Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0403-2008

for

Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition and Standard Edition 1

with Critical Patch Update July 2007

from

Oracle Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0403-2008

Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition and Standard Edition 1
with Critical Patch Update July 2007

from	**Oracle Corporation**
PP Conformance:	**U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.1, June 7, 2006**
Functionality:	**PP conformant plus product specific extensions Common Criteria Part 2 extended**
Assurance:	**Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3**

Common Criteria Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using *the Common Methodology for IT Security Evaluation, Version 2.3* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)*.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

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

Bonn, 24th January 2008
For the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

---

1 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretations of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3rd March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

The Common Criteria Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition and Standard Edition 1, with Critical Patch Update July 2007 has undergone the certification procedure at BSI.

The evaluation of the product Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition and Standard Edition 1, with Critical Patch Update July 2007 was conducted by atsec information security GmbH. The evaluation was completed on 22. November 2007. The atsec information

security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is:

Oracle Corporation
520 Oracle Parkway, Thames Valley Park
Reading, Berkshire, RG6 1RA,
United Kingdom .

The product was developed by:

Oracle Corporation.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The following Certification Results contain pages B-1 to B-17.

---

[6] Information Technology Security Evaluation Facility

The product Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition and Standard Edition 1, with Critical Patch Update July 2007 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Security Evaluations Manager,
Oracle Corporation
520 Oracle Parkway, Thames Valley Park
Reading, Berkshire, RG6 1RA,
UNITED KINGDOM

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The target of evaluation (TOE) is "Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition and Standard Edition 1, with Critical Patch Update July 2007". Oracle Database 10g Release 2 is an object-relational database management system (ORDBMS), providing security functionality for multi-user distributed database environments.

Subject of the certification was the Enterprise Edition, the Standard Edition and the Standard Edition One of the Oracle 10g Release 2 Database. Concerning the functions, the differences between those three products are:

- Standard Edition One does not support Real Application Clusters.
- Standard Edition supports only up to 4 CPUs (including CPUs in a cluster used with Real Application Clusters).
- Enterprise Edition has no limitations on the number of CPUs.
- Standard Edition One supports only up to 400 users.
- Standard Edition supports only up to 1000 users.
- Enterprise Edition has no limitation on the number of users.
- Standard Edition and Standard Edition One support databases up to 500 GB size while Enterprise Edition supports databases up to a size of 8 Exabyte.
- Standard Edition and Standard Edition One do not support fine-grained access control and fine grained auditing
- Standard Edition and Standard Edition One do not support Partitioning.
- Standard Edition and Standard Edition One do not support Enterprise Users

All three product variations are generated from the same code base and provide the same functionality with the differences indicated above and the omission of Real Application Clusters in Standard Edition One. All three product variations are available on all the operating system platforms as listed in the Security Target.

The Security Target [6] is the basis for this certification. It is based on the Protection Profile U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.1, June 7, 2006 [8].

The TOE Security Assurance Requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C or [1], part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5. They are selected from Common

Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-environment of the TOE are also outlined in the Security Target [6], chapter 5.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	Addressed issue
F.IA	Identification and authentication
F.LIM	Resource control for database resources
F.DAC	Discretionary access control
F.APR	Privileges and roles (management)
F.PRI	Effective privileges
F.AUD	Audit and accountablilty
F.CON	Data consistency

Table 1: TOE Security Functions

Please note that those TOE Security Functions are further broken down in the Security Target into sub-functions and that the Standard Edition and the Standard Edition One do not offer sub-functions. For more details please refer to the Security Target [6], chapter 6. There each of the security functions is broken down into smaller units and those units are explained in detail.

The claimed TOE's strength of functions is high (SOF-high) for specific functions as indicated in the Security Target [6], chapter 6 is confirmed. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3 and the Protection Profile [8]. Based on these assets the security environment is defined in terms of assumptions, threats and policies. The security environment is outlined in the Security Target [6], chapter 3.

The TOE configuration that was covered by this certification is defined by the ST and further detailed by the guidance documentation a user has to follow. For further details on this topic please refer to chapter 8 of this report.

The certification results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Oracle Database 10g Release 2 (10.2.0.3)
Enterprise Edition, Standard Edition and Standard Edition 1,
with Critical Patch Update July 2007

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition Standard Edition 1 and the CPUs (Critical Patch Updates) up to and including July 2007	10.2.0.3 with all CPUs up to and including July 2007	Electronically, secured by hashes/message digests.
2	DOC	Evaluated Configuration for Oracle Database 10g Release 2 (10.2.0)	Issue 0.6, November 2007	Electronically via download or by mail[8].

Table 2: Deliverables of the TOE

Since Oracle database patches produced by Oracle as part of their Critical Patch Update process are cumulative, the July 2007 CPU database patches include CPU database patches from all earlier CPUs and security alerts.

In order to verify that the correct delivery items have been received, a customer has to check the message digests related to the specific items.

3 Security Policy

The security policy is expressed by the set of security functionl requirements and implemented by the TOE. It covers the following issues:

Explicit Security Policies:

- Discretionary Access Control Policy

Implicitly modeled Security Policies:

- Quota Policy
- Identification and Authentication Policy
- Auditing Policy
- Security Management Policy

[8] The guidance document can be obtained at http://www.oracle.com/technology/deploy/security/seceval/oracle-common-criteria-evaluated.html or requesting a copy by mailing seceval_us@oracle.com

- Consistency of replicated TSF Data Policy

For details on the SFRs used to implement those policies please refer to the Security Target [6], chapter 5.

4 Assumptions and Clarification of Scope

The assumptions defined in the Security Target and some aspects of threats and organisational security policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: OE.USERS, OE.DIR_CONTROL, OE.COM_PROT and OE.CLIENT_AP. Details can be found in the Security Target [6], chapter 4 or in the Protection Profile the ST is claiming conformance to [8].

5 Architectural Information

General overview of the TOE

Oracle Database 10g Release 2 is an object-relational database management system (ORDBMS), providing advanced security functionality for multi-user distributed database environments.

Oracle Database 10g Release 2 supports both client/server and standalone architectures. In addition, Oracle Database 10g Release 2 supports multi-tier architectures, however in this environment any tier (middle-tier) that communicates directly with the server is actually an Oracle client and any lower tiers are outside of the scope of this ST. In all architectures, the Oracle Database 10g Release 2 Server acts as a data server, providing access to the information stored in a database. Access requests are made via Oracle Database 10g Release 2 interface products that provide connectivity to the database and submit Structured Query Language (SQL) statements to the Oracle Database 10g Release 2 data server.

Each database user establishes a database connection to a database server. If the user is defined as a valid user for the database and has the required privileges, then the server will create a database session for the user. While connected, the user can make requests to the server to read and write information in the database. The server handles each request, performing the read and write accesses to database objects and returning data and results to the user in accordance with the user's privileges to database objects and other constraints configured by a database administrative user.

In a distributed environment, a user may access database objects from multiple databases. After establishing an initial database session on one instance, the user can transparently establish database sessions on other (remote) database instances using database links. A database link identifies a remote database and provides authentication information. By qualifying references to database objects with the name of a database link, a user can access remote database objects. However, each Oracle Database 10g Release 2 database instance is

autonomous with respect to security – a remote server enforces security based on the privileges of the user as defined in that remote database.

The Oracle Database 10g Release 2 server supports the ANSI/ISO SQL standard at the entry level of compliance and provides Oracle-specific SQL language extensions. All operations performed by the Oracle Database 10g Release 2 server are executed in response to an SQL statement that specifies a valid SQL command.

- Data Definition Language (DDL) statements are statements which create, alter, drop, and rename database objects, grant and revoke privileges and roles, configure audit options, add comments to the data dictionary, and obtain statistical information about the database and its use.
- Data Manipulation Language (DML) statements are statements which manipulate the data controlled by database objects in one of four ways: by querying the data held in a database object, by row insertions; by row deletion, by column update. They include the command to lock a database object.
- Transaction Control statements are statements which manage changes made by DML statements and help to ensure the integrity of the database. They include commits and rollbacks for individual transactions, and checkpoints for the database.
- Session Control statements dynamically manage the properties of a user's database session.
- System Control statements dynamically manage the processes and parameters of an Oracle Database 10g Release 2 instance.
- Embedded SQL statements incorporate DDL, DML, and transaction control statements within a procedural language program.

Programming Language/SQL (PL/SQL) is a procedural language supported by Oracle Database 10g Release 2 that provides program flow control statements as well as SQL statements. Program units written in PL/SQL can be stored in a database and executed during the processing of a user's SQL command.

An Oracle database contains the data dictionary and two different types of database objects:

- schema objects that belong to a specific user schema and contain user-defined information; and
- non-schema objects to organise, monitor, and control the database.

The data dictionary is a set of internal Oracle tables that contain all of the information the Oracle database server needs to manage the database. The data dictionary tables are owned by the user SYS and can only be modified by highly privileged users. A set of read-only views is provided to display the contents of the internal tables in a meaningful way and also allow Oracle users to query the data dictionary without the need to access it directly.

All of the information about database objects is stored in the data dictionary and is updated by the SQL DDL commands that create, alter, and drop database objects. Other SQL commands also insert, update, and delete information in the data dictionary in the course of their processing.

A schema is a collection of user-defined database objects that are owned by a single database user. A special schema PUBLIC is provided by Oracle Database 10g Release 2 to contain objects that are to be accessible to all users of the database. Other object types can be created and manipulated with SQL, but are not contained within a schema, such as user definitions for the database.

Oracle Database 10g Release 2 has two kinds of user connection: administrative connection (connecting AS SYSDBA or AS SYSOPER) and normal connection. Users making an administrative connection are authorized to access the database by virtue of having the SYSDBA or SYSOPER system privilege.

Apart from that, database security is managed by privileged users through the maintenance of users, roles, and profiles.

- USERS identify distinct database user names and their authentication method.
- ROLES provide a grouping mechanism for a set of privileges.
- PROFILES provide a set of properties (e.g., resource limits, password management options) that can be assigned to individual users.

The TOE allows users to be managed either locally or centrally within a directory. Users managed within a directory are called enterprise users. Each enterprise user has a unique identity across the enterprise. Users defined locally in the database are called local users. Please note that enterprise user feature is only available in the Enterprise Edition of the TOE.

Single password authentication lets users authenticate to multiple databases with a single global password although each connection requires a unique authentication. A password verifier, which is the hash of the password, is securely stored in the centrally located, LDAP compliant directory. In addition the directory also stores a user's global roles. Please note that the LDAP compliant directory is part of the TOE environment and not of the TOE itself.

Oracle Database 10g Release 2 provides mechanisms to ensure that the consistency and integrity of data held in a database can be maintained. These mechanisms are transactions, concurrency controls, and integrity constraints. Transactions ensure that updates to the database occur in well-defined steps that move the database from one consistent state to another. Transactions and concurrency controls together ensure that multiple users can have shared access to the database with consistent and predictable results: each user sees a consistent state of the database and can make updates without interfering with other users. Integrity constraints ensure that the values of individual data

items are of the defined type and within defined limits, and that defined relationships between database tables are properly maintained.

Real Application Clusters (RAC) comprises several Oracle instances running on multiple clustered computers, which communicate with each other by means of a so-called interconnect. RAC uses cluster software to access a shared database that resides on shared disk. RAC combines the processing power of these multiple interconnected computers to provide system redundancy, near linear scalability, and high availability. Please note that the RAC feature is not available in the Standard Edition One of the TOE.

Security Functions

The security functions that have been evaluated include:

- Identification and authentication

  The TOE provides identification and authentication (by password) of users managed locally in the database. Optionally, Oracle's Enterprise Users feature is supported and the TOE authenticates users based on user attributes managed in an LDAP repository in the environment (only for the Enterprise Edition of the TOE).

- Privileges

  The TOE enforces privileges assigned to individual users, both for requested operations on user data (e.g., access to data stored in tables) as well as TSF data (like management of user security attributes). Privileges can be granted to either individual users or roles that are assigned to users.

- Resource control

  The TOE provides the concept of Resource Profiles, which can be assigned to individual users to specify limitations on resource usage, such as maximum connect times, number of simultaneous sessions, or CPU usage.

- Object re-use

  The TOE provides interference between individual database sessions and ensures that information in memory that was previously allocated to a different session is not made available to the current session.

- Data consistency

  The TOE ensures the consistency of data held in the database and accessed by multiple users. This is also the case for Real Application Clusters (please note that Real Application Clusters are not available in the Standard One Edition of the TOE).

- Auditing

  The TOE is able to generate records of security-relevant events (e.g., attempts to establish a session or access specific data in the database), and provides facilities for the review of audit records stored in the database.

- TSF management

  The TOE provides management functionality for its security functions.

TOE Editions

The TOE comes in three editions: Enterprise Edition (EE), Standard Edition (SE), and Standard Edition One (SE1). The following differences between the editions with respect to security functionality that has been evaluated have to be noted:

- The SE1 does not support Real Application Cluster
- Only the EE supports Fine-grained Access Conrol
- Only the EE supports enterprise users and the authentication with the support of a TOE external LDAP directory

Please refer to the Security Target especially chapter 1 "TOE overview" for more details on the differences between the TOE editions.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

Test configuration

The Security Target defines the following operating system platforms for the TOE:

- Red Hat Enterprise Linux AS (Version 4, Update 2)
- SuSE Linux Enterprise Server 9

The developer has performed his tests on the above listed operating system platforms. The software was installed and configured as defined in [9].

Depth/Coverage of Testing

The developer has done substantial functional testing of all externally visible interfaces (TSFI). The TSF behaviour defined by the High-level design has been entirely covered mostly by indirect testing. The evaluators repeated or witnessed the developer tests (because of the highly automated testing approach of the developer) and conducted additional independent tests and penetrations tests.

Summary of Developer Testing Effort

Test configuration:

The sponsor/developer has performed the tests on the operating system platforms listed above.

The software was installed and configured as required by the Security Target [6] and the document [9] (evaluated configuration guide).

Testing approach:

The sponsor/developer used a mixture of automated and manual tests to verify the expected behaviour of TOE.

Testing results:

All actual test results were consistent with the expected test results.

Summary of Evaluator Testing Effort

The evaluators successfully covered all of the TOE Security Functions except for F.CON.RAC by either evaluator defined tests or a re-run of a selected set of vendor tests.

The evaluators conclude that sufficient functional testing has been achieved on the TOE to give the appropriate level of assurance that the TOE software has no security functionality flaws when running on Red Hat Enterprise Linux AS Version 4 and SuSE Linux Enterprise Server 9 operating systems.

Testing results:

All actual test results were consistent with the expected test results.

Evaluator penetration testing:

The evaluator used a two folded penetration test strategy for the TOE in its evaluated configuration:

- Manual tests, devised from the vendor's vulnerability analysis as well as publicly available sources
- An automated scanner has been used to further asses the TOE and possibly devise further penetration tests depending on the results obtained by the scan

The penetration testing showed no vulnerabilities which are exploitable in the intended operating environment with the attack potential assumed for the chosen EAL.

8 Evaluated Configuration

The TOE subject of this report is Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition, Standard Edition and Standard Edition 1, with Critical Patch Update July 2007. The conditions set by the documents [6] (the Security Target) and [9] (the evaluated configuration guide) have to be met in order to result in an evaluated configuration of the TOE.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components up to EAL4 (including ALC_FLR).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)
- The component
  ALC_FLR.3 – Systematic flaw remediation
  as augmentation of the EAL package of the TOE evaluation.

The evaluation has confirmed:

- for PP Conformance: U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.1, June 7, 2006 [8]
- for the functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the assurance: Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3
- The following TOE Security Functions fulfil the claimed Strength of Function high:
  F.IA.DBA (DBMS Identification and Authentication) supported by the password management functions F.IA.PWD, F.IA.ATT and F.IA.USE (please refer to the Security Target [6], chapter 6 for more details)

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Security Target

For the purpose of publishing, the Security Target [6] of the target of evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-0403, Issue 2.0 Release 11, October 2007, "Security Target for Oracle Database 10g Release 2 (10.2.0)", Oracle Corporation

[7] Evaluation Technical Report BSI-DSZ-CC-0403, Release 2, 2007-11-21, atsec information security GmbH (confidential document)

[8] U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.1, June 7, 2006

[9] Evaluated Configuration for Oracle Database 10g Release 2 (10.2.0), Issue 0.6, November 2007, Oracle Corporation

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result."

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

"The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry."

"Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements "

Security Target criteria overview (Chapter 8.3)

"The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation."

"Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements "

Assurance categorisation (chapter 7.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

"The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

Evaluation assurance level (EAL) overview (chapter 11.1)

"Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary"

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

"Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats."

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

"Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited."

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

"Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

"Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

"Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

"Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

"Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

"Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."