Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0621-2010

for

Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)

from

Oracle Corporation

BSI - Federal Office for Information Security, 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-0621-2010

Enterprise Management Software

Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)

from	Oracle Corporation
PP Conformance:	None
Functionality:	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, 27 August 2010

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Irmela Ruhrmann
Head of Division

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

This page is intentionally left blank.

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 (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

---

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

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC – Certificates (CCRA)

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 Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) has undergone the certification procedure at BSI. Specific results from the evaluation process BSI-DSZ-CC-0577-2009 were re-used.

The evaluation of the product Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) was conducted by atsec Information Security GmbH. The evaluation was completed on 24 August 2010. 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

The product was developed by: Oracle Corporation

[6] Information Technology Security Evaluation Facility

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 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 evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

5 Publication

The product Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://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 94065, 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 enterprise management software solution Oracle Enterprise Manager Grid Control 10g Release 5 (10.2.0.5), or EMGC for short. It provides access to network management functions to administrators through either web-based or command-line interfaces. EMGC comprises an Oracle Management Server (OMS) providing interfaces to the EMGC to users for managing remote hosts and applications (targets) as well as viewing system measurements including diagnose performance and health issues of the target systems. In the evaluated configuration only an Oracle Database as application on a target host can be managed. Oracle Enterprise Manager Grid Control is a distributed software application including a centralized, integrated framework for managing other products in an enterprise grid. Management functionality includes performing software installation, patching, upgrading, workload balancing on the products that EMGC manages.

The Oracle Management Server component of the TOE requires installation of an appropriate Oracle Application Server and an Oracle Database available for storing data. More details on the definition of the runtime environment of the TOE are given in Security Target [6].

Security functionality provided by the TOE includes

- authentication of users using the OMS-provided GUI and CLI to administrate remote targets,
- enforcement of access control granting users certain privileges to access managed objects,
- secure communications between the OMS and the agents,
- management of security compliance of managed targets,
- management of the TOE's security functions and
- auditing of security-relevant events.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

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 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 6. They are selected from Common Criteria Part 2 and one of them is newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Function	Addressed issue
SF 1	Identification and authentication The TOE enforces authentication decisions made by the OM repository in the IT environment on users accessing the TOE via the OMS-provided GUI or CLI interface. In

TOE Security Function	Addressed issue
	addition, the TOE maintains security attributes (ID, role, privileges) of its users. Additional forms of authentication performed by the TOE involve the use of SSL certificates, agent registration passwords, and agent keys. Agent registration passwords and agent keys are used during the registration phase of a new agent. Upon a successful registration, the OMS generates SSL certificates to be used by an agent for further communication with the OMS. In addition, the TOE performs termination of an interactive session after a period of user inactivity defined by the administrator.
SF 2	Privilege-based access control The TOE enforces a privilege-based access control policy for administrators using the TOE interfaces to manage targets. Roles allow to group privileges and to grant these to individual users or other roles. Privileges give the user or members of specific roles rights to perform certain management actions within EMGC. Together privileges and roles control the targets a user can manage and the specific types of tasks the user can perform.
SF 3	Auditing The TSF implements generation of audit records of security-relevant activities. The auditing functionality covers the following types of events: ● authentication attempts ● logon / logoff ● user management ● security attribute management ● job management ● file transfer ● remote operations Audit records contain the following information: ● type of event ● date and time of the event ● user identity (if applicable) ● outcome of the event (success/failure) ● name and IP address of the user's host system
SF 4	Protected data transfer The TOE implements SSL v3[12] on target hosts[8] to secure communication between the OMS host and agents against eavesdropping and unauthorized modification of TSF data and user data.
SF 5	Compliance management The TOE performs comparison between configurations of managed targets and configurations defined by administrators (baseline configurations/policies). Additionally, the TOE can generate reports on and notify administrators of any violations of compliance policies resulting from the performed comparison. Examples of violations include inappropriate settings and incorrect system configurations.
SF 6	Security management

[8] On the OMS-side the SSL-functionality is provided by the underlying Oracle Application Server.

TOE Security Function	Addressed issue
	The TOE offers administrative interfaces such as OMS-provided GUI and CLI to manage the TOE security functions like: ● Management of security attributes used for the enforcement of the Privilege-Based Access Control policy. ● Management of TSF data including the restriction to query, modify or delete the definition of target configuration baselines. ● Management functions including audit management, security attribute management, baseline configuration management, and credential management of target objects. ● Management of SSL certificates. ● Management of security roles.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. Based on these assets the TOE Security Environment is defined in terms of Assumptions and Threats. This is outlined in the Security Target [6], chapter 3.

This certification of the TOE consists of Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5). For details refer to chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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 Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1.	SW	Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)	10.2.0.5	DVD or SSL-secured download
2.	SW	Oracle Patch 8814764		SSL-secured download
3.	SW	Oracle Patch 8968670		SSL-secured download
4.	SW	Oracle Patch 9019231		SSL-secured download

No	Type	Identifier	Release	Form of Delivery
5.	SW	Oracle Enterprise Manager Agent for each of the supported target host platforms as described in chapter 8.	10.2.0.5	SSL-secured download
6.	DOC	Evaluated Configuration for Oracle Enterprise Manager 10g Grid Control Release 5	10.2.0.5 (Version 2.1)	Download or provision via email
7.	DOC	Oracle Enterprise Manager Grid Control Online Documentation Library 10g Release 5	10.2.0.5	Download or provision via email

Table 2: Deliverables of the TOE

The following table contains, for item 6 and for each of the relevant guidance documents included in item 7 of table 2 above, a SHA-1 checksum in order to enable customers to verify the correctness of the guidance documents obtained.

No	Title	Version / Date	SHA-1 value
1.	Evaluated Configuration for Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)	Version 2.1, August 2010	ea78ef09a844ded0288cd4bdd655113b7ce53c1d
2.	Command Line Interface 10g Release 5 (10.2.0.5)	B40004-06, August 2009	d6cb17eb424e21e8808cb9542c49e29870333b2e
3.	Advanced Configuration 10g Release 5 (10.2.0.5)	E10954-03, June 2009	e8e84e529e81179ebb99529adf85a3afd0db7441
4.	Grid Control Installation and Configuration Guide 10g Release 5 (10.2.0.5.0)	E10953-10, August 2009	e2fd582015d14a26408e76ae47cfe9c8209c7624
5.	Framework, Host, and Services Metric Reference Manual 10g Release 4 (10.2.0.4)	B16230-03, October 2007	d5660671ce93f2c29c31b4a3151dfa9228427506
6.	Grid Control Quick Start Guide 10g Release 2 (10.2)	B28678-03, July 2006	5565785014c9123244c94c8193cc4d3df28bcac9
7.	Policy Reference Manual 10g Release 5 (10.2.0.5)	B16231-02, August 2009	e127986859a89fcd0bfd07a7c70c4a51feea8847
8.	Concepts 10g Release 5 (10.2.0.5)	B31949-10, March 2009	94f7e53ed6a35219ceddd9a7727a4dd9ab492bbc
9.	Administration 10g Release 5 (10.2.0.5)	E14586-02, August 2009	1c4e3f5d52f21546912168df9201f31235dccb73

Table 3: SHA-1 Checksums for Guidance Documents

2.1 Delivery of the TOE

Upon ordering, the product Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) (item no. 1 in Table 2) is shipped to the customer on DVD-media which are packaged in a sealed cardboard box. As an alternative, customers may chose to download the TOE from an Oracle website. After installing the TOE, customers need to apply the patches listed above (items 2, 3, 4 in Table 2). Those need to be downloaded from an Oracle website as well as the guidance documentation for the TOE.

All downloads listed above are secured by HTTPS, i.e. they are SSL-secured. On the Oracle website, SHA-1 and MD5 checksums for each downloadable item are published allowing the customer to verify the integrity of the downloads afterwards.

The URL http://www.oracle.com/technetwork/indexes/documentation/index.html which is available for downloading guidance documentation is not secured by SSL. Customers also may request the documents from the vendor by sending an email to seceval_us@oracle.com as specified at the following adress: http://www.oracle.com/technetwork/topics/security/oracle-common-criteria-095703.html.

To ensure that the correct versions of the relevant guidance documentation are obtained the customers may generate SHA-1 checksums that can be compared against the checksums provided in table 3 above.

2.2 Identification of the TOE

Customers can verify the correct TOE version by issuing commands from the operating system command line available on the OMS host as well as on each of the target hosts having installed management agents. Those commands are:

- For the OMS:

  "emctl status oms" resulting in the output "Oracle Enterprise Manager 10g Release 5 Grid Control".

- For the agents:

  "emctl status agent" resulting in the output "Agent Version: 10.2.0.5.0".

In order to verify that all required patches have been applied, customers need to issue the following command from the OMS host command line:

"opatch lsinventory -oh $OMS_HOME"

or in case of the agent

"opatch lsinventory -oh $AGENT_HOME"

The resulting output contains for each patch the patch number that can be verified against the list of required patches mentioned in items 2, 3, 4 in Table 2.

Customers may verify that correct versions of the relevant guidance documents for the evaluated configuration of the TOE were made available by generating SHA-1 checksums for the documents obtained and comparing them against the respective checksums provided in table 3.

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:

- The TOE must ensure that only authenticated users can gain access to the TOE and that they must be successfully authenticated before performing any TOE security relevant actions.
- The TOE shall enforce a Privilege-Based Access Control policy in order to allow administrators to restrict access to managed objects to authorized users.
- The TOE shall generate audit records for security-relevant actions and make that information available to authorized personnel.
- The TSF with support from the environment must ensure that data transferred between the remote parts of the TOE is protected against disclosure and modification.

- The TOE shall offer a mechanism to detect deviations between configurations of managed targets and administrator-defined baseline configurations and report on any compliance violations.
- The TSF must provide the capability to consistently interpret X.509 certificates (according to specified implementation standards) being shared between the TOE and the trusted underlying operating system of the OMS.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of the Threats 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:

- The runtime environment for the TOE shall implement authentication mechanisms sought by the TOE.
- The runtime environments for the OMS shall supply a reliable time source for the TOE's usage.
- Those responsible for the administration of the TOE are competent and trustworthy individuals.
- No other application is allowed to run on the systems hosting the TOE to prevent unauthorized access to the TOE and the corresponding assets.
- The runtime environment for the TOE shall securely generate, store, and import X.509 certificates to the TOE for secure communication between the OMS and the agent. On the server side mechanisms must be in place to use these certificates for the secure communication with the agents.

Details can be found in the Security Target [6], chapter 4.

5 Architectural Information

Oracle Enterprise Manager Grid Control (EMGC) is an enterprise management software solution that provides network management functions including performance queries and health measurements of managed network systems, configuration of policies, and automation of routine tasks. The TOE is especially capable of managing databases in the network.

Oracle Enterprise Manager Grid Control consists of three major components:

- the Oracle Management Server (OMS),
- remote agents installed on the hosts of managed applications ("targets"), and an
- Oracle Database that serves as a repository for management information.

This is depicted in the following figure.

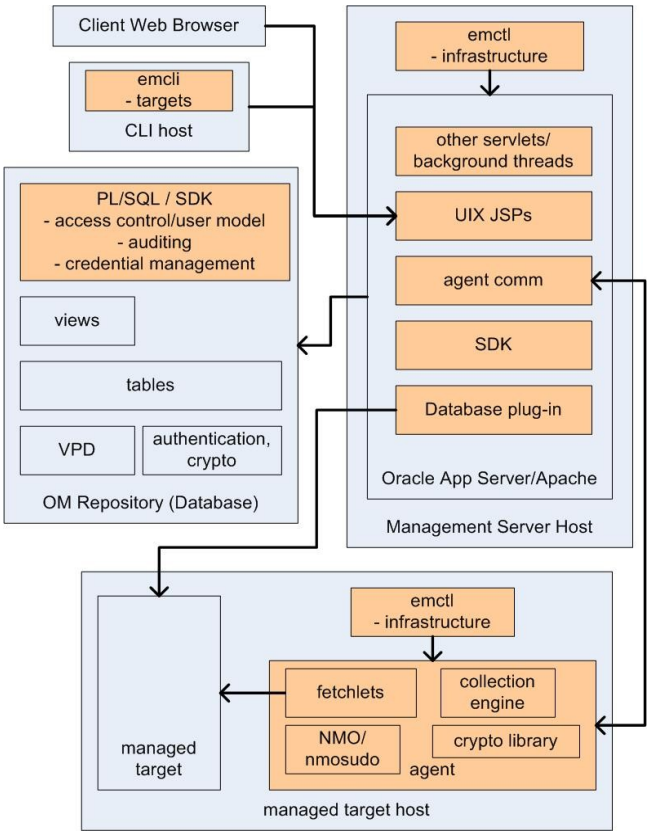

Figure 1: TOE Architecture

Figure 1 presents an architectural overview of an EMGC, illustrating the various components that comprise the TOE. Orange shaded (dark-shaded) boxes show parts of the TOE, (blue (light-shaded boxes) boxes name parts of its IT environment. Arrows are used to generally indicate information flows/connectivity between components (e.g., an arrow pointing from component A to component B would indicate that component A initiates communication with component B).

5.1 Oracle Management Server

The Oracle Management Server (OMS, orange-shaded boxes within the Oracle Application Server in Figure 1) provides the TOE user with web-based and command-line interfaces to manage and control the TOE and the systems that it manages, and most of the interaction between the user and the TOE take place through the OMS. Because of this, the OMS is central to the control of the entire TOE. The functionality of the OMS application is implemented within the Java-based Oracle Web Application Server.

The OMS web interface allows TOE users to view system measurements and perform management tasks. System measurements are provided by agents and can be used to monitor activity and diagnose performance and health issues of managed systems. Tasks such as system provisioning, remotely installing updates and patches, adjusting system configuration, and performing maintenance actions can all be run manually or automated to run regularly.

In the evaluated configuration of the TOE, a database plug-in is installed along with the standard installation procedure that can perform direct database queries and commands, allowing the TOE user to create and schedule database maintenance commands and collect customized information about the database. According to the user guidance [10],

any other plug-ins not being part of the product installation is not allowed to be installed and used in the evaluated configuration.

5.2 Agent/Target

In the evaluated configuration the TOE has the ability to manage a variety of remote hosts and an Oracle Database as application on the remote host referred to as a target (OMA, orange-shaded boxes within the OM Repository in Figure 1). In order to perform remote actions within a managed network, each managed target has an agent that is installed to facilitate the management actions of the OMS. This agent communicates with the OMS to receive instructions executing them on the target. Monitoring and collecting credentials, for example user name and password needed to execute commands in a managed database, are stored by the agent on the target host. Host credentials are passed to the target's operating system for identification and authentication when requesting management actions on the operating system level.

Agents communicate over the network with the OMS via HTTPS in order to receive commands and deliver target information.

5.3 Repository

Data collected by the agents as well as a large amount of TOE configuration information is stored in the repository, which is implemented by an Oracle Database (OMR, orange-shaded boxes within the Oracle Application Server in Figure 1). The repository is also used to host and execute a number of OMS-provided PL/SQL packages. In addition, EMGC uses the repository as an authentication provider: the repository provides decisions on authentication requests that are then enforced by the OMS.

Access control is enforced with the help of explicit checks for privileges. Privilege checking is implemented by the PL/SQL scripts which check the access control lists to allow or deny the authenticated user from performing requested operations on defined objects.

Access control for queries directly accessing data about managed targets in the database is not enforced by the TOE as the queries are executed by the repository. In this case the functionality of the database system is used to deny or grant access to the corresponding data.

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 Developer Tests

The developer performed the tests mostly in virtual machines.

For the OMS, the following software components were used. Other software like a JVM required for running the Oracle Application Server, etc. were installed according to the guidance of the corresponding product:

- Oracle Application Server 10.1.2.3 hosting the OMS
- Oracle Database 11g Release 1 (11.1.0.7) hosting the Repository
- Operating system Red Hat Enterprise Linux AS Release 5 (32 bit)

For the target hosts, the TOE-software was run by means of the following software:

- Java Runtime Environment 1.4.2
- Operating system Red Hat Enterprise Linux AS Release 5 (32 bit)

The developer performed functional tests within the test environment located at the Oracle data center in Austin,TX. The test approach chosen by the developer is based on running regression tests of all TOE functionality including security related aspects. The regression tests are run at least once a week and all differences between expected test results archived an actual test results obtained are subject to investigation.

Although some deviations of actual test results from the expected results were identified, none of those deviations was related to the TOE functionality or had a security impact.

7.2 Independent evaluator tests

The evaluator set up an own test installation in the evaluation lab in Munich according to the developer guidance on installation and secure configuration. This test installation has been used to perform tests devised by the evaluator.

For the OMS and the OMR:

- Oracle Application Server 10.1.2.3
- Oracle Database 11g Release 1 (11.1.0.7) hosting the Repository
- Operating system SuSE Linux Enterprise Server 10 SP1 (64 bit)

For the target hosts, the TOE-software was run by means of the following software:

- Java Runtime Environment 1.4.2
- One agent for each of the following operating systems:
  - Red Hat Enterprise Linux AS Release 5 (64 bit)
  - SuSE Linux Enterprise Server 10 SP1 (32 bit and 64 bit)
  - Oracle Enterprise Linux Version 4 Update 5 (32 bit and 64 bit)

The evaluator verified the correct operation of the TSF by successfully repeating nearly all of the developer tests for the RHEL 5 32-bit platform. In addition, own test cases for a broad selection of TSF covering the remaining supported platforms for the agent and a 64-bit platform for the OMS were all executed successfully. As all Linux versions base on the same Linux Kernel version and the code base for all versions is the same, the evaluator considered this test coverage to assure a correct functioning on all platforms.

Thus the evaluator concedes an appropriate level of assurance to the TOE software that the software runs on Red Hat Enterprise Linux AS Version 5, Oracle Enterprise Linux Version 4 Update 5 and SuSE Linux Enterprise Server 10 SP1 operating systems both in the 32-bit and 64-bit mode without flaws in the security functionality.

7.3 Penetration Testing

The evaluator used publicly documented vulnerabilities in CVE and general search engines for devising his vulnerability analysis.

The main attention of the evaluator's assessment was put on the OMS/repository part of the TOE, as this is the central point of security management. The agents, that can be compared to probes installed on many locations within a network, only serve as data collectors with no direct security-impact on the central part of the TOE.

The following list summarizes areas considered for vulnerability testing:

- Corrupted agent scenarios
- Web pages accessible without authentication
- Privilege escalation
- Disclosure of sensitive information
- Code injections
- Insecure interfaces
- Random number generation

None of the penetration tests performed by the evaluator revealed an exploitable vulnerability of the TOE.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The evaluated configuration of the TOE consists of Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) with patches 8814764, 8968670, and 9019231 being applied. The evaluated configuration may also comprise one or more management agents installed on the managed target hosts. The runtime environment of the TOE is defined as follows:

- Java Runtime Environment 1.4.2 for target hosts and command line interface (CLI) hosts
- Software being installed by the standard installation procedure including the Oracle Application Server 10.1.2.3 hosting the OMS
- Oracle Database 11g Release 1 (11.1.0.7) hosting the Repository

The following Linux OS both in the 32-bit and the 64-bit version are supported for hosting target hosts and hosts to use the command line interface from:

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

The following configuration specifics apply to the evaluated configuration of the TOE:

- SSL must be enabled for network communications in secure-lock mode
- The only supported application on a target host in the evaluated configuration is an Oracle Database. Especially the support for Oracle Application Server and Collaboration suite is not included in this evaluation.
- Audit must always be turned on

- For configuration of systems, EMGC 10.2.0.5 Security best practices [9] should be used and the measures described in Evaluated Configuration for Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) [10] must be applied.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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. As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The component ALC_FLR.3 augmented for this TOE evaluation.

Result of site visits carried out for the certification procedure BSI-DSZ-CC-0577-2009 were re-used for this certification procedure.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: 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 vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for:

- The TOE Security Function SF 1, Identification and authentication:
  - Encryption and decryption in accordance with 3-DES (CBC mode) and cryptographic key sizes 168 Bits (3-DES) that meet the standards FIPS46-3 [16], FIPS81 [17]
- The TOE Security Function SF 4, protected data transfer. This security function uses:
  - RSA with a bit length of 1024 or 2048 bits in combination with SHA-1 for signature creation and verification according to the standards RFC 2313 [11], and the SSL Protocol,Version 3 [12],
  - Key wrapping in accordance with RSA and cryptographic key sizes 1024 or 2048 bits that meet the standards RFC 2313 [11], RFC 2437 [13] and the SSL Protocol Version 3 [12],

- Data authentication in accordance with the cryptographic algorithm HMAC-SHA-1 and cryptographic key sizes 160 bits that meet the standards FIPS180 [14], FIPS198 [15] and the SSL Protocol, Version 3 [12].
- Encryption and decryption in accordance with 3-DES (CBC mode) and cryptographic key sizes 168 Bits (3-DES) that meet the standards FIPS46-3 [16], FIPS81 [17]
- Generation of cryptographic keys in accordance with the key generation algorithm SSLv3 symmetric key and secret key generation and specified cryptographic key sizes of 168 Bits for 3-DES keys and 160 Bits for HMAC SHA-1 secret that meet the SSL Protocol Version 3 (SSLv3 symmetric key and secret generation) [12] and SP800-67 [18] (3-DES key generation).

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. In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE shall be used. If non-certified updates or patches are available he should request the developer for providing a re-certification. In the meantime risk management process of the system using the TOE shall investigate and decide on the usage of not yet certified updates and patches or to take additional measures in order to maintain system security.

The customer is required to verify the correctness of all relevant guidance documentation obtained by generating SHA-1 checksums and comparing those against the values provided in table 3 prior to installation and configuration of the TOE. This procedure only applies to the guidance documents listed in that table.

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-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

CLI	Command line interface
EAL	Evaluation Assurance Level
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
PL/SQL	Procedural Language/SQL
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.

OMS - Oracle Management Server; a middle tier between "Oracle agents" and management consoles hosted centrally.

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 - combined functionality of all hardware, software, and firmware of a 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[9].

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

[6] Security Target BSI-DSZ-0621-2010, Version 3.9, 2010-08-19, Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Security Target, Oracle Corporation

[7] Evaluation Technical Report, Version 6, 2010-08-24, Final Evaluation Technical Report, atsec information security GmbH (confidential document)

[8] Configuration list for the TOE, 2010-08-24, Configuration List for Oracle Enterprise Manager Grid Control (10.2.0), (confidential document)

[9] Guidance documentation, June 2009, Enterprise Manager Grid Control 10g Release 5 Security Deployment - Best Practices, Oracle Corporation

[10] Guidance documentation, Issue 2.1, August 2010, Evaluated Configuration for Oracle Enterprise Manager 10g Grid Control Release 2 (10.2.0.5), Oracle Corporation

[11] RFC 2313: PKCS#1: RSA Cryptography Specification, Version 1.5, March 1998, ISOC

[12] The SSL Protocol, Version 3, November 1996, Alan O. Freier, Philip Karlton, Paul C. Kocher

[13] RFC 2437: PKCS #1: RSA Cryptography Specifications, Version 2.0, October 1998, ISOC

[14] FIPS 180, Secure Hash Standard, 1993-05-11, NIST

[15] FIPS 198, The Keyed-Hash Message Authentication Code (HMAC), 2002-03-06, NIST

[16] FIPS46-3, Data Encryption Standard (DES), 1999-10-25, NIST

[17] FIPS PUB 81: DES Modes of Operations, 1980-12-2, NIST

[18] SP800-67, NIST Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 2008-05-19, NIST

[9] specifically

- AIS 32, Version 5, 17 May 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- 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 10.4)

„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 D.”

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	1	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

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0621-2010

Evaluation results regarding development and production environment

The IT product Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) (Target of Evaluation, TOE) 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.

As a result of the TOE certification, dated 27 August 2010, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_FLR.3, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

Site	Postal Address
Redwood Shores	Oracle Corporation, 500 Oracle Parkway, Redwood Shores, CA 94065, USA
Austin	Oracle Austin Data Center, 11400 N Lamar Blvd, Austin, TX 78753-2663, USA
Belmont	Oracle Manufacturing & Distribution, 300 Harbor Drive, Belmont, CA 94002, USA
Dublin	Oracle EMEA, Block C Eastpoint Business Park, Alfie Byrne Road, Dublin 3, Ireland
Bangalore	Oracle Technology Park, India Development Centre No. 3, Bannerghatta Road, Bangalore, Karnataka 560 029, India
Bangalore	Oracle India Pvt. Ltd., Prestige Lexington, Prestige St. John's Woods, No. 18, 2nd Cross Road Chikka Audugodi, Bangalore, Karnataka 560 029, India
Nashua	Oracle Nashua, One Oracle Drive, Nashua, NH 03062-2833, USA

Table 4: Development and production sites

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target) are fulfilled by the procedures of these sites.

This page is intentionally left blank.