Connections AS SYSDBA and AS SYSOPER along with attempts to startup or shutdown an instance are always recorded in the OS platform audit trail because they are OS events and because the database may not be available to be written into.

Oracle Database 10*g* provides for information to be written to the OS platform audit trail about all SQL commands performed by users connected as the special user SYS and users connected through the keywords AS SYSDBA and AS SYSOPER. Such OS audit trail files should have OS DAC protection set by the OS system administrator to prevent all database users being able to tamper with them (including those users who are able to connect to the database as the special user SYS or through the keywords AS SYSDBA or AS SYSOPER). Note that this auditing is still performed by the TOE but using an object provided by the underlying OS instead of the database audit trail.

Additional Auditing for OLS

OLS auditing supplements standard Oracle auditing by tracking use of its own administrative operations, and use of the policy privileges. Administrators can use either the SA_AUDIT_ADMIN package or Oracle Policy Manager to set and change the auditing options for an OLS policy.

When administrators create a new OLS policy, a label column for that policy is added to the database audit trail. The label column is created regardless of whether auditing is enabled or disabled, and independent of whether database auditing or operating system auditing is used. Whenever a record is written to the audit table, each policy provides a label for that record to indicate the session label. The label column is hidden (and hence cannot be explicitly selected by the user), but the administrator can create audit views to display these labels. Note that in the audit table, the label does not control access to the row; instead, it simply records the sensitivity of the row.

The auditing options which administrators specify apply only to subsequent sessions, not to the current session.

Notes:

- All audit records for OLS events are written directly to the database audit trail, even if operating system auditing is enabled.
- If auditing is disabled, then no OLS audit records are generated.
- Labels are not present in audit data written to the operating system audit trail.
- The audit trail is held in a table called AUD$, which is moved from the SYS schema to the SYSTEM schema when OLS is installed.

Security Management

Oracle Database 10*g* provides a number of mechanisms to support the management of database security. This section discusses the administrative system privileges, the importance of the initialisation file, the use of AS SYSOPER and AS SYSDBA, and Oracle Database 10*g* server dependencies on the administration of the underlying OS platform.

Administrative Privileges

Oracle Database 10*g* 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.

Database Administrative Users acquire the ability to perform administrative functions by being granted specific administrative system privileges. Other users are given only a minimal set of privileges allowing them to connect to the database and access the necessary data.

Oracle Database 10*g* security management can be delegated to any number of users. Site-specific roles can be defined to delegate administrative responsibilities based on organisational structures.

Initialisation File

When an Oracle Database 10*g* instance is started, the parameters specified in an initialisation file specify operational characteristics of Oracle Database 10*g* server functionality, including security functionality. It is critical that the security parameters specified in the initialisation 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 the TOE's Evaluated Configuration Document [OLS_ECD].

SYSDBA and SYSOPER

When a user is connected AS SYSOPER or AS SYSDBA, the user is authorised to perform special database operations. Authorisation to connect as 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), or by an Oracle Database 10*g* password.

A user connected AS SYSOPER is authorised to perform database startup, shutdown, create server parameter file and backup operations. A user connected via AS SYSDBA has the same authorisations as SYSOPER with the additional capabilities to create databases and perform the operations allowed by all system privileges WITH ADMIN option. Users who connect via AS SYSDBA have access to all of the data dictionary tables and can grant and/or revoke object privileges on other users' objects.

OS Administration

The security of the data managed by the Oracle Database 10*g* data server is dependent not only on the secure administration of Oracle Database 10*g*, 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 the TOE's Evaluated Configuration Document [OLS_ECD]. Guidance on the correct configuration of Oracle Database 10*g* for a specific OS platform is contained in the *Oracle Database 10g Installation and Configuration Guide* [ICG] for that platform. Finally, *Oracle Label Security Installation Notes* [OLS_IN] defines additional OS settings that are necessary when installing OLS.

Enterprise User Administration

In addition the security management also includes the management of the user information for Enterprise users which is stored in the Oracle Internet Directory. The roles and privileges for Enterprise users are determined form roles and privileges stored locally in the database as well as global roles stored and managed in the directory. Only the management of local roles and privileges as well as the assignment of priviliges to global roles is part of the TOE management functions while the assignment of global roles to Enterprise users is performed within the TOE environment (the directory server). The requirements for the protection and management of Enterprise users specific for the evaluated configuration are also identified in the TOE's Evaluated Configuration Document [OLS_ECD]. The standard procedures for management of Enterprise Users are described in *Oracle Database 10g Enterprise User Administrator's Guide* [EUA].

Consistency of Replicated TSF Data

TSF data is replicated in the TOE in the following situations:

- TSF data is stored in the system global area (SGA) or in the database cache in addition to its storage on disk. TSF data is held in data structures that are part of the database and the mechanisms used for maintaining the consistency between the cache/SGA and the data stored on disk apply for all database objects. Transaction management ensures the consistency of data between the cache and the disk.
- In the case of Real Application Clusters, the SGA and the cache are replicated in each node. Consistency for this replicated data is achived by having each item in the cache or SGA being managed by one dedicated master node for the item which initiates and controls the update of SGA and cache on the other nodes. Those updates are done using the interconnect. In addition the interconnect is also used for a heartbeat of each node. If a node fails to present the heartbeat, other nodes will take over the responsibility for the items managed by this node. Global locking mechanism are used to synchronize concurrent database updates in a RAC environment.

Secure Distributed Processing

The basic distributed features included in the Oracle Database 10*g* 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 (Oracle Database 10*g* 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 (see [SG, 15] and [DAG, Part VII]). Access to non-Oracle distributed databases is provided by Oracle Database 10*g*, but such databases are not part of the evaluated configuration.

OLS supports distributed operation when labels in the local and remote databases are compatible. Distributed databases behave in the standard way with OLS: the local user ends up connected as a particular remote user. OLS protects the labelled data, whether the user connects locally or remotely. If the remote user has the appropriate labels, he or she can access the data. If not, then access will be prevented.

Other Oracle Database 10*g* Security Features

In addition to the security features described above, Oracle Database 10*g* provides features which are related to security but do not directly address any of the functional requirements identified in this Oracle Database 10*g* Security Target. These features provide significant security capabilities to support robust and reliable database applications. Apart from Data Integrity, for which no specific security functionality is claimed in Chapter 6, the features described below are not part of the evaluated configuration defined in [OLS_ECD].

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.

When tables protected by label-based access controls (LBAC) are exported via OLS, their label columns and the applied policies are also exported automatically.

Backup and Recovery

Backup of an Oracle database can be performed using platform-specific backup programs, the Oracle database import/export utilities, or the Oracle database 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 Oracle Database 10*g* transaction integrity mechanisms also provide the basis for secure recovery following the failure of an Oracle Database 10*g* instance or platform operating system. Whenever an Oracle Database 10*g* 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.

Oracle Advanced Security

Oracle Advanced Security is an optional product which 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.

Supplied Packages

A number of standard packages are available to install in an Oracle 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.

Oracle Policy Manager

A set of standard packages is provided when OLS is installed. They implement the majority of OLS's facilities. Administrators may choose to use these packages via the Oracle Policy Manager GUI rather than by making direct calls.

External Authentication Services

In addition to the authentication methods described above, Oracle Database 10*g* can be configured to use an external third party authentication service. Only the use of Enterprise Users managed in a directory server is supported in the evaluated configuration as an authentication service based on information stored external to the TOE. In the case of Enterprise users the TOE will request the password verifier from the directory, compute the hash of the passowrd entered by the user and perform the comparison. Therefore Enterprise users are authenticated by the TOE based on a password verifier that is generated and managed in the TOE environment.

Application-Specific Security

Roles can be protected by use of a password. Applications can be created specifically to enable a role when the application is supplied with the correct password. Users can not enable the database role if they do not know the password.

Support for SQLJ

SQLJ allows application programmers to embed static SQL operations in Java code in a way that is compatible with the Java design philosophy. Oracle provides support for SQLJ at both the client and server, so that database applications written in Java may be executed at the client or at the server.

Oracle supports two SQLJ client side models; a thick client model where Java programs can make calls to the database via OCI using Oracle Net Services, and a thin client model where Java programs can call the database server directly bypassing the Oracle Net Services interface.

CHAPTER

3 Security Environment

Threats

[BR-DBMSPP], section 3.1 provides the characterization of the threat agents considered as well as the threats to be countered. The following additional threats are handled by the TOE:

T.RESOURCE Excessive Consumption of Resources. An authenticated database user consumes global database resources, in a way which compromises the ability of other database users to access the DBMS.

T.AUDIT_COMPROMISE A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.

T.LBAC Unauthorised Access to Labelled Information. An authorised database user accesses labelled information contained within a database without having the authorisation to access that information.

Organisational Security Policies

[BR-DBMSPP], section 3.2 provides the definition of the organizational security policies that apply for the TOE. The following policies are additional in this security target:

P.LABEL Labels can be associated with subjects and with storage objects which are rows within tables:

a) A label is composed of an hierarchic level (classification), a set of non-hierarchic categories, and a set of hierarchic groups, as determined by the organisation who owns the information stored in the database.

b) A storage object label reflects the sensitivity of the information stored in the object.

c) A subject label reflects the authorisation of the subject to access the organisation's labelled information according to defined access rules.

P.INFOFLOW Information flow from entity A to entity B shall be permitted only if it does not result in a subject being able to observe labelled information that the subject is not authorised to see.

Assumptions

As per [BR-DBMSPP], section 3.3. The following additions have been added to reflect the specific architecture of the TOE:

Underlying System Assumptions

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

A.DIR_PROT The directory server used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the directory. This includes the assumptions that queries are properly authenticated, that the TSF data stored in the directory is protected by the access control mechanisms of the directory server, that the TSF data in the directory server is properly managed by the administrative personnel, and that the directory server as well as its network connections are physically and logically protected from access and interference by unuathorized persons.

A.DIR_MGMT The information about enterprise users stored in the directory (password verifier, password policy, global roles and privileges) is managed correctly by authorized personnel of the Enterprise.

A.COM_PROT Interal TSF communication as well as communication between the TOE and the directory server are protected from unauthorized access to the transmitted data and ensure that the communication piers are the intended ones.

A.CLIENT_AP Client applications are assumed to be developed in accordance with Oracle's application development documentation and not use any undocumented interfaces of the client part of the TOE.

CHAPTER

4 Security Objectives

TOE Security Objectives

As per [BR-DBMSPP], section 4.1 with the addition of the following objectives:

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

O.AUDIT_REVIEW The TOE must provide the means of reviewing the audit log entries allowing user with the required access rights to the audit log to evaluate the audit log entries.

O.AUDIT_PROTECTION The TOE will provide the capability to protect audit information.

O.ACCESS.LBAC The TOE must provide the ability for labels to be associated with subjects and database objects in accordance with the P.LABEL security policy. For entities which have been associated with labels, the TOE must use these labels as a basis for implementing an information flow control policy in accordance with the P.INFOFLOW policy.

Environmental Security Objectives

As per [BR-DBMSPP], section 4.2 with the following addition:.

OE.USERS Those responsible for the TOE must ensure that users are assigned label authorisations and policy privileges commensurate with the degree of trust placed in them by the organisation that owns, or is responsible for, the information processed by or stored in the TOE.

OE.DIR_CONTROL The directory server must provide access control mechanisms to prohibit unauthorized access to directory entries. The directory server must authenticate users before it allows them to access TSF data stored in the directory.

OE.COM_PROT The environment must provide protection mechanisms that prohibit unauthorized access to data the TOE tranfers over communication links. This applies to data the TOE transmits to another part of itself as well as data exchanged between the TOE and the external directory server. This protection may be provided by physical protection, logical protection or a combination of both.

OE.CLIENT_AP The environment must ensure that only applications developed in accordance with the Oracle development guidance using the published interfaces are installed on the client system.

CHAPTER

5 IT Security Requirements

TOE Security Functional Requirements

Table 3 below lists each Security Functional Requirement (SFR) included in this Security Target. Since this Security Target claims compliance to [BR-DBMSPP], all SFRs listed in this Protection Profile are part of this table. Additional SFRs not contained in [BR-DBMSPP] are marked in bold.

For each SFR, Table 3 identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have additionally been applied, namely:
a) (for SFRs that are in [BR-DBMSPP]): the operations additional to those in [BR-DBMSPP]; or
b) (for SFRs that are not in [BR-DBMSPP]): the operations additional to Part 2 of [CC].

The remainder of this section details the functional requirements as completed for this Security Target. The text for completed operations which have been applied to the requirement relative to the Basic Robustness DBMS Protection Profile [BR-DBMSPP] or relative to Part 2 of [CC] (for SFRs that are not in [BR-DBMSPP]) is highlighted with *ITALICISED CAPITAL LETTERS* within each requirement. Annex B provides definitions for various terms used in the functional requirements.

Note that the SFRs for label-based access control are listed at the end of Table 3 (marked with a '*' in the first column) and are specified in a section entitled "LBAC SFRs Additional to those in [BR-DBMSPP]", which occurs after the specifications for the other SFRs.

Table 3: List of Security Functional Requirements

Component	Name	A	S	R	I
FAU_GEN.1-NIAP-0410	Audit Data Generation	X	X	X	
FAU_GEN_EXP.2	User and/or Group Identity Association				
FAU_SAR.1	**Audit Review**	**X**			
FAU_SAR.3	**Selectable Audit Review**	**X**	**X**		
FAU_SEL.1-NIAP-0407	Selective Audit	X	X		
FAU_STG.1	**Protected Audit Trail Storage**		**X**		
FAU_STG.4	**Prevention of Audit Data Loss**	**X**		**X**	
FDP_ACC.1	Subset Access Control				
FDP_ACF.1-NIAP-0407	Security Attribute Based Access Control	X	X		
FDP_RIP.1	Subset Residual Information Protection	X			
FIA_AFL.1	**Authentication Failure Handling**	**X**	**X**		
FIA_ATD.1	User Attribute Definition	X			
FIA_SOS.1	**Verification of Secrets**	**X**		**X**	
FIA_UAU.1	**Timing of Authentication**	**X**			
FIA_UID.1	**Timing of Identification**	**X**			
FIA_USB.1	**User-Subject Binding**	**X**			
FMT_MOF.1(1)	Management of Security Functions Behaviour				
FMT_MSA.1(1)	Management of Security Attributes				
FMT_MSA_EXP.3	Static Attribute Initialisation				
FMT_MTD.1(1)	Management of TSF Data (auditable events)				X
FMT_MTD.1(2)	**Management of TSF Data (other than auditable events)**	**X**	**X**	**X**	**X**
FMT_REV.1(1)	Revocation (User Attributes)	X			X
FMT_REV.1(2)	Revocation (Subject, Object Attributes)	X			X
FMT_SMF.1	Specification of Management Functions	X			
FMT_SMR.1	Security Roles	X			
FPT_RVM.1	**Non-Bypassability of the TSP**				

Component	Name	A	S	R	I
FPT_SEP_EXP.1	TSF Domain Separation				
FPT_TRC_EXP.1	Internal TSF Consistency				
FRU_RSA.1	**Maximum Quotas**	**X**	**X**		
FTA_MCS.1	Basic Limitation on Multiple Concurrent Sessions		X		
FTA_TAH_EXP.1	TOE Access History				
FTA_TSE.1	TOE Session Establishment	X			
FDP_IFC.1 *	**Subset Information Flow Control**	**X**			
FDP_IFF.2 *	**Hierarchical Security Attributes**	**X**		**X**	
FMT_MOF.1(2) *	**Management of Security Functions Behaviour**	**X**	**X**		**X**
FMT_MSA.1(2) *	**Management of security attributes**	**X**	**X**		**X**
FMT_MSA.3 *	**Static attribute initialisation**	**X**	**X**		

Note also that there is the possibility of confusion between the Common Criteria [CC] term “policy” and the OLS term “policy”. The Common Criteria term is used in the context of the phrase “Security Function Policy” (SFP) which is the security policy enforced by a particular Security Function (SF). OLS policies are established by a database administrator to specify how Label-Based Access Control is to be enforced on a database. Such a policy will always be referred to in this document via the phrase “OLS policy”.

Security Audit

FAU_GEN.1.1-NIAP-0410 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the *minimum* level of audit listed in table 9 *OF [BR-DBMSPP] AND TABLE 4 BELOW*; and
c) Start-up and shutdown of the DBMS;
d) Use of special permissions (e.g., those often used by authorized administrators to circumvent access control policies); and
e) *NO ADDITIONAL EVENTS.*

Table 4: List of Auditable Events for the additional SFRs

Component	Event	Additional Data
FAU_SAR.1	Reading of information from the DATABASE audit records	None
FAU_SAR.3	None	None
FAU_STG.1	None	None

Table 4: List of Auditable Events for the additional SFRs

Component	Event	Additional Data
FAU_STG.4	Actions taken due to audit storage failure	None
FIA_AFL.1	Locking of an account due to too many failed authentication attempts	None
FIA_SOS.1	Successful and unsuccessful attempts to change a user's password	None
FIA_UAU.1	All use of the DATABASE user authentication mechanism, including success or failure of the authentication attempt	None
FIA_UID.1	All use of the DATABASE user identification mechanism, including the DATABASE user identity provided	None
FIA_USB.1	Success and failure of binding of DATABASE user security attributes to a DATABASE subject (e.g. success and failure to create a DATABASE subject)	None
FMT_MTD.1(2)	None	None
FPT_RVM.1	None	None
FRU_RSA.1	All attempted uses of the DATABASE resource allocation functions for resources that are under control of the TSF	None
FDP_IFC.1	None	None
FDP_IFF.2	All decisions on requests for information flow	None
FMT_MOF.1(2)	All modifications in the behaviour of the functions in the TSF	None
FMT_MSA.1(2)	All modifications of the values of DATABASE OBJECT LABELS	NEW DATABASE OBJECT LABEL
FMT_MSA.3	Modifications of the default setting of permissive or restrictive DATABASE OBJECT LABEL rules	None

FAU_GEN.1.2-NIAP-0410 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column 3 of table 9 *OF [BR-DBMSPP]*.

FAU_GEN_EXP.2.1 For audit events resulting from actions of identified users and/or identified groups, the TSF shall be able to associate each auditable event with the identity of the user and/or group that caused the event.

FAU_SAR.1.1 The TSF shall provide *USERS WITH READ ACCESS TO SYS.AUD$* with the capability to read *ALL DATABASE AUDIT INFORMATION* from the audit records.

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

Application note:

In addition users can read their own audit records but do not have access to other audit records unless they satisfy the criteria defined by FAU_SAR.1.1.

FAU_SAR.3.1 The TSF shall provide the ability to perform *SEARCHES AND SORTING* of audit data based on *THE VALUES OF AUDIT DATA FIELDS*.

FAU_SEL.1.1-NIAP-0407 The TSF shall allow only the administrator to include or exclude auditable events from the set of audited events based on the following attributes:

a) user identity and/or group identity;
b) event type;
c) object identity;
d) *SUBJECT IDENTITY*;
e) success of auditable security events;
f) failure of auditable security events;
g) *DATABASE SYSTEM PRIVILEGE*;
h) *STATEMENT AUDITING*;
i) *PRIVILEGE AUDITING*;
j) *SCHEMA AUDITING*.

Application note:

[BR-DBMSPP] requires the ST writer to define the event type, but does not have an assignment or selection option in the SFR to do this. The ST author has therefore decided to to refine the requirement to include also the following criteria an administrator can use to include or exclude an auditable event:

1 Statement auditing
2 Privilege auditing
3 Schema object auditing

For additional information on those event types see [SG, chapter 8].

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to *PREVENT* unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.4.1 The TSF shall *PREVENT AUDITABLE EVENTS, EXCEPT THOSE TAKEN BY THE AUTHORISED USER WITH SPECIAL RIGHTS*, if the audit trail is full.

User Data Protection

FDP_ACC.1.1 The TSF shall enforce the Discretionary Access Control policy on all subjects, all DBMS-controlled objects and all operations among them.

Note that the Label-Based Access Control SFP is also to be applied to database subjects, objects and operations as specified in SFR FDP_IFC.1.1 and SFRs FDP_IFF.2.1 to FDP_IFF.2.7. These SFRs are given in the "SFRs Additional to those in [BR-DBMSPP]" section near the end of this chapter. The Label-Based Access Control SFP applies controls that are additional to the database object access control SFP.

FDP_ACF.1.1-NIAP-0407 The TSF shall enforce the Discretionary Access Control policy to objects based on the following:

a) the authorized user identity and/or group membership associated with a subject;
b) access operations implemented for DBMS-controlled objects; and
c) object identity.

FDP_ACF.1.2-NIAP-0407 The TSF shall enforce the following rules to determine if an operation among controlled subjects and DBMS-controlled objects is allowed:

The Discretionary Access Control policy mechanism shall, either by explicit authorized user/group action or by default, provide that database management system controlled objects are protected from unauthorized access according to the following ordered rules:

a) IF THE REQUESTED MODE OF ACCESS IS DENIED TO THAT AUTHORIZED USER, DENY ACCESS;
b) IF THE REQUESTED MODE OF ACCESS IS PERMITTED TO THAT AUTHORIZED USER, PERMIT ACCESS;
c) IF THE REQUESTED MODE OF ACCESS IS DENIED TO EVERY GROUP OF WHICH THE AUTHORIZED USER IS A MEMBER, DENY ACCESS;
d) IF THE REQUESTED MODE OF ACCESS IS PERMITTED TO ANY GROUP OF WHICH THE AUTHORIZED USER IS A MEMBER, GRANT ACCESS;
e) ELSE, DENY ACCESS

Application note:

[BR-DBMSPP] includes an application note for FDP_ACF.1.2-NIAP-0407 stating that the deny mode of access may be implicit. Oracle Database 10g does not have explicit deny lists, but satisfies the requirement by implicitly denying access unless it is explicitly allowed. As the application note in [BR-DBMSPP] explains this is compliant with the requirement FDP_ACF.1.2-NIAP-0407 as included in [BR-DBMSPP].

FDP_ACF.1.3-NIAP-0407 The TSF shall explicitly authorise access of subjects to DBMS-controlled 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 SYSDBA THEN THE REQUESTED ACCESS IS ALLOWED; OR*
c) *IF THE SUBJECT IS CONNECTED AS SYSOPER AND THE REQUESTED ACTION IS ONE OF THE OPERATIONS PERMITTED FOR THE SYSOPER USER SPECIFIED IN [DAG, 1], THEN THE REQUESTED ACCESS IS ALLOWED.*

FDP_ACF.1.4-NIAP-0407 The TSF shall explicitly deny access of subjects to objects based on the following rules: *NO ADDITIONAL EXPLICIT DENIAL RULES.*

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to *SCHEMA OBJECTS (INCLUDING NON-SCHEMA OBJECTS, WHICH ARE STORED IN THE SYS SCHEMA).*

Identification and Authentication

FIA_AFL.1.1 The TSF shall detect when *AN ADMINISTRATOR CONFIGURABLE POSITIVE INTEGER WITHIN THE RANGE 1 TO 2,147,483,646* unsuccessful authentication attempts occur related to *A LOCAL USER'S LAST SUCCESSFUL DATABASE SESSION ESTABLISHMENT.*

Application note:

The values allowed for those parameter in the evaluated configuration are defined in [OLS_ECD].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall *LOCK THE DATABASE USER'S ACCOUNT.*

Application note:

In the case of Enterprise Users no such counter is held and managed globally. Also for Enterprise Users the counters are held locally on each database instance.

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

a) Database user identifier and/or group memberships;
b) Security-relevant database roles;
c) *DATABASE OBJECT ACCESS PRIVILEGES*;
d) *DATABASE ADMINISTRATIVE PRIVILEGES*;
e) *AND FOR EACH OLS POLICY FOR WHICH THE USER HAS AUTHORISATION:*
A MAXIMUM LEVEL;
A MINIMUM LEVEL;
A (POSSIBLY EMPTY) SET OF AUTHORISED COMPARTMENTS;
FOR EACH AUTHORISED COMPARTMENT, A SPECIFICATION OF READ ACCESS OR READ-WRITE ACCESS;
A (POSSIBLY EMPTY) SET OF AUTHORISED GROUPS;
FOR EACH AUTHORISED GROUP, A SPECIFICATION OF READ ACCESS OR READ-WRITE ACCESS;

AN INITIAL SESSION LABEL;
A (POSSIBLY EMPTY) SET OF LABEL-BASED ACCESS CONTROL PRIVILEGES.

Application note:

Also in the case of Enterprise users the TSF will maintain the list of security attributes of the user once the user has been authenticated. The TSF will extract global roles of an Enterprsie user from the directory once the user is successfully authenticated and set the user's roles and privileges as the combination of both his local and global roles and the privileges assigned to those roles. After this step the directory is not contacted again during a user's session. All access decisions are performed by the TSF based on the user's security attributes determined after successful authentication.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets *(PASSWORDS FOR LOCAL USERS)* meet *REUSE, LIFETIME, AND CONTENT METRICS AS DEFINED BY AN AUTHORISED ADMINISTRATIVE USER.*

Application note:

In the case of Enterprise Users the Directory Server checks the password policy. This SFR for the TOE applies therefore only for local users. In the case of Enterprise Users the IT environment (the directory) will enforce the password policy defined by the directory.

FIA_UAU.1.1 The TSF shall allow *THE FOLLOWING LIST OF ACTIONS* on behalf of the user to be performed before the user is authenticated:

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

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

FIA_UID.1.1 The TSF shall allow *THE FOLLOWING LIST OF ACTIONS* on behalf of the user to be performed before the 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 user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user:
a) *USER IDENTIFIER, PRIVILEGES AND ROLES.*
b) *USER LABEL AUTHORISATIONS, INITIAL SESSION LABEL, INITIAL DEFAULT ROW LABEL AND POLICY PRIVILEGES.*

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users:

a) *ONCE A USER HAS BEEN SUCCESSFULLY IDENTIFIED AND AUTHENTICATED AT THE START OF A SESSION WITH THE TSF, THE USER'S IDENTIFIER IS ACCESSIBLE THROUGHOUT THAT SESSION.*
b) *AN OBJECT OR SYSTEM PRIVILEGE IS EFFECTIVE AT THE START OF A USER SESSION IF IT WAS PREVIOUSLY GRANTED TO THE USER (AND NOT SUBSEQUENTLY REVOKED) DIRECTLY, VIA THE PUBLIC USER GROUP OR VIA A ROLE, OR (IN THE CASE OF EN ENTERPRISE USER) GRANTED AS A GLOBAL ROLE OR PRIVILEGE IN THE DIRECTORY.*
c) *A USER ESTABLISHING A PROXY SESSION WITH THE TSF ON BEHALF OF ANOTHER USER CAN CONTROL WHICH ROLES ARE AVAILABLE TO THAT USER AT THE START OF THE SESSION.*
d) *AN OLS POLICY PRIVILEGE WILL BE EFFECTIVE FOR THE POLICY IN A USER SESSION ONLY IF THE USER HAD THE PRIVILEGE FOR THE POLICY BEFORE THE START OF THE SESSION.*
e) *AT THE START OF A USER SESSION, THE SESSION LABEL AND DEFAULT ROW LABEL FOR EACH APPLICABLE OLS POLICY ARE SET TO THE USER'S INITIAL SESSION LABEL AND INITIAL DEFAULT ROW LABEL ATTRIBUTES. THE EXCEPTION TO THIS IS THAT, IF OCI IS USED TO BEGIN A NEW SESSION WITHIN AN EXISTING SESSION, THE VALUES OF ANY APPROPRIATE SYS_CONTEXT VARIABLES INITIAL_LABEL AND INITIAL_ROW_LABEL FOR APPLICABLE OLS POLICIES ARE USED FOR SETTING THE SESSION LABEL AND DEFAULT ROW LABEL.*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

a) *IF AN OBJECT OR SYSTEM PRIVILEGE APPLYING TO A USER IS GRANTED OR REVOKED WHILE THE USER HAS A CURRENT SESSION WITH THE TSF, THIS CHANGE APPLIES TO THE SET OF LOCALLY MANAGED PRIVILEGES EFFECTIVE DURING THE USER SESSION. THIS RULE APPLIES TO PRIVILEGES GRANTED TO THE USER DIRECTLY OR VIA THE PUBLIC USER GROUP OR VIA A ROLE. IN THE CASE OF AN ENTERPRISE USER CHANGES TO HIS GLOBAL ROLES AND PRIVILEGES BECOME EFFECTIVE THE NEXT TIME THE USER LOGS ON.*
b) *DURING A SESSION WITH THE TSF, THE USER CAN CONTROL WHICH ROLES GRANTED TO THAT USER ARE EFFECTIVE.*
c) *IF A USER EXECUTES A VIEW OR A PROGRAM UNIT OWNED BY ANOTHER USER THAT WAS CREATED WITH "DEFINER'S RIGHTS", THE PRIVILEGES OF THE OWNING USER ARE EFFECTIVE DURING THE EXECUTION OF THE VIEW OR PROGRAM UNIT.*

d) *A LOCAL USER CAN CHANGE THE PASSWORD ASSOCIATED WITH THAT USER IF THE NEW PASSWORD COMPLIES WITH THE CONFIGURABLE CONTROLS INCLUDED IN THE PASSWORD MANAGEMENT INFORMATION THAT APPLIES TO THE USER.*
e) *A USER CAN CHANGE THE SESSION LABEL AND DEFAULT ROW LABEL FOR THE USER'S SESSION PROVIDED THESE LABELS REMAIN WITHIN THE USER'S LABEL AUTHORISATIONS.*
f) *AN OLS POLICY PRIVILEGE CHANGED DURING A SESSION ONLY BECOMES EFFECTIVE AT THE START OF THE NEXT USER SESSION.*
g) *DURING THE EXECUTION OF A STORED PROCEDURE, FUNCTION OR PACKAGE, THE USER'S SESSION LABEL AND THE OLS POLICY PRIVILEGES OF THE USER AND OF THE STORED PROCEDURE, FUNCTION OR PACKAGE ARE EFFECTIVE.*
h) *DURING THE EXECUTION OF A TRIGGER, THE SESSION LABEL AND THE POLICY PRIVILEGES OF THE USER THAT INVOKED THE TRIGGER ARE EFFECTIVE.*

Security Management

FMT_MOF.1.1(1) The TSF shall restrict the ability to disable and enable the functions relating to the specification of events to be audited to authorized administrators.

FMT_MSA.1.1(1) The TSF shall enforce the Discretionay Access Control policy to restrict the ability to manage all the security attributes to authorized administrators.

Application note:

This requirements is implemented as follows:

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 as sysdba.
c) database roles to database users authorized to modify roles.

This requirement applies to all security attributes stored and managed by the TSF. For security attributes managed outside of the TSF, the IT environment needs to ensure proper management.

FMT_MSA_EXP.3.1 The TSF shall enforce the Discretionary Access Control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

Application note:

This requirements applies to all security attributes managed locally by the TSF. For secuirty attributes managed outside of the TSF, the IT environment needs to ensure proper management.

FMT_MTD.1.1(1) The TSF shall restrict the ability to include or exclude the auditable events to authorized administrators.

FMT_MTD.1.1(2) The TSF shall, *ACCORDING TO TABLES* 5 *BELOW*, restrict the ability to *PERFORM OPERATIONS ON* the *TSF DATA* to *AUTHORIZED ADMINISTRATORS*.

FMT_REV.1.1(1) The TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to the authorised administrator.

Application note:

This requirements applies to all security attributes managed locally by the TSF. For secuirty attributes managed outside of the TSF, the IT environment needs to ensure proper management.

FMT_REV.1.2(1) The TSF shall enforce the *FOLLOWING* rules:

a) *REVOCATION OF DATABASE ADMINISTRATIVE PRIVILEGES SHALL TAKE EFFECT PRIOR TO WHEN THE DATABASE USER BEGINS THE NEXT DATABASE SESSION*;

FMT_REV.1.1(2) The TSF shall restrict the ability to revoke security attributes associated with the objects within the TSC to the authorised administrator and database users as allowed by the Discretionary Access Control policy.

FMT_REV.1.2(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 DATABASE USER BEGINS THE NEXT DATABASE SESSION*;

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

a) *THE OPERATIONS ON TSF DATA SPECIFIED IN TABLE 5 BELOW*;
b) *MODIFICATION OF THE DATABASE OBJECT SECURITY ATTRIBUTES AS SPECIFIED IN SFR FMT_MSA.1.1*.
c) *MODIFICATION OF THE LABEL-BASED ACCESS CONTROL SECURITY ATTRIBUTES AS SPECIFIED IN SFR FMT_MSA.1.1.2;*
d) *SETTING THE PRIVILEGES THAT PERMIT AUTHORISED ADMINISTRATIVE USERS TO MODIFY THE BEHAVIOUR OF THE LABEL-BASED ACCESS CONTROL FUNCTIONS.*

Table 5: Required Management Events

Component	Operation	TSF Data
FAU_GEN.1-NIAP-0410	-	-
FAU_GEN_EXP.2	-	-

Component	Operation	TSF Data
FAU_SAR.1	deletion, modification, addition	the group of database users with read access right to the database audit records
FAU_SAR.3	-	-
FAU_SEL.1-NIAP-0407	maintenance of the right to view / modify	the database audit events
FAU_STG.1	-	-
FAU_STG.4	a) maintenance b) deletion, modification, addition	actions to be taken in case of DATABASE audit storage failure
FDP_ACC.1	-	-
FDP_ACF.1-NIAP-0407	managing	the attributes used to make explicit access or denial based decisions
FDP_RIP.1	-	-
FIA_AFL.1	management	a) the threshold for unsuccessful DATABASE authentication attempts b) actions to be taken in the event of an DATABASE authentication failure
FIA_ATD.1		
FIA_SOS.1	management	the metric used to verify the DATABASE secrets
FIA_UAU.1	management	a) the DATABASE authentication data b) the DATABASE authentication data by the associated DATABASE user c) the action lists, if an authorised DATABASE administrator can change the actions allowed before authentication
FIA_UID.1	management	the user identities
FIA_USB.1	-	-
FMT_MOF.1(1)	manage	auditable events

Component	Operation	TSF Data
FMT_MSA.1(1)	manage	the group of DATABASE roles that can interact with the DATABASE security attributes
FMT_MSA_EXP.3	manage	a) the group of DATABASE roles that can specify initial values b) the permissive or restrictive setting of default values for a given DATABASE access control SFP
FMT_MTD.1	manage	the group of DATABASE roles that can interact with the TSF data
FMT_REV.1(1)		
FMT_REV.1(2)		
FMT_SMR.1	manage	the group of DATABASE users that are part of a DATABASE role
FMT_RVM.1	-	-
FPT_SEP_EXP.1	-	-
FRU_RSA.1	specify	maximum limits for a resource for DATABASE groups and/or individual DATABASE users and/or DATABASE subjects by a DATABASE administrator
FTA_MCS.1	manage	the maximum allowed number of concurrent DATABASE user DATABASE sessions by a DATABASE administrator
FTA_TAH_EXP.1	-	-
FTA_TSE.1	-	-
FDP_IFC.1	-	-
FDP_IFF.2	Managing	The attributes used to make explicit access ordenial based decisions
FMT_MOF.1(2)	Managing	The group of roles that can interact with the functions in the TSF
FMT_MSA.1(2)	Manage	The group of database roles that can interact with the *DATABASE OBJECT LABELS*
FMT_MSA.3	Manage	The permissive or restrictive setting of default values for the *LABEL-BASED ACCESS CONTROL SFP*

FMT_SMR.1.1 The TSF shall maintain the roles:

a) authorized administrator; and
b) *DATABASE USER*;
c) *DATABASE ROLES DEFINED BY SUITABLY PRIVILEGED DATABASE ADMINISTRATIVE USERS.*

FMT_SMR.1.2 The TSF shall be able to associate users with 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 the TSC is allowed to proceed.

FPT_SEP_EXP.1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.2 The TSF shall enforce separation between the security domains of subjects in the TOE Scope of Control.

FPT_TRC_EXP.1.1 The TSF shall ensure that TSF data is consistent between parts of the TOE by providing a mechanism to bring inconsistent TSF data into a consistent state in a timely manner.

Application note:

It should be noted that the TOE holds TSF data like all the user related data, all the privileges and user roles as well as its configuration data and audit data in data structures that are part of the database. The TOE replicates TSF data between the disk and its cache and system global area to ensure fast access to the data. Consistency between the data on disk and the data in the cache is achieved using the database mechanisms to ensure data integrity on database update.

In the case of Real Application Cluster, the cache and system global area itself are replicated on each node and consistency is achieved using RAC specific functions to manage the update of items in the cache or system global area on each node.

It should be noted that other mechanisms like RAID may optionally be used to ensure consistency of replicated data on disks. Those mechanism are not part of the TOE but are part of the TOE environment. They are neither mandated by the TOE, nor are they - if used - evaluted in any way in this evaluation.

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 USER* can use *OVER A SPECIFIED PERIOD OF TIME.*

TOE Access

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

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of *AN ADMIN CONFIGURABLE NUMBER OF* sessions per user.

FTA_TAH_EXP.1.1 Upon successful session establishment, the TSF shall store and retrieve the date and time of the last successful session establishment to the user.

FTA_TAH_EXP.1.2 Upon successful session establishment, the TSF shall store and retrieve the date and time of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on attributes that can be set explicitly by authorized administrator(s), including user identity and/or group identity, time of day, day of the week, and *NO ADDITIONAL ATTRIBUTES.*

Application note:

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

LBAC SFRs Additional to those in [BR-DBM-SPP]:

.

User Data Protection

FDP_IFC.1.1 The TSF shall enforce the *LABEL-BASED ACCESS CONTROL SFP* on:

a) DATABASE SUBJECTS;
b) LABELLED DATABASE OBJECTS;
c) ALL PERMITTED OPERATIONS ON LABELLED OBJECTS BY A DATABASE SUBJECT COVERED BY THE SFP.

FDP_IFF.2.1 The TSF shall enforce the *LABEL-BASED ACCESS CONTROL SFP* based on the following types of subject and information security attributes:

a) DATABASE SUBJECT LABELS; AND
b) LABELS OF THE DATABASE OBJECT CONTAINING THE INFORMATION.

Note: Labels shall include an hierarchic classification level and a (possibly empty) set of non-hierarchic categories and a (possibly empty) set of hierarchic groups. An object is to have one label for each OLS policy that applies to it.

FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and a controlled object via a controlled operation if the following rules, based on the ordering relationships between security attributes, hold:

a) A DATABASE SUBJECT MAY OBSERVE THE CONTENTS OF A DATABASE OBJECT ONLY IF, FOR EVERY OLS POLICY THAT APPLIES TO THE OBJECT:
READ_CONTROL FOR THE POLICY IS OFF OR THE SESSION LABEL OF THE DATABASE SUBJECT DOMINATES THE LABEL OF THE DATABASE OBJECT; AND

b) A DATABASE SUBJECT MAY MODIFY A DATABASE OBJECT ONLY IF, FOR EVERY OLS POLICY THAT APPLIES TO THE OBJECT:
THE RELEVANT WRITE_CONTROL IS OFF FOR THE POLICY
OR
IF THE POLICY WAS NOT CREATED WITH THE INVERSE GROUP OPTION,
THEN
(*THE LEVEL IN THE OBJECT'S LABEL IS GREATER THAN OR EQUAL TO THE SUBJECT'S MINIMUM LEVEL AND LESS THAN OR EQUAL TO THE SUBJECT'S SESSION LEVEL,*
AND
(THE OBJECT'S LABEL CONTAINS GROUPS AND THE SUBJECT'S LABEL ALLOWS WRITE ACCESS TO ONE OF THE GROUPS (OR ITS PARENT) IN THE OBJECT'S LABEL AND THE SUBJECT'S LABEL INCLUDES ALL THE COMPARTMENTS IN THE OBJECT'S LABEL,
OR
THE OBJECT'S LABEL CONTAINS NO GROUPS AND THE SUBJECT'S LABEL ALLOWS WRITE ACCESS TO ALL THE COMPARTMENTS IN THE OBJECT'S LABEL
))
ELSE
(*THE LEVEL IN THE OBJECT'S LABEL IS GREATER THAN OR EQUAL TO THE SUBJECT'S MINIMUM LEVEL AND LESS THAN OR EQUAL TO THE SUBJECT'S SESSION LEVEL,*
AND
THE GROUPS IN THE OBJECT'S LABEL FORM A SUPERSET OF THE GROUPS IN THE SUBJECT'S LABEL,
AND
THE MAXIMUM SET OF AUTHORISED INVERSE GROUPS THAT CAN BE SET IN ANY SUBJECT'S SESSION LABEL IS A SUPERSET OF THE GROUPS IN THE OBJECT'S LABEL
AND
THE SUBJECT'S LABEL ALLOWS WRITE ACCESS TO ALL THE COMPARTMENTS IN THE OBJECT'S LABEL
).

Note: OLS policies assigned to objects shall specify which controls are to be applied when a subject attempts to access an object.
Note also that the phrase "OR ITS PARENT" in the above SFR is to be taken to mean "OR ITS PARENT OR ITS PARENT'S PARENT OR ITS PARENT'S PARENT'S PARENT ETC.".

FDP_IFF.2.3 The TSF shall enforce the *RULE TO ALLOW A USER TO CHANGE THE SESSION LABEL TO A COMBINATION OF ANY OF THE USER'S AUTHORISED COMPARTMENTS AND GROUPS WITH A LEVEL IN THE RANGE BOUNDED BY THE USER'S MAXIMUM AND MINIMUM LEVEL*.

FDP_IFF.2.4 The TSF shall provide the following *ADDITIONAL SFP CAPABILITY*:
THE TSF WILL EXECUTE A STORED PROCEDURE, FUNCTION OR PACKAGE AT THE EXECUTING USER'S CURRENT SESSION LABEL AND WITH THE SET OF LABEL-BASED ACCESS CONTROL PRIVILEGES FORMED BY THE UNION OF THE PRIVILEGES OF THE EXECUTING USER AND THE PRIVILEGES GIVEN TO THE STORED PROCEDURE, FUNCTION OR PACKAGE.

FDP_IFF.2.5 The TSF shall explicitly authorise an information flow based on the following rule:
IF THE SUBJECT HAS THE APPROPRIATE LABEL-BASED ACCESS CONTROL PRIVILEGE FOR THE OPERATION, THEN THE INFORMATION FLOW WILL BE PERMITTED.

FDP_IFF.2.6 The TSF shall explicitly deny an information flow based on the following rules: *NONE*.

FDP_IFF.2.7 The TSF shall enforce the following relationships for any two valid information flow control security attributes (*LABELS)*:

a) There exists an ordering function that, given two valid *LABELS*, determines if the *LABELS* are equal, if one *LABEL* is greater than the other, or if the *LABELS* are incomparable; and.
b) There exists a "least upper bound" in the set of *LABELS*, such that, given any two valid *LABELS*, there is a valid *LABEL* that is greater than or equal to the two valid *LABELS*; and
c) There exists a "greatest lower bound" in the set of *LABELS*, such that, given any two valid *LABELS*, there is a valid *LABEL* that is not greater than the two valid *LABELS.*

Note: The TSF is to enforce an ordering function "greater than" whereby Label1 is greater than Label2 if Label1 dominates Label2 and Label1 is not equal to Label2. Label1 and Label2 are incomparable if Label1 does not dominate Label2 and Label2 does not dominate Label1.

Security Management

FMT_MOF.1.1(2) The TSF shall restrict the ability to *MODIFY THE BEHAVIOUR OF* the *LABEL-BASED ACCESS CONTROL* functions to *AUTHORISED ADMINISTRATIVE USERS.*

FMT_MSA.1.1(2) The TSF shall enforce the *LABEL-BASED ACCESS CONTROL SFP* to restrict the ability to *MODIFY* the security attributes *LABELS AND PRIVILEGES* to *SUITABLY PRIVILEGED USERS.*

FMT_MSA.3.1 The TSF shall enforce the *LABEL-BASED ACCESS CONTROL SFP* to provide *NO* default values for *DATABASE OBJECT* security attributes that are used to enforce the *LABEL-BASED ACCESS CONTROL SFP*.

Note: The TSF is to ensure that, when a user creates an object which is controlled by the Label-Based Access Control SFP, a value must be specified for the label.

FMT_MSA.3.2 The TSF shall allow *NO DATABASE USERS* to specify alternative initial values to override the default values *FOR LABEL-BASED ACCESS CONTROL SECURITY ATTRIBUTES* when *A DATABASE OBJECT* is created.

Note: The TSF is to ensure that, when an object is created which is controlled by the

Label-Based Access Control SFP, no database user can cause a value to be given to the label other than that specified for the label in conformance with the rules of the SFP.

TOE Security Assurance Requirements

The target assurance level is EAL4 as defined in Part 3 of the CC, augmented with ALC_FLR.3. This is a superset of the security assurance requirements of [BR-DBMSPP]

Security Requirements for the IT Environment

This section defines the security functional requirements for the IT environment. The SFRs additional to the ones defined in [BR-DBMSPP] are related to the external directory server used to support authentication for Enterprise Users.

Since all the requirements in this section are related to the IT environment, a refinement has been made in all the SFRs that substitutes "TSF" be "IT Environment". This refinement is maked in *CAPITAL, ITALICS AND UNDERLINE*.

As per [BR_DBMSPP, section 5.2] plus:

FDP_ACC.1.1 The *IT ENVIRONMENT* shall enforce the *DIRECTORY ACCESS CONTROL POLICY* on *USERS OF THE DIRECTORY* as subjects and *TSF DATA FOR USERS OF THE TOE* as objects and *ALL OPERATIONS THAT CREATE, READ, MODIFY OR DELETE THOSE OBJECTS.*

FDP_ACF.1.1 The *IT ENVIRONMENT* shall enforce the *DIRECTORY ACCESS CONTROL POLICY* to objects based on *SUCCESSFUL AUTHENTICATION OF ANY USER OF THE DIRECTORY.*

FDP_ACF.1.2 The *IT ENVIRONMENT* shall enforce the following rules to determine if an operation among a controlled subject and a controlled object is allowed:
IF THE USER HAS THE ROLE OF AN ENTERPRISE SECURITY MANAGER AND HAS THE REQUIRED DISCRETIONARY ACCESS RIGHTS TO THE DIRECTORY ENTRIES HE WANTS TO ACCESS, ACCESS IS ALLOWED. OTHERWISE ACCESS IS DENIED.

FDP_ACF.1.3 The *IT ENVIRONMENT* shall explicitly authorize access of subjects to objects based on the following additional rules: *NONE.*

FDP_ACF.1.4 The *IT ENVIRONMENT* shall explicitly deny access of subjects to objects based on the *FOLLOWING ADDITIONAL RULES: NONE.*

FIA_SOS.1.1 The *IT ENVIRONMENT* shall provide a mechanism to verify that secrets *(PASSWORDS FOR TOE USERS MANAGED IN THE DIRECTORY)* meet *REUSE, LIFETIME, AND CONTENT METRICS AS DEFINED BY AN AUTHORISED ADMINISTRATIVE USER.*

FIA_UAU.2.1 The *IT ENVIRONMENT* shall require each *DIRECTORY* user to be successfully authenticated before allowing any other *DIRECTORY*-TSF-mediated actions on behalf of that *DIRECTORY* user.

FIA_UID.2.1 The *IT ENVIRONMENT* shall require each *DIRECTORY* user to identify itself before allowing any other *DIRECTORY*-TSF-mediated actions on behalf of that *DIRECTORY* user.

FMT_MSA.1.1 The *IT ENVIRONMENT* shall enforce the *DIRECTORY ACCESS CONTROL POLICY* to restrict the ability to *QUERY, MODIFY, OR DELETE* the *SECURITY ATTRIBUTES OF ENTERPRISE USERS AND THE LDAP SERVER* to *THE ENTERPRISE SECURITY MANAGER AND* [assignment: *OTHER* authorized identified roles].

Application Note: In order not to prescribe the exact securty functions of the directory server some instantiations have not been performed. It is left up to the individual directory server product to define the roles that are allowed to perform those operations or define additional operations that are controlled. The requirement is just that at a minimum the operations defined are controlled and that they can be restricted to some role. Therefore the definition of the roles is left open here as well as in other SFRs for the directory server.

FMT_MSA.3.1 The *IT ENVIRONMENT* shall enforce the *DIRECTORY ACCESS CONTROL POLICY* to provide [selection: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The *IT ENVIRONMENT* shall allow the [assignment: the authorized identified roles] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1.1 The *IT ENVIRONMENT* shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the *DIRECTORY-TSF*].

FMT_SMR.1.1 The *IT ENVIRONMENT* shall maintain the roles *ENTERPRISE SECURITY MANAGER AND* [assignment: *OTHER* authorized identified roles].

FMT_SMR.1.2 The *IT ENVIRONMENT* shall be able to associate users with roles.

Note that [BR-DBMSPP] requires the underlying operating system to satisfy the requirements of either a Basic Robustness Protection Profile for operating systems or the Controlled Access Protection Profile [CAPP]. In the case of this Security Target all operating systems listed in chapter 1 have been evaluated for compliance with [CAPP] and all security functional requirements of [CAPP] are therefore considered to be SFRs for the operating system component of the IT environment.

Minimum Strength of Function

The minimum strength of function for the TOE is *SOF-High*. This exceeds the requirements in [BR-DBMSPP], where an SOF claim of SOF-basic is made.

This Page Intentionally Blank

CHAPTER

6 TOE Summary Specification

TOE Security Functionality

This section contains a high-level specification of each Security Function (SF) of the TOE that contributes to satisfaction of the Security Functional Requirements of chapter 5. The specifications cover five major areas: identification and authentication, database resource quotas, access controls, privileges and roles, and auditing.

Table 6 below shows that all the SFRs are satisfied by at least one SF and that every SF is used to satisfy at least one SFR (but note that SFRs FDP_ACF.1.4 and FDP_IFF.2.6 are not satisfied by any particular SF because these SFRs specify null functionality).

Table 6: Mapping of SFs to non-LBAC SFRs

	FIA										
	AFL.1.1	AFL.1.2	ATD.1.1	SOS.1.1	UAU.1.1	UAU.1.2	UID.1.1	UID.1.2	USB.1.1	USB.1.2	USB.1.3
F.IA.PRE					Y	Y	Y	Y			
F.IA.UID								Y			
F.IA.DBA						Y		Y		Y	
F.IA.EUA						Y		Y		Y	
F.IA.CNF											
F.IA.IDE								Y		Y	
F.IA.CSA						Y		Y			
F.IA.CSN						Y		Y			
F.IA.PWD	Y	Y		Y							
F.IA.ATT			Y						Y		
F.IA.ATT-EU			Y						Y		
F.IA.USE				Y							Y
F.LIM.CNF				Y							
F.LIM.POL											
F.LIM.NSESS											
F.LIM.TIME											
F.LIM.RSESS											
F.LIM.RCALL											
F.ACCESS											
F.DAC.OBID											
F.DAC.OBREF											
F.DAC.SUA											
F.DAC.OBA											
F.DAC.POL											
F.DAC.SEP											
F.DAC.OR											
F.APR.GOP											
F.APR.ROP											
F.APR.GRSP											
F.APR.GRR											
F.APR.DER											
F.APR.EDR											Y
F.PRI.SPRIV										Y	Y
F.PRI.XVP											Y
F.PRI.PRX										Y	
F.PRI.DEF											
F.AUD.SOM											
F.AUD.SEV											
F.AUD.ALW											
F.AUD.CNF											
F.AUD.ACC											
F.AUD.DEL											
F.AUD.INF											
F.AUD.LCOL											
F.AUD.LAUD											
F.AUD.LEN											
F.AUD.LDIS											
F.AUD.VIEW											
F.AUD.LVIEW											
F.AUD.FULL											
F.CON.DIC											
F.CON.RAC											

	FDP					
	ACC.1.1	ACF.1.1-NIAP	ACF.1.2-NIAP	ACF.1.3-NIAP	ACF.1.4-NIAP	RIP.1.1
F.IA.PRE						
F.IA.UID						
F.IA.DBA						
F.IA.EUA						
F.IA.CNF			Y			
F.IA.IDE						
F.IA.CSA						
F.IA.CSN						
F.IA.PWD						
F.IA.ATT						
F.IA.ATT-EU						
F.IA.USE						
F.LIM.CNF						
F.LIM.POL						
F.LIM.NSESS						
F.LIM.TIME						
F.LIM.RSESS						
F.LIM.RCALL						
F.ACCESS	Y	Y	Y	Y		
F.DAC.OBID	Y	Y	Y			
F.DAC.OBREF	Y	Y	Y			
F.DAC.SUA	Y	Y				
F.DAC.OBA	Y	Y				
F.DAC.POL		Y	Y	Y		
F.DAC.SEP						
F.DAC.OR						Y
F.APR.GOP						
F.APR.ROP						
F.APR.GRSP						
F.APR.GRR						
F.APR.DER						
F.APR.EDR						
F.PRI.SPRIV		Y	Y	Y		
F.PRI.XVP						
F.PRI.PRX						
F.PRI.DEF						
F.AUD.SOM						
F.AUD.SEV						
F.AUD.ALW						
F.AUD.CNF			Y	Y		
F.AUD.ACC						
F.AUD.DEL						
F.AUD.INF						
F.AUD.LCOL						
F.AUD.LAUD						
F.AUD.LEN						
F.AUD.LDIS						
F.AUD.VIEW						
F.AUD.LVIEW						
F.AUD.FULL						
F.CON.DIC						
F.CON.RAC						

	FMT											
	MOF.1.1	MSA.1.1	MSA_EXP.3.1	MTD.1.1(1)	MTD.1.1(2)	REV.1.1(1)	REV.1.2(1)	REV.1.1(2)	REV.1.2(2)	SMF.1.1	SMR.1.1	SMR.1.2
F.IA.PRE												
F.IA.UID											Y	
F.IA.DBA												
F.IA.EUA												
F.IA.CNF												
F.IA.IDE												
F.IA.CSA											Y	Y
F.IA.CSN											Y	
F.IA.PWD												
F.IA.ATT					Y					Y		
F.IA.ATT-EU					Y					Y		
F.IA.USE												
F.LIM.CNF					Y	Y				Y		
F.LIM.POL												
F.LIM.NSESS												
F.LIM.TIME												
F.LIM.RSESS												
F.LIM.RCALL												
F.ACCESS												
F.DAC.OBID												
F.DAC.OBREF												
F.DAC.SUA												
F.DAC.OBA												
F.DAC.POL			Y									
F.DAC.SEP												
F.DAC.OR												
F.APR.GOP		Y			Y					Y		
F.APR.ROP		Y			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
F.PRI.SPRIV			Y				Y		Y			
F.PRI.XVP												
F.PRI.PRX												Y
F.PRI.DEF			Y									
F.AUD.SOM												
F.AUD.SEV				Y								
F.AUD.ALW												
F.AUD.CNF	Y											
F.AUD.ACC					Y					Y		
F.AUD.DEL					Y					Y		
F.AUD.INF												
F.AUD.LCOL												
F.AUD.LAUD												
F.AUD.LEN												
F.AUD.LDIS												
F.AUD.VIEW												
F.AUD.LVIEW												
F.AUD.FULL												
F.CON.DIC												
F.CON.RAC												

	FPT				FRU	FTA				
	RVM.1.1	SEP_EXP.1.1	SEP_EXP.1.2	TRC_EXP.1.1	RSA.1.1	MCS.1.1	MCS.1.2	TAH_EXP.1.1	TAH_EXP.1.2	TSE.1.1
F.IA.PRE										
F.IA.UID										
F.IA.DBA										
F.IA.EUA										
F.IA.CNF										
F.IA.IDE	Y	Y	Y							
F.IA.CSA								Y	Y	Y
F.IA.CSN								Y	Y	Y
F.IA.PWD										
F.IA.ATT										
F.IA.ATT-EU										
F.IA.USE										
F.LIM.CNF					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.ACCESS										
F.DAC.OBID										
F.DAC.OBREF										
F.DAC.SUA										
F.DAC.OBA										
F.DAC.POL	Y									
F.DAC.SEP		Y	Y							
F.DAC.OR										
F.APR.GOP										
F.APR.ROP										
F.APR.GRSP										
F.APR.GRR										
F.APR.DER										
F.APR.EDR										
F.PRI.SPRIV										
F.PRI.XVP										
F.PRI.PRX										
F.PRI.DEF										
F.AUD.SOM										
F.AUD.SEV										
F.AUD.ALW										
F.AUD.CNF										
F.AUD.ACC										
F.AUD.DEL										
F.AUD.INF										
F.AUD.LCOL										
F.AUD.LAUD										
F.AUD.LEN										
F.AUD.LDIS										
F.AUD.VIEW										
F.AUD.LVIEW										
F.AUD.FULL										
F.CON.DIC				Y						
F.CON.RAC				Y						

	FAU									
	GEN.1.1-NIAP	GEN.1.2-NIAP	GEN_EXP2.1	SAR.1.1	SAR.1.2	SAR.3.1	SEL.1.1NIAP	STG.1.1	STG.1.2	STG4.1
F.IA.PRE										
F.IA.UID										
F.IA.DBA										
F.IA.EUA										
F.IA.CNF										
F.IA.IDE										
F.IA.CSA										
F.IA.CSN										
F.IA.PWD										
F.IA.ATT										
F.IA.ATT-EU										
F.IA.USE										
F.LIM.CNF										
F.LIM.POL										
F.LIM.NSESS										
F.LIM.TIME										
F.LIM.RSESS										
F.LIM.RCALL										
F.ACCESS										
F.DAC.OBID										
F.DAC.OBREF										
F.DAC.SUA										
F.DAC.OBA										
F.DAC.POL										
F.DAC.SEP										
F.DAC.OR										
F.APR.GOP										
F.APR.ROP										
F.APR.GRSP										
F.APR.GRR										
F.APR.DER										
F.APR.EDR										
F.PRI.SPRIV										
F.PRI.XVP										
F.PRI.PRX										
F.PRI.DEF										
F.AUD.SOM	Y						Y			
F.AUD.SEV	Y						Y			
F.AUD.ALW	Y						Y			
F.AUD.CNF							Y			
F.AUD.ACC				Y		Y				
F.AUD.DEL								Y	Y	
F.AUD.INF		Y	Y							
F.AUD.LCOL		Y								
F.AUD.LAUD	Y									
F.AUD.LEN	Y									
F.AUD.LDIS	Y									
F.AUD.VIEW					Y	Y				
F.AUD.LVIEW					Y	Y				
F.AUD.FULL										Y
F.CON.DIC										
F.CON.RAC										

Table 7: Mapping of SFs to LBAC SFRs

	FDP								FMT			
	IFC.1.1	IFF.2.1	IFF.2.2	IFF.2.3	IFF.2.4	IFF.2.5	IFF.2.6	IFF.2.7	MOF.1.1(2)	MSA.1.1.(2	MSA.3.1	MSA.3.2
F.IA.PRE												
F.IA.UID												
F.IA.DBA												
F.IA.EUA												
F.IA.CNF												
F.IA.IDE												
F.IA.CSA												
F.IA.CSN												
F.IA.PWD												
F.IA.PWD-EU												
F.IA.ATT												
F.IA.USE												
F.IA.POLICY		Y								Y		
F.IA.SESSION		Y										
F.IA.SESSUPD				Y								
F.LIM.CNF												
F.LIM.POL												
F.LIM.NSESS												
F.LIM.TIME												
F.LIM.RSESS												
F.LIM.RCALL												
F.ACCESS	Y											
F.DAC.OBID												
F.DAC.OBREF												
F.DAC.SUA												
F.DAC.OBA												
F.DAC.POL												
F.DAC.SEP												
F.DAC.OR												
F.LBAC.POL	Y	Y	Y			Y		Y				
F.LBAC.LABSET		Y									Y	Y
F.LBAC.LABUPD		Y								Y		
F.LBAC.REF	Y	Y										
F.LBAC.TRIGGER		Y				Y						
F.LBAC.XVP					Y							
F.LBAC.MOD									Y			
F.APR.GOP												
F.APR.ROP												
F.APR.GRSP												
F.APR.GRPP										Y		
F.APR.GRR												
F.APR.DER												
F.APR.EDR												
F.PRI.SPRIV												
F.PRI.PPRIV						Y						
F.PRI.XVP												
F.PRI.PRX												
F.AUD.SOM												
F.AUD.SEV												
F.AUD.ALW												
F.AUD.CNF												
F.AUD.ACC												
F.AUD.DEL												
F.AUD.INF												
F.AUD.LCOL												
F.AUD.LAUD												
F.AUD.LEN												
F.AUD.LDIS												
F.AUD.VIEW												
F.AUD.LVIEW												
F.AUD.FULL												

	FDP								FMT			
	IFC.1.1	IFF.2.1	IFF.2.2	IFF.2.3	IFF.2.4	IFF.2.5	IFF.2.6	IFF.2.7	MOF.1.1(2)	MSA.1.1.(2)	MSA.3.1	MSA.3.2
F.CON.DIC												
F.CON.RAC												

Identification and Authentication

F.IA.PRE The TOE shall only allow users to:

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

b) establish a connection;

c) receive error messages upon error.

before identifying and authenticating the user.

Note that users can obtain the current Oracle version string and version number by calling OCIServerVersion, as described in [OCI, 16: OCIServerVersion].

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

F.IA.DBA DBMS Identification and Authentication:

If a user is configured in the TOE as a *local user* being *authenticated by* a password then the TOE will:

a) identify the user by confirming that the user provides a valid user identifier, and

b) authenticate the user by confirming that the user provides a password corresponding to the stored password for that user.

F.IA.EUA Enterprise User Identification and Authentication:

If a user is configured in the TOE as an *Enterprise User* being *authenticated* by a password then the TOE will:

a) identify the user by confirming with a reqeust to the directory that the user provides a valid user identifier or a global user, and

b) authenticate the user by confirming that the value of the password presented by the user is identical to the password verifier retrieved for that user from the directory.

Note that in the case of an enterprise user the TOE is still mediating the authentication, obtains the user's password, computes the hash value of the password, obtains the password verifier for that user from the directory and compares the two values. Only in this case the TOE will allow the user login to proceed and will establish a session for the user. In the case the two values don't match the TOE will reject the user.

The TOE therefore is directly involved in the authentication process, although the hash value of the password is stored and managed outside of the TOE. The TOE therefore has to rely on the correct operation of the directory server, the correct management of the user's password and security attributes in the directory server, the protection of the user's password and security attributes in the directory server, and the protection of the communication between the TOE and the directory server. Still

the TOE is directly involved in the user identification and authentication process since the external user will use the same TSF interface for authentication and perform the comparison of the hash vcalues, regardless if the TOE uses local authentication or Enterprise User authentication.

F.IA.OSA (deleted)

SF F.IA.OSA concerns OS Identification and Authentication, which is not appropriate for use with UNIX and Linux operating systems. F.IA.OSA is mentioned here because it was included in the Security Target for the evaluation of Oracle9i, which had Microsoft Windows NT 4.0 as one of its operating system platforms. All references to OS Identification and Authentication functionality in the other SFs in this chapter have been removed for this evaluation.

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. The supplied LOGON trigger function can be used to restrict the ability of a user to login to specific days of the week and specific times of the day. Such a LOGON trigger can also be used to store and retrieve the time and day of the last successful login as well as the number of unsuccessful login attempts since the last successful login.

(Note: triggers are functions the database calls upon specific events. Login is one of the those events a trigger can be assigned to.)

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 the SYS user (for AS SYSDBA connections) or the PUBLIC user (for AS SYSOPER connections) only if the provided user identifier and password correspond to users stored in the Oracle password file as being allowed SYSDBA or SYSOPER connections, respectively.

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

F.IA.PWD The TOE provides the following configurable controls on passwords for *local users*: [SQL, 15: CREATE PROFILE]

a) the number of failed login attempts before the user account is locked,

b) the number of days the same password can be used before expiring,

c) the number of days before which a password cannot be reused,

d) the number of password changes required before the current password can be reused,

e) the number of days a user account will be locked after the specified number of consecutive failed logins,

f) the number of days of grace period after a password expires before the user account is locked,

g) a password complexity check to screen passwords selected by the user.

F.IA.ATT The data dictionary contains a unique set of security attributes for each user including their username, password management information, account status (i.e. locked or unlocked), privileges, roles and resource limits that can be displayed and modified by suitably authorised users using standard SQL commands.

F.IA.ATT-EU In the case of an enterprise user the password management information is held in the directory. Privileges and roles are determined by the TOE using a combination of the local privileges and roles stored for the user in the local database and the global roles stored and managed for the user in the directory.

Note that the determination of a user's privileges and attributes is still a function of the TOE even in the case of enterprise users, although this function then may retrieve and use also information about the user from the directory. Note that the directory stores only information about the global roles a user has. Assigning privileges to those global roles is still done in each database. The privileges assigned to global roles may therefore differ from database to database. Managing the privileges assigned to global roles is therefore done in each database and uses the same management functions as are used for managing local roles.

F.IA.USE A local database user is authorised to change the password associated with that user within the following constraints:

a) If the user's profile includes a complexity check function, then the new password is accepted only if it meets the criteria of the complexity check.

b) If the user's profile specifies password reuse constraints and the user attempts to reuse a password, the TOE rejects the change if the reuse constraints are not met. [SQL, 15: CREATE PROFILE].

F.IA.POLICY For each OLS policy defined for the database, the data dictionary contains a set of security attributes for each user authorised to access data protected by that policy. These security attributes include the user label authorisations, initial session label, initial default row label and policy privileges. The user label authorisations consist of a maximum and minimum level, a set of authorised compartments, a set of authorised groups, and, for each such compartment and group, a specification of read-only access or read-write access. When first created, a user has no such security attributes, but they can be set and modified by suitably authorised users.

F.IA.SESSION When starting a new database session, the session label and default row label for each applicable OLS policy are set as follows:

a) When a user connects to the database, for each OLS policy for which the user is authorised, the TOE will set the session label and default row label for the user's session using the user's initial session label and initial default row label attributes defined for the policy in the data dictionary;

b) If a user is already connected to the database, but uses OCI to begin a new database session, for each OLS policy for which there is a SYS_CONTEXT, if the SYS_CONTEXT variables INITIAL_LABEL and INITIAL_ROW_LABEL are within the user's label authorisations, then they are used instead of the user's attributes in the data dictionary in setting the session label and default row label.

F.IA.SESSUPD A user can change the session label and default row label for the user's session provided these labels remain within the user's label authorisations.

Resource 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.ACCESS For all attempts by subjects to access objects which are subject to the administration of rights, the TOE shall:

a) verify the validity of the request on the basis of the discretionary access control policy and, if the object has a label, the label-based access control policy; and

b) reject the attempt if either the discretionary or the label-based access checks fail.

Note that if the discretionary access check fails, the label-based access check will not be made.

Discretionary 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, 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;

c) and any security policies providing fine-grained access control for 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

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.

allowed. The object privileges relevant to different types of objects are specified in [SQL, 18: GRANT (*grant_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 schema-specific operations are specified in [SQL, 18: GRANT (*grant_system_privileges)*] and provide the ability to restrict a user's use of operations to those operations which do not modify objects.

d) To perform DML operations that are required to issue a DDL statement the user must have all the privileges required as directly granted privileges. Privileges received through a role will not be evaluated in this case.

e) If the user is connected AS SYSDBA (the database session has the privilege to override the access controls) then the requested access is allowed.

f) If the user is connected AS SYSOPER and the operation is one of those specified in [DAG, 1: Database Administrator Authentication (OSDBA and OSOPER)], 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].
Label-Based Access Control	**F.LBAC.POL**	The label-based access policy of the TOE shall permit a subject to access an object which has a label only if, for all OLS policies protecting the object: a) the LBAC access mediation rules permit the subject to perform the operation as follows: observation of the contents of a database object by a database subject is governed by the rules as specified in FDP_IFF.2.2a, and elaborated in [OLSAG, 3: The Oracle Label Security Algorithm for Read Access, [OLSAG, 8: READ CONTROL_ Reading Data, and [OLSAG, 14: Algorithm for Read Access with Inverse Groups],

modification of a database object by a database subject is governed by the rules as specified in FDP_IFF.2.2b, and elaborated in [OLSAG, 3: The Oracle Label Security Algorithm for Write Access, [OLSAG, 8: WRITE_CONTROL: Write Data, and [OLSAG, 14: Algorithm for Write Access with Inverse Groups]; or

b) the subject's database session has the necessary OLS policy privileges which enable override of the LBAC access mediation rules (see [OLSAG, 3: Using Oracle Label Security Privileges] and [OLSAG, 14: Algorithms for COMPACCESS Privilege with Inverse Groups]); or

c) the user is SYS or LBACSYS or is connected AS SYSDBA; or

d) the subject's database session has the system privilege EXEMPT ACCESS POLICY effective.

Note that the LBAC policy applies to subjects which are database users and processes and tasks running on behalf of such users and applies to objects which are rows in tables that have been assigned one or more OLS policies. Further details on the LBAC policy are provided in:

- *[OLSAG, 8: Choosing Policy Options] and [OLSAG, 14: How Inverse Groups Work], which describe the various policy options*
- *[OLSAG, 8: Exemptions from Oracle Label Security Policy Enforcement], which describes the exemptions that are allowed from OLS policy enforcement*
- *[OLSAG, 8: Inserting Labeled Data Using Policy Options and Labeling Functions], [OLSAG, 8: Updating Labeled Data Using Policy Options and Labeling Functions], [OLSAG, 8: Deleting Labeled Data Using Policy Options and Labeling Functions] and [OLSAG, 14], which describe how the enforcement options and labelling functions affect the insertion, update and deletion of labelled data*
- *[OLSAG, 8: Using a SQL Predicate with an Oracle Label Security Policy], which describes the use of SQL predicates with an LBAC policy*
- *[OLSAG, 4: Determining Upper and Lower Bounds of Data] and [OLSAG, 14: LEAST_UBOUND with Inverse Groups] and [OLSAG, 14: GREATEST_LBOUND with Inverse Groups], which describe the Least Upper Bound and Greatest Lower Bound functions which relate to the dominance relationship used for some of the LBAC mediation rules*
- *[OLSAG, A: Analyzing the Relationship Between Labels] and [OLSAG, 14: Dominance Rules for Labels with Inverse Groups], which describe functions to calculate whether a label dominates another label*
- *[OLSAG, 14] which describes the releasabilities scheme which is implemented via the INVERSE_GROUP policy enforcement option .*

Note that an implication of this SF is that a subject can only access an object that has been put under the protection of more than one OLS policy if the LBAC mediation rules for <u>all</u> of these OLS policies permit the subject to access the object.

F.LBAC.LABSET When inserting a row in a table protected by an OLS policy, the row's label for each such policy is set according to the

enforcement options defined for the policy (see [OLSAG, 4: Inserting Labeled Data] and [OLSAG, 8: The Label Management Enforcement Options] up to and including the section headed "Understanding Labeling Functions in Oracle Label Security Policies").

F.LBAC.LABUPD Attempts to update the label of a row in a table protected by an OLS policy are subject to the enforcement options defined for the policy (see [OLSAG, 8: The Overriding Enforcement Options] and [OLSAG, 8: Evaluating Enforcement Control Options and UPDATE]).

F.LBAC.REF If a child row is being inserted or updated when the parent row is in a table protected by an OLS policy, then if the child row is in a table which has a referential integrity constraint, the user must have LBAC read access to the parent row.

F.LBAC.TRIGGER The TOE will execute a trigger with the session label and with the policy privileges of the user that invoked the trigger.

F.LBAC.XVP The TOE will execute a stored procedure, function or package with the user's session label and with the set of OLS policy privileges which is the union of:

a) the OLS policy privileges of the executing user; and

b) the OLS policy privileges assigned to the stored procedure, function or package.

Note that if another stored procedure, function or package (which is known as a "stored program unit") is called within the execution of the original stored program unit, it runs with the same OLS policy privileges as the original stored program unit.

F.LBAC.MOD The TOE only allows suitably privileged users to modify or delete the packages that implement LBAC.

Note that only trusted administrators have sufficient privilege to affect the way LBAC operates by modifying or deleting the relevant packages.

Privileges and Roles

Oracle Database 10*g* has implemented a role concept that allows to define new roles, assign privileges (including privileges to access database objects) to a role and assign roles to users. This mechanism allows to model the concept of a "group" where system privileges and object privileges are assigned to a group and users inherit such privileges when they become a member of the group. Therefore "group access rights to database objects" as required by [BR-DBMSPP] can be easily modelled in Oracle Database 10*g* using the role model and assigning object privileges to roles. The privileges assigned to roles are always defined in the local database, but an Enterprise user may have global roles assigned to him, which are stored and maintained in the directory. The privileges that a user gets assigned via those roles are those that are associated with this role in each local database.

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 connected AS SYSDBA; *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.GRPP For a given OLS policy, *policy*, a user (the grantor) can grant a policy privilege to another user or to a stored program unit and can revoke a policy privilege from the grantee, only if the grantor (or revoker) has been granted the *policy*_DBA role and has the EXECUTE privilege for the SA_USER_ADMIN package.

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 connected AS SYSDBA; *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.

To create a role a user must have the CREATE ROLE system privilege.

Note that c) includes the case where the grantor is the user who created the role - see [SG, 11: Granting the ADMIN OPTION], which states:"When a user creates a role, the role is automatically granted to the creator with the ADMIN OPTION.".

Enabling and Disabling Roles

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

a) As a default role, in which case the role will be enabled automatically for each database session created by that user[1].

b) As a non-default role, in which case

i. if the role is configured in the TOE as being *identified* using a package, then that package must explicitly enable the role during a database session in order for any other roles within that role to be

1. A default role is enabled at session creation bypassing any authorisation required for that role.

enabled and any privileges within that role to become effective for that user; or

ii. if the role is configured in the TOE as being *not identified*, then 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.

iii. if the role is configured in the TOE as being *identified globally* then the user can only be authorized to use the role by an enterprise directory service. The role is defined in the database by granting privileges and roles to it, but the global role can not be granted itself to any user or other role in the database. When a global user attempts to connect to the database, the enterprise directory is queried to obtain any global roles associated with the 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[1]), subject to the following restrictions which apply to 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.

Note: the 'set role' command can not be implemented on a remote database via a Database link. You cannot specify a role identified globally. Global roles are enabled by default at login, and cannot be reenabled later.

Effective Privileges

F.PRI.SPRIV An object or system 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.

1. When a role that has been granted other roles is enabled all the indirectly granted roles are implicitly enabled.

F.PRI.PPRIV An OLS policy privilege will be effective for the policy in a user session only if the privilege was set in the user's data dictionary entry for the policy before the start of the 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 directly granted privileges of the owning user) to allow other users to have controlled access to specified aggregations of data.

F.PRI.PRX A suitably authorised user can provide other users with the ability to establish a proxy connection for another user. The authorised user can control which user roles are available to the proxy session.

F.PRI.DEF When a new user is created, by default the new user's objects are stored in the database default tablespace. If no default tablespace is assigned for the database, the user's objects are stored in the SYSTEM tablespace.

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;

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;

d) by use of data access based on content;

e) 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;

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

g) for each event of type a) and c);

i. for all users;

ii. for specified users;

iii. for specified proxies on behalf of any user;

iv. for specified proxies on behalf of specified users;

F.AUD.ALW Irrespective of the TOE's audit configuration, the TOE will audit every successful occurrence of the following events to the operating system:

a) start-up;

b) shut-down;

c) connection through the keywords AS SYSDBA or AS SYSOPER.

Note that for the Solaris and Linux platforms, OS auditable Oracle records are written to standard text file audit logs in the OS.

F.AUD.CNF The TOE will allow only a suitably authorised user to set or alter the audit configuration for a database. This includes also enabling or disabling of the audit function in general.

Note that, by default (after installation), the TOE allows only SYS and SYSTEM (who are granted the DBA role during installation) and users connected AS SYSDBA *to set and alter the audit configuration. It is possible for these users to grant the relevant privileges to other users.*

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 authorised user can view all audit records;

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

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 number 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 connection to a database, whether successful or not, at least the following information is recorded when the TOE is configured to audit connection

1. By default, the TOE allows only SYS and SYSTEM (who are granted the DBA role during installation) and users connected AS SYSDBA to delete or update rows from the database audit trail (which is held in SYSTEM.AUD$ for OLS). 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.

attempts: date and time of event, username, instance number 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, starting 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.LCOL Whenever an audit record is written to the database audit trail, for each OLS policy that has been created for the database, a label column is present which can hold the session label.

F.AUD.LAUD The TOE will allow a suitably authorised user to enable or disable auditing of labels for a specified OLS policy.

F.AUD.LEN The TOE will allow a suitably authorised user to enable auditing of OLS events to the database audit trail for a particular OLS policy, specifying options for:

a) specific users to be audited;

b) whether auditing is BY ACCESS or BY SESSION;

c) whether events with SUCCESSFUL and/or NOT SUCCESSFUL outcomes are to be audited;

d) specific OLS events to be audited:

i. application of specified OLS policy to tables or schemas;

ii. removal of specified OLS policy from tables or schemas;

iii. the setting of user authorisations and user and program privileges;

iv. the use of all policy-specific privileges.

Note that audit records for OLS events will not be written to the audit trail unless the AUDIT_TRAIL initialisation parameter has been set to DB or OS in the database's parameter file prior to starting up the database.

F.AUD.LDIS The TOE will allow a suitably authorised user to disable auditing of OLS events to the database audit trail for a particular OLS policy, specifying options for:

a) specific users not to be audited;

b) specific OLS events not to be audited:

i. application of specified OLS policy to tables or schemas;

ii. removal of specified OLS policy from tables or schemas;

iii. the setting of user authorisations and user and program privileges;

iv. the use of all policy-specific privileges.

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

F.AUD.LVIEW The TOE allows a suitably authorised user to create a view of the audit trail which contains the specified policy's label column as well as all the entries in the audit trail written on behalf of the policy.

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.

Data Consistency

F.CON.DIC TSF data used by the database is stored in the database dictionary, which is itself treated as a database object. The data dictionary is a collection of database tables and views containing reference information about the database, its structures, and its users. Oracle accesses the data dictionary frequently during SQL statement parsing. This access is essential to the continuing operation of Oracle.

The data dictionary is accessed so often by Oracle that two special locations in memory are designated to hold dictionary data. One area is called the data dictionary cache, also known as the row cache because it holds data as rows instead of buffers (which hold entire blocks of data). The other area in memory to hold

dictionary data is the library cache. All Oracle user processes share these two caches for access to data dictionary information.

When accessing data in the dictionary the Oracle database first checks if the requested data is in the cache. If not, the cache functions are used to load the data into the cache potentially overwriting another block in the cache. The Oracle database includes functions that will ensure that cache entries are marked dirty when they are updated and will ensure that dirty cache entries are written back to disk in due time (at least before they are overwritten by another block retrieved from disk).

F.CON.RAC Real Application Clusters (RAC) use a cache-to-cache block transfer mechanism known as Cache Fusion to transfer read-consistent images of blocks from one instance to another. RAC does this using high speed, low latency interconnects to satisfy remote requests for data blocks. This ensures that all nodes will access the latest version of a block of the database (including one from the dictionary) they need to read or update. RAC includes protocols that tell other nodes when it needs shared or exclusive access to a block, get this access granted using a global locking mechanism, control that no other node has any conflicting lock, write dirty blocks to disk, update the information about the block in other nodes and release any lock granted.

Note: This Security Function applies only when the TOE is configured with Real Application Clusters(RAC). In configurations without RAC, data consistency in a clustered configuration is not considered and consistency is achieved solely by the security function F.CON.DIC.

Security Mechanisms and Techniques

When authentication is performed by Oracle Database 10*g*, a password is used for authentication. The TOE performs a cryptographic hash function (using a modified Data Encryption Standard (DES) algorithm) on passwords prior to storing them in the database. The TOE password management functions (together called the PWD mechanism) provide a Strength of Function level of *SOF-high* for the passwords of local users. This exceeds the DBMS PP Strength of Function level of *SOF-basic* as required by [BR-DBMSPP].

Specific SFs supporting the claimed SOF are:

- F.IA.DBA (SOF-High); *and*
- F.IA.PWD, F.IA.ATT & F.IA.USE support F.IA.DBA by providing password management mechanisms for passwords of local users.

In the case of en enterprise user, the password is managed in the directory server and stored there in the same way as the password for local users is stored in the database dictionary. The directory server allows to define a password policy ensuring that the passwords meet a Strength of Function level of *SOF-high* but passwords managed by the directory server are not rated since the directory server is part of the TOE environment.

Assurance Measures

The target assurance level is EAL4 augmented with ALC_FLR.3, which exceeds the assurance requirements for basic robustness as stated in [BR-DBMSPP]. No other specific assurance measures are claimed. The following table identifies the Oracle Database 10*g* documentation that supports each security assurance requirement for EAL4 and also the assurance requirement for ALC_FLR.3.

Table 8: TOE 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	[OQM]
ADO_IGS.1	Installation, Generation, and Startup	[ICG] [OLS_IN] [OLS_ECD]
ADV_FSP.2	Fully Defined External Interfaces	[ERR] [OCI]
ADV_HLD.2	Security Enforcing High-level Design	[AD] [OLS_AD]
ADV_IMP.1	Subset of the TSF Implementation	[SRC] [OLS_SRC]
ADV_LLD.1	Descriptive Low-level Design	[DD] [OLS_DD]
ADV_RCR.1	Informal Correspondence Demonstration	[AD] [OLS_AD] [DD] [OLS_DD] [DT] [SRC]
ADV_SPM.1	Informal TOE Security Policy Model	[OLS_SPM]
AGD_ADM.1	Administrator Guidance	[OLS_ECD] [GA] [OLS_GA] and Oracle publications relevant to administrators
AGD_USR.1	User Guidance	[GA] [OLS_GA] and Oracle publications relevant to users
ALC_DVS.1	Identification of Security Measures	[SODE]
ALC_LCD.1	Developer Defined Life Cycle Model	[LCS]
ALC_TAT.1	Well Defined Development Tools	[CM]
ATE_COV.2	Analysis of Coverage	[TP]
ATE_DPT.1	Testing - High-level Design	[TP]

Table 8: TOE Assurance Measures

Component	Name	Documents
ATE_FUN.1	Functional Testing	[TP]
ATE_IND.2	Independent Testing	[TP]
AVA_MSU.2	Validation of Analysis	[GA] [OLS_GA]
AVA_SOF.1	Strength of TOE Security Functions	[SOF]
AVA_VLA.2	Independent Vulnerability Analysis	[VA] [OLS_VA]
ALC_FLR.3	Systematic Flaw Remediation	[FLR]

CHAPTER

7 Protection Profile Claims

PP Reference

The TOE conforms to the U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.1 [BR-DBMSPP].

PP Tailoring

Table 3 in chapter 5 identifies each SFR for this Security Target that was derived from [BR-DBMSPP] and the tailoring operations performed relative to [BR-DBMSPP]. The tailoring is identified in *ITALICISED CAPITAL LETTERS* within the text of each SFR in chapter 5. All of the tailoring operations are in conformance with the assignments and selections in [BR-DBMSPP]. Security functional requirements additional to those defined in [BR-DBMSPP] are marked bold in table 3 of chapter 5. Tailoring of those SFRs with respect to part 2 of the CC is also identified in *ITALICISED CAPITAL LETTERS.*

PP Additions

There are three additional threats not listed in [BR-DBMSPP]:

T.RESOURCE has been added as the threat of a single user attempting to consume database reources in a way that would prohibit other users from accessing the DBMS.

T.AUDIT_COMPROMISE has been added as the threat of an unauthorized user to compromise the audit trail such that accountability of a user for his actions is no longer given.

T.LBAC has been added to address the threat of a user getting access to labelled information without having the appropriate clearance.

There are two additional organisational security policies not listed in [BR-DBMSPP]:

P.LABEL addresses the policy to assign the appropriate label to database objects and subjects.

P.INFOFLOW addresses the policy to ensure that the rules of the label based access control prohibits users to get access to information they are not cleared for.

There are the following additional security objectives not listed in [BR-DBMSPP]:

O.ACCESS.LBAC has been added to address the threat T.LBAC.

O.RESOURCE has been added to address the threat T.RESOURCE.

O.AUDIT_REVIEW has been added to address the ability of the TOE to provide functions for authorized administartors to evaluate the audit log entries. This objective supports the organizational security policy P.ACCOUNTABILITY included in [BR-DBMSPP]. Reviewing the audit records is a function [BR-DBMSPP] allows to be done in the IT-environment, but Oracle Database 10g provides its own functions to do this.

O.AUDIT_PROTECTION has been added to address the ability of the TOE to protect its audit trail. While [BR-DBMSPP] allows to store the audit trail in storage managed and protected by the IT environment, Oracle Database 10g uses objects it controls itself to store the audit trail. Therefore the TOE is also responsible for the protection of the audit trail.

Note that the additional objectives O.AUDIT_REVIEW and O.AUDIT_PROTECTION have been taken from [BR-MAN] with O.AUDIT_REVIEW being phrased more specific.

There is an additional security objective for the IT environment, OE.DIR_CONTROL addressing the objective for a controlled directory server in the IT environment to support authetication of Enterprise Usrers.

There is another additional security objective for the environment, OE.COM_PROT addressing the objective of securing the communication between distributed parts of the TOE and between the TOE and the external directory server.

There is an additional underlying system assumption, A.MIDTIER, which is included to ensure accountability in multi-tier environments. Although the O-RDBMS can audit the actions of a proxy user, accountability relies upon the correct identity of the client (given during the connection by the middle-tier). As explained in chapter 1 (TOE Overview), this type of environment is an addition to the scope of evaluation (which was first introduced for Oracle8i).

An additional assumption A.DIR_PROT is included to address the issue of users managed centrally in a directory server.

An additional assumption A.COM_PROT is included to address the issue of secure communication between different parts of the TOE as well as between the TOE and the directory server.

Table 3 and Table 4 in chapter 5 list each Security Functional Requirement (SFR) included in this Security Target not related to the label based access control. These SFRs were all included in [BR-DBMSPP], with the exception of those additional SFRs marked in bold in tables 3 and 4 of chapter 5. Table 4 in chapter 5 lists the additional Security Functional Requirements related to the label based access control function.

The assurance requirements specified in this security target are those for EAL4 augmented with ALC_FLR.3. This is a superset of all assurance requirements listed in [BR-DBMSPP].

The additional threats and objectives have been included to address the additional se-

curity functional requirements in the ST. Some of the additional security functional requirements address also security objectives listed in [BR-DBMSPP]. They actually address the sometimes incomplete coverage of the objectives listed in [BR-DBMSPP] by the security functional requirements listed in [BR-DBMSPP]. The rationale chapter in this document will discuss this in more detail.

A number of security functional requirements for the IT environment has been added to address the use of an external directory server for the support of the authentication of Enterprise Users and the management of security attributes od such users.

This Page Intentionally Blank

CHAPTER

8 Rationale

Security Objectives Rationale

As per [BR-DBMSPP, chapter 6] with the additional TOE security objectives O.RESOURCE, O.AUDIT_REVIEW, O.AUDIT_PROTECTION, O.ACCESS.LBAC and the additional environmental security objectives OE.DIR_CONTROL and OE.COMPROT.

This section therefore discusses only the additional security objectives not included in [BR-DBMSPP].

O.RESOURCE helps to mitigate the threat T.RESOURCE by ensuring that individual users can not use more of specific resources than defined in their quota. An authorized administrator that can assign quotas to users can use this function to ensure that a sufficient amount of resources of a specific kind is always available allowing authorized users to use the DBMS at any time they are allowed by the TOE policy to use it.

O.AUDIT_REVIEW helps to address the organizational security policy P.ACCOUNTABILITY by providing authorized administrators with the ability to selectively review the audit log information.

O.AUDIT_PROTECTION helps to mitigate the threat T.AUDIT_COMPROMISE by protecting the audit trail from unauthorized access and loss of audit records.

O.ACCESS.LBAC helps to mitigate the threat T.LBAC and also addresses the policies P.LABEL and P.INFOFLOW.

OE.DIR_CONTROL addresses the need to control an external directory server used as an external entity supporting the TOE in the authentication of Enterprise Users. Proper authentication and access control is required to prohibit that user information stored in the directory is accessed in an unauthorized way. OE.DIR_CONTROL is mapped to SFRs for the IT environment (specific for the directory server).

OE.COM_PROT addresses the need to protect communication links between distributed parts of the TOE as well as between the TOE and the external directory server.

OE.CLIENT_AP addresses the need to have only applications installed on the client system that are developed in accordance with the Oracle development guidance and

use only the interefaces published there.

The rationales for T.LBAC, P.LABEL and P.INFOFLOW are given below.

T.LBAC Rationale

T.LBAC (*Unauthorised Access to Labelled Information*) is directly countered by O.ACCESS.LBAC, which ensures that labels are provided for objects and subjects and uses these labels to enforce an information flow control policy. OE.USERS ensures that administrators assign appropriate label authorisations and policy privileges to users.

P.LABEL Rationale

P.LABEL is directly satisfied by O.ACCESS.LBAC, which requires provision of labels for subjects and database objects as defined by P.LABEL. OE.USERS supports this OSP by ensuring that administrators assign appropriate label authorisations and policy privileges to users in accordance with P.LABEL.

P.INFOFLOW Rationale

P.INFOFLOW is directly satisfied by O.ACCESS.LBAC, which requires provision of an information flow control policy as defined by P.INFOFLOW. OE.USERS supports this OSP by ensuring that administrators assign appropriate label authorisations and policy privileges to users.

Assumptions Rationale

The assumptions rationale in [BR-DBMSPP, chapter 6.2] applies to the TOE, with the following additions:

A.MIDTIER states that any middle-tier must pass the original client ID through to the TOE. A.MIDTIER is directly provided by OE.NO_EVIL because [ECD] includes this requirement for the use of a middle-tier and advises the administrator how to configure it correctly.

A.DIR_PROT states that the directory server used to store information for Enterprise Users is protected from unauthoized access and managed correctly. A.DIR_PROT is provided by OE.DIR_CONTROL and the guidance for the configuration and management of the directory server. OE.DIR_CONTROL is an objective for the IT environment, since the directory server is not part of the TOE.

A.DIR_MGMT states that the the information about Enterprise uers stored in the directory is managed by authorized personnel only. This is provided by OE.DIR_CONTROL which allows to restrict access to the information on Enterprise users to defined users.

A.COM_PROT states that communication links between distributed parts of the TOE as well as communication links between the TOE and the external directory server need to be protected. This assumption is covered by OE.COM_PROT.

A.CLIENT_AP states that client applications shall be developed in accordance with the Oracle development documentation and only use the published interfaces. This assumption is covered by OE.CLIENT.AP.

Security Requirements Rationale

Suitability of Security Requirements

[BR-DBMSPP, section 6.3] show that the SFRs defined in [BR-DBMSPP, sections 5.1 and 5.2 and 5.3] satisfy the IT security objectives defined in [BR-DBMSPP].

The table below correlates the IT security objectives to the SFR that is additional to those provided in [BR-DBMSPP] which satisfy them (as indicated by a *Y*), showing that each IT security objective is satisfied by the additional SFR, and that the additional SFR satisfies at least one IT security objective. Note that some additional SFRs actually contribute to satisfy security objectives defined in [BR-DBMSPP]. Therefore the security objectives those SFRs contribute to are listed in the table, while those security objectives listed in [BR-DBMSPP] where none of the additional SFRs contribute to are not listed.

Table 9: Correlation of IT Security Objectives to SFRs Additional to [BR-DBMSPP]

Requirement	O.RESOURCE	O.AUDIT_REVIEW	O.AUDIT_PROT.	O.PART_SELF_P	O.TOE_ACCESS	O.ACCESS.LBAC
FAU_SAR.1		Y				
FAU_SAR.3		Y				
FAU_STG.1			Y			
FAU_STG.4			Y			
FIA_AFL.1					Y	
FIA_SOS.1					Y	
FIA_UAU.1					Y	
FIA_UID.1					Y	
FIA_USB.1					Y	
FPT_RVM.1				Y		
FRU_RSA.1	Y					
FDP_IFC.1						Y
FDP_IFF.2						Y
FMT_MOF.1(2)						Y
FMT_MSA.1(2)						Y
FMT_MSA.3						Y

O.ACCESS.LBAC Suitability

O.ACCESS.LBAC is directly provided by FDP_IFC.1 which defines the objects of

the information control policy and FDP_IFF.2 which defines the information control policy rules. FMT_MOF.1 and FMT_SMF.1 ensure that the behaviour of the information control policy mechanism is protected from unauthorised modification. FMT_MSA.1.1.2, FMT_SMF.1, FMT_MSA.3.1.2 and FMT_MSA.3.2.2 provide support for the management of the information control security attributes used in controlling access to database objects.

Thus the extra IT security objective for OLS is satisfied by the SFRs which are additional to those provided in [BR-DBMSPP] and each such additional SFR is necessary to satisfy the extra IT security objective for OLS.

Suitability of the additional SFRs

FAU_SAR.1 in conjunction with FMT_MTD.1(2) and FMT_SMF.1 allows an authorized administrator to read the audit records.

FAU_SAR.3 in combination with FAU_SAR.1 allows to evaluate the audit records thus assisting in making users accountable for their actions.

FAU_STG.1 in combination with FPT_SEP_EXP.1 allows the TOE to protect the audit records from unauthorized deletion.

FAU_STG.4 in combination with FPT_SEP_EXP.1, FMT_MTD.1(2) and FMT_SMF.1 allows to limit the loss of audit records in the event the audit log gets full.

FIA_AFL.1 in combination with FMT_MTD.1(2) and FMT_SMF.1 allows an authorized administrator to limit the number of unsuccessful authentication attempts.

FIA_SOS.1 in combination with FMT_MTD.1(2) and FMT_SMF.1 allows an authorized administrator to define a password policy enforcing a defined metric for password quality.

FIA_UAU.1 in combination with FIA_UID.1 ensures that users must identify and authenticate correctly before they are allowed to use TOE functions that require access control, accountability or the use of resources that can be limited.

FIA_UID.1 supports FIA_UAU.1 and ensures that the TOE is able to identify the identity of users as required for the access control, accountability and resource control functions.

FIA_USB.1 relies on FIA_UAU.1 and FIA_UID.1 to provide the correct user identity and allows database subjects to identify the user they are action on behalf of. This function allows the TSF to link calls of TSF interfaces by database subjects with the user this call is associated with and thus perform access control, accountability and resource control also for functions a database subject performs on behalf of a user.

FPT_RVM.1 ensures that any access to controlled resources of the TOE that is performed using interfaces of the TOE is mediated by the access control functions of the TOE.

FRU_RSA.1 in combination with FMT_MTD.1(2) and FMT_SMF.1 ensures that an authorized administrator is able to define resource limits for defined resources that a user is allowed to use and ensure that the user does not exceed the defined limits.

FDP_IFC.1 in combination with FDP_IFF.2, FMT_MOF.1(2), FMT_MSA.1(2) and FMT_MSA.3 defines the rules and management activities for the label based access control.

FDP_IFC.1 defines the subjects and objects for which label based access control applies.

FDP_IFF.2 defines the rules used by the label based access control policy to make access decisions.

FMT_MOF.1(2) restricts to ability to modify the behaviour of label based access control specifically authorized administrators.

FMT_MSA.1(2) restricts the modification of labels to specifically authorized users.

FMT_MSA.3 defines that no default values for labels are applied. Instead the creator needs to assign a label.

In addition with the rationale provided in [BR-DBMSPP], this rationale thus demonstrates the suitability of the TOE security requirements.

Security Requirements for the IT environment

All security functional requirements for the IT environment together address the objective OE.DIR_CONTROL, which requires that access to directory items is controlled. The SFRs for the IT environment together define a set of minimum requirements for controlling and managing access to the directory items related to Enterprise Users.

FDP_ACC.1 together with FDP_ACF.1, FMT_MSA.1 and FMT_MSA.3 define the basics of the scope of the access control policy the Directory Server needs to enforce on the TSF data the TOE stores in that directory. Access control is required to protect those items from unauthorized access.

FIA_SOS.1 extends the TOE SFR of FIA_SOS.1 to enterise users, allowing to configure the TOE environment that manages enterprise users to enforce the same password policy as the TOE.

FIA_UAU.2 and FIA_UID.2 require identification and authentication of users that want to access directory items. Those SFRs are prerequisites for an access control policy.

FMT_MSA.1 and FMT_MSA.3 are the management parts of the access control policy. FMT_MSA.1 requires that at least the role Enterprise Security Manager is able to manage the directory items. Other roles may also be assigned.

FMT_SMF.1 requires the definition of security management functions. The list of security management functions has not been assigned to not restrict this list uneccessarily.

FMT_SMR.1 requires to support at least the role of an Enterprise Security Manager that is allowed to query, modify or delete security attributes of Enterprise Users. Other roles may exist, for example roles that allow to manage directory items not related to Enterprise Users but stored and managed on the same directory server.

OE.COM_PROT has not been refined to SFRs for the IT environment, since the protection of the commuinication links may be provided by technical or procedural means. This security target will not prescribe how the communication links are protected but just remind the reader that such protection is required.

Dependency Analysis

Table 16 in [BR-DBMSPP] provides the dependency analysis for the SFRs included there. The following modifications to the arguments provided there apply for this TOE:

FAU_GEN_EXP.2: Due to the additional functions included in the TOE the depend-

ency on FIA_UID.1 is satisfied by the TOE, not the TOE environment.

FMT_SMR.1: Due to the additional functions included in the TOE the dependency on FIA_UID.1 is satisfied by the TOE, not the TOE environment.

FTA_MCS.1: Due to the additional functions included in the TOE the dependency on FIA_UID.1 is satisfied by the TOE, not the TOE environment.

The following table includes the dependency analysis for the additional SFRs included

Table 10: Functional Component Dependency Analysis

Requirement	Dependencies	Satisfied
FAU_SAR.1	FAU_GEN.1	Yes, by FAU_GEN.1-NIAP-0410
FAU_SAR.3	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Yes, by FAU_GEN.1-NIAP-0410
FAU_STG.4	FAU_STG.1	Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_SOS.1	-	-
FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	-	-
FIA_USB.1	FIA_ATD.1	Yes
FMT_MTD.1(2)	FMT_SMF.1 FMT_SMR.1	Yes
FPT_RVM.1	-	-
FRU_RSA.1	-	-
FDP_IFC.1	FDP_IFF.1	Yes (by FDP_IFF.2)
FDP_IFF.2	FDP_IFC.1 FMT_MSA.3	Yes
FMT_MOF.1(2)	FMT_SMR.1 FMT_SMF.1	Yes

Requirement	Dependencies	Satisfied
FMT_MSA.1(2)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes

Note: The dependency of FDP_IFC.1 on the functionality of FDP_IFF.1 (see section 6.5 of [CC, Part 2]) has been satisfied for this Security Target via the use of FDP_IFF.2, which provides a superset of FDP_IFF.1's functionality.

For the dependency analysis of the security assurance requirements: EAL4 is a self-contained assurance package and ALC_FLR.3 has no dependencies on any other component.

Dependency Analysis for the SFRs for the IT Environment

The following table includes the dependency analysis for the SFRs for the IT environment:

Table 11: Functional Component Dependency Analysis

Requirement	Dependencies	Satisfied
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FDP_MSA.3	Yes
FIA_UAU.2	FIA_UID.1	Yes
FIA_SOS.1	-	-
FIA_UID.2	-	-
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	Yes

Demonstration of Mutual Support

The supportive dependencies discussed in [BR-DBMSPP] apply to the TOE. The following additional supportive dependencies exist for the TOE with the SFRs that are

not present in [BR-DBMSPP]:

FAU_SAR.1 and FAU_SAR.3 are supported by FMT_SMF.1 and FMT_SMR.1 to manage the privileges allowing an authorized administrator to read and evaluate the audit records, by FAU_STG.1 to protect the audit trail from unauthorized access and by FAU_STG.4 to ensure the completeness of the audit trail.

FAU_STG.1 supports FAU_SAR.1 by preventing unauthorized access to the audit trail.

FAU_STG.4 supports FAU_SAR.1 and FAU_SAR.3 by ensuring the completeness of the audit trail.

FIA_AFL.1 supports FIA_UAU.1 and FIA_SOS.1 by ensuring that the authentication function is not weakened by allowing unlimited authentication attempts.

FIA_SOS.1 supports FIA_UAU.1 by ensuring that passwords are not easily guessable thereby reducing the probability of an unauthorized person getting access to the TOE.

FIA_UAU.1 together with FIA_USB.1 supports almost all other functions by ensuring that the TOE can make decisions (access, audit, management) based on the verified identity of the user.

FIA_UID.1 supports FIA_USB.1 allowing to bind database subjects to users.

FPT_RVM.1 supports all other functions by ensuring that the security policy of the TOE is enforced at all of its external interfaces.

FRU_RSA.1 is a security function of its own. It is supported by the user identification and authentication allowing to enforce quotas for users and FMT_MTD.1 allowing to manage those quotas.

FDP_IFC.1 combines with FDP_IFF.2 to the define the subjects, objects and rules of the label based access control. They are supported by the management function requirements for the label based access control defined by FMT_MOF.1(2), FMT_MSA.1(2) and FMT_MSA.3. As with the discretionary access control policy, also the label based access control policy is supported by the functions of user identification and authentication.

The additional SFRs do not offer any further support to the other SFRs.

Strength of Function Validity

The strength of function specified, SOF-*high*, exceeds the strength of function required by [BR-DBMSPP] (SOF-basic). The password mechanism for local users is the only TOE mechanism that is probabilistic or permutational, and has a strength of SOF-*high*. This strength of function is intended to provide enough protection against straightforward or intentional attack from threat agents having a high attack potential.

Assurance Requirements Appropriate

The target assurance level is EAL4, augmented with ALC_FLR.3, which exceeds the minimum assurance requirement for basic robustenss as stated in [BR-DBMSPP]. EAL4 is appropriate for the TOE because it is designed for use in environments where EAL4 assurance is required to reduce the risk to the assets that the TOE is intended to protect.

ALC_FLR.3 has been included in addition to EAL4 to cause the evaluation of the TOE's flaw remediation procedures which Oracle database users need to be in place following the release of the TOE. These procedures are required to offer continuing assurance to users that Oracle Database 10*g* provides secure storage of and access to

the data which is crucial to their enterprise's success.

To meet this requirement, the flaw remediation procedures must offer:

- the ability for TOE users to report potential security flaws to Oracle,
- the resolution and correction of any flaws with assurance that the corrections introduce no new security flaws, and
- the timely distribution of corrective actions to users.

ALC_FLR.3 is the ALC_FLR component which is at an appropriate level of rigour to cover these requirements.

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

Tables 6 and 7 of chapter 6 identify the Oracle Database 10*g* TOE Security Functions that address each of the SFRs in chapter 5.

The table below demonstrates that 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:

Table 12: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FIA_AFL.1.1	F.IA.PWD	The number of allowed failed logon attempts for local users can be configured.
FIA_AFL.1.2	F.IA.PWD	When the configured number of failed logon attempts is reached the account is locked.
FIA_ATD.1.1	F.IA.ATT F.IA.ATT-EU	The data dictionary stores the required security attributes. In the case of Enterprise Users some security attributes are stored in the directory server.
FIA_SOS.1.1	F.IA.PWD F.LIM.CNF F.IA.USE	F.IA.PWD specifies the controls available on database secrets (passwords) for local users. These controls are implemented via profiles which are required by F.LIM.CNF. F.IA.USE allows local users to change their own passwords within the limits configured by an administrator. In the case of Enterprise Users the password policy is stored and enforced by the directory server.
FIA_UAU.1.1	F.IA.PRE	F.IA.PRE maps onto FIA_UAU.1.1 and FIA_UID.1.2 directly.

Table 12: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FIA_UAU.1.2	F.IA.PRE F.IA.DBA F.IA.CSA F.IA.CSN F.IA.EUA	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.DBA. F.IA.PRE is relevant because one of the actions allowed prior to session creation is attempting to establish a session. In the case of Enterprise Users the authentication is supported by the external directory server as described in F.IA.EUA.
FIA_UID.1.1	F.IA.PRE	F.IA.PRE satisfies FIA_UAU.1.1 and FIA_UID.1.1 directly.
FIA_UID.1.2	F.IA.PRE F.IA.UID F.IA.DBA F.IA.IDE F.IA.CSA F.IA.CSN F.IA.EUA	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.DBA. F.IA.PRE is relevant one of the actions allowed prior to session creation is attempting to establish a session. F.IA.IDE ensures that the identity of the user is known for the duration of the session, once created. In the case of Enterprise Users the user identification is supported by the external directory server as described in F.IA.EUA.
FIA_USB.1.1	F.IA.ATT F.IA.ATT-EU	F.IA.ATT and F.IA.ATT-EU cover the security attributes for each user.
FIA_USB.1.2	F.IA.DBA F.IA.IDE F.PRI.SPRIV F.PRI.PRX F.IA.EUA	F.IA.DBA covers user identification, and the authentication of the user by a password when starting a database session. F.IA.IDE ensures that the TSF is able to establish the identity of the user during a database session. F.PRI.PRX defines the rules governing privileges in proxy user sessions, whilst F.PRI.SPRIV defines rules for which privileges are effective when starting a session. In the case of Enterprise Users, the user security attributes are stored in the external directory server and trabsferred to the TOE such that the TOE can assign the correct user security attributes to the subject that is bound to the user. This is described in F.IA.EUA.
FIA_USB.1.3	F.IA.USE F.APR.EDR F.PRI.SPRIV F.PRI.XVP	F.PRI.SPRIV governs the effect of changing privileges during a session. F.APR.EDR defines which roles are effective at any time during the course of the database session. F.PRI.XVP governs which privileges are effective when executing a view or program owned by another user. F.IA.USE governs when a user is authorised to make changes to a password associated with that user.
FDP_ACC.1.1	F.DAC.OBID F.DAC.OBREF F.DAC.SUA F.DAC.OBA F.ACCESS	F.DAC.OBID and F.DAC.OBREF ensure 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. F.ACCESS specifies that in order to get access both the discretionary and the mandatory access control rules must allow access.

Table 12: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FDP_ACF.1.1-NIAP-0407	F.DAC.OBID F.DAC.OBREF F.DAC.SUA F.DAC.OBA F.DAC.POL F.PRI.SPRIV F.ACCESS	F.DAC.OBID and F.DAC.OBREF ensure 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. F.ACCESS specifies that in order to get access both the discretionary and the mandatory access control rules must allow access.
FDP_ACF.1.2-NIAP-0407	F.IA.CNF F.DAC.OBID F.DAC.OBREF F.DAC.POL F.PRI.SPRIV F.AUD.CNF F.ACCESS	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. F.ACCESS specifies that in order to get access both the discretionary and the mandatory access control rules must allow access.
FDP_ACF.1.3-NIAP-0407	F.DAC.POL F.PRI.SPRIV F.AUD.CNF F.ACCESS	F.DAC.POL c) specifies access to objects based on enabled system privileges. F.DAC.POL d) and e) cover access via connections AS SYSDBA and AS SYSOPER. F.PRI.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. F.ACCESS specifies that in order to get access both the discretionary and the mandatory access control rules must allow access.
FDP_ACF.1.4-NIAP-0407	N/A	This SFR does not mandate any functionality. It is included for compliance with the CC.
FDP_RIP.1.1	F.DAC.OR	F.DAC.OR satisfies FDP_RIP.1.1 directly.
FMT_MOF.1.1(1)	F.AUD.CNF	F.AUD.CNF restricts all functions related to the
FMT_MSA.1.1(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_EXP.3.1	F.DAC.POL F.PRI.SPRIV F.PRI.DEF	F.DAC.POL and F.PRI.SPRIV implicitly include restrictive default values. If a user has not been explicitly granted the necessary privilege or a role containing the required privilege then the requested action will not succeed. F.PRI.DEF defines the default rights for new users, which are the most restrictive rights that just allow to use the DBMS.
FMT_MTD.1.1(1)	F.AUD.SEV	F.AUD.SEV covers the requirement to restrict the ability to select the events to be audited to an authorized administrator.

Table 12: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FMT_MTD.1.1(2)	F.IA.ATT F.IA.ATT-EU 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 data and resource limit attributes. F.APR.* cover privilege and role TSF data. F.AUD.* cover audit data. Note that security attributes of enterprise users may be stored and managed external to the TOE in the directory server.
FMT_REV.1.1(1)	F.LIM.CNF F.APR.GRSP F.APR.GRR	Only suitably privileged users can revoke (or modify) the following attributes: resource limits (F.LIM.CNF), system privileges (F.APR.GRSP) and roles (F.APR.GRR).
FMT_REV.1.2(1)	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_REV.1.1(2)	F.APR.ROP	Only suitably privileged users can revoke (or modify) the object privileges (F.APR.ROP),
FMT_REV.1.2(2)	F.PRI.SPRIV	Directly granted privileges are revoked immediately. This is more rigorous than SFR FMT_REV.1.2.
FMT_SMF.1.1	F.IA.ATT F.IA.ATT-EU 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 management functions provided by the TOE. These functions relate to 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 data and resource limit attributes. F.APR.* cover privilege and role TSF data. F.AUD.* cover audit data. Note that security attributes of enterprise users may be stored and managed external to the TOE in the directory server.
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 authorised user.
FMT_SMR.1.2	F.IA.CSA F.APR.DER F.APR.EDR F.PRI.PRX	F.APR.DER and F.APR.EDR cover granting database roles to database users. F.IA.CSA is relevant because it specifies how to allow a user to connect AS SYSDBA or AS SYSOPER. F.PRI.PRX covers database roles available to a proxy user session.
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 that the database access control policy is upheld for this user.
FPT_SEP_EXP.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.

Table 12: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FPT_SEP_EXP.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.
FPT_TRC_EXP.1.1	F.CON.DIC F.CON.RAC	F.CON.DIC ensures consistency when multiple users simultaneously query and update an item in the dictionary. A locking concept ensures that no conflicting updates can be made. Modified dictionary entries are written back to disk as fast as possible using the mechanism provided by the caching function. F.CON.RAC ensures that data is consistent when the Real Application Clusters function is used.
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_TAH_EXP.1.1	F.IA.CSN F.IA.CSA	F.IA.CSN is the function that creates a session as a normal user. A LOGON trigger can be used to store and manage the date and time of login and retrieve the date and time of the last successful login. For a SYS user, F.IA.CSA (with a LOGON trigger) can perform the same function.
FTA_TAH_EXP.1.2	F.IA.CSN F.IA.CSA	F.IA.CSN is the function that creates a session as a normal user. A LOGON trigger can be used to record the number of unsuccessful login attempts since the last successful login. For a SYS user, F.IA.CSA (with a LOGON trigger) can perform the same function.
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 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-NIAP-0410	F.AUD.SOM F.AUD.SEV F.AUD.ALW F.AUD.LAUD F.AUD.LEN F.AUD.LDIS	The database audit functionality is always active. Whether or not auditing is actually performed is dependent on the 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, F.AUD.LAUD, F.AUD.LEN and F.AUD.LDIS ensure all actions configured to be audited are audited.
FAU_GEN.1.2-NIAP-0410	F.AUD.INF F.AUD.LCOL	F.AUD.INF and F.AUD.LCOL directly satisfies FAU_GEN.1.2-NIAP-0410

Table 12: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FAU_GEN_EXP.2.1	F.AUD.INF	F.AUD.INF directly satisfies FAU_GEN_EXP.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.LVIEW	F.AUD.VIEW directly satisfies FAU_SAR.1.2. For labels this aspect is covered by F.AUD.LVIEW
FAU_SAR.3.1	F.AUD.VIEW F.AUD.LVIEW F.AUD.ACC	F.AUD.VIEW togethr with F.AUD.LVIEW (for labels) satisfy FAU_SAR.3.1. Additionally F.AUD.ACC determines which records are available to the user for selection.
FAU_SEL.1.1-NIAP-0407	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 satisfies 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
FDP_IFC.1.1	F.ACCESS F.LBAC.POL F.LBAC.REF	F.ACCESS states that access control (both discretionary and label based) needs to be performed. F.LBAC.POL (implicitly) defines the subjects and objects covered by the label based access control policy and F.LBAC.REF defines a special case.
FDP_IFF.2.1	F.IA.POLICY F.IA.SESSION F.LBAC.POL F.LBAC.LABSET F.LBAC.LABUPD F.LBAC.REF F.LBAC.TRIGGER	F.IA.POLICY defines the security attributes used for the label based access control policy. F.IA.SESSION defines the rules how a label is assigned when a new session is started. F.LBAC.LABSET defines how the label is set when a new row is created and F.LBAC.LABUPD defines the rules for updating a label. F.LBAC.REF defines a special case and F.LBAC.TRIGGER defines that a trigger is executed with the label of the user that invoked the trigger.
FDP_IFF.2.2	F.LBAC.POL	F.LBAC.POL defines the access control rules of the label based access control policy.
FDP_IFF.2.3	F.IA.SESSUPD	F.IA.SESSUPD describes that a user may change the session label and the default row label
FDP_IFF.2.4	F.LBAC.XVP	F.LBAC.XVP defines the rules how the label is set when a user executes a strored procedure, function or package.
FDP_IFF.2.5	F.LBAC.POL F.LBAC.TRIGGER F.PRI.PPRIV	F.LBAC.POL defines the access control rules of the label based access control policy and F.LBAC.TRIGGER states that a trigger will be executed with the label of the calling user.
FDP_IFF.2.6	-	Since instantiated with NONE, this is a null function

Table 12: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FDP_IFF.2.7	F.LBAC.POL	F.LBAC.POL defines the ordering relationship between different labels.
FMT_MOF.1.1(2)	F.LBAC.MOD	F.LBAC.MOD states that a user needs specific privileges to delete or modify the packages that implement the label based access control policy.
FMT_MSA.1.1(2)	F.IA.POLICY F.LBAC.LABUPD F.APR.GRPP	F.IA.POLICY defines the user security attributes, F.LBAC.UPD defines when a user is allowed to modify the label of a row and F.APR.GRPP defines the privilege management for privileges associated with the label based access control function.
FMT_MSA.3.1	F.LBAC.LABSET	F.LBAC.LABSET defines how the label of a new row is set.
FMT_MSA.3.2	F.LBAC.LABSET	Also covered by F.LBAC.LABSET (one can also state that FMT_MSA.3.2is a null function)

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 [BR-DBMSPP]. All of the operations applied to the SFRs derived from the [BR-DBMSPP] are in accordance with the requirements of this Protection Profile.

Assurance Measures Rationale

Table 8 in Chapter 6 demonstrates that all assurance requirements are suitably met by one or more assurance measures.

This Page Intentionally Blank

ANNEX

A Glossary

Acronyms

DAC	Discretionary Access Control
DDL	Data Definition Language
DES	Data Encryption Standard
DML	Data Manipulation Language
LBAC	Label-Based Access Control
OLS	Oracle Label Security
O-RDBMS	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 Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Terms

Authorised administrative user	Another name for a Database Administrative User.
Data Definition 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 46-3 and FIPS PUB 81. [FIPS46-3],[FIPS81]
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 [SCN]
Database administrative user	A database user to whom one or more administrative privileges have been granted. [DPP] This includes users connected AS SYSOPER or AS SYSDBA as well as Normal Users who are authorised to perform an administrative task via the posession of an administrative privilege which permits the operation of the task.
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 performed. [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]
Enterprise User	A user managed centrally in a directory server. For those users the userid and password, global user roles and privileges, and the password policy are centrally managed.
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]
Label-Based Access Control	This type of access control is based on access rights granted by the system administrator. The administrator chooses which data in the database are to be protected by Label-Based Access Control according to OLS policies which he or she defines. The administrator uses these OLS policies to control the allocation of labels to objects to reflect their sensitivity. The administrator provides users with authorisations to permit access to an appropriate subset of the labelled data. [OLSAG]
LBAC administrator	A user who is able to create, alter and drop OLS policies in the database by virtue of possessing the LBAC_DBA role and `EXECUTE` privilege on the SA_SYSDBA package.
Normal User	A database user who has made a normal connection to the database. This can include the users SYS and SYSTEM but excludes users connected AS SYSOPER or AS SYSDBA.
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]
Object-Relational Database Management System (ORDBMS)	A DBMS that supports object-oriented technology as well as relational databases. [SCN]
OLS Policy	OLS policies are established by LBAC administrators and OLS policy administrators to specify how Label-Based Access Control is to be enforced on a database. [OLSAG]
OLS Policy administrator	A user who is able to execute the administrative packages for the OLS policy for which they also possess the corresponding *policy*_DBA role.
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]
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, policy	Administrators give policy privileges to a user or stored program unit to allow aspects of the label-based access control policy to be bypassed. In addition, the administrator can give policy privileges to authorise the user to perform specific actions, such as the ability of one user to assume the authorisations of a different user. [OLSAG]
Privilege, system	An Oracle privilege that allows users to perform a particular system-wide 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 Functional 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]

Session label	When the administrator sets up the user label authorisations for the user, he or she also specifies the user's initial session label. The session label is the particular combination of level, compartments, and groups at which a user works at any given time. The user can change the session label provided that it remains within the user's label authorisations. [OLSAG]
SOF-high	A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high 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 qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms. [CC]
Structured Query Language (SQL)	A standardised database access language; 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]
Suitably authorised user	A user who is authorised to perform an administrative task via the posession of an administrative privilege which permits the operation of the task. This includes users connected AS SYSOPER or AS SYSDBA as well as privileged Normal Users.
System	A specific IT installation, with a particular purpose 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 Functions (TSF)	A set consisting of all the software of the TOE that must be relied on for the correct 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 (application 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 Label Authorisations	Each user authorised to access data protected by a given OLS policy has *user label authorisations* which include a maximum and minimum level, a set of authorised compartments, a set of authorised groups, and, for each compartment and group, a specification of read-only access, or read-write access. [OLSAG]

User process

A process that requests services, on behalf of a user or application, from an Oracle server process. [SCN]

ANNEX

B References

[AD] *Architecture for Oracle Database 10g Release 2 (10.2.0),* Oracle Corporation.

[ADG] *Oracle Database Application Developer's Guide - Fundamentals, 10g Release 2 (10.2),* Oracle Corporation.

[BR-DBMSPP] *U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.1, June 7, 2006,* Information Assurance Directorate, National Security Agency

[CAPP] *Controlled Access Protection Profile, Version 1.d, 8 October 1999*, Information Assurance Directorate, National Security Agency

[CC] *Common Criteria for Information Technology Security Evaluation,* Version 2.3, ISO/IEC 15408, CCIMB-2005-08,-001 to CCIMB-2005-08-003, August 2005.

[CM] *Oracle Database Configuration Management Plan, 10g Release 2 (10.2.0),* Oracle Corporation.

[CON] *Oracle Database Concepts, 10g Release 2 (10.2),* Oracle Corporation.

[CR-383-4-26] *Certification Report, EAL4+ Evaluation of Sun Microsystems Inc. Solaris 9 Release 8/03,* Version 1.0, Evaluation Number 383-4-26-CR, Government of Canada Communications Security Establishment, 27th January 2005.

[CRP200] *Common Criteria Certification Report No. P200,* Red Hat Enterprise Linux 3 Version 3 Issue 1.0, UK IT Evaluation and Certification Scheme, February 2004.

[DAG] *Oracle Database Administrator's Guide, 10g Release 2 (10.2),*

Oracle Corporation.

[DD] *Detailed Design for Oracle Database 10g Release 2 (10.2.0),* Oracle Corporation.

[DPP] *Database Management System Protection Profile (DBMS PP),* Issue 2.1, Oracle Corporation, May 2000.

[DT] *Design Traceability for Oracle Database 10g Release 2(10.2.0),* Oracle Corporation.

[DSZ0256] *Certification Report BSI-DSZ-CC-0256-2005,* for SuSE Linux Enterprise Server V9, March 2005. Available from http://www.bsi.bund.de/zertifiz/zert/reporte/0256a.pdf.

[ERR] *Oracle Database Error Messages, 10g Release 2(10.2),* Oracle Corporation.

[EUA] *Oracle Database Enterprise User Administrator's Guide, 10g Release 2 (10.2),* Oracle Corporation.

[FIPS46-3] *Federal Information Processing Standard Publication 46-3,* National Institute of Standards and Technology (NIST), October 1999.

[FIPS81] *Federal Information Processing Standard Publication 81,* National Institute of Standards and Technology (NIST), December 1980.

[FLR] *Oracle Flaw Remediation Procedures,* Oracle Corporation.

[GA] *Guidance Analysis for Oracle Database 10g Release 2 (10.2.0),* Oracle Corporation.

[ICG] *Oracle Database Installation and Configuration Guide, 10g Release 2 (10.2),* Oracle Corporation.

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

[LBACFS] *Functional Specification for Label-based Access Controls,* Oracle Corporation.

[LCS] *Life Cycle Support for Oracle Database 10g, Release 2 (10.2.0),* Oracle Corporation.

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

[OCI] *Oracle Database Call Interface Programmers Guide, 10g Release 2 (10.2),* Oracle Corporation.

[OLS_AD] *OLS Architecture for Oracle Database 10g Release 2 (10.2.0),* Oracle Corporation.

[OLSAG] *Oracle Label Security Administrator's Guide, 10g Release 2 (10.2),* Oracle Corporation.

[OLS_DD] *OLS Detailed Design for Oracle Database 10g Release 2 (10.2.0),* Oracle Corporation.

[OLS_ECD] *OLS Evaluated Configuration Document for Oracle Database 10g Release 2 (10.2.0),* Oracle Corporation.

[OLS_GA] *OLS Administrator and User Guidance Analysis for Oracle Database 10g Release 2 (10.2.0),* Oracle Corporation.

[OLS_IN] *Oracle Label Security Installation Notes, Release 10.2,* Oracle Corporation.

[OLS_SPM] *OLS Security Policy Model for Oracle Database 10g Release 2 (10.2.0),* Oracle Corporation.

[OLS_SRC] *OLS Source Code for Oracle Database 10g Release 2 (10.2.0),* Oracle Corporation.

[OLS_ST10gR1] *OLS Security Target for Oracle10i Release 1 (10.1.0)*, Issue 1.2, Oracle Corporation.

[OLS_VA] *OLS Vulnerability Analysis for Oracle Database 10g, Release 2 (10.2.0),* Oracle Corporation.

[OQM] *Quality Manual for Manufacturing & Distribution,* Oracle Corporation.

[PLS] *PL/SQL User's Guide and Reference, 10g Release 2 (10.2),* Oracle Corporation.

[SAPAFS] *Functional Specification for Secure Access Policy Adapter*, Oracle Corporation.

[SG] *Oracle Database Security Guide, 10g Release 2 (10.2),* Oracle Corporation.

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

[SOF] *Strength of Function Analysis for Oracle Database 10g, Release 2 (10.2.0),* Oracle Corporation.

[SQL] *Oracle Database SQL Reference, 10g Release 2 (10.2),* Oracle Corporation.

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

[SRC] *Oracle Database 10g Source Code, Release 2 (10.2.0),* Oracle Corporation.

[SRF] *Oracle Database Reference*, 10g *Release 2 (10.2),*

Oracle Corporation.

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

[TP] *Test Plan, Procedures, Results, and Analysis for Oracle Database 10g,Release 2 (10.2.0)*, Oracle Corporation.

[VA] *Vulnerability Analysis for Oracle Database 10g, Release 2 (10.2.0)*, Oracle Corporation.