CSEC
Swedish Certification Body for IT Security

Certification Report - Oracle DataBase 12c Release 1 Enterprise Edition

Issue: 1.0, 2017-apr-03

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a relational database management system (RDBMS), which is accessible directly, or through a front end using Structured Query Language (SQL). The TOE is software only, and is designed to run on top of Oracle Linux 7 and a general purpose computing hardware.

The certified version of the TOE is Oracle Database 12c Release 1 Enterprise Edition, version 12.1.0.2 with Critical Patch Update January 2017.

The evaluation covers the following configurations of the TOE: Standalone, Client-Server, Distributed (with a redundant database instance), and Multi-tier.

The TOE features a number of security features, such as security audit, user data protection, identification and authentication of users, security management, redundant data storage, and TOE access conditions.

The following features are supported by the TOE but has not been evaluated: Kerberos and PKI authentication of users, Real Application Clusters, Oracle Label Security, Database Vault, Multitenant, and external clients.

The TOE claims strict conformance with the Base Protection Profile for Database Management Systems (DBMS PP), version 2.07, 2015-09-09.

The evaluation has been performed by Combitech AB in Sundbyberg, Sweden, partly with the assistance of Electronic Warfare Associates-Canade Ltd. in Ottawa, Canada.

The evaluation was completed on the 13th of March 2017. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT Security Evaluation, version 3.1, release 4. The evaluation was performed at the evaluation assurance level EAL 2, augmented by ALC_FLR.2 Flaw reporting procedures.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

Electronic Warfare Associates-Canada Ltd. operates as a Foreign Location for Combitech AB within the scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 2 + ALC_FLR.2.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Combitech AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.

This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2015009
Name and version of the certified IT product	Oracle Database 12c Release 1Enterprise Edition, version 12.1.0.2 with Critical Patch Update January 2017, Patch 24917069: Combo OJVM PSU 12.1.0.2.170117 and Database PSU 12.1.0.2.170117
Security Target Identification	Oracle Database 12c Enterprise Edition Security Target, Oracle America Inc., 2017-03-06, v 1.2
EAL	EAL 2 + ALC_FLR.2
Sponsor	Oracle America Inc.
Developer	Oracle America Inc.
ITSEF	Combitech AB and EWA-Canada
Common Criteria version	v3.1 release 4
CEM version	v3.1 release 4
QMS version	1.20.2
Recognition Scope	CCRA, SOGIS and EA/MLA
Certification date	2017-04-03

3 Security Policy

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

3.1 Security Audit

Oracle DB 12c R1 supports two auditing mechanisms: traditional auditing and unified auditing. For the purposes of meeting the auditing requirements of the DBMS PP, either method, or a combination of both methods may be used.

The AUDIT statement is used to track the issuance of specific SQL statements, or all SQL statements authorized by a particular system privilege. It may also be used to track operations on a specific schema object. The AUDIT_TRAIL system parameter may be used to determine the format and location of the audit entries. Entries for startup and shutdown events are sent to the operating system for logging.

Audit policies may be created (using the CREATE AUDIT POLICY statement) to determine exactly which events are audited, based on numerous criteria including use of particular roles or privileges. Each record includes the date and time of the event (EVENT_TIMESTAMP), type of event (ACTION_NAME),

3.2 User Data Protection

Database objects are defined as any object in the database that may be manipulated with SQL. This includes, but is not limited to tables, rows, columns, cases, files, and views.

Access may be granted in one of several ways:

a. An object privilege is a system-defined privilege that controls access to a specific object. A database user has access to an object if the user is the owner of the object. In this case, the user has object privileges for the object. Object privileges may be granted to other users, as well. These privileges may be limited to certain operations. For example, the owner may be able to perform any operation (e.g. read, write, etc.), but another user may have read only access to the object;

b. A system privilege may be granted to or revoked from a user by an administrator. These privileges allow users to perform specific database operations. For example, a user with the CREATE TABLE system privilege may create a table within that user’s schema;

c. A role is a collection of privileges and other roles. Some system-defined roles exist, but most are created by administrators to provide the least privilege required to perform the assigned tasks. Roles group together privileges and other roles, which facilitates the granting of multiple privileges and roles to users. Roles may be granted object privileges and system privileges in much the same way that users may be granted these privileges. A user in a role would have the ability to perform actions permitted by the privileges;

d. Users may be granted access to objects based on any attribute. A policy rule must be created to allow this access. For example, in a table of human resources data, a user may be granted access to his or her own information by creating a rule that provides access to a row in a table if the database user account name matches a username field in that row; and

e. An object privilege may grant access to users in the ‘PUBLIC’ role. The PUBLIC role is a special role automatically provided to every database account. By default, it has no privileges assigned to it, but it is granted access to many objects. The PUBLIC role may not be granted or revoked because the user account will always assume this role. Because all database user accounts assume the PUBLIC role, it does not appear in any list of roles.

Once a resource is allocated to a table, row or other database object, the previous content of that resource is no longer available.

3.3 Identification and Authentication

To create a user, the administrator must provide a user account name and a password, and limitations on the resources available to the user. These limitations are in the form of defined tablespace and profile information. The tablespace assignment limits the number of resources available to the user and is measured in bytes. The profile associates the user with session limitations, such as number of concurrent sessions allowed, and password parameters, such as the number of failed login attempts allowed before the account is locked.

Users are granted privileges, such as the right to run a particular type of SQL statement, or the right to access an object that belongs to another user. Roles are created to group together privileges and other roles, making it easier to grant multiple privileges to a new user. A role must first be created by identifying the role, and then adding privileges. Once the role is defined, it may be granted to a user.

In addition to granting object and system privileges to users through roles, these privileges may also be granted to users individually.

Users may be granted access to database objects based on any attribute. When configured, the policy appends a WHERE clause to queries to control access at the row and column level. This could be used to allow users to query a human resources table, but only see their own information, or only certain columns associated with the employees who report to these users. This policy (and therefore, this attribute) is not directly associated with the database user’s account. Please note that these users must also have object or system privileges to access the database objects. Attributes may be used to provide a more fine-grained access control to data within accessible objects.

Oracle DB 12c R1 ensures that users are identified and authenticated prior to being allowed access to database objects or resources. Although several authentication mechanisms are supported, only local username and password authentication is examined for the purposes of this evaluation.

One database user may act with the privileges of another as a proxy user. To enable this, the user must be granted permission to access the database through a proxy. This grant operation may specify which roles (and therefore which privileges) are enabled for this access. In this way, the proxy access may be limited to a specific set of required privileges, rather than all of the primary user’s privileges. This is typically used in cases where the proxy user is an application server or middle tier entity.

When a directly assigned privilege is granted or revoked, this takes effect immediately. This includes granting or revoking object privileges or system privileges, or granting or revoking object or system privileges from a role. When an indirectly assigned privilege is granted or revoked, this is effective at the next login. This includes adding or removing a role from a user account.

3.4 Security Management

An audit policy determines which events are to be audited. The privileges required to specify this policy are only available to authorized administrators.

The access control decision for the Discretionary Access Control Policy is made based on object privileges, system privileges, roles and any attribute. All of these attributes may be managed by authorized administrators. Object privileges and attributes may also be managed by their owners, or users to whom the owner has granted that privilege. In this case, the owner or delegated user is considered to be an authorized administrator of the object or attribute. The default values for these attributes are restrictive. System privileges, object privileges and roles must be specifically granted to users. Attribute values do not permit access until a policy granting that access has been created by an authorized administrator.

Only authorized administrators may revoke system privileges and roles. Revocation of directly assigned system privileges (i.e. system privileges granted directly to a user or a role) takes effect immediately. Revocation of a role from a user account is effective at the next login.

Authorized administrators and object owners may revoke object privileges. The ability to grant and revoke object privileges may also be granted to other users by an authorized administrator, or the object owner.

The TOE is managed by submitting SQL statements to the database using the SQL *Plus command line interface. The commands allow authorized administrators to perform all of the security management functionality required to manage the claimed security features of the TOE including:

a. management of the events to be audited;

b. changes to the system privileges;

c. changes to the object privileges;

d. changes to user accounts (including changes to authentication options) and roles;

e. configuration of Data Guard options in support of the replication requirements;

f. configuration of the maximum number of concurrent sessions for an individual user;

g. configuration of logon triggers to support maintenance of information on successful and unsuccessful login attempts; and

h. configuration of logon triggers to be able to deny logon based on time of day and day of week.

Each database requires at least one user in the database administrator role. (This role is described as ‘authorized administrator’ in the SFRs.) Other administrative roles may be created by authorized administrators with the unique set of system and object privileges required to perform assigned tasks.

Database users make use of the database, but do not typically have administrative system privileges.

3.5 Protection of the TSF

The TOE provides replication of data using the Data Guard feature. Primary database transactions generate redo records. A redo record is made up of a group of change vectors, each of which is a description of a change made to a single block in the database. For example, if a value is changed in a table, a redo record containing change vectors that describe changes to the data segment block for the table, the undo segment data block and the transaction table of the undo segments is generated. Data Guard works by shipping the redo to the replicated database and then applying that redo.

Redo records contain all the information needed to reconstruct changes made to the database. During media recovery, the database will read change vectors in the redo records and apply the changes to the relevant blocks. When configured to use the Synchronous transport method (also called the "zero data loss" method), the commit operation will not be confirmed until it is written to both the local and the remote database. If the connection between the databases is lost, updates to the primary database are halted until the secondary database is reconnected, thereby assuring consistency of the replicated data.

3.6 TOE Access

The TSF may restrict the maximum number of concurrent sessions for a user. This is configured using the SESSIONS_PER_USER option in the resource parameters of a profile assigned to a user. Although the default value is unlimited, in the evaluated configuration, an authorized administrator must select a finite number for this limit.

Upon user login, the date and time of the successful or unsuccessful login attempt is saved in the audit records. The audit records also maintain a count of successive unsuccessful login attempts. In order to maintain the date and time of the last successful login, the last unsuccessful login attempt and the number of unsuccessful attempts since the previous last successful login, and make that data accessible to the user, a logon trigger must be configured. This will set up a table with the required information, and make that table accessible to the user.

The TOE is able to deny session establishment based on user identity by dropping the user account. In order to deny a session based on time of day or day of week, a logon trigger must be configured. This will cause the TOE to check the time of day and day of week before allowing the login to succeed.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes three assumptions on the usage of the TOE.

A.AUTHUSER - Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.

A.MANAGE - The TOE security functionality is managed by one or more competent administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.

A.TRAINEDUSER - Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.

4.2 Environmental Assumptions

The Security Target [ST] makes five assumptions on the operational environment of the TOE.

A.PHYSICAL - It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

A.NO_GENERAL _PURPOSE - There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.

A.PEER_FUNC _&_MGT - All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.

A.SUPPORT - Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.

A.CONNECT - All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

4.3 Clarification of Scope

The Security Target contains six threats, which have been considered during the evaluation.

T.ACCESS_TSFDATA - A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.

T.ACCESS_TSFFUNC - A threat agent may use or manage TSF, bypassing protection mechanisms of the TSF.

T.IA_MASQUERADE - A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.

T.IA_USER - A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public objects without being identified and authenticated.

T.RESIDUAL_DATA - A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.

T.TSF_COMPROMISE - A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.

The Security Target contains three Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.ACCOUNTABILITY - The authorized users of the TOE shall be held accountable for their actions within the TOE.

P.ROLES - Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.

P.USER - Authority shall only be given to users who are trusted to perform the actions correctly.

5 Architectural Information

The TOE Security Functional Interfaces (TSFI) and subsystems that support the TOE Security Functional Requirements (SFRs) are shown in Figure 1.

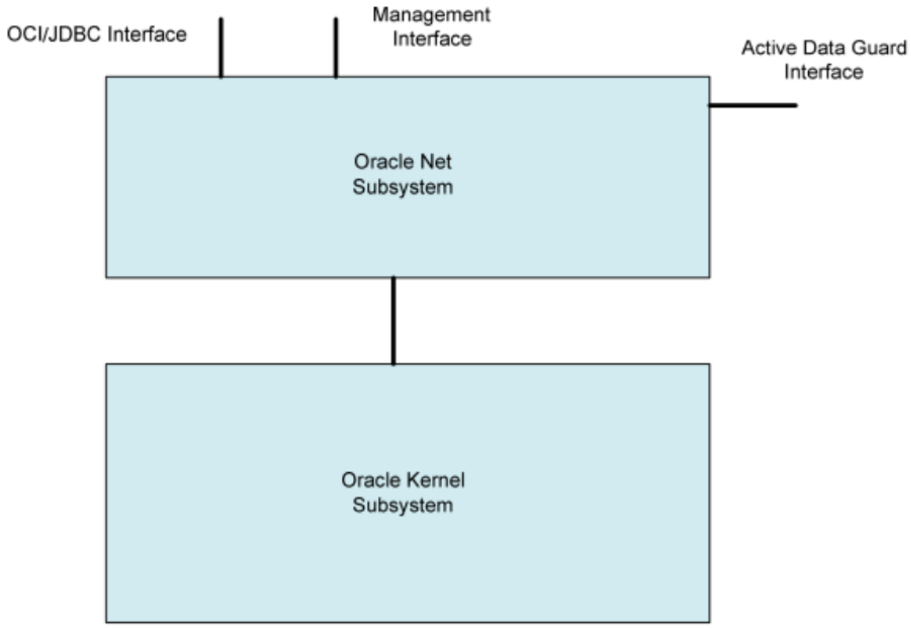

Figure 1, TOE Diagram

The TOE is comprised of the following subsystems:

Oracle Net Subsystem

The Oracle Net Subsystem provides the following services:

- Session establishment
- Communications
- Network management

In order for a client application to be able to communicate with the database server, it must first establish a connection. This is accomplished through the Oracle Net Listener service. The 'listener' process waits for a connection request from a client, and then spawns a server process to handle the client request. The client is then provided with the address, and is able to make direct contact with the new server process.

Oracle Net Subsystem also provides the transport infrastructure for client-server communications, hiding the underlying network protocols from calling applications.

Oracle Kernel Subsystem

The Oracle Kernel Subsystem performs all of the necessary tasks for managing a database. The security enforcing features of the database are enforced within the kernel.

By design, the database server functionality is organized into the following operational layers which combine to make up the Oracle Kernel Subsystem:

a) SQL Layer – This Layer contains the SQL language parser and optimizer, and driving routines for all phases of statement execution;

b) Kompile Layer – This layer is responsible for shared cursors;

c) eXecute Layer – This layer is responsible for executing shared cursors and the triggers associated with these shared cursors;

d) 2-phase commit Layer – This layer handles the two-phase commit protocol necessary for remote updates;

e) Zecurity Layer – This layer provides discretionary access control checking including system and object privileges;

f) Query Layer – This layer provides a cache for objects in the data dictionary;

g) Access Layer – This layer implements the single-table access method by supporting select, insert, update, and delete operations on single tables;

h) Data Layer – This layer handles actual structuring of data as stored on the disk, and implements all row structuring and indexing algorithms;

i) Transaction Layer – This layer is responsible for providing atomic transactions including beginning and aborting transactions, setting savepoints, committing, and locking;

j) Cache Layer – This layer is responsible for all disk input/output, including caching of disk buffers, opening and closing of files, and guaranteeing the preservation of changes made by higher layers;

k) Service Layer – This layer contains low-level services needed to support higher-level functions;

l) Generic Layer – This layer generically names internal objects and handles heap memory allocation;

m) Object Layer – This layer provides the functionality required to support objects; and

n) Operating System Dependent (OSD) Layer – This layer is responsible for interfacing with the host operating system.

6 Documentation

The following documents are included in the scope of the TOE:

CCADM	Oracle® Database 12c Enterprise Edition, Guidance Supplement
INST	Oracle® Database Installation Guide 12c Release 1 (12.1) for Linux
ADM	Oracle® Database Administrator's Guide 12c Release 1 (12.1)
SQL	Oracle® Database SQL Language Reference 12c Release 1 (12.1)
PL/SQL	Oracle® Database PL/SQL Language Reference 12c Release 1 (12.1)
SEC	Oracle® Database Security Guide 12c Release 1 (12.1)
DG	Oracle® Data Guard Concepts and Administration 12c Release 1 (12.1)

7 IT Product Testing

Both developer and evaluator testing was executed on Oracle Database 12c Release 1 Enterprise Edition, version 12.1.0.2, Critical Patch Update October 2016.

The Critical Patch Update January 2017 is an add-on to solve security issues. This Critical Patch Update contains five new security fixes for the Oracle Database Server divided as follows:

- Two new security fixes for the Oracle Database Server. One for the OJVM Create Session, Create Procedure functionality and the other for RDBMS Security local logon functionality.
- Two new security fixes for Oracle Secure Backup.
- One new security fix for Oracle Big Data Graph.

The independent evaluator tests, covering all SFRs, have been rerun on the certified TOE version with the Critical Patch Update January 2017.

7.1 Developer Testing

The developer testing was done using automated test scripts, launched one by one or in test sequences. The testing has a good coverage of the SFRs.

7.2 Evaluator Testing

The evaluator has studied the developer test scripts in detail and repeated a selection of developer tests to gain confidence in the results.

The evaluators also performed independent tests with complete coverage of the SFRs.

7.3 Penetration Testing

The evaluators performed negative testing as part of the independent evaluator testing, and also performed tool based penetration testing in the form of port scans, vulnerability scanning, in particular SQL injection tests, and fuzzing.

8 Evaluated Configuration

The TOE is intended to run on top of Oracle Linux 7, and a non-specific general purpose computing hardware.

The deployment configurations considered in the evaluation are:

- Standalone Database Configuration
- Distributed Database Configuration
- Client Server Database Configuration
- Multi-tier Database Configuration

as defined in the ST.

Installation and configuration of the TOE shall be done in accordance with the guidance documentation, in particular with the Guidance Supplement [CCADM].

Features supported by Oracle DB 12c R1, but that were not included in the evaluated configuration and have not been evaluated:

- Authentication using Kerberos and PKI
- Real Application Clusters
- Oracle Label Security
- Database Vault
- Multitenant
- External clients.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class/Family	*Component*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE Design	ADV_TDS.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Flaw Remediation	ALC_FLR.2	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria for Information Technology Security, a set of three documents describing different aspects of Common Criteria evaluations
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
PP	Protection Profile,
SFR	Security Functional Requirement, a requirement included in the ST, on the TOE
TOE	Target of Evaluation, the (part of a) product that is evaluated
TSF	TOE Security Function(s), the part of TOE that implements security mechanisms, as defined in the ST
RDBMS	Relational Database Management System
SQL	Structured Query Language

12 Bibliography

CC Common Criteria for Information Technology Security Evaluation, CCMB-2012-09-001 through 003, document versions 3.1 revision 4

CEM Common Methodology for Information Technology Security Evaluation, CCMB-2012-09-004, document version 3.1 revision 4

ST Oracle Database 12c Enterprise Edition, Security Target, Oracle, 2017-03-06, document version 1.2, FMV ID 15FMV9479-40

DBMS PP Base Protection Profile for Database Management Systems, version 2.07, 2015-09-09, available at www.commoncriteriaportal.org

CCADM Oracle® Database 12c Enterprise Edition, Guidance Supplement v1.2, 6 March 2017

INST Oracle® Database Installation Guide 12c Release 1 (12.1) for Linux E41491-16, August 2016

ADM Oracle® Database Administrator's Guide 12c Release 1 (12.1) E41484-12, October 2016

SQL Oracle® Database SQL Language Reference 12c Release 1 (12.1) E41329-20, January 2016

PL/SQL Oracle® Database PL/SQL Language Reference 12c Release 1 (12.1) E50727-04, July 2014

SEC Oracle® Database Security Guide 12c Release 1 (12.1) E48135-15, September 2016

DG Oracle® Data Guard Concepts and Administration 12c Release 1 (12.1) E48552-07, November 2015

Appendix A Scheme Versions

A.1 Scheme/Quality Management System

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used:

Version	Introduced	Impact of changes
1.20.2	2017-02-27	*None*
1.20.1	2017-01-12	*None*
1.20	2016-10-20	*None*
1.19.3	Application	Initial version

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system. The changes between consecutive versions are outlined in “Ändringslista QMS 1.20.2”. The certifier concluded that, from QMS 1.19.3 to the current QMS 1.20.2, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target