Common Criteria

Security Target for

Oracle Database 11*g* Release 1 (11.1.0)
with Oracle Database Vault

September 2009
Version 6.0

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

Security Target for Oracle Database 11*g* with Oracle Database Vault
Release 1 (11.1.0)

Author: Helmut Kurth

Contributors: Shaun Lee, Petra Manche

Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The information in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. Oracle Corporation does not warrant that this document is error free.

Contents

CHAPTER

1 Introduction

This document is the security target for the Common Criteria evaluation of Oracle Database 11*g*, Release 1 (11.1.0.7) Enterprise Edition with Oracle Database Vault.

ST Reference

Title: Security Target for Oracle Database 11*g* Release 1 Enterprise Edition with Oracle Database Vault, Version 6.0

TOE Reference

Target of Evaluation (TOE): Oracle Database 11*g* Release 1 Enterprise Edition with Oracle Database Vault.

Release: 11.1.0.7 with all critical patch updates up to and including July 2009

Note: This includes the guidance documentation which consists of [ECD] and the Oracle Database 11*g* Release 1 documentation library (Part No. B28359-01).

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 11.1.0.7 with no platform.

Operating System Platforms: Red Hat Enterprise Linux AS (version 5)
for which [CCEVS-VR-07-0054] is the Common Criteria certification report;
SuSE Linux Enterprise Server 10 SP1

for which [CCEVS-VR-VID10271-2007] is the Common Criteria Certification Report;

Oracle Enterprise Linux Version 4 Update 5 for which [DSZ0468] is the Common Criteria Certification Report.

This security target is an extension of the Oracle Database 11*g* Enterprise Edition security target [ST_ENT_11GR1] where the general security functionality of the Oracle Database is described. Oracle Database Vault is an option for the Oracle Database that extends the security functionality of the Oracle Database with additional access control and auditing fucntionality. To avoid redundancy with the Oracle Database 11*g* Enterprise Edition security target, this document only describes the additional or modified security functionality introduced by Oracle Database Vault. Some SFR(s) that appear to have the same name in both security targets may apply to different security objects. For instance, FMT_SMF.1.1 in the Oracle Database 11g Enterprise Edition security target applies to the audit data in database while FMT_SMT.1.1 in this document applies to the Database Vault audit trails. The reader is expected to interpret the SFRs with their intended security objects. For the modified security functionality, if the same SFRs shown both in the Security Target of the Oracle Database 11g Release 1 Enterprise Edition and this document, the SFR specified in this document takes the precedence. Because of the very purpose of the Database Vault, the SYSDBA user's privileges are limited and he is not able to manage the security attributes of the Database Vault roles (e.g. DV_OWNER, DV_ADMIN) when the Database Vault is running on the top of the Oracle Database Enterprise Edition. As a consequence, FIA_ATD.1.1 in this document states that Database Vault maintains all Database Vault defined roles, and then FIA_ATD.1.1 in the Oracle Database 11g Enterprise Edition security target has to be understood that it maintains all roles other than Database Vault roles.

It is intended to evaluate Oracle Database Vault as a component that extends the functionality of the Oracle Database. This evaluation is based on the evaluation of the Oracle Database itself and will therefore only claim security functionality provided by Oracle Database Vault.

Note that Oracle Database Vault also requires Oracle Label Security to be installed, but it may not be configured as defined in [OLS_ST11GR1]. Therefore the "base" security target for the evaluation of Database Vault is [ST_ENT_11GR1] and not [OLS_ST11GR1].

TOE Overview

For an overview of the Oracle Database 11*g* Release 1 Enterprise Edition, see the related security target. This security target only describes the additional or modified functionality implied by Oracle Database Vault.

Oracle Database Vault is an option for the Oracle Database that an additional fine-grained access control functionality for separation of duties and access protection even from highly privileged users. In addition it extends the auditing functionality with specific auditing and audit evaluation functions related to the additional access control functionality. There are further additions to the management functionality with new roles defined by Database Vault and the management functionality for managing the additional access control and audit functions.

The TOE under the evaluation is Oracle Database 11g Release 1 Enterprise Edition with Oracle Database Vault option on. This means that the Oracle Server executable must be linked with DV_ON and that the Oracle Database Vault must be enabled using the command "dvca -action enable" with appropriate parameters that is provided by the Oracle Database Vault Configuration Assistant (DVCA). Only when the Oracle Database Vault is enabled and it is linked to the Oracle Server, its security functionality is effective and it extends the access control functionality, auditing functionality and management functionality on the top of what are provided by the Oracle Server. This is the intended TOE subject to the current evaluation.

The following section provides a short description of the security functionality provided by Oracle Database Vault. A more detailed description is provided in chapters 2 and 6 of this document.

Oracle Database Vault provides

- a fine-grained access control functionality that allows to group database schemas, objects, and roles into **realms**, define **command rules** that allow controling how users can execute SQL statements, define and use **factors** that can be evaluated as part of the rules, define and use **rule sets** as collection of rules that can be associated with realm authorizations and **secure application roles**. A rule set associated with a secure application role decides, if a role is granted to a user logging in.
- additional audit capabilities related to management activities of Oracle Database Vault and the access decisions made by Oracle Database Vault.
- Components that allow the management of Oracle Database Vault, including additional, Oracle Database Vault specific roles.

The metadata of Oracle Database Vault including the roles introduced by the Database Vault and AUDIT_TRAIL$ table is stored and owned by the DVSYS schema. This schema supports the administration and run-time processing of Oracle Database Vault, and most importantly, this schema is protected against the improper use of system privileges (for the details of the ensured protection, please refer to "DVSYS Schema" section in chapter 6). In a default installation, the DVSYS account is locked and all objects in the DVSYS schema must be created or modified by the schema account itself. In situations where the password for the Oracle Database Vault account manager (with role DV_ACCTMGR) has been forgotten or the Database Vault Owner (with role DV_OWNER) or Database Vault Administrator (with role DV_ADMIN) accounts have been inadvertently locked out, the Oracle Database Vault must not be running on the top of the Oracle Server to apply repairs. In order to stop the added security functionality from Oracle Database Vault, the Oracle Server executable must be linked with DV_OFF and Database Vault must be disabled using the command "dvca -action disable" with appropriate parameters via DVCA. By removing the designed protection imposed on the DVSYS schema, the SYSTEM user or SYS user can then apply the appropriate repairs in order for the Database Vault roles to recover from the erroneous situations. The reader is referred to ANNEX B (on page B-1) in [DBV_ADMIN] for a complete list of situations where Oracle Database Vault must be disabled. With Oracle Database Vault disabled, the binary of the Oracle Server executable is changed. Strictly speaking, the resulting binary is not the intended TOE any more. Hereafter the state where the Oracle Server running with disabled Oracle Database is referred as the maintenance mode. In the mode, the Oracle Server run-time access control mediation is not influenced by the Database Vault, although the Oracle Database Vault API functions are still available through its PL/SQL packages. Since security functionality provided by the Oracle Database Vault is not integrated into the Oracle Server in the maintenance mode, this mode shall not be subject to the current evaluation.

TOE Product Components

The Oracle Database 11*g* with Oracle Database Vault includes the products identified in Table 1. Access to the Oracle Database 11*g* server is provided via the interface products identified in Table 2.

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

Note that this document only describes the additional security functionality introduced by Oracle Database Vault. For a description of the security functionality provided by the Oracle Database 11*g* Release 1, see the security target document for this product.

Table 1: TOE Server Products

TOE Server Product
Oracle Database 11*g* Enterprise Edition 11.1.0.7
Oracle Label Security 11.1.0.7
Oracle Database Vault 11.1.0.7

Table 2: TOE Interface Products

TOE Interface Products
SQL*Plus 11.1.0.7
Oracle Call Interface 11.1.0.7
Oracle Net Services 11.1.0.7

Document Overview

This document describes the security problem definition and the security functionality of Oracle Database Vault. Oracle Database Vault is an optional functionality of the Oracle Database that provides additional access control, auditing and management functionality.

Chapter 2 of this security target provides a high-level overview of the security features of Oracle Database Vault. Chapter 3 describes the security problem definition with the identification of the assumptions, threats, and security policies of the TOE environment, all related to Oracle Database Vault. For a complete security problem definition, the assumptions, threats, and security policies defined in the Oracle Database 11*g* security target need to be added. Chapter 4 describes the security objectives for Oracle Database Vault and for the environment needed to address the assumptions, threats, and security policies identified in Chapter 3 for Oracle Database

Vault. Chapter 5 identifies the Security Functional Requirements (SFRs) and the Security Assurance Requirements (SARs) for Oracle Database Vault. Chapter 6 summarises each Security Function (SF) provided by for Oracle Database Vault to meet the security requirements.Chapter 6 also provides an overview how Oracle Database Vault is integrated into Oracle Database 11*g*.

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

Conformance Claims

CC Conformance

The CC conformance claim is: part 2 extended (part 2 conformant for the SFRs defined in this document) and part 3 conformant
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 11*g*, Oracle Database Vault, O-RDBMS, database, security target, EAL4

Version of the Common Criteria [CC] used to produce this document: 3.1.

Protection Profile Conformance

None for the Oracle Database Vault security functionality.

Note that the Oracle Database 11*g* is evaluated for compliance with the U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2. ([BR-DBMSPP]). The additional security functionality defined in this security target does not contradict the requirements defined in this Protection Profile and therefore also the Oracle Database 11*g* with Oracle Database Vault is compliant to [BR-DBMSPP]. Therefore the conformance claim also applies for the TOE with Database Vault included. The additional assumption made in this document does not invalidate this conformance claim, since it is solely related to Database Vault functionality which is beyond the requirements defined in [BR-DBMSPP].

[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.

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 11*g* with Oracle Database Vault. For a detailed description of the security features of Oracle Database 11*g* the reader is referred to the security target document for the Oracle Database 11*g* and the documents referred there.

The security functionality of Oracle Database Vault is described in [DBV_ADMIN]. 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 Vault architecture, the objects and security attributes defined and used by Oracle Database Vault, the components of Oracle Database Vault and how they are integrated into the Oracle Database 11*g*.

Oracle Database Vault Architecture

The Oracle Database Vault objects, security fucntionality and architectural components are described in detail in [DBV_ADMIN].

Oracle Database Vault Access Control Components

Oracle Database Vault defines a set of components used in the additional access control policy that Oracle Database Vault implements. Those are:

Realms

A **realm** is a functional grouping of database schemas, objects, and roles that must be secured. For example, one can group a set of schemas, objects, and roles that are related to accounting, sales, or human resources. After having grouped these into a realm, one can use the realm to control the use of system privileges to specific accounts or roles. This enables providing fine-grained access controls for anyone who wants to use these schemas, objects, and roles. Chapter 4, "Configuring Realms" discusses realms in detail.

Think of a realm as zone of protection for specific database objects. A **schema** is a logical collection of database objects such as tables, views, and packages, and a **role** is a collection of privileges. By classifying schemas and roles into functional groups, one can control the ability to use system privileges against these groups and prevent unauthorized data access by the DBA or other powerful users with system privileges. Oracle Database Vault does not replace the discretionary access control model in the existing Oracle database. It functions as a layer on top of this model for both realms and command rules.

After creating a realm, one can register a set of schema objects or roles (secured objects) for realm protection and authorize a set of users or roles to access the secured objects.

Command Rules

A **command rule** is a special rule that one can create to control how users can execute almost any SQL statement, including SELECT, ALTER SYSTEM, database definition language (DDL), and data manipulation language (DML) statements. To customize and enforce the command rule, you associate it with a rule set, which is a collection of one or more rules. The command rule executes at run time. Command rules affect anyone who tries to use the SQL statements it protects, regardless of the realm in which the object exists.

A command rule has the following attributes, in addition to its bonding operations and authorization functionality:

- SQL statement the command rule will protect
- Owner of the object the command rule will affect
- Database object the command rule will affect
- Whether the command rule is enabled or not
- An associated rule set

Command rules can be categorized as follows:

- **Command rules that have a system-wide scope.** With this type, one can only create one command rule for each database instance. Examples are command rules for the ALTER SYSTEM and CONNECT statements.
- **Command rules that are schema specific.** An example is creating a command rule for the DROP TABLE statement.
- **Command rules that are object specific.** An example is creating a command rule for the DROP TABLE statement with a specific table included in the command rule definition.

When a user executes a statement affected by a command rule, Oracle Database Vault checks the realm authorization first. If it finds no realm violation and if the associated command rules are enabled, then Database Vault evaluates the associated rule sets. If all the rule sets evaluate to TRUE, then the statement is authorized for further processing. If any of the rule sets evaluate to FALSE, then the statement is not authorized and a command rule violation is created. More information can be found in chapter 5, "Configuring Rule Sets" of [DBV_ADMIN].

Factors

A **factor** is a named variable or attribute, such as a user location, database IP address, or session user, which Oracle Database Vault can recognize and secure. You can use factors for activities such as authorizing database accounts to connect to the database or creating filtering logic to restrict the visibility and manageability of data. Each factor can have one or more identities. An identity is the actual value of a factor. A factor can have several identities depending on the factor retrieval method or its identity mapping logic. Oracle Database Vault provides a set of default factors. For each of these factors, there is an associated function that retrieves the value of the factor. The default factors are:

- Authentication method
- Client IP address
- Database domain
- Database hostname
- Database instance
- Database server IP address
- Database name
- Domain: a collection of physical, configuration, or implementation-specific factors
- Enterprise identity
- Identification type
- Language
- Host name
- Network protocol used
- Oracle Internet Directory DN (if the proxy user is an enterprise user)
- Database user name

A full list of Oracle Database Vault default factor functions is contained in [DBV_ADMIN] in table 14-8.

Rule Sets

A **rule set** is a collection of one or more rules that you can associate with a realm authorization, command rule, factor assignment, or secure application role. The rule set evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (*All True* or *Any True*). The rule within a rule set is a PL/SQL expression that evaluates to true or false. It is possible to have the same rule in multiple rule sets.

By default, Oracle Database Vault provides the following selections for rule sets:

- **Allow Sessions**: Controls the ability to create a session in the database. This rule set enables you to add rules to control database logins using the CONNECT command rule. The CONNECT command rule is useful to control or limit SYSDBA access to programs that require its use. This rule set is not populated.
- **Allow System Parameters**: Controls the ability to set system initialization parameters. See Oracle Database Reference for detailed information about initialization parameters.
- **Can Grant VPD Administration**: Controls the ability to grant the GRANT EXECUTE or REVOKE EXECUTE privileges on the Oracle Virtual Private Database DBMS_RLS package, with the GRANT and REVOKE statements.
- **Can Maintain Accounts/Profiles**: Controls the roles that manage user accounts and profiles, through the CREATE USER, DROP USER, CREATE PROFILE, ALTER PROFILE, or DROP PROFILE statements.

- **Can Maintain Own Account**: Allows the accounts with the DV_ACCTMGR role to manage user accounts and profiles with the ALTER USER statement. Also allows individual accounts to change their own password using the ALTER USER statement.
- **Disabled**: Convenience rule set to quickly disable security configurations like realms, command rules, factors, and secure application roles.
- **Enabled**: Convenience rule set to quickly enable system features.

Secure Application Roles

A **secure application role** is a special Oracle Database role that can be enabled based on the evaluation of an Oracle Database Vault rule set. [DBV_ADMIN], chapter 8, "Configuring Secure Application Roles for Oracle Database Vault" discusses secure application roles in detail.

In Oracle Database Vault, a secure application role can be created that is enabled with an Oracle Database Vault rule set. Regular Oracle Database secure application roles are enabled by custom PL/SQL procedures. Secure application roles can be used to prevent users from accessing data from outside an application. This forces users to work within the framework of the application privileges that have been granted to the role.

The advantage of basing database access for a role on a rule set is that one can store database security policies in one central place, as opposed to storing them in all the applications. Basing the role on a rule set provides a consistent and flexible method to enforce the security policies that the role provides. In this way, if the security policy for the application role must be updated, it can be done in one place, the rule set.

Furthermore, no matter how the user connects to the database, the result is the same, because the rule set is bound to the role. Oracle Database Vault automatically creates the secure application role to use invoker's rights. All one needs to do is to create the role and then associate it with a rule set. The rule definition should validate the user who is trying to log in.

Oracle Database Vault Administrator (DVA)

Oracle Database Vault Administrator is a Java application that is built on top of the Oracle Database Vault PL/SQL application programming interfaces (API). This application allows security managers who may not be proficient in PL/SQL to configure the access control policy through a user-friendly interface. Oracle Database Vault Administrator provides an extensive collection of security-related reports that assist in understanding the baseline security configuration. These reports also help point out deviations from this baseline.

[DBV_ADMIN], Chapter 4 through Chapter 9 explain how to use Oracle Database Vault Administrator to configure access control policy defined in realms, command rules, factors, rule sets, secure application roles, and how to integrate Oracle Database Vault with other Oracle products.

Oracle Database Vault Configuration Assistant (DVCA)

To perform maintenance tasks on your Oracle Database Vault installation, the command-line utility Oracle Database Vault Configuration Assistant (DVCA) can be used. DVCA can be used to enable or disable Oracle Database Vault. Although it is a prerequisite to have Database Vault enabled in order to make its security functionality effective, DVCA itself does not satisfy any SFRs of the Database Vault. For more information, see [DBV_ADMIN], Appendix C, "Post-Installation Oracle Database Vault Procedures".

Oracle Database Vault DVSYS and DVF Schemas

Oracle Database Vault provides a schema, DVSYS, which stores the database objects needed to process Oracle data for Oracle Database Vault. This schema contains the roles, views, accounts, functions, and other database objects that Oracle Database Vault uses. The DVF schema contains public functions to retrieve (at run time) the factor values set in the Oracle Database Vault access control configuration.

[DBV_ADMIN], Chapter 10, "Oracle Database Vault Objects" describes these schemas in detail.

Oracle Database Vault PL/SQL Interfaces and Packages

Oracle Database Vault provides a collection of PL/SQL interfaces and packages that allow security managers or application developers to configure the access control policy as required. The PL/SQL procedures and functions allow the general database account to operate within the boundaries of access control policy in the context of a given database session.

See [DBV_ADMIN], Chapter 14, "Using the Oracle Database Vault PL/SQL Interfaces" and Chapter 11, "Using the DVSYS.DBMS_MACADM Package" for more information.

Oracle Database Vault and Oracle Label Security PL/SQL APIs

Oracle Database Vault provides access control capabilities that can be integrated with Oracle Label Security. The Oracle Label Security database option is integrated with Oracle Enterprise Manager Database Control, which enables the security manager to define label security policy and apply it to database objects. Oracle Label Security also provides a collection of PL/SQL APIs that can be used by a database application developer to provide label security policy and protections.

See "Integrating Oracle Database Vault with Oracle Label Security" in [DBV_ADMIN], page 9-2 for more information on how Oracle Database Vault works with Oracle Label Security. See also Oracle Label Security Administrator's Guide for more information about Oracle Policy Manager.

Oracle Database Vault Reporting and Monitoring Tools

Reports on the various activities that Oracle Database Vault monitors can be generated. In addition, one can monitor policy changes, security violation attempts, and database configuration and structural changes.

See [DBV_ADMIN], chapter 16, "Oracle Database Vault Reports" for more information about the reports that you can generate. [DBV_ADMIN], chapter 15, "Monitoring Oracle Database Vault" explains how to monitor Oracle Database Vault.

Oracle Database Vault Roles

Oracle Database Vault defines a set of additional roles and modifies the privileges assigned to existing roles. Note that installation specific roles may be also defined by using the the functionality of Oracle Database Vault.

Modifications to Existing Roles

To support the separation of duty policies and restrict the possibilities of database administrators, a number of privileges are revoked from existing users and roles during installation of Oracle Database Vault. The following sections describe the privileges that are revoked from the individual roles:

DBA Role

- BECOME USER
- SELECT ANY TRANSACTION

- CREATE ANY JOB
- CREATE EXTERNAL JOB
- EXECUTE ANY PROGRAM
- EXECUTE ANY CLASS
- MANAGE SCHEDULER
- DEQUEUE ANY QUEUE
- ENQUEUE ANY QUEUE
- MANAGE ANY QUEUE

IMP_FULL_DATABASE Role

- BECOME USER
- MANAGE ANY QUEUE

EXECUTE_CATALOG_ROLE Role

- EXECUTE ON DBMS_LOGMNR
- EXECUTE ON DBMS_LOGMNR_D
- EXECUTE ON DBMS_LOGMNR_LOGREP_DICT
- EXECUTE ON DBMS_LOGMNR_SESSION
- EXECUTE ON DBMS_FILE_TRANSFER

PUBLIC user

- EXECUTE ON UTL_FILE

SCHEDULER_ADMIN Role

- CREATE ANY JOB
- CREATE EXTERNAL JOB
- EXECUTE ANY PROGRAM
- EXECUTE ANY CLASS
- MANAGE SCHEDULER

SYS User

- ALTER USER
- DROP USER

SYSTEM User

- ALTER USER
- CREATE USER
- DROP USER

NEW Roles Defined by Oracle Database Vault

When Oracle Database Vault is installed, a set of new roles is defined that can be used to configure and manage Oracle Database Vault and the realms defined by an installation. Those roles are:

DV_OWNER

The DV_OWNER role can be used to manage the Oracle Database Vault roles and its configuration. The DV_OWNER role has the administrative capabilities that the DV_ADMIN role provides, and the reporting capabilities the DV_SECANALYST role provides. It also provides privileges for monitoring Oracle Database Vault. It is created when Oracle Database Vault is installed, and has the most privileges on the DVSYS schema.

DV_REALM_OWNER

The DV_REALM_OWNER role can be used to manage database objects in multiple schemas that define a realm. This role should be granted to the database account owner who is responsible for managing one or more schema database accounts within a realm and the roles associated with the realm. A user granted this role can use powerful system privileges like CREATE ANY, ALTER ANY, and DROP ANY within the realm.

DV_REALM_RESOURCE

The DV_REALM_RE SOURCE role provides the same system privileges as the Oracle RESOURCE role. In addition, both CREATE SYNONYM and CREATE VIEW are granted to this role.

DV_ADMIN

The DV_ADMIN role has the EXECUTE privilege on the DVSYS packages (DBMS_MACADM, DBMS_MACSECROLES, and DBMS_MACUTL). DV_ADMIN also has the capabilities provided by the DV_SECANALYST role, which allow the user to run Oracle Database Vault reports and monitor Oracle Database Vault.

DV_ACCTMGR

The DV_ACCTMGR role can be used to create and maintain database accounts and database profiles. A user who has been granted this role can use the CREATE, ALTER, and DROP statements for users or profiles. However, a user with this role cannot use the DROP or ALTER statements for the DVSYS account, nor change the DVSYS password.

DV_PUBLIC

The DV_PUBLIC role can be used to grant privileges on specific objects in the DVSYS schema. (Remember that in a default installation, the DVSYS schema is locked.).

Oracle Database Vault does not enable users to directly grant object privileges in the DVSYS schema to PUBLIC. One must grant the object privilege on the DVSYS schema object the DV_PUBLIC role, and then grant DV_PUBLIC to PUBLIC. However, if one does this, it is important to not add more object privileges to the PUBLIC role. Doing so may undermine Oracle Database Vault security.

DV_SECANALYST

The DV_SECANALYST role can be used to run Oracle Database Vault reports and monitor Oracle Database Vault. (This role is also used for database-related reports.) In addition, this role enables a user to check the DVSYS configuration by querying the DVSYS views described in "Oracle Database Vault Data Dictionary Views" on page 10-9 in [DBV_ADMIN]. The DV_ SECANALYST role has SELECT privileges on the DVSYS schema objects and portions of the SYS and SYSMAN schema objects for reporting on DVSYS- and DVF-related entities.

Oracle Database Vault Accounts

Oracle Database Vault prompts for two accounts during installation: *Oracle Database Vault Owner* and *Oracle Database Vault Account Manager*. An account name and password for the Oracle Database Vault Owner account must be supplied during installation. Creating an Oracle Database Vault Account Manager is optional.

The Oracle Database Vault Owner account is granted the DV_OWNER role. This account can manage Oracle Database Vault roles and configuration.

The Oracle Database Vault Account Manager account is granted the DV_ACCTMGR role. This account is used to manage database user accounts to facilitate separation of duties.

Oracle Database Vault Schemas (TSF Data)

The Oracle Database Vault TSF data include two schemas with database tables, sequences, views, triggers, roles, packages, procedures, functions, and contexts that support the administration and run-time processing of Oracle Database Vault.

Oracle Database Vault has the following schemas:

- DVSYS Schema: Owns the Oracle Database Vault schema and related objects
- DVF Schema: Owns the Oracle Database Vault functions that are created to retrieve factor identities

DVSYS Schema

The DVSYS schema contains Oracle Database Vault database objects, which store Oracle Database Vault configuration information and support the administration and run-time processing of Oracle Database Vault. In a default installation, the DVSYS schema is locked. The DVSYS schema also owns the AUDIT_TRAIL$ table. Oracle Database Vault secures the DVSYS schema by using a protected schema design.

A protected schema design guards the schema against improper use of system privileges (for example, SELECT ANY TABLE, CREATE ANY VIEW, or DROP ANY).

DVF Schema

The DVF schema is the owner of the Oracle Database Vault DBMS_MACSEC_FUNCTION PL/SQL package, which contains the functions that retrieve factor identities. After installation of Oracle Database Vault, the installation process locks the DVF account to better secure it. When a new factor is created, Oracle Database Vault creates a new retrieval function for the factor and saves it in this schema.

Access Control Functions of Oracle Database Vault

Oracle Database Vault extends the access control functionality of Oracle Database in two ways:

- objects within a realm are protected from being accessed by database users that use a system privilege to execute a SQL statement. In this case Oracle Database Vault checks if the SQL statement affects any object secured by a realm. If this is the case, Oracle Database Vault checks if the database account that attempts to perform the SQL statement is the owner or a participant of the realm where the affected object belongs to. If this is the case, the following special case occurs:

  - If the command is a GRANT or REVOKE of a role protected by the realm or a GRANT or REVOKE of an object privilege protected by the realm. In this case the session needs to be authorized as the realm owner or a protected role in the realm that has the privilege for those commands.

  In any case, if the realm authorization is based on a rule set, this rule set is evaluated and needs to evaluate to true.
- For all SQL statements it is checked if there is a command rule guarding the statement. If this is the case, the command rule needs to evaluate to true for the SQL

statement to be executed.

Oracle Database Vault does not replace the discretionary access control model in the existing Oracle database. It functions as a layer on top of this model for both realms and command rules.

Oracle Database Vault Security Management

Oracle Database Vault provides a collection of PL/SQL package APIs to support the maintenance and run-time behavior of Oracle Database Vault. Those are:

DVSYS.DBMS_MACADM

This package API provides for the administration of all aspects of the secure and access control configuration data. The realm owner of the Oracle Database Vault realm can grant the ability to run this package.

DVSYS.DBMS_MACSEC_ ROLES

This package API provides the CAN_SET_ROLE method to check whether the user invoking the method is authorized to use the specified Oracle Database Vault secure application role. The authorization is determined by checking the rule set associated with the role.

The API also provides a method to issue the SET ROLE statement for a Oracle Database Vault Secure Application Role. Before SET ROLE is issued, the CAN_SET_ROLE method is called to check the rule set associated with the role.

Run-time rule set behavior such as auditing, failure processing, and event handling occur during this process. The package is available to the general database account population.

DVSYS.DBMS_MACUTL

This package API defines several constants and utility methods that are commonly used by other Oracle Database Vault packages, such as code/message lookup, error handling, data conversion, and privilege checks. This package can be run by the general database account population. This allows for security developers to leverage the constants in scripted configuration files. Utility methods such as USER_HAS_ROLE can also be used in Oracle Database Vault rules.

Oracle Database Vault Auditing

Oracle Database Vault defines a set of additional audit events as well as functions to manage and evaluate the audit trail. The audit trail of Oracle Database Vault is different from the audit trail of the Oracle Database and can therefore be set and managed independently from the Oracle Database auditing.

In addition, some parameter settings for the regular Oracle Database auditing are modified when Oracle Database Vault is installed. Those settings are effective only if auditing is enabled for the database. The modifications to the parameter settings for the Oracle Database audit trail are defined in [DBV_ADMIN], table A-2.

Oracle Database Vault Audit Events

Oracle Database Vault defines custom events to track violations in realms, command rules, and so on. One can audit the following in Oracle Database Vault:

Rule Set Audit

Audits the rule set processing results. One can audit both successful and failed processing. Realm authorizations can be managed using rule sets. One can audit the rule set processing results. Factor assignments and secure application roles audits can be managed using a rule set.

Realm Audit

Audits the processing of management activities related to a realm. A realm violation occurs when a database account, performing an action on a realm object, is not authorized to perform that action in the realm. One can audit realm violations.

Factor Audit

Audits the evaluation of a factor function. One can audit both successful and failed factor processing. For failed factor processing, one can audit on all or any of the following events: Retrieval Error, Retrieval Null, Validation Error, Validation False, Trust Level Null, or Trust Level Less Than Zero.

Oracle Label Security Session Initialization Failed

:Audits instances where the Oracle Label Security session fails to initialize.

Oracle Label Security Attempt to Upgrade Session Label Failed

Audits instances where the Oracle Label Security component prevents a session from setting a label that exceeds the maximum session label.

Format of the Oracle Database Vault Audit Trail

The Oracle Database Vault custom audit event records are stored in the AUDIT_ TRAIL$ table, which is part of the DVSYS schema. These audit records are not part of the typical Oracle Database audit trail. (In fact, if auditing has been disabled in Oracle Database, the Oracle Database Vault audit will continue to write to the AUDIT_ TRAIL$ table.).

A description of the format of the audit records can be found in [DBV_ADMIN], table A-1.

To save and evaluate the audit records generated by Oracle Database Vault, one has to export the AUDIT_TRAIL$ table to a dump file.

CHAPTER

3 Security Problem Definition

Threats

[ST11_ENT_GR1] provides the characterization of the threat agents considered as well as the threats to be countered by the Oracle Database 11*g*R1.

Oracle Database Vault has a user with administrative privileges (other than the privileges to access database objects of Oracle Database Vault) as an additional threat agent. Such a user may attempt to misuse his privileges and access database objects protected by the additional access control functionality of Oracle Database Vault. It is assumed that such users have a low attack potential, i. e. they do not attempt to bypass the security functionality of Oracle Database Vault using sophisticated attack methods.

Oracle Database Vault addresses the following additional threats:

T.ADMIN_ACCESS A user with administrative privileges accesses database objects or perform SQL statements unrelated to his administrative duties.

T.DBV_MGMT A user without a defined Oracle Database Vault Management role modifies Oracle Database Vault access control policies or security attributes used in the Oracle Database Vault access control rules.

T.DBV_ACCOUNT Users can attempt or perform actions within the realm they are authorized to or attempt to perform SQL statments without the possibility to be held accountable for those actions.

Organisational Security Policies

There are no organisational security ploicies related to Oracle Database Vault.

Assumptions

As per [ST11_ENT_GR1]. The following additions have been added to reflect the specific architecture of the TOE:

Underlying System Assumptions

A.DBV_INSTALL Oracle Database Vault is installed and configured as defined in [ECD].

CHAPTER

4 Security Objectives

TOE Security Objectives

As per [ST11_ENT_GR1] with the addition of the following objectives:

O.PROTECT_REALM

The TOE must provide the means of controlling access to objects within a realm even for authorized database administrators.

O.PROTECT_COMMAND

The TOE must provide means to control the execution of defined SQL statements by installation specific rules.

O.RESTRICT_MGMT

The TOE must provide means to restrict the management of the access control policy and the management of the security attributes to users in defined administrative roles.

O.DBV_ACCOUNT

The TOE must provide the means of auditing actions of users when accessing objects within a realm and when administering Oracle Database Vault.

Environmental Security Objectives

As per [ST11_ENT_GR1]. with the following additional environmental security objectives for Oracle Database Vault.

OE.DBV_INSTALL

The persons responsible for the installation and configuration of Oracle Database Vault must perform this in accordance with the guidance provided by [ECD] and must ensure that they define their realms in accordance with their organization’s protection needs, define the rule sets that protect the realms in accordance with their organization’s protection needs and guard the execution of SQL statements using command rules in accordance with their organization's protection needs.

Security Objectives Rationale

As per [ST11_ENT_GR1] with the following Oracle Database Vault specific additions:.

O.PROTECT_REALM helps to mitigate the threat T.ADMIN_ACCESS by ensuring that users with administrative privileges can be prohibited from accessing database objects within a defined realm.

O.PROTECT_COMMAND helps to mitigate the threat T.ADMIN_ACCESS by ensuring that the execution of SQL statement can be guarded by a command rule that is evaluated when a user attempts to execute the statement.

O.RESTRICT_MGMT helps to mitigate the threat T.DBV_MGMT by ensuring that only users with a defined Oracle Database Vault administrative role are able to manage the Oracle Database Vault access control policy or modify security attributes associated with Oracle Database Vault.

O.DBV_ACCOUNT helps to mitigate the threat T.DBV_ACCOUNT by ensuring that the Oracle Database Vault specific management activities as well as the results of the evaluation of rule sets (for access to objects protected by a realm) and the results of the evaluation of command rules can be audited.

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.

Assumptions Rationale

The assumptions rationale in [ST11_ENT_GR1] applies to the TOE, with the following additions:

A.DBV_INSTALL states that Oracle Database Vault needs to be installed in accordance with [ECD]. This is provided by OE.DBV_INSTALL which requires that Oracle Database Vault is installed in accordance with the guidance and configured and managed in accordance with the protection needs of the organization operating the DBMS.

CHAPTER

5 IT Security Requirements

TOE Security Functional Requirements

Table 3 below lists each Security Functional Requirement (SFR) included in this Security Target. Security Functional Requirements for the Oracle Database itself are defined in [ST11_ENT_GR1] and not repeated here.

For each SFR, Table 3 identifies which Common Criteria operations (assignment (A), selection (S), refinement (R), and/or iteration (I)) have additionally been applied

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 CC part 2 is highlighted with *ITALICISED CAPITAL LETTERS* within each requirement. Annex B provides definitions for various terms used in the functional requirements. The only exception is SFR FDP_ACF.1 where in FDP_ACF.1.2, FDP_ACF.1.3 and FDP_ACF.1.4 the operations are just highlighted with *italics* for better readability.

Refinements are marked in *ITALICISED UNDERLINED CAPITAL LETTERS.*

Table 3: List of Security Functional Requirements

Component	Name	A	S	R	I
FAU_GEN.1	Audit Data Generation	X	X		
FAU_GEN.2	User and/or Group Identity Association				
FAU_SAR.1	Audit Review	X			
FAU_STG.1	Protected Audit Trail Storage		X		
FDP_ACC.1	Subset Access Control	X			
FDP_ACF.1	Security Attribute Based Access Control	X		X	

Component	Name	A	S	R	I
FIA_ATD.1	User Attribute Definition	X			
FIA_USB.1	User-Subject Binding	X			
FMT_MOF.1	Management of Security Functions Behaviour	X	X		
FMT_MSA.1	Management of Security Attributes	X			
FMT_MSA.3	Static Attribute Initialisation	X	X		
FMT_MTD.1	Management of TSF Data	X	X	X	
FMT_SMF.1	Specification of Management Functions	X			
FMT_SMR.1	Security Roles	X			

Security Audit

FAU_GEN.1.1 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 *not specified* level of audit; and
c) *THE FOLLOWING ADDITIONAL EVENTS:*
1) ASSIGNMENT OR EVALUATION OF A FACTOR
2) REALM AUTHORIZATION MANAGEMENT
3) REALM AUTHORIZATION VIOLATION
4) COMMAND AUTHORIZATION MANAGEMENT
5) COMMAND AUTHORIZATION VIOLATION
4) *SECURE APPLICATION ROLE MANAGEMENT*

Table 4: List of Auditable Events

Component	Event	Additional Data
FAU_SAR.1	None	None
FAU_SAR.3	None	None
FAU_STG.1	None	None
FDP_ACC.1	None	None
FDP_ACF.1	Attempted access	None
FIA_USB.1	None (will be audited in the database audit)	None
FMT_MOF.1	Modifications to access control functionality	None
FMT_MSA.1	Modifications of Oracle Database Vault security attributes	None
FMT_MSA.3	None	None
FMT_MTD.1	None	None
FMT_SMF.1	Management operations	None
FMT_SMR.1	Assignment of a role to a user	None

FAU_GEN.1.2 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 ST, and the information specified in column 3 of table 4.

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1.1 The TSF shall provide *USERS WITH READ ACCESS TO THE AUDIT_TRAIL$ TABLE OF THE DVSYS SCHEMA* with the capability to read *ALL DATABASE VAULT 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.

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.

User Data Protection

FDP_ACC.1.1 The TSF shall enforce the *DATABASE VAULT ACCESS CONTROL POLICY* on *ALL SUBJECTS, ALL OBJECTS WITHIN A DEFINED REALM AND ALL OPERATIONS PROTECTED BY THE AUTHORIZATION RULESET FOR THE REALM*.

FDP_ACF.1.1 The TSF shall enforce the *DATABASE VAULT ACCESS CONTROL POLICY* to objects based on the following: *THE REALM AN OBJECT BELONGS TO AND THE AUTHORIZATION RULE SET DEFINED FOR THE REALM THAT IS EVALUATED WHEN A SUBJECT ATTEMPTS TO PERFORM AN OPERATION ON AN OBJECT BELONGING TO A REALM*.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and objects BELONGING TO A REALM is allowed:

When a database account that has the appropriate privileges issues a SQL statement (that is, DDL, DML, EXECUTE, GRANT, REVOKE, or SELECT) that affects an object within a customer-defined realm, the following actions occur:

1. *Is the database account using a system privilege to execute the SQL statement?*
   If yes, then go to Step 2. If no, then go to Step 6. If the session has object privileges on the object in question for SELECT, EXECUTE, and DML only, then the realm protection is not enforced. Realms protect against the use of the any system privileges on objects or roles protected by the realm.
2. *Does the SQL statement affect objects secured by a realm?*
   If yes, then go to Step 3. If no, then realms do not affect the SQL statement; go to Step 6. If the object affected by the command is

not secured in any realms, then realms do not affect the SQL statement being attempted.

3. *Is the database account a realm owner or realm participant? If yes, and if the command is a GRANT or REVOKE of a role that is protected by the realm, or the GRANT or REVOKE of an object privilege on an object protected by the realm, the session must be authorized as the realm owner directly or indirectly through a protected role in the realm. Then go to Step 4. Otherwise, realm violation occurs and the statement is not allowed to succeed. Note that SYS is the only realm owner in the default Oracle Data Dictionary Realm, and only SYS can grant system privileges to a database account or role.*
4. *Is the realm authorization for the database account conditionally based on a rule set? If yes, then go to Step 5. If no, then go to Step 6.*
5. *Does the rule set evaluate to true? If yes, then go to Step 6. If no, then there is a realm violation, so the SQL statement is not allowed to succeed.*
6. *Does a command rule prevent the command from executing? If yes, then there is a command rule violation and the SQL statement fails. If no, there is no realm or command rule violation, so the command succeeds.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to DBMS-controlled objects based on the following additional rules:

Views that have been created on a table before the table was added to the realm are not protected by the authorization rule set of the realm

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules:

Invoker's rights procedures that access realm protected objects are denied access to those objects unless the invoker is authorized to the realm (in which case the authorization rule set is evaluated for the invoker.

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

a) *DATABASE VAULT DEFINED ROLE*;

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:
DATABASE VAULT ROLES.

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

THE SAME RULES APPLY FOR DATABASE VAULT ROLES AS FOR OTHER DATABASE ROLES.

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:

THE SAME RULES APPLY FOR DATABASE VAULT ROLES AS FOR OTHER DATABASE ROLES.

Security Management

FMT_MOF.1.1 The TSF shall restrict the ability to *DETERMINE AND MODIFY THE BEHAVIOUR OF* the functions *DATABASE VAULT ACCESS CONTROL FUNCTIONALITY* to *USERS IN THE DV_ADMIN OR DV_OWNER ROLE*.

FMT_MSA.1.1 The TSF shall enforce the *DATABASE VAULT ACCESS CONTROL POLICY* to restrict the ability to *MANAGE ALL THE SECURITY ATTRIBUTES OF ORACLE DATABASE VAULT* to *AUTHORIZED ADMINISTRATORS*.

FMT_MSA.3.1 The TSF shall enforce the *DATABASE VAULT ACCESS CONTROL POLICY* to provide *RESTRICTIVE* default values for security attributes that are used to enforce the SFP.

FMT_MTD.1.1 The TSF shall, <u>*ACCORDING TO TABLES* 5 *BELOW,*</u> restrict the ability to *PERFORM OPERATIONS ON* the *TSF DATA* to *AUTHORIZED ADMINISTRATORS.*

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.*

Table 5: Required Management Events

Component	Operation	TSF Data
FAU_GEN.1	-	-
FAU_GEN.2	-	-
FAU_SAR.1	deletion, modification, addition	the database users with read access right to the AUDIT_TRAIL$ table in the DVSYS schema
FAU_SAR.3	-	-
FAU_STG.1	-	-
FDP_ACC.1	-	-
FDP_ACF.1	managing	definition of realms, rule sets, command rules, factors
FIA_ATD.1	-	-
FIA_USB.1	-	-
FMT_MOF.1	manage	management of realms, rule sets, command rules, factors
FMT_MSA.1	manage	

Component	Operation	TSF Data
FMT_MSA.3	manage	
FMT_MTD.1	manage	
FMT_SMR.1	manage	assignment of roles to users

FMT_SMR.1.1 The TSF shall maintain the roles:

a) *DV_OWNER*
b) DV_REALM_OWNER
c) DV_REALM_RESOURCE
d) DV_ADMIN
e) DV_ACCTMGR
f) DV_PUBLIC
g) DV_SECANALYST

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

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 the same set of the security assurance requirements as for the evaluation of the Oracle Database itself.

Security Requirements Rationale

Suitability of Security Requirements

The SFRs satisfy the security objectives in the following way:

O.PROTECT_REALM: “The TOE must provide the means of controlling access to objects within a realm even for authorized database administrators” is addressed by the SFRs FDP_ACC.1 and FDP_ACF.1 which define the access control policy for objects within a realm enforced by Oracle Database Vault. This supported by FMT_MSA.1, which explains how the Oracle Database Vault access control policy itself is used to protect security attributes and it is supported by FMT_MSA.3 which defines the default values for the security attributes used in the Oracle Database Vault access control policy.

O.PROTECT_COMMAND: “The TOE must provide means to control the execution of defined SQL statements by installation specific rules” is actually implemented also by the Oracle Database Vault access control policy and therefore is addressed by the same SFRs as O.PROTECT_REALM.

O.RESTRICT_MGMT: “The TOE must provide means to restrict the management of the access control policy and the management of the security attributes to users in defined administrative roles” is addressed by the SFRs FIA_ATD.1, FIA_USB.1 and FMT_SMR.1 which define the administraive roles (FMT_SMR.1) and ensure that users get their roles correctly assigned (FIA_ATD.1, FIA_USB.1) together with FMT_MOF.1, FMT_MSA.1 and FMT_MTD.1, which all define that the management activities for the management of the Oracle Database Vault access control policy rules and the security attributes used in those rules can only be managed by the defined administrative roles.

O.DBV_ACCOUNT: “The TOE must provide the means of auditing actions of users when accessing objects within a realm and when administering Oracle Database Vault” is addressed by the SFRs FAU_GEN.1 and FAU_GEN.2 that define the events that can be audited, by FAU_SAR.1 that ensures that audit records can be evaluated and by FAU_STG.1 which ensures that the audit records are protected from unauthorized deletion and modification.

Table 6: Correlation of IT Security Objectives to the SFRs

Requirement	O.PROTECT_REALM	O.PROTECT_COMMAND	O.RESTRICT_MGMT	O.DBV_ACCOUNT
FAU_GEN.1				X
FAU_GEN.2				X
FAU_SAR.1				X
FAU_STG.1				X
FDP_ACC.1	X	X		
FDP_ACF.1	X	X		
FIA_ATD.1			X	
FIA_USB..1			X	
FMT_MOF.1			X	
FMT_MSA.1	X	X	X	
FMT_MSA.3	X	X		
FMT_MTD.1			X	
FMT_SMF.1			X	
FMT_SMR.1			X	

Dependency Analysis

The following table includes the dependency analysis for the SFRs included in this

ST:

Table 7: Functional Component Dependency Analysis

Requirement	Dependencies	Satisfied
FAU_GEN.1	FPT_STM.1	Yes, indirect[a]
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes Yes, indirect[b]
FAU_SAR.1	FAU_GEN.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes
FIA_ATD.1	-	-
FIA_USB.1	FIA_ATD.1	Yes
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	Yes Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes Yes
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	Yes, indirect[c]

[a] This dependency is resolved by the Oracle Database itself, where the security target contains the FPT-STM.1 security functional requirement.

[b] This dependency is resolved by the Oracle Database itself, where the security target contains the FIA_UID.1 security functional requirement.

[c] See note above

This shows that all dependencies are resolved with the security functionality of user identification and authentication and the reliable time stamp provided by the Oracle Database 11*g* R1 itself and not by Oracle Database Vault. Since Oracle Database Vault is an optional add-on to the Oracle Database and the Oracle Database 11*g* R1 Enterprise Edition being separately evaluated, the dependencies not resolved within this security target are resolved for Oracle Database 11*g* R1 with Oracle Database Vault.

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 11*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.

Assurance Measures Rationale

Table ~~7~~9 in Chapter 6 demonstrates that all assurance requirements are suitably met by one or more assurance measures.

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 8 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 SFR FDP_ACF.1.4 is not satisfied by any particular SF because this SFR specifies null functionality).

Table 8: Mapping of SFs to SFRs

	FAU							FDP					FMT							FIA			
	GEN.1.1	GEN.1.2	GEN.2.1	SAR.1.1	SAR.1.2	STG.1.1	STG.1.2	ACC.1.1	ACF.1.1	ACF.1.2	ACF.1.3	ACF.1.4	MOF.1.1	MSA.1.1	MSA.3.1	MTD.1.1	SMF.1.1	SMR.1.1	SMR.1.2	ATD.1.1	USB.1.1	USB.1.2	USB.1.3
F.DBV.ATT														Y	Y	Y							
F.DBV_REALM_MANAGE													Y	Y		Y	Y						
F.DBV_RULESET_MANAGE													Y	Y		Y	Y						
F.DBV_REALM_ACCESS								Y	Y	Y	Y	Y											
F.DBV_CMDRULE_MANAGE													Y	Y		Y	Y						
F.DBV_CMDRULE_ACCESS								Y	Y	Y	Y	Y											
F.DBV_FACTOR_MANAGE													Y	Y		Y	Y						
F.DBV_SECAPPROL_ACCESS								Y	Y	Y	Y	Y											
F.DBV_SECAPPROL_MANAGE													Y	Y		Y	Y						
F.DBV_ROLES																		Y	Y	Y	Y	Y	Y
F.AUD.DBV	Y	Y	Y			Y	Y																
F.AUD.DBV.VIEW				Y	Y																		

Database Vault Schemas

F.DBV.ATT

The Oracle Database Vault objects include two schemas with database tables, sequences, views, triggers, roles, packages, procedures, functions, and contexts that support the administration and run-time processing of Oracle Database Vault.

Oracle Database Vault has the following schemas:

- DVSYS Schema: Owns the Oracle Database Vault schema and related objects
- DVF Schema: Owns the Oracle Database Vault functions that are created to retrieve factor identities

DVSYS Schema

The DVSYS schema contains Oracle Database Vault database objects, which store Oracle Database Vault configuration information and support the administration and run-time processing of Oracle Database Vault. In a default installation, the DVSYS schema is locked. The DVSYS schema also owns the AUDIT_TRAIL$ table.

Oracle Database Vault secures the DVSYS schema by using a protected schema design. A protected schema design guards the schema against improper use of system privileges (for example, SELECT ANY TABLE, CREATE ANY VIEW, or DROP ANY).

Oracle Database Vault protects and secures the DVSYS schema in the following ways:

- The DVSYS protected schema and its administrative roles cannot be dropped. By default, the DVSYS account is locked.
- Statements such as CREATE USER, ALTER USER, DROP USER, CREATE PROFILE, ALTER PROFILE, and DROP PROFILE can only be issued by a user with the DV_ACCTMGR role. SYSDBA can issue these statements only if it is allowed to do so by modifying the Can Maintain Accounts/Profiles rule set.
- The powerful ANY system privileges for database definition language (DDL) and data manipulation language (DML) commands are blocked in the protected schema. This means that the objects in the DVSYS schema must be created by the schema account itself. Also, access to the schema objects must be authorized through object privilege grants.

- Object privileges in the DVSYS schema can only be granted to administrative roles in the schema. This means that users can access the protected schema only through predefined administrative roles.
- Only the protected schema account DVSYS can issue ALTER ROLE statements on predefined administrative roles of the schema.
- Only the protected schema account DVSYS can grant predefined roles to users along with the ADMIN OPTION. This means that a grantee with the ADMIN OPTION can grant the role to another user without the ADMIN OPTION.

The SYS.DBMS_SYS_SQL.PARSE_AS_USER procedure cannot be used to run SQL statements on behalf of the protected schema DVSYS.

Note: In the maintenance mode, the above stated protection of DVSYS schema is not effective.

DVF Schema

The DVF schema is the owner of the Oracle Database Vault DBMS_MACSEC_FUNCTION PL/SQL package, which contains the functions that retrieve factor identities. After Oracle Database Vault is installed, the installation process locks the DVF account to better secure it. When a new factor is created, Oracle Database Vault creates a new retrieval function for the factor and saves it in this schema.

Database Vault Access Control

Realm Access Control

F.DBV.REALM_ACCESS

Realms protect data from access through system privileges; realms do not give additional privileges to its owner or participants. The realm authorization provides a runtime mechanism to check logically if a user’s command is allowed to access objects specified in the command and to proceed with its execution.

When a database account that has the appropriate privileges issues a SQL statement (that is, DDL, DML, EXECUTE, GRANT, REVOKE, or SELECT) that affects an object within a customer-defined realm, the following actions occur:

1. Is the database account using a system privilege to execute the SQL statement? If yes, then go to Step 2. If no, then go to Step 6. If the session has object privileges on the object in question for SELECT, EXECUTE, and DML only, then the realm protection is not enforced. Realms protect against the use of the any system privileges on objects or roles protected by the realm.
2. Does the SQL statement affect objects secured by a realm? If yes, then go to Step 3. If no, then realms do not affect the SQL statement; go to Step 6.
   If the object affected by the command is not secured in any realms, then realms do not affect the SQL statement being attempted.
3. Is the database account a realm owner or realm participant? If yes, and if the command is a GRANT or REVOKE of a role that is protected by the realm, or the GRANT or REVOKE of an object privilege on an object protected by the realm, the session must be authorized as the realm owner directly or indirectly through a protected role in the realm. Then go to Step 4.
   Otherwise, realm violation occurs and the statement is not allowed to succeed.
   Note that SYS is the only realm owner in the default Oracle Data Dictionary Realm, and only SYS can grant system privileges to a database account or role.

4. Is the realm authorization for the database account conditionally based on a rule set? If yes, then go to Step 5. If no, then go to Step 6.
5. Does the rule set evaluate to true? If yes, then go to Step 6. If no, then there is a realm violation, so the SQL statement is not allowed to succeed.
6. Does a command rule prevent the command from executing? If yes, then there is a command rule violation and the SQL statement fails. If no, there is no realm or command rule violation, so the command succeeds.

Oracle Database Vault does not replace the discretionary access control model in the existing Oracle database. It functions as a layer on top of this model for both realms and command rules.

Realms do not protect views that had been created on a table before the table was added to a realm. To protect the view, explicitly add it to the realm.

For invoker's right procedures that access realm protected objects, the invoker of the procedure must be authorized to the realm.

Command Rule based access control

F.DBV.CMDRULE_ACCESS

Command rule access is defined in step 6 of the algorithm defined in the description of the F.DBV.REALM_ACCESS security function.

Secure Application Roles based access control

F.DBV.SECAPPROL_ACCESS

In Oracle Database Vault, a secure application role can be created that can be enabled with an Oracle Database Vault rule set. Regular Oracle Database secure application roles are enabled by custom PL/SQL procedures. Secure application roles can be used to prevent users from accessing data from outside an application. This forces users to work within the framework of the application privileges that have been granted to the role.

The advantage of basing database access for a role on a rule set is that one can store database security policies in one central place, as opposed to storing them in all the applications. Basing the role on a rule set provides a consistent and flexible method to enforce the security policies that the role provides. In this way, if the security policy for the application role must be updated, it can be done in one place, the rule set.

Furthermore, no matter how the user connects to the database, the result is the same, because the rule set is bound to the role. Oracle Database Vault automatically creates the secure application role to use invoker's rights. All one need to do is to create the role and then associate it with a rule set. The rule definition should validate the user-who is trying to log in.

Once a secure application role is created in Oracle Database Vault, an application can call the role by using the DVSYS.DBMS_MACSEC_ROLES.SET_ROLE function.

Oracle Database Vault then evaluates the rule set associated with the secure application role.

If the rule set evaluates to true, then Oracle Database Vault enables the role for the current session and assigns the privileges associated with the role. If the rule set evaluates to false, the role is not enabled. In either case, Oracle Database Vault processes the associated auditing and custom event handlers for the rule set associated with the secure application role.

Database Vault Management

Realm Management

F.DBV.REALM_MANAGE

To perform realm management functions, a user must have either the DV_ADMIN or DV_OWNER role.

The procedures in the DVSYS.DBMS_MACADM package can be used to configure and manage realms. They allow to:

- create a realm
- delete a realm
- rename a realm
- authorize a user or role to access a realm as an ownwe or a participant
- remove authorizations of a user or role to access the realm
- specify a ruleset for authorization
- define or update realm attributes
- register a set of objects for realm protection

Realm attributes that can be set or updated are:

- realm description (not used for any security checking)
- enabling or disabling realm checking
- realm audit options. Possible settings are: off, success, fail

Command Rule Management

F.DBV.CMDRULE_MANAGE

To perform command rule management functions, a user must have either the DV_ADMIN or DV_OWNER role.

The procedures in the DVSYS.DBMS_MACADM package can be used to configure and manage command rules. They allow to:

- create a command rule
- delete a command rule
- update a command rule

Ruleset Management

F.DBV.RULESET_MANAGE

To perform rule set management functions, a user must have either the DV_ADMIN or DV_OWNER role.

The procedures in the DVSYS.DBMS_MACADM package can be used to configure and manage rule sets. They allow to:

- create a rule or rule set
- delete a rule or rule set
- remove a rule from a rule set
- add a rule to a rule set
- rename a rule or a rule set

- update a rule
- update rule set attributes (enabled or diabled, evaluation option (*Always True* or *Any True*), rule set audit options, option for reporting factor errors, error handling options)
- synchronize the rules in Oracle Database Vault and the Advanced Queuing Rules engine. This operation must be performed immediately after a rollback of an Add, Delete, or Modify rule operation

Factor Management

F.DBV.FACTOR_MANAGE

To perform factor management functions, a user must have either the DV_ADMIN or DV_OWNER role.

The procedures in the DVSYS.DBMS_MACADM package can be used to configure and manage factors. They allow to:

- create a factor or factor type
- delete a factor or factor type
- rename a factor or factor type
- create an identity
- remove an identity
- create a factor identity mapping
- remove a factor identity mapping
- associate an identity with a different factor
- create a parent-child relationship between two factors
- update a factor

Secure Application Role Management

F.DBV.SECAPPROL_MANAGE

To perform secure application role management functions, a user must have either the DV_ADMIN or DV_OWNER role.

The procedures in the DVSYS.DBMS_MACADM package can be used to configure and manage secure application roles. They allow to:

- create a secure application role
- delete a secure application role
- rename a secure application role
- update a secure application role

Applications can use secure application roles by using procedures in the DVSYS.DBMS_MACSEC_ROLES package.

They can use the CAN_SET_ROLE Function to check whether the user invoking the method is authorized to use the specified Oracle Database Vault secure application role. Returns a BOOLEAN value.

They can use the SET_ROLE Procedure to issue the SET ROLE statement for an Oracle Database Vault secure application role. If a rule set that is associated with the role evaluates to false, then the role is not set.

Database Vault Roles

F.DBV_ROLES

When installed, Oracle Database Vault defines the following additional roles:

DV_OWNER

This role is used to manage the Oracle Database Vault roles and its configuration. The DV_OWNER role has the administrative capabilities that the DV_ADMIN role provides, and the reporting capabilities the DV_SECANALYST role provides. It also provides privileges for monitoring Oracle Database Vault. It is created when you install Oracle Database Vault, and has the most privileges on the DVSYS schema.

The first account, which is typically the account created during the installation as the Database Vault Owner, granted with this role and the ADMIN OPTION can grant any Oracle Database Vault roles (except DV_ACCTMGR) without the ADMIN OPTION to any account. Users granted this role also can run Oracle Database Vault reports and monitor Oracle Database Vault.

Anyone with the DV_OWNER role or privilege can grant the DV_OWNER role to another user. The account granted this role and with the ADMIN OPTION can revoke any granted protected schema role from another account. Accounts such as SYS or SYSTEM, with the GRANT ANY ROLE system privilege alone (directly granted or indirectly granted using a role) do not have the rights to grant or revoke the DV_ OWNER role from any other database account.

The granting and revoking of all protected schema roles, including DV_OWNER, are enforced only by an instance with the Oracle executable linked with DV_ON, which enables Oracle Database Vault security. When the Oracle executable is linked with DV_ OFF, then an instance can use an account GRANT ANY ROLE system privilege for GRANT and REVOKE operations. In the later case, the Oracle Server enters into a maintenance mode in the relation to the Oracle Database Vault and hence the DV_OWNER role loses its impact on the access control on database operations.

DV_REALM_OWNER

This role is used to manage database objects in multiple schemas that define a realm. This role should be granted to the database account owner who is responsible for managing one or more schema database accounts within a realm and the roles associated with the realm. A user granted this role can use powerful system privileges like CREATE ANY, ALTER ANY, and DROP ANY within the realm.

DV_REALM_RESOURCE

The DV_REALM_RESOURCE role provides the same system privileges as the Oracle RESOURCE role. In addition, both CREATE SYNONYM and CREATE VIEW are granted to this role.

This role can be granted to a database account that will own database tables, objects, triggers, views, procedures, and so on that are used to support any database application. This is a role geared toward a schema type database account. The realm owner of the Oracle Data Dictionary realm, such as SYS, can grant this role to any database account or role. Note that though this role has system privilege grants that SYS controls, it does not have the DV_OWNER or DV_ADMIN privileges.

DV_ADMIN

The DV_ADMIN role has the EXECUTE privilege on the DVSYS packages (DBMS_MACADM, DBMS_MACSECROLES, and DBMS_MACUTL). DV_ADMIN also has the capabilities provided by the DV_SECANALYST role, which allow the user to run Oracle Database Vault reports and monitor Oracle Database Vault.

Accounts such as SYS or SYSTEM, with the GRANT ANY ROLE system privilege alone do not have the rights to grant or revoke DV_ADMIN from any other database account. The first user with the DV_ADMIN role and the ADMIN OPTION can grant this role without the ADMIN OPTION to any database account and revoke this role from another account.

The granting and revoking of protected schema roles, including DV_ADMIN, are enforced only by an instance with the Oracle executable linked with DV_ON, which enables Oracle Database Vault security features. When the Oracle executable is linked with DV_OFF, then an instance can use an account GRANT ANY ROLE system privilege for GRANT and REVOKE operations.

DV_ACCTMGR

Use the DV_ACCTMGR role to create and maintain database accounts and database profiles. A user who has been granted this role can use the CREATE, ALTER, and DROP statements for users or profiles. However, a person with this role cannot use the DROP or ALTER statements for the DVSYS account, nor change the DVSYS password.

Any account, such as SYS or SYSTEM, with the GRANT ANY ROLE system privilege alone does not have the rights to grant this role to or revoke this role from any other database account. The account with the DV_ACCTMGR role and the ADMIN OPTION can grant this role without the ADMIN OPTION to any given database account and revoke this role from another account.

The granting and revoking of protected schema roles are enforced only by an instance with the Oracle executable linked with DV_ON, which enables Oracle Database Vault. When the Oracle executable is linked with DV_OFF, then an instance can use an account with GRANT ANY ROLE system privilege for GRANT and REVOKE operations.

DV_PUBLIC

Use the DV_PUBLIC role to grant privileges on specific objects in the DVSYS schema. (in a default installation, the DVSYS schema is locked.)

Oracle Database Vault does not enable any user to directly grant object privileges in the DVSYS schema to PUBLIC. One must grant the object privilege on the DVSYS schema object to the DV_PUBLIC role, and then grant DV_PUBLIC to PUBLIC. However, if one does this, it is important that to not add more object privileges to the PUBLIC role. Doing so may undermine Oracle Database Vault security.

DV_SECANALYST

Use the DV_SECANALYST role to run Oracle Database Vault reports and monitor Oracle Database Vault. (This role is also used for database-related reports.) In addition, this role enables you to check the DVSYS configuration by querying the DVSYS views described in [DBV_ADMIN] on page 10-9. The DV_SECANALYST role has SELECT privileges on the DVSYS schema objects and portions of the SYS and SYSMAN schema objects for reporting on DVSYS- and DVF-related entities.

Audit and Accountability

F.AUD.DBV

Oracle Database Vault defines custom events to track violations in realms, command rules, and so on. It is possible to audit the following in Oracle Database Vault:

- **Rule Set Audit**: Audits the rule set processing results. You can audit both successful and failed processing. Realm authorizations can be managed using rule sets. You can audit the rule set processing results. Factor assignments and secure application roles audits can be managed using a rule set.
- **Realm Audit**: A realm violation occurs when a database account, performing an

action on a realm object, is not authorized to perform that action in the realm. You can audit realm violations.

- **Factor Audit**: You can audit both successful and failed factor processing. For failed factor processing, you can audit on all or any of the following events: Retrieval Error, Retrieval Null, Validation Error, Validation False, Trust Level Null, or Trust Level Less Than Zero.
- **Oracle Label Security Session Initialization Failed**: Audits instances where the Oracle Label Security session fails to initialize.
- **Oracle Label Security Attempt to Upgrade Session Label Failed**: Audits instances where the Oracle Label Security component prevents a session from setting a label that exceeds the maximum session label.

The Oracle Database Vault custom audit event records are stored in the AUDIT_TRAIL$ table, which is part of the DVSYS schema. These audit records are not part of the typical Oracle Database audit trail. (In fact, if auditing has been disabled in Oracle Database, the Oracle Database Vault audit will continue to write to the AUDIT_TRAIL$ table.). The Oracle Database Vault audit trail is protected from unauthorized access by the protection of the DVSYS schema.

When Oracle Database Vault is installed, it creates a number of AUDIT settings in the database. However, in order for these audit settings to take place, auditing must be enabled in this database. By default, auditing is disabled in Oracle Database and therefore when Oracle Database Vault is installed the AUDIT_TRAIL parameter must be set. For detailed information about the AUDIT_TRAIL parameter settings, see Oracle Database Security Guide and Oracle Database Reference.

When installed Oracle Database Vault adds a number of settings to the Oracle Database settings. Those are defined in detail in [DBV_ADMIN] in table A-2.

F.AUD.DBV.VIEW

Authorized administrators can check for security violations, such as realm or command rule violations. This feature displays data such as the user name of the person committing the violation, the action they committed, and a time stamp of the activity. For a user who has read access to AUDIT_TRAIL$ table in the DVSYS schema, he can retrive and view the audit data from the AUDIT_TRAIL$ table using the standard SQL procedures. The user may also choose to use a more user friendly graphic interface as stated below. However, this GUI is not a TSFI.

To check for security violations one needs to:

- Log in to Oracle Database Vault Administrator with an account that uses the DV_OWNER, DV_ADMIN, or DV_SECANALYST role.
- In the Administration page, click Monitor.
- At the top of the Monitor page, set a period of time for the monitoring action by selecting from the Show Records For list and clicking Go. This section of the Monitor page also indicates the last time the data on the page was refreshed.
- In the Monitor page, click Security Violation Attempts. A table appears, listing security policy changes.

An archive of the Oracle Database Vault audit trail can be created by exporting the AUDIT_TRAIL$ system table, which is owned by DVSYS, to a dump file. This should be done periodically to archive and then purge the audit trail to prevent it from growing too large.

Table A-1 in [DBV_ADMIN] describes the format of the audit trail in the AUDIT_TRAIL$ table in the DVSYS schema. This format definition can be used when creating custom reports.

Assurance Measures

The target assurance level is EAL4 augmented with ALC_FLR.3. No other specific assurance measures are claimed. The following table identifies the Oracle Database 11*g* documentation that supports each security assurance requirement for EAL4 and also the assurance requirement for ALC_FLR.3. Note that Oracle Database Vault is an option integrated into the Oracle Database and therefore follows the same development process. Also the design information for Oracle Database Vault is part of the design documents for the Oracle Database 11*g* R1.

TOE Security Assurance Requirements

Table 9: TOE Security Assurance Requirements

Component	Name	Documents
ALC_CMC.4	Production support, acceptance procedures and automation	[CM]
ALC_CMS.4	Problem tracking CM coverage	[CM]
ALC_DEL.1	Delivery procedures	[OQM]
ALC_DVS.1	Identification of security measures	[SODE]
ALC_FLR.3	Systematic flaw remediation	[FLR]
ALC_LCD.1	Developer defined life-cycle model	[LCS]
ALC_TAT.1	Well-defined development tools	[CM]
AGD_OPE.1	Operational user guidance	[ECD] [GA] [DBV_ADMIN]
AGD_PRE.1	Preparative procedures	[ICG] [ECD] [GA] [DBV_ADMIN]
ADV_ARC.1	Security architecture description	[AD]
ADV_FSP.4	Complete functional specification	[ERR] [OCI]
ADV_TDS.3	Basic modular design	[AD]
ADV_IMP.1	Implementation representation of the TSF	[SRC]
ATE_COV.2	Analysis of coverage	[TP]
ATE_DPT.2	Testing: security enforcing modules	[TP]

Component	Name	Documents
ATE_FUN.1	Functional testing	[TP]
ATE_IND.2	Independent testing - sample	[TP]
AVA_VAN.3	Focused vulnerability analysis	[VA]

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

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 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FAU_GEN.1.1	F.AUD.DBV	The audit events are defined in the description of this function.
FAU_GEN.1.2	F.AUD.DBV	The audit record format is defined in this function (with a reference to the detailed format description in the Database Vault documentation)
FAU_GEN.2.1	F.AUD.DBV	The function associates the event audit records with the identified users that caused the events.
FAU_SAR.1.1	F.AUD.DBV.VIEW	The functions that can be used to review the audit records as well as the roles that are allowed to access the audit trail are defined here.
FAU_SAR.1.2	F.AUD.DBV.VIEW	The function describes the monitor interface that can be used to view the audit records. In addition the description of the audit trail format allows to develop own tools for evaluation of the audit records.
FAU_STG.1.1	F.AUD.DBV	The audit trail is part of the DVSYS schema and protected by the protection mechanisms for this schema.
FAU_STG.1.2	F.AUD.DBV	The audit trail is part of the DVSYS schema and protected by the protection mechanisms for this schema.
FDP_ACC.1.1	F.DBV_REALM_ACCESS F.DBV_CMDRULE_ACCESS F.DBV_SECAPPROL_ACCESS	The security functions listed describe the objects protected as well as the access control rules.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FDP_ACF.1.1	F.DBV_REALM_ACCESS F.DBV_CMDRULE_ACCESS F.DBV_SECAPPROL_ACCESS	The security functions listed describe the objects protected as well as the access control rules.
FDP_ACF.1.2	F.DBV_REALM_ACCESS F.DBV_CMDRULE_ACCESS F.DBV_SECAPPROL_ACCESS	The security functions listed describe the objects protected as well as the access control rules.
FDP_ACF.1.3	F.DBV_REALM_ACCESS F.DBV_CMDRULE_ACCESS F.DBV_SECAPPROL_ACCESS	Listed as worded in the functions
FDP_ACF.1.4	F.DBV_REALM_ACCESS F.DBV_CMDRULE_ACCESS F.DBV_SECAPPROL_ACCESS	Listed as worded in the functions
FIA_ATD.1.1	F.DBV_ROLES	The function lists all the roles that are maintained by Oracle Database Vault
FIA_USB.1.1	F.DBV_ROLES	Binding roles to subjects is done be the Oracle Database. Oracle Database roles are handled in the same way as other roles within the database.
FIA_USB.1.2	F.DBV_ROLES	Binding roles to subjects is done be the Oracle Database. Oracle Database roles are handled in the same way as other roles within the database.
FIA_USB.1.3	F.DBV_ROLES	Binding roles to subjects is done be the Oracle Database. Oracle Database roles are handled in the same way as other roles within the database.
FMT_MOF.1.1	F.DBV_REALM_MANAGE F.DBV_RULESET_MANAGE F.DBV_CMDRULE_MANAGE F.DBV_FACTOR_MANAGE F.DBV_SECAPPROL_MANAGE	The restrictions on managing the behaviour of the Oracle Database Vault access control function are defined in the sections describing the management of the realms, rulesets, command rules and secure application roles.
FMT_MSA.1.1	F.DBV_ATT F.DBV_REALM_MANAGE F.DBV_RULESET_MANAGE F.DBV_CMDRULE_MANAGE F.DBV_FACTOR_MANAGE F.DBV_SECAPPROL_MANAGE	The restrictions on managing the behaviour of the Oracle Database Vault access control function are defined in the sections describing the management of the realms, rulesets, command rules and secure application roles.

Table 10: TOE Security Function Suitability and Binding

SFR	TOE Security Functions	Rationale
FMT_MSA.3.1	F.DBV_ATT	The function F.DBV_ATT desribes the schemas used by Oracle Database Vault as well as the restrictive settings with respect to access to those schemas.
FMT_MTD.1.1	F.DBV_ATT F.DBV_REALM_MANAGE F.DBV_RULESET_MANAGE F.DBV_CMDRULE_MANAGE F.DBV_FACTOR_MANAGE F.DBV_SECAPPROL_MANAGE	The restrictions on managing the behaviour of the Oracle Database Vault access control function are defined in the sections describing the management of the realms, rulesets, command rules and secure application roles.
FMT_SMF.1.1	F.AUD.DBV F.DBV_REALM_MANAGE F.DBV_RULESET_MANAGE F.DBV_CMDRULE_MANAGEF.DBV_FACTOR_MANAGE F.DBV_SECAPPROL_MANAGE	The management functions that can be performed are defined in the descriptions of the security function mentioned in the second column.
FMT_SMR.1.1	F.DBV_ROLES	The roles defined by Oracle Database Vault are defined in this security function.
FMT_SMR.1.2	F.DBV_ROLES	See the descriptions of the DV_OWNER and DV_ADMIN roles on the restrictions on granting Oracle Database Vault roles to users.

This Page Intentionally Blank

ANNEX

A References

[AD] *Architecture for Oracle Database 11g Release 1 (11.1.0),* Oracle Corporation.

[ADG] *Oracle Database Application Developer’s Guide - Fundamentals,11g Release 1 (11.1),* Oracle Corporation.

[BR-DBMSPP] *U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, July 25, 2007,* 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 3.1.

[CCEVS-VR-07-0054] Common Criteria Evaluation and Validation Scheme Validation Report, Red Hat Enterprise Linux, Version 5, NIAP-CCEVS

[CCEVS-VR-VID10271] Common Criteria Evaluation and Validation Scheme Validation Report, SUSE LINUX Enterprise Server, Version 10 Service Pack 1, NIAP-CCEVS

[CM] *Oracle Database Configuration Management Plan, 11g Release 1 (11.1.0),* Oracle Corporation.

[CON] *Oracle Database Concepts, 11g Release 1 (11.1),* Oracle Corporation.

[DAG] *Oracle Database Administrator’s Guide, 11g Release 1 (11.1),* Oracle Corporation.

[DBV_ADMIN] *Oracle Database Vault Administrator’s Guide, 11g Release 1 (11.1),* Oracle Corporation.

[DD] *Detailed Design for Oracle Database 11g Release 1 (11.1.0),*
Oracle Corporation.

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

[DT] *Design Traceability for Oracle Database 11g Release 1 (11.1.0),*
Oracle Corporation.

[DSZ0486] *Certification Report BSI-DSZ-CC-0486-2004,*
for Oracle Enterprise Linux, Version 4 Update 5, July 2007.
Available from http://www.bsi.bund.de/zertifiz/zert/reporte/0486a.pdf.

[ECD] *Evaluated Configuration Document for Oracle Database 11g Release 1 (11.1.0),*
Oracle Corporation.

[ERR] *Oracle Database Error Messages, 11g Release 1 (11.1),*
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, 11g Release 1 (11.1.0),*
Oracle Corporation.

[ICG] *Oracle Database Installation and Configuration Guide, 11g Release 1 (11.1),*
Oracle Corporation.

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

[LCS] *Life Cycle Support for Oracle Database 11g, Release 1 (11.1.0),*
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, 11g Release 1 (11.1),*
Oracle Corporation.

[OLS_ST11GR1] *OLS Security Target for Oracle Database 11g Release 1 (11.1),* Issue 3.0,
Oracle Corporation.

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

[PLS] *PL/SQL User's Guide and Reference, 11g Release 1 (11.1),* Oracle Corporation.

[SG] *Oracle Database Security Guide, 11g Release 1 (11.1),* Oracle Corporation.

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

[SOF] *Strength of Function Analysis for Oracle Database 11g Release 1 (11.1.0),* Oracle Corporation.

[SQL] *Oracle Database SQL Reference, 11g Release 1 (11.1),* Oracle Corporation.

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

[SPM] *Security Policy Model for Oracle Database 11g Release 1 (11.1.0)*, Oracle Corporation.

[SRC] *Oracle Database Source Code 11g, Release 1 (11.1.0),* Oracle Corporation.

[SRF] *Oracle Database Reference*, *11g Release 1 (11.1),* Oracle Corporation.

[ST10_ENT_GR2] *Security Target for Oracle10g, Release 2 (10.2.0)*, *Enterprise Edition,* Issue 2.0, Oracle Corporation.

[ST11_ENT_GR1] *Security Target for Oracle11g, Release 1 (11.1.0), Enterprise Edition*, Version 4.0, 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 11g Release 1 (11.1.0),* Oracle Corporation.

This Page Intentionally Blank

ANNEX

B Glossary

Acronyms

DAC	Discretionary Access Control
DDL	Data Definition Language
DES	Data Encryption Standard
DML	Data Manipulation Language
O-RDBMS	Object-Relational Database Management System
RAC	Real Application Clusters
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]

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]

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, 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]SQL statement

A string of SQL text containing a command and supporting clauses. All access to an Oracle database is via SQL statements. [SCN]

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

This Page Intentionally Blank