Evaluated Configuration for Oracle8 Database Server
Release 8.0.5

March 2000

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

Evaluated Configuration for Oracle8 Database Server
Release 8.0.5

March 2000

Authors: Rajiv Sinha & Howard Smith

Contributors: Duncan Harris, Steve Pannifer, Paul Nesfield

Contents

March 2000

Contents

March 2000

CHAPTER

1 Introduction

The Target of Evaluation (TOE) is the Oracle8 Release 8.0.5 Object-Relational Database Management System (O-RDBMS).

The TOE is hosted on the Microsoft Windows NT Version 4.0 operating system.

This *Evaluated Configuration for Oracle8 Database Server* document explains the manner in which the TOE must be configured along with the host operating system and network services so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

The Evaluation Assurance Level for the TOE is EAL4. The Protection Profile used for the evaluation of the TOE is the [G.DBMS PP]. The Security Target used for the evaluation of the TOE is the [ST].

1.1 Intended Audience

The intended audience for this document includes evaluators of the TOE, system integrators who will be integrating the TOE into systems, and accreditors of the systems into which the TOE has been integrated.

1.2 Organization

This document is composed of the following sections:

Chapter 1 contains the introduction to the document;

Chapter 2 describes the physical environment of the TOE and the network services required to support the TOE;

Chapter 3 describes the host operating system, network services, and client application configurations required to support the TOE;

Chapter 4 describes the configuration of the TOE, and all TOE-related network services and applications;

Chapter 5 contains a step by step guide to installation of the TOE in its evaluated configuration; *and*

Appendix A lists the references that are used in this document.

1.3 Format

Assertions for the physical, host, and Oracle configurations are enumerated to the left of each evaluation configuration requirement in bold Helvetica font, e.g., **[A-1]**.

Mandatory evaluation configuration requirements use the words “must” and/or “shall” in each assertion.

Strongly recommended evaluation configuration requirements use the words “may” and/or “should” in each assertion.

CHAPTER

2 Physical Configuration

This chapter described the physical and procedural requirements for maintaining the security of the TOE.

2.1 Physical Environmental Assumptions

[A-1] The processing resources of the TOE shall be located within controlled access facilities which will prevent unauthorized physical access, to the TOE by unprivileged users. Only authorised DBA or operator users (i.e. users who are allowed corresponding SYSDBA or SYSOPER access rights withing the database) shall have physical access to the server machines.

[A-2] The processing resources of the underlying operating system required to support the TOE shall be located within controlled access facilities which will prevent unauthorized physical access.

[A-3] The processing resources of the network services required to support the TOE shall be located within controlled access facilities which will prevent unauthorized physical access.

[A-4] The media on which authentication data for the underlying operating system data resides shall not be physically removable from the underlying operating system by unauthorized users.

[A-5] The media on which the TOE audit data resides shall not be physically removable from the underlying operating system by unauthorized users.

[A-6] Any on-line and/or off-line storage media on which security relevant data resides shall be located within controlled access facilities which will prevent unauthorized physical access.

2.2 Supporting Procedures

Procedures for the administration of TOE security shall be established based on the contents of this document, the Security Target [ST], [NTINST] and any site security policy that may be in force. In particular procedures shall be established such that:

- users must not disclose their operating system passwords to other individuals;
- operating system passwords generated by the system adminstrator shall be distributed in a secure manner;
- procedures and/or mechanisms shall assure that, after system failure or other discontinuity, recovery without a protection (i.e. security) compromise is obtained;
- the on-line and off-line storage media on which security related data (such as operating system backups, database backups and transaction logs, and audit trails) are held shall be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security related data;
- the media on which database-related files (including database files, export files, redo log files, control files, trace files, and dump files) have been stored shall be purged prior to being re-used for any non-database purpose;
- the predefined normal user SYS, the DBA user and the OPER user are highly trusted users, who are required by the architecture of the TOE to be able to perform privileged database operations for which the TOE records only limited information. It is assumed that appropriate personnel and procedural measures (such as procedural two-person control) will be provided to ensure that operations performed under these trusted user accounts conform to the system security policy. (In general the TOE does not record accounting information for operations performed by SYS, DBA and OPER. However, in certain restricted circumstances, such as instance start-up and shut-down, the TOE does write accounting information for these users to the OS audit trail only. This helps to support reliability and availability by avoiding any possibility that these users could be locked out of the TOE in the event that the database audit trail should become completely full.).

  It is assumed that the abuse of trust by such users is not considered a threat or is an acceptable security risk.

  For more routine administration tasks it is recommended that alternative, less privileged, database user accounts are configured and used to perform a more restricted set of privileged database operations (for which the TOE will record accounting information in full).
- a user who grants the REFERENCES privilege on one or more columns of a table shall understand the possible interactions between database referential integrity controls and access controls. Specifically, a referential constraint has the following implications:
  - if the referential constraint specifies DELETE RESTRICT then a user will not be able to delete referenced parent rows even though the user has DELETE access on the parent table;
  - if the referential constraint specifies SET TO NULL or SET TO DEFAULT then when a parent row is deleted from the parent table the corresponding child row(s) will be updated regardless of whether the deleting user has UPDATE access on that child table.
  - if the referential constraint specifies DELETE CASCADE then when a parent row is deleted from the parent table the corresponding child row(s) will be deleted from the child table regardless of whether the deleting user has DELETE access on that child table.

CHAPTER

3 Host Configuration

The TOE was evaluated and tested on two (2) Compaq Proliant 4500 x86 (Family 5 Model 2 Stepping 5) server machines and one (1) Compaq Deskpro 4200 client machine. All the three machines were connected by a Local Area Network (LAN).

The TOE was evaluated and tested on Microsoft Windows NT Server (build 1381 with Service Pack 3) operating systems running on both server machines, and on one Microsoft Windows NT Workstation operating system running on the client machine.

3.1 Operating System

[OS-1] The underlying operating system shall be the Microsoft Windows NT Version 4.0 Server operating system, build 1381, with Service Pack 3.

[OS-2] The underlying operating system identified in [OS-1] should satisfy the requirements of the [ITSEC] Functionality Class F-C2 or greater, the requirements of the [TCSEC] Class C2 or greater, or the requirements of the [CC] Evaluation Assurance Level EAL3 or greater.

[OS-3] The underlying operating system identified in [OS-1] should be installed and operated in a manner as described in the [ITSEC] or [CC] Certification Report or in the [TCSEC] Final Evaluation Report, and in accordance with its evaluated configuration and operational documentation, if available.

[OS-4] The Windows NT File System (NTFS) shall be used on all host machines supporting the TOE.

[OS-5] The operating system administrator shall ensure that only users in the `ADMINISTRATORS` and/or `DOMAIN ADMINS` groups are able to perform administrative tasks in the operating system.

This should be achieved by editing the System Policy Editor of Windows NT to reflect the privileges for administrative and normal operating system users.

3.1.1 Identification and Authentication

[OS.IA-1] The operating system shall provide and implement authentication for database users

attempting to connect to the TOE.

[OS.IA-2] The operating system shall protect its authentication mechanism against modification.

[OS.IA-3] The operating system shall support the creation and maintenance of uniquely identified operating system users accounts.

[OS.IA-4] The operating system shall prevent unauthorized modification of operating system users accounts.

[OS.IA-5] The operating system shall allow only users in the `ADMINISTRATORS` group to access the operating system registry. No other user should be permitted to access the operating system registry.

This should be accomplished by ensuring that only the operating system administrator belongs to the `ADMINISTRATORS` operating system group. The operating system administrator may also belong to the `DOMAIN ADMINS` group to create and administer user accounts on other machines within a domain.

[OS.IA-6] No other users (existing or newly created) shall belong to either the `ADMINISTRATORS` or `DOMAIN ADMINS` groups on either the host machine on which the TOE is installed, or on their local (client) machines from which they will connect to the TOE.

[OS.IA-7] The operating system shall support a single domain of identification for all normal users of the TOE.

[OS.IA-8] All normal operating system users shall belong to either the `USERS` or other (non-administrator) domain level operating system group such as `DOMAIN USERS`.

[OS.IA-9] In a networked environment, this single domain of identification shall be configured in the operating system and the TOE, for each node on the underlying network by the administrators of the TOE.

[OS.IA-10] In order to support operating system authentication of normal TOE users, the operating system administrator shall set the following NT registry parameter in the `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE` home hive:

```
osauth_enforce_strict = TRUE
```

This NT registry parameter enables the TOE to differentiate between its administrative and normal (non-administrative) users during identification to the TOE as described in [STARTED, 11-7].

[OS.IA-11] The operating system administrator shall delete the `DBA_AUTHORIZATION` parameter (if present) from the NT registry.

[OS.IA-12] The operating system administrator shall delete the `ORA_PWFILE` and/or the `ORA_<SID>_PWFILE` parameters (if present) from the NT registry.

[OS.IA-13] Command shell and other logical access (either locally or remotely) to machines hosting the database server shall be restricted to users holding SYSDBA or SYSOPER level access to the database. Unless otherwise required by this document no user level network shares are to be established to the server machines.

3.1.2 Protection of Resources

[OS.PR-1] The operating system shall protect all of the installed TOE-related files and directories by means of its Discretionary Access Control mechanisms to ensure that they are accessible to authorized users only.

These TOE directories containing all TOE executables and parameter and control files

are located in the ORACLE_HOME directory and its subdirectories.

[OS.PR-2] The permissions set on TOE directory, sub directories and all files contained within these directories identified in [OS.PR-1] should be set as illustrated in table 3-1 for server installations:

User/Group	Permission
Administraor	FULL CONTROL
SYSTEM	FULL CONTROL
ORA_DBA, ORA_OPER	FULL_CONTROL
ORA_<sid>_DBA, ORA_<sid>_OPER	FULL_CONTROL

Table 3-1: Acces permissions for ORACLE_HOME on database servers

Any other permission entries should be deleted.

Access permissions for client installations should be set as illustrated in table 3-2 below:

User/Group	Permission
Administrator[a]	FULL CONTROL
SYSTEM	FULL CONTROL
An Oracle user[b]	SPECIAL ACCESS (READ) on all files and subdirectories, except: READ (Includes execute) on *.DLL (all DLL files), PLUS80.EXE and PLUS80W.EXE in the ORACLE_HOME\bin directory. NO ACCESS on all other .EXE files in the ORACLE_HOME\bin directory. LIST on the ORACLE_HOME directory only. READ on the ORACLE_HOME\bin directory.

Table 3-2: Acces permissions for ORACLE_HOME on database clients

a. Domain Admins may be added also if desired.
b. An entry needs to be made for each authorised user of the oracle software on this machine. Alternatively a global user group (e.g. Oracle_users) could be established and entered here. Oracle users would then need to be a member of this global user group in order to be able to access the database.

[OS.PR-3] The operating system shall protect system clocks against unauthorized modification so as to maintain the integrity of audit timestamps.

[OS.PR-4] [OS.PR-3] should be accomplished by permitting only operating system administrators to access the operating system clock configuration. Access permissions for all other users should be set to NO ACCESS for the operating system clock.

3.1.3 Accounting and Auditing

[OS.AA-1] The operating system shall protect operating system audit trails or any other audit trails used by the O-RDBMS against unauthorized modification and deletion by means of its Discretionary Access Control mechanisms.

[OS.AA-2] The directory containing audit trail files shall be set to `FULL CONTROL` permissions for users in the local TOE administrator operating group, and `NO ACCESS` for all other users.

[OS.AA-3] The operating system shall include procedures that support the archiving of operating system audit trails prior to audit trail exhaustion.

[OS.AA-4] The operating system shall support the audit of TOE generated audit records of all TOE privileged connections, and TOE startup and shutdown operations in the its audit trail irrespective of whether or not auditing is turned on in the TOE.

3.2 Network Services

[OS.NS-1] The underlying network services should satisfy the requirements of the [ITSEC] Functionality Class F-C2 or greater, the requirements of the [TCSEC] Class C2 or greater, or the requirements of the [CC] Evaluation Assurance Level EAL3 or greater.

[OS.NS-2] The underlying network services should be installed, and operated in a manner as described in the [ITSEC] or [CC] Certification Report, or the [TCSEC] Final Evaluation Report, and in accordance with their evaluated configuration and operational documentation, if available.

[OS.NS-3] In a distributed environment, the underlying network services shall be based on the available Windows NT secure communication protocols which ensure the authenticity of the operating system users.

[OS.NS-4] Only users in the `ADMINISTRATORS` group shall be able to modify the network services configuration parameters.

[OS.NS-5] No other user shall be permitted to modify any network services configuration parameter.

3.3 Client Applications

[OS.CA-1] No applications shall be permitted to run on any client or server machines which access the network, unless they have been shown not to compromise the TOE's security objectives stated in the [G.DBMS PP] and the [ST].

CHAPTER

4

Oracle Configuration

The TOE consists of software only. The TOE contains no hardware or firmware components and there are no hardware or firmware dependencies which affect the evaluation.

[DB-1] The TOE shall be installed, configured, and maintained in accordance with this document and with the instructions provided in the [IUG].

[DB-2] The TOE shall be installed using the Oracle Installer Release 3.3.0.1.3 and within it, the Custom Installation option.

[DB-3] During installation, the following software components shall be selected from the list of available products presented on the product installation screen:

- Oracle8 Enterprise Edition 8.0.5.0.0
- Oracle8 Objects Option 8.0.5.0.0[1]
- Oracle8 Utilities 8.0.5.0.0
- Oracle Installer 3.3.0.1.3
- Oracle Call Interface 8.0.5.0.0
- SQL*Plus 8.0.5.0.0
- Net8 Client 8.0.5.0.0
- Net8 Server 8.0.5.0.0

In addition to these components, the following software components are automatically installed by the Oracle Installer:

- Required Support Files 8.0.5.0.0
- Oracle Named Pipes Protocol Adapter 8.0.5.0.0
- Oracle TCP/IP Protocol Adapter 8.0.5.0.0

1. Optional component which may be installed.

- Oracle Names Server 8.0.5.0.0
- Oracle Database Assistant 2.0.0.0.0
- Java (TM) Runtime Environment 1.1.1.0.0
- Oracle Trace Collection Services 8.0.5.0.0
- Oracle8 Enterprise Edition Release Notes 8.0.5.0.0
- Oracle Net8 Assistant 8.0.5.0.0
- Oracle8 JDBC Drivers 8.0.5.0.0
- Assistant Common Files 1.0.1.0.0

4.1 Evaluated Configuration Boundaries

SQL*Plus Release 8.0.5.0.0 is used by the evaluators for testing the TOE components. However, it is not part of the evaluated configuration.

[DB-4] The evaluated configuration of the TOE shall therefore comprise exactly the following software components:

- Oracle8 Enterprise Edition 8.0.5.0.0
- Oracle8 Objects Option 8.0.5.0.0[2]
- Oracle8 Utilities 8.0.5.0.0
- Oracle Installer 3.3.0.1.3
- Net8 Client 8.0.5.0.0
- Net8 Server 8.0.5.0.0
- Oracle Named Pipes Protocol Adapter 8.0.5.0.0
- Oracle TCP/IP Protocol Adapter 8.0.5.0.0
- Required Support Files 8.0.5.0.0
- Oracle Call Interface 8.0.5.0.0

4.2 O-RDBMS Server

4.2.1 Identification and Authentication

In the evaluated configuration, the TOE supports Identification.

[DB.IA-1] The TOE shall be configured to use O-RDBMS identification and operating system authentication for all users connecting to the TOE.

[DB.IA-2] Administrators that create normal users within the O-RDBMS shall create appropriately privileged accounts for those users in the operating system as well. See [EC, OS.IA-5] and [EC, OS.IA-8] for details.

[DB.IA-3] Direct connections to the `SYS` account such as `SYS/<password>` shall not be permitted. Database administrators shall set the `ORACLE_HOME\INIT<`*`SID`*`>.ORA` parameter as follows:

2. Optional component.

```
o7_dictionary_accessibility = FALSE
```

Disabling the SYS account provides additional accountability of the user trying to connect as SYS by ensuring that only those operating system users who are included in the local operating system DBA group can connect to the O-RDBMS as SYS. See section 4.2.1, [DB.IA-10] for details.

[DB.IA-4] After creating and setting up a database, all database user accounts must be configured to use DBMS Identification and OS Authentication. This includes any pre-defined accounts (such as SYS and SYSTEM) and any demonstration accounts (such as SCOTT) created during installation.

[DB.IA-5] deleted.

[DB.IA-6] deleted.

[DB.IA-7] The following parameter shall be set in each O-RDBMS parameter file, `INIT<SID>.ORA` located in each `ORACLE_HOME\DATABASE` directory, for each of the O-RDBMS instances:

```
sql92_security = TRUE
```

[DB.IA-8] To additionally permit operating system authentication of all users in each of the O-RDBMS instances, the following `INIT<SID>.ORA` configuration file parameters shall be set:

```
remote_os_authent = TRUE
os_authent_prefix = ""
```

[DB.IA-9] The TOE shall support both privileged and non-privileged database users.

[DB.IA-10] Only connections made to the O-RDBMS as `CONNECT /` shall be supported for normal (non-privileged) database users.

[DB.IA-11] Normal database users may belong to one or more of the following operating system local groups.

```
ora_user
ora_<sid>_user
```

This step is discretionary, it may help distinguish database users from other users in the NT User Manager, however it is not necessary for users to belong to this user group in order to connect to the database.

[DB.IA-12] Only connections made to the O-RDBMS using `CONNECT / AS SYSDBA` and/or `CONNECT / AS SYSOPER` shall be supported and treated as privileged connections for privileged database users.

[DB.IA-13] Privileged connections to the O-RDBMS as defined in DB.IA-12 shall be only made using Oracle Server Manager (in Line Mode)[3].

[DB.IA-14] To connect to the O-RDBMS as a privileged database user such as a database administrator, the following parameter shall be set in the appropriate `INIT<SID>.ORA` file:

```
remote_login_passwordfile = NONE
```

3. Server manager has two operational modes, line mode and screen mode. Line mode is the only mode supported in the evaluated configuration, however it is also the only mode available in the NT port of Server Manager [STARTED, 3-10].

Allowing only one type of privileged connection for privileged database users further enhances the accountability of users trying to connect as database administrators. See section 4.3, [DB.NS-6] for an additional parameter required to be initialized to permit such connections.

[DB.IA-15] Database administrators who are required to use the `CONNECT / AS SYSOPER` syntax to connect to an O-RDBMS shall belong to one or more of the following operating system local groups:

`ora_oper`

`ora_<sid>_oper`

[DB.IA-16] Database administrators who are required to use the `CONNECT / AS SYSDBA` syntax to connect to an O-RDBMS shall belong to one or more of the following operating system local groups:

`ora_dba`

`ora_<sid>_dba`

An O-RDBMS privileged user who belongs to an operating system local group (on that host machine itself) having a particular O-RDBMS *<SID>* as defined above, can connect as a privileged user only to that database. When the *<SID>* is not specified for a particular operating system local group, then a user belonging to such a local group can connect as a privileged user to all instances of the O-RDBMS.

[DB.IA-17] The operating system administrator shall delete the O-RDBMS password file, `PWD<SID>.ORA` which is located in the local `ORACLE_HOME\DATABASE` directory.

4.2.2 Accounting and Auditing

The TOE supports and implements Accounting and Auditing.

[DB.AA-1] The TOE can record all auditing or accounting information for all database users and operations except for a few privileged operations by database administrators.

Privileged operations such as O-RDBMS startup and shutdown, and privileged connections such as `AS SYSDBA`, and `AS SYSOPER` are always audited and recorded directly in the operating system audit trail.

[DB.AA-2] In the evaluated configuration for a specific O-RDBMS, the `audit_trail` parameter in the appropriate `INIT<SID>.ORA` parameter file for that O-RDBMS shall be assigned in one of the following two ways:

```
audit_trail = OS
```

```
audit_trail = DB
```

[DB.AA-3] The `audit_trail` parameter should be set to `OS` to ensure that the TOE audit records are recorded only in the operating system audit trail.

[DB.AA-4] The `audit_trail` parameter should be set to `DB` to ensure that the TOE audit records are written to the database audit trail.

The database audit trail is a `SYS`-owned table, `SYS.AUD$`. Only users connected as `AS SYSDBA` can directly read and write all rows in `SYS.AUD$`.

[DB.AA-5] Database administrators shall create database audit trail views for all other appropriately privileged O-RDBMS users to be able to read and analyse database audit trail

data.

Pre-defined database audit trail views are automatically created during the installation and creation of the database.

Only highly trusted users shall have the privilege which allows them to:

- set or alter the audit trail configuration for the database;
- alter or delete any audit record in the database audit trail.

[DB.AA-6] Database administrators shall perform regular archiving of database and operating system audit trails before audit trail exhaustion to ensure sufficient free space for continued auditing operations. See section 3.1.3 for details.

4.2.3 Availability and Reliability

In the evaluated configuration, the TOE supports and implements Availability and Reliability.

[DB.AR-1] Only privileged O-RDBMS users such as database administrators shall be permitted to perform privileged O-RDBMS operations such as backup and recovery, and enforce tablespace quotas and resource profiles.

[DB.AR-2] [DB.AR-1] should be accomplished by ensuring that only privileged O-RDBMS users have the necessary administrative system privileges to perform these types of operations.

[DB.AR-3] Administrative system privileges shall not be granted to normal O-RDBMS users directly or through the use of database roles. See section 4.2.5 for details.

For example, a normal O-RDBMS user must not be granted the `ALTER PROFILE` system privilege either directly or through a database role.

[DB.AR-4] Each user of the TOE is configured with appropriate tablespace quotas that are

- sufficiently permissive to allow the user to perform the operations for which the user has access rights;
- sufficiently restrictive that the user cannot abuse the access rights and thereby waste or monopolise resources.

4.2.4 Access Controls

In the evaluated configuration, the TOE supports and implements Access Controls. The O-RDBMS implements Discretionary Access Controls to implement access controls.

[DB.AC-1] Normal O-RDBMS users shall have access to only those database objects which they own (ownership of an object being defined as storage of that object within a user's schema).

[DB.AC-2] Normal O-RDBMS users shall only have access to database objects they do not own if they possess appropriate privileges to access database objects in other O-RDBMS user schemas.

[DB.AC-3] Privileged users such as database administrators (connecting AS SYSDBA) shall have access to all database objects in any user schema.

[DB.AC-4] Objects in the SYS schema shall not be accessible to normal O-RDBMS users even if these users possess system privileges. See section 4.2.5 for details.

Only privileged database users connected AS SYSDBA will have access to objects in the SYS schema. Normal O-RDBMS user will be able to access an object in the SYS schema only if they have been granted the explicit object privilege.

[DB.AC-5] If the UTL_FILE PL/SQL package is used to provide database access to host OS files the configuration parameter UTL_FILE_DIR must not be set to "*", but to explicit values so as to protect against overriding the operating system DAC mechanisms.

[DB.AC-6] Each database link must be defined such that users who refer to the link are connected to an identically named normal user account in the secondary or remote database, that is the database link must be defined without reference to a single normal user account to which all users referencing the link would otherwise be connected.

[DB.AC-7] The EXECUTE privilege on the DBMS_JOB PL./SQL package is granted to PUBLIC by default. This should be revoked by executing the following SQL statement from an administrative connection to the database:

```
REVOKE EXECUTE ON DBMS_JOB FROM PUBLIC;
```

4.2.5 Security Administration and Management

In the evaluated configuration, the TOE supports and implements Security Administration and Management by the use of over ninety distinct and separately managed object and system privileges.

System privileges which are administrative in nature such as those which allow database-wide object, role, user, privilege, and profile manipulation should generally not be granted to normal O-RDBMS users either directly or through database roles.

[DB.SAM-1] Only highly trusted O-RDBMS users and database administrators should be allowed to posses system privileges which are administrative in nature.

An example of such a privilege is the ALTER PROFILE system privilege which can be used to alter any user profile in the O-RDBMS.

Object privileges and other system privileges (which are non-administrative in nature) are required by normal O-RDBMS users to perform their tasks under the *Principle of Least Privilege.*

[DB.SAM-2] The privileges described in [DB.SAM-1] should be grouped together into database roles and granted to normal O-RDBMS users.

An example of these types of privileges is the CREATE TABLE privilege which by default allows O-RDBMS users to create and modify tables within their own schema, but not in any other user schema.

[DB.SAM-3] The system privileges of SYSDBA and SYSOPER shall not be granted to any normal O-RDBMS user, including the user SYSTEM.

Database administrators are externally authenticated by the operating system, and thereby possess these system privileges by virtue of being in the local operating system DBA groups. Normal O-RDBMS users are also externally identified, and thus can only connect to the TOE as DBA or OPER users if they are individually identified in the local operating system DBA groups.

[DB.SAM-4] The absence of the O-RDBMS password file (see section 4.2.1, [DB.IA-11] for details) shall prevent a grant of either the SYSDBA or SYSOPER system privilege to O-RDBMS authenticated users.

[DB.SAM-5] The `CREATE LIBRARY` and `CREATE ANY LIBRARY` system privileges shall not be granted to any user of the TOE.

This restriction is imposed so as to prevent the use of libraries which would enable callouts to external C programs which could be misused against the TOE's security features.

[DB-SAM-6] The `CREATE SNAPSHOT`, `CREATE MATERIALIZED VIEW`, `CREATE ANY SNAPSHOT`, `CREATE ANY MATERIALIZED VIEW`, `ALTER ANY SNAPSHOT` or `ALTER ANY MATERIALIZED VIEW` privileges shall only be assigned to trusted (e.g. DBA) users.

4.2.6 Secure Data Exchange

In the evaluated configuration, the TOE supports and implements Secure Data Exchange.

[DB.SDE-1] Database administrators shall ensure that any system privilege (directly or through the use of roles) required to implement database import and export be only granted to O-RDBMS users who are trusted to perform these operations, and who normally do not have the appropriate privileges for read and write access to such data.

4.2.7 Secure Distributed Processing and Databases

In the evaluated configuration, the TOE supports and implements Secure Distributed Processing and Distributed Databases.

The TOE can be operated in standalone, client/server and server/server configurations. Database links may be used to connect between different O-RDBMS servers over a network. The TOE provides site autonomy which implies that each server participating in a distributed environment is administered independently from other servers in the distributed system.

[DB.SDD-1] Database administrators should implement a site-specific security policy as per their security requirements.

4.3 Oracle Network Services

[DB.NS-1] The network services that shall be installed using the Oracle Installer Release 3.3.0.1.3 and by using the Custom Installation option are:

- Net8 Client 8.0.5.0.0
- Net8 Server 8.0.5.0.0

In addition to these network services, the following service is also automatically installed:

- Oracle Net8 Assistant 8.0.5.0.0

[DB.NS-2] The installed network services shall be configured in the manner described in the [NP-IUG].

[DB.NS-3] Only users in the operating system `ADMINISTRATORS` group or the database administrator shall be able to modify the installed network services configuration parameters.

[DB.NS-4] No other user should be permitted to modify any network services configuration parameter in the O-RDBMS network configuration files such as `TNSNAMES.ORA`,

LISTENER.ORA and SQLNET.ORA.

[DB.NS-5] The network services configuration files specified in [DB.NS-4] are generally located in ORACLE_HOME\NET80\ADMIN. Permissions on this directory should be set to FULL CONTROL for users in the operating system ADMINISTRATORS group, and READ ACCESS to all other operating system users.

[DB.NS-6] The ORACLE_HOME\NET80\ADMIN\SQLNET.ORA parameter required to support operating system authentication of privileged database users shall be set as follows:

```
sqlnet.authentication_services = (NTS)
```

[DB.NS-7] The parameters in the network configuration files specified in [DB.NS-4] shall use a consistent O-RDBMS naming convention, this helps ensure database uniqueness throughout the domain.

4.4 Oracle Client Applications

[DB.CA-1] The only client application that shall be installed using the Oracle Installer Release 3.3.0.1.3 and by using the Custom Installation option is:

- SQL*Plus 8.0.5.0.0
- Oracle Call Interface 8.0.5.0.0

Note that only the “thick client” JDBC drivers are to be installed. Thin client drivers are not supported in the evaluated configuration.

[DB.CA-2] No database applications except those based on OCI (e.g. SQL*Plus Release 8.0.5.0.0, JDBC thick client) shall be permitted to run on any client or server host machines which access the network, unless they have been shown not to compromise the TOE’s security objectives as stated in the [G.DBMS PP] and the [ST] (see [OS.CA-1]).

CHAPTER

5 Step by Step Guide

This chapter contains a step by step guide to installing the TOE in its evaluated configuration.

Readers unfamiliar with Oracle products should read this section in conjunction with [STARTED]. Note that in some cases changes are not effective until the database is restarted or for membership of an NT user group, until the user has logged out and back in again.

5.1 Server Installation

5.1.1 Software Installation

5.1.1.1 Installation of Windows NT 4.0

Ensure that the intended physical environment is in accordance with the assumptions [A-1] to [A-6] listed in section 2.1 of this document.

Install the base OS in accordance with [NTINST], note that Service pack 3 and the gina hot fix are mandatory in the NT 4.0 evaluated configuration and should be obtained and installed as described in [NTINST]. The Y2K and Euro hot fixes are *not* mandatory and may be installed at the discretion of the user. Service Packs later that SP3 are not covered under the ITSEC evaluation of NT 4 and are therefore not supported in a strict evaluated configuration.

Installation in accordance with [NTINST] satisfies requirements [OS-1] to [OS-5] listed in section 3.1. In addition this also satisfies requirements [OS.IA-1] to [OS.IA-9] as listed in section 3.1.1, [OS.PR-3] and [OS.PR-4] of section 3.1.2, [OS.AA-1] to [OS.AA-4] of section 3.1.3, [OS.NS-1] to [OS.NS-5] of section 3.2 and [OS.CA-1] of section 3.3.

5.1.1.2 Installation of the database

Install the database using the Oracle installer in accordance with steps [DB-1] to [DB-4] of section 4 and section 4.1. Network services are installed in accordance with [DB.NS-1] and [DB.NS-2] of section 4.3.

5.1.2 Enable OS Authentication

OS authentication is enabled in accordance with [STARTED, 11] as described in the following steps [OS.IA-10], [DB-IA-8] and [DB.NS-6].

In order to make privileged connections to the database users must belong to the OS user groups described in steps [DB.IA-15] and [DB.IA-16].

Note steps [DB.IA-1] and [DB.IA-2] imply that privileged users in the database are also privileged users in the OS (e.g. member of the Administrators group).

The above steps satisfy the following: [DB.IA-9], [DB.IA-10] and [DB.IA-12].

It should be noted that the `OSAUTH_PREFIX_DOMAIN` parameter described in [STARTED, 11], should not be set, since setting this parameter will preclude the use of database links in the evaluated configuration.

5.1.3 Disable the password file

The following steps disable the use of the password file used to authenticate privileged users. Following these steps the *only* users able to connect as administrators will be members of the OS user group ORA_DBA or ORA_*sid*_DBA.

The following steps are required: [OS.IA-11], [OS-IA-12], [DB.IA-14], [DB.IA-17].

5.1.4 Protection of database files

Protect the database files from unauthorised access using steps [OS.PR-1] and [OS.PR-2] of section 3.1.2. Network files shall be protected as described in steps [DB.NS-3] to [DB.NS-5] of section 4.3.

5.1.5 Miscellaneous

The following steps are also required:

[DB.IA-3] - prevents use of the “ordinary” (unprivileged) SYS account.

[DB.IA-7] ensures that DAC is correctly enforced.

[DB.IA-13] ensures that privileged connections to the database are correctly audited.

[DB.AC-7] ensures that only users granted the explicit right to use the DBMS_JOB PL/SQL package are allowed to do so.

5.1.6 Completing Installation

The above steps are necessary for achieving an initial evaluated configuration. The remaining steps in this document (sections 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6, 4.2.7, [DB.NS-7] and [OS.IA-13]) cover the general administration of the TOE in order that the evaluated configuration is maintained.

5.2 Client Installation

Client installation is completed as follows:

- Install the host operating system as described in section 5.1.1.1 above;
- Install the client Oracle software as described in section 4.4 above;
- Configure SQL*Net authentication as laid out in DB-NS-6;
- Configure the network services configuration parameters as described in DB-NS-2 to DB-NS-4;

- Protect the client applications from unauthorised use by setting the access control permissions as described in OS.PR-2.

Note that untrusted users of the TOE are not expected to be Administrators of their local machines in accordance with [NTINST].

This Page Intentionally Blank

APPENDIX

A References

[CC] *Common Criteria for Information Technology Security Evaluation,* Version 2.0 Draft CCIB-97/081R

[G.DBMS PP] *Government Database Management System Protection Profile,* Version 2.0

[ITSEC] *Information Technology Security Evaluation Criteria,* Version 1.2, June 1991, UK IT Security Evaluation and Certification Scheme

[IUG] *Oracle8 Enterprise Edition Installation, Release 8.0.5 for Windows NT,* Oracle Corporation

[NP-IUG] *Oracle Networking Products, Release 8.0 for Windows Platforms,* A53746-1, Oracle Corporation

[ST] *Oracle8 Security Target, Release 8.0.5,* Version 0.8, Oracle Corporation

[TCSEC] *Trusted Computer System Security Evaluation Criteria,* 5200 28-STD, December 1985, US Department of Defense

[STARTED] *Getting Started,* Release 8.0.5 for Windows NT, July 29 1998, Part No. A64416-01, Oracle Corporation.

[NTINST] ITSEC FC2-E3 Installation of Windows NT™ Workstation™ 4.0 and Windows NT™ Server™ 4.0, Version 2.4, June 1999, Microsoft Corporation. Available from: http://www.microsoft.com/security

This Page Intentionally Blank