Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0577-2009

for

Oracle Database 11g Enterprise Edition with Oracle Label Security, Release 11.1.0.7 with Critical Patch Updates up to and including July 2009

from

Oracle Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0577-2009

Database

Oracle Database 11g Enterprise Edition with Oracle Label Security,
Release 11.1.0.7 with Critical Patch Updates up to and including July 2009

from	Oracle Corporation
PP Conformance:	U.S. Government Protection Profile Database Management Systems for Basic Robustness Environments, Version 1.2, July 25, 2007
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 Recognition Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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, 16 September 2009

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 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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.

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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

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 Recognition 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 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 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, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition 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 11g Enterprise Edition with Oracle Label Security Release 11.1.0.7 with Critical Patch Updates up to and including July 2009 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0402-2008. Specific results from the evaluation process BSI-DSZ-CC-0402-2008 were re-used.

The evaluation of the product Oracle Database 11g Enterprise Edition with Oracle Label Security, Release 11.1.0.7 with Critical Patch Updates up to and including July 2009 was conducted by atsec information security GmbH. The evaluation was completed on 14 September 2009. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the developer, sponsor and applicant is: Oracle Corporation

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.

[6] Information Technology Security Evaluation Facility

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 as specified in the following report and in the Security Target.

For the meaning of the assurance levels 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 product Oracle Database 11g Enterprise Edition with Oracle Label Security, Release 11.1.0.7 with Critical Patch Updates up to and including July 2009 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de and [5]). 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] Oracle Corporation
500 Oracle Parkway
Redwood Shores,CA
USA

This page is intentionally left blank.

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.

1 Executive Summary

The Target of Evaluation (TOE) is the software application Oracle Database 11g Enterprise Edition with Oracle Label Security, Release 11.1.0.7 with all critical patch updates up to and including July 2009.

Oracle Database 11g is an object-relational database management system (O-RDBMS), providing advanced security functionality for multi-user distributed database environments.

The security functionality in Oracle Database 11g includes:

- user identification and authentication, with password management options and support for enterprise users (password option only). In the case of Enterprise Users this function is partly provided by the IT-environment.
- discretionary access controls on database objects, which controls access to objects based on the identity of the subjects or groups to which the subjects and objects belong, and which allows authorized users to specify how the objects that they control are protected;
- granular privileges for the enforcement of least privilege;
- user-configurable roles for privilege management, including an authorized administration role to allow authorized administrators to configure the policies for discretionary access control, identification and authentication, and auditing;
- quotas on the amount of processing resources a user can consume during a database session;
- audit capture is the function that creates information on all auditable events;
- extensive and flexible auditing options;
- secure access to remote Oracle databases; and
- stored procedures, triggers and security policies for user-defined access controls and auditing.

Additionally, Oracle Label Security (OLS) enables application developers to add label-based access control (LBAC) to their Oracle Database 11g applications. In addition to discretionary access control (DAC) that is provided by Oracle Database 11g, it mediates access to rows in database tables based on a label (or labels) contained in each row, and the labels and privileges associated with each user session. Such labels quantify the sensitivity of data and the clearance of users to access sensitive data.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile U.S. Government Protection Profile Database Management Systems for Basic Robustness Environments, Version 1.2, July 25, 2007 [7].

The TOE Security Assurance Requirements (SAR) 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 EAL4 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and the PP [8], chapter 5. They are selected from Common Criteria Part 2 and some of them are newly defined in the PP [8].) Thus the TOE is CC Part 2 extended.

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 – Database Resources
F.ACCESS	Object Access Control
F.DAC	Discretionary Access Control
F.APR	Granting and Revoking privileges and Roles
F.PRI	Effective Privileges
F.AUD	Audit and Accountability
F.CON	Data Consistency
F.LBAC	Label-based Access Control

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6. Each of the security functions is broken down into smaller units and those units are explained in detail.

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 TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This 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 11g Enterprise Edition with Oracle Label Security, Release 11.1.0.7 with Critical Patch Updates up to and including July 2009

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Oracle Database 11g Release 1 (11.1.0.6.0) Media Pack for Linux x86	11.1.0.6.0	electronic or on physical media
2	SW	11.1.0.7.0 PATCH SET FOR ORACLE DATABASE SERVER	11.1.0.7.0	electronic
3	SW	CPUJUL2009 DATABASE 11.1.0.7	11.1.0.7.0	electronic
4	Guidance	Evaluated Configuration for Oracle Database 11g Release 1 (11.1.0)	11.1.0	electronic
5	Guidance	Oracle Database 11g Release 1 (11.1) Documentation	11.1	electronic

Table 2: Deliverables of the TOE

The TOE is delivered either in electronic form or physically on CD-ROMs.

For electronic delivery of the TOE, deliverable No. 4 provides instructions for verifying SHA-1 checksums provided for the software to the consumer. The availability of this checksum data and the instructions for its use enable customers to verify the integrity of the downloaded TOE. In order to trust the hash sums and the downloaded software packages, trust in the web server must be established by verifying the server's SSL server certificate. For electronic delivery of the TOE guidance, there is an available option for consumers to verify with the developer via email that they received the correct guidance documents.

For the delivery of physical media to consumers, the following measures contribute to integrity and authenticity of the TOE:

- original Oracle graphics and logos on packaging material, boxes, and CD-ROMs;
- sealed CD-ROM envelopes; invoice, reference, and tracking numbers for the shipment are communicated to the consumer;
- the product is shipped by trusted carriers.

The consumer can issue the command “opatch lsinventory -detail” in order to verify the release and patch sets installed on a system. Deliverable No. 4 provides details about the patches that need to be installed for the evaluated configuration.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Discretionary Access Control Policy
- Label-based Access Policy
- Quota Policy
- Identification and Authentication Policy
- Auditing Policy
- Security Management Policy
- 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

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.

In an Oracle database there are two types of connections for users of the database:

- Administrator connection. This covers users who connect to the database via AS SYSOPER or AS SYSDBA by virtue of possessing either the SYSOPER or SYSDBA system privilege. Users making a connection AS SYSOPER are allowed to perform operator administrative tasks (e.g. database startup and shutdown, and ALTER DATABASE commands). Users making a connection AS SYSDBA are allowed to perform all administrative tasks (including granting and/or revoking object privileges on other users' objects);
- Normal connection (note that this includes users SYS and SYSTEM). This covers users who are authorised to access the database by virtue of being explicitly defined and identified to an instance of the Oracle database server.

5.1 Data Dictionary and Database

At the centre of an Oracle database is the data dictionary - 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. Technically, a set of server processes (a so-called instance) operates on a database, i.e., the files which contain the data. Users employ interface products to establish database connections with a database instance, and to query the database using the Structured Query Language (SQL) and Oracle-specific extensions of it.

5.2 Distributed Databases

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.

5.3 Enterprise Users

The TOE supports Enterprise Users. If configured, users are authenticated against a centrally managed directory in the TOE environment, rather than against the TOE's local database.

5.4 Partitioning

The TOE supports Partitioning, which addresses key issues in supporting very large tables and indexes by letting you decompose them into smaller and more manageable pieces called partitions. SQL queries and DML statements do not need to be modified in order to access partitioned tables. However, after partitions are defined, DDL statements can access and manipulate individual partitions rather than entire tables or indexes.

5.5 Real Application Clusters

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.

5.6 Oracle Label Security

OLS provides label-based access control, which mediates access to data at a row level. Each data row is given one or more labels, each of which is used to store information about data sensitivity.

To be allowed access to a row, a user must satisfy both OLS label-based access control (LBAC) and Oracle Database 11g DAC requirements which are based on the user's system-level privileges and database object privileges.Thus, to gain access to a row, a user must first be authenticated to the Oracle database. Second, the user must have the DAC object and system privileges required for the operation. Finally, the user must meet the criteria enforced by LBAC, which are based on the labels of the user and the data row.

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

7.1 Test configuration

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

- Red Hat Enterprise Linux AS (version 5) (RHEL)
- SuSE Linux Enterprise Server 10 SP1 (SLES10)
- Oracle Enterprise Linux Version 4 Update 5 (OEL)

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

7.2 Developer Testing

Developer testing provided coverage for all TSFs and all TSF related subsystems. The evaluator was satisfied with the results witnessed for both the automated tests and manual tests and confirmed all tests passed successfully.

7.3 Evaluator Testing Effort

The evaluator followed a threefold, non-symmetric approach to test the TOE. The following test configurations were used:

The evaluator test environment set up in Munich. The evaluator's test environment set up in the Munich lab consisted of a OEL, RHEL and SLES10 installation of the TOE in a Non-RAC configuration.

Furthermore, the evaluator witnessed a controlled run of the vendor's test suites.

A RAC cluster running on Linux has been set up by the evaluator at the developer's site in Reading, UK. The evaluator used this configuration to directly assess the provided installation guidance for RAC clusters as well as to perform some RAC related tests. The RAC results, although run against a pre-TOE patchlevel are considered to be valid because, after examination of the details of all applied changes, the evaluator determined that they did not have any impact on RAC-functionality.

In summary, the evaluator successfully covered all of the TOE Security Functions 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 5, Oracle Enterprise Linux Version 4 Update 5 and SuSE Linux Enterprise Server 10 SP1 operating systems.

7.4 Evaluator Penetration Testing

The evaluator used the information on potential vulnerabilities collected by the evaluator during the evaluation that should be considered in the vulnerability analysis.

In addition, the evaluator took into account the ST, guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE.

As result of these activities, the evaluator defined a penetration test framework and produced penetration tests to verify the vulnerabilities. None of the penetration test were successful.

In addition, the evaluator used a commercial scanner to scan the TOE for known vulnerabilities. No applicable vulnerabilities were deteced.

The penetration was carried out using the external interfaces of the TOE, namely the OCI interface stack as well as the "sqlplus" command interface. The subsystems subject to penetration testing were all parts of the TOE.

In summary, no exploitable vulnerabilities were identified.

8 Evaluated Configuration

The TOE subject of this report is Oracle Database 11g Enterprise Edition with Oracle Label Security, Release 11.1.0.7 with all critical patch updates up to and including July 2009. 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.

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

- All components of the EAL4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3 - Systematic flaw remediation augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0402-2008, re-use of specific evaluation

tasks was possible. The focus of this re-evaluation was on the integration of new and modified features from the previously evaluated version of the Oracle database.

The evaluation has confirmed:

- PP Conformance: U.S. Government Protection Profile Database Management Systems for Basic Robustness Environments, Version 1.2, July 25, 2007 [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 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

BSIG BSI-Errichtungsgesetz

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

EAL Evaluation Assurance Level

IT Information Technology

ITSEC Information Technology Security Evaluation Criteria

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SAR Security Assurance Requirement

SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

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

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certifcates (BSI 7148, BSI 7149), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-0577, Version 5.0, September 2009, OLS Security Target for Oracle Database 11g Release 1 (11.1.0), Oracle Corporation

[7] Evaluation Technical Report BSI-DSZ-CC-0577, Version 2, 2009-09-11, atsec information security GmbH (confidential document)

[8] U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, July 25, 2007

[9] OLS Evaluated Configuration for Oracle Database 11g Release 1 (11.1.0), July 2009, Oracle Corporation

[10] Configuration list for the TOE, July 28, 2009 (confidential document)

[11] Oracle Database 11g Release 1 (11.1) Documentation, Version 11.1, Documentation part number B28359-01

[8] specifically

- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex A.

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
	level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“ 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 8.1)

“Table 1 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 CC 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.