Swedish Certification Body for IT Security

Certification Report - Oracle Database 12c Release 2

Issue: 1.0, 2018-dec-18

Authorisation: Helén Svensson, Lead Certifier , CSEC

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a relational database management system (RDBMS). The system is built around a relational database framework in which data objects may be directly accessed by users, or an application front end, through 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 2 Enterprise Edition, version 12.2.0.1 with Critical Patch Update October 2018.

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

The following features are supported by the TOE but have not been evaluated: Kerberos and PKI authentication of users, Real Application Clusters (RAC), Oracle Label Security (OLS) and external clients

The TOE for this ST claims demonstrable conformance with the Base Protection Profile for Database Management Systems (DBMS PP) version 2.12, dated March 23, 2017 and with the DBMS PP Extended Package – Access History version 1.02, dated March 23, 2017.

There are eight assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the seven threats and comply with the three organisational security policy (OSP) in the ST. The assumptions, the threat and the OSP are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB and EWA-Canada. The evaluation was completed in 2018-02-06. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. 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 also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA-Canada operates as a Foreign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluators 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 have been reached in agreement with the requirements of the Common Criteria 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	CSEC2017015
Name and version of the certified IT product	Oracle Database 12c Release 2 Enterprise Edition, version 12.2.0.1 with Critical Patch Update October 2018
Security Target Identification	Oracle Database 12c Release 2 Enterprise Edition (with Database Vault and Multitenant) Security Target, Oracle America, Inc., 13 December 2018, v 1.4
EAL	EAL 2+ ALC_FLR.2
Sponsor	Oracle America, Inc.
Developer	Oracle America, Inc.
ITSEF	Combitech AB and EWA-Canada
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.21.5
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2018-12-18

3 Security Policy

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

Below is a summary of the TOE security policy. For detailed information, see [ST] section 7 TOE Summary Specification.

3.1 Security Audit

Audit entries are generated for security related events. Audit policies may be created to generate logs based on details such as the user, the object being accessed, event type or success or failure of the operation.

3.2 User Data Protection

The TOE provides a discretionary access control policy to provide fine-grained access control between users and database objects. The TOE provides a Database Vault access control policy to enforce additional access controls to user data. In a multitenant environment, resources in pluggable databases are logically separate and inaccessible by local users in any other pluggable database or Container Database (CDB). Once data is allocated to a resource, the previous information content is no longer available.

3.3 Identification and Authentication

Users must identify and authenticate prior to gaining TOE access. Attributes are maintained to support the access control policy.

3.4 Security Management

The TOE provides management capabilities via SQL statements. Management functions allow the administrators to:

- configure auditing and access control options (including granting and revoking privileges)
- configure users (including the maximum number of concurrent sessions) and roles
- configure replication options
- configure Database Vault functions
- configure separate domains for pluggable databases within a container database
- assess roles and privileges in use at run-time

Database Vault management capabilities are provided through designated PL/SQL procedures.

3.5 Protection of the TSF

Data may be consistently replicated to a secondary DBMS server.

3.6 TOE Access

The number of concurrent user sessions may be limited by policy. User login may be restricted based on user identity.

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 seven 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.

T.UNAUTHORIZED_ACCESS - A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.

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

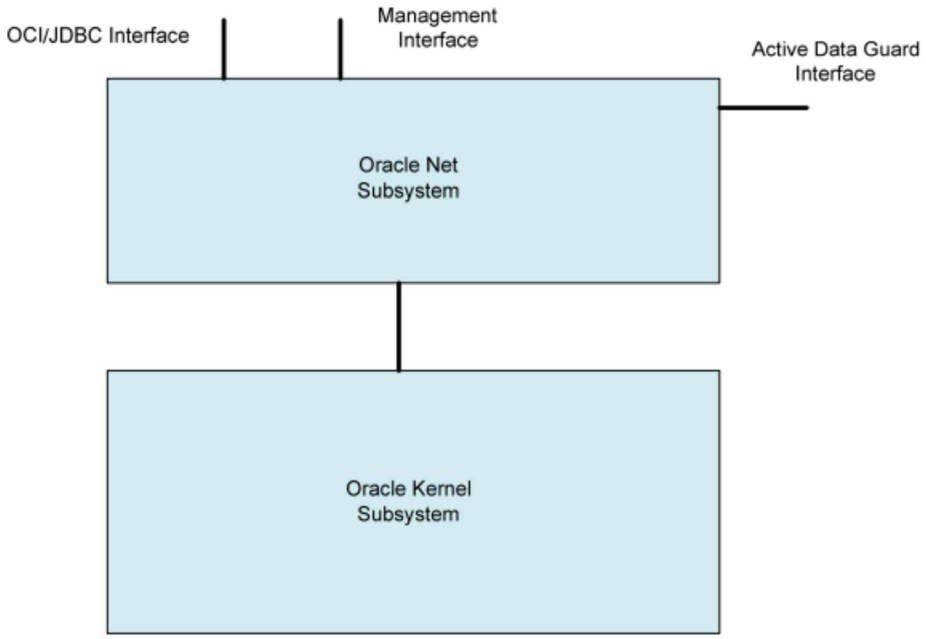

Figure 1, TOE Diagram

The TOE is comprised of the following subsystems:

Oracle Net Subsystem

The Oracle Net Subsystem is an SFR-supporting subsystem. It 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 also provides the transport infrastructure for client-server communications, hiding the underlying network protocols from calling applications.

Oracle Kernel Subsystem

The 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 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 TOE includes the following guidance documentation:

- Oracle Database 12c Release 2 Enterprise Edition (with Database Vault and Multitenant) Common Criteria Guidance Supplement, version 1.3, 6 November 2018
- Oracle® Database Installation Guide 12c Release 2 (12.2) for Linux E85758-02, January 2018
- Oracle® Database Administrator's Guide 12c Release 2 (12.2) E85760-06, March 2018
- Oracle® Database SQL Language Reference 12c Release 2 (12.2) E83703-01, April 2017
- Oracle® Database PL/SQL Language Reference 12c Release 2 (12.2) E85773-02, December 2017
- Oracle® Database Security Guide 12c Release 2 (12.2) E85682-02, December 2017
- Oracle® Data Guard Concepts and Administration 12c Release 2 (12.2) E85767-01, May 2017
- Oracle® Database Vault Administrator’s Guide 12c Release 2 (12.2) E85657-02, March 2018

7 IT Product Testing

Both developer and evaluator testing was executed on Oracle Database 12c R2 (12.2.0.1) Enterprise Edition with Critical Patch Update (CPU) October 2018. The Critical Patch Update October 2018 is an add-on to solve security issues.

7.1 Developer Testing

All developer tests are in the form of scripts to be started manually one by one or automatically in a test sequence. The actual results from each test script are compared with the results from previous, approved, execution of the script. Since neither the scripts test steps nor the expected results are detailed described in the test documentation, the evaluator studied the scripts and their outcome at the developer's site in Redwood Shores, USA, during 21-22 May 2018.

The evaluator examined the test scripts in order to verify that the security functionality claimed to be tested by the developer's test coverage analysis was actually tested.

7.2 Evaluator Testing

The test cases provide coverage for the TOE interfaces and SFRs. Some tools for fuzzing – Burp Suite, port scanning – nmap, and vulnerability scanning – Nessus, were used.

7.3 Penetration Testing

The following types of penetration tests were performed: Port scan, Vulnerability scan including web application vulnerability scan, Web interface fuzzing and SQL injection tests.

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:

- the DBMS server operated with a co-located client;
- the DBMS server operated with a remote client;
- a primary DBMS server and a secondary DBMS server with replicated data; and
- a DBMS server accessed by a thin client through a middle tier application proxy 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 R2, but that were not included in the evaluated configuration and have not been evaluated:

- Authentication using Kerberos and Public Key Infrastructure
- Real Application Clusters (RAC)
- Oracle Label Security (OLS)
- 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 evaluators 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.1	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

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 an evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
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, Part 1-3, CCMB-2017-04-001 through 003, version 3.1, revision 5
CEM	Common Methodology for Information Technology Security Evaluation, CCMB-2017-04-004, version 3.1, revision 5
ST	Oracle Database 12c Release 2 Enterprise Edition (with Database Vault and Multitenant) Security Target, Oracle America, Inc., 13 December 2018, v 1.4
DBMS PP	Base Protection Profile for Database Management Systems (DBMS PP) version 2.12, dated March 23, 2017 and with the DBMS PP Extended Package – Access History version 1.02, dated March 23, 2017
SP-002	Evaluation and Certification, CSEC, 2018-04-24, version 29.0
SP-188	Scheme Crypto Policy, CSEC, 2017-04-04, version 7.0
CCADM	Oracle Database 12c Release 2 Enterprise Edition (with Database Vault and Multitenant) Common Criteria Guidance Supplement, version 1.3, 6 November 2018
INSTALL	Oracle® Database Installation Guide 12c Release 2 (12.2) for Linux E85758-02, January 2018
ADMIN	Oracle® Database Administrator's Guide 12c Release 2 (12.2) E85760-06, March 2018
SQL	Oracle® Database SQL Language Reference 12c Release 2 (12.2) E83703-01, April 2017
PL/SQL	Oracle® Database PL/SQL Language Reference 12c Release 2 (12.2) E85773-02, December 2017
SEC	Oracle® Database Security Guide 12c Release 2 (12.2) E85682-02, December 2017
DG	Oracle® Data Guard Concepts and Administration 12c Release 2 (12.2) E85767-01, May 2017
DV	Oracle® Database Vault Administrator’s Guide 12c Release 2 (12.2) E85657-02, March 2018

Appendix A Scheme Versions

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

A.1 Scheme/Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.21.3 valid from 2018-05-24

QMS 1.21.4 valid from 2018-09-13

QMS 1.21.5 valid from 2018-11-19

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 CSEC QMS 1.21.5". The certifier concluded that, from QMS 1.21.3 to the current QMS 1.21.5, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

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