Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0427-2007

for

Oracle Enterprise Linux
Version 4 Update 4

from

Oracle Corporation UK Limited

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0427-2007

Oracle Enterprise Linux Version 4 Update 4

from

Oracle Corporation UK Limited

Common Criteria Arrangement

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

Evaluation Results:

PP Conformance:	**Controlled Access Protection Profile (CAPP), Issue 1.d, 08.10.1999**
Functionality:	**PP conformant plus product specific extensions** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 augmented by** **ALC_FLR.3 – Systematic flaw remediation**

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 19. July 2007

The President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht 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)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

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.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

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

---

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

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

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

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

2 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-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 the arrangement has been signed by the national bodies of:

Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America.

The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

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 Linux Version 4 Update 4 has undergone the certification procedure at BSI.

The evaluation of the product Oracle Enterprise Linux Version 4 Update 4 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponso, vendor and distributor is:

Oracle Corporation UK Limited
520 Oracle Parkway, Thames Valley Park
Reading, Berkshire, RG6 1RA, UK

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 19. July 2007.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-30.

The product Oracle Enterprise Linux Version 4 Update 4 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Oracle Corporation UK Limited
520 Oracle Parkway, Thames Valley Park
Reading, Berkshire, RG6 1RA, UK

B Certification Results

The following results represent a summary of

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

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) is the operating system Oracle Enterprise Linux Version 4 Update 4 (with the capp-eal4-config-oracle package).

The TOE is a general purpose, multi-user, multi-tasking Linux based operating system. It provides a platform for a variety of applications in the governmental and commercial environment. It is available on a broad range of computer systems, ranging from departmental servers to multi-processor enterprise servers.

The evaluation covers a potentially distributed, but closed network of servers running the evaluated version of the TOE. The hardware platforms selected for the evaluation consist of machines which are available when the evaluation has completed and to remain available for a substantial period of time afterwards.

The TOE includes software components only and provides CAPP compliant security functionality plus product specific extentions. Among these functions are:

- Identification and Authentication
- Discretionary Access Control
- Secure Communication
- Audit
- Object reuse functionality
- Security Management
- TSF Protection

The evaluated version of the TOE can be run on Dell PowerEdge 1850 (EM64T) and HP ProLiant DL380 G5 (EM64T). For a detailed description of the system the tests were performed on, please refer to chapter 7 of this report.

The product Oracle Enterprise Linux Version 4 Update 4 is delivered by Oracle Corporation UK Limited via electronic download. It contains a set of ISO CD images and additional software packages as listed in chapter 2 of this report. The additional packages contain the Evaluated Configuration Guide, updates to fix problems and scripts that can be used for the secure installation process. The user needs to verify the integrity and authenticity of the downloaded software before installing the TOE.

For a detailed listing of the software packages that are part of the TOE please refer to chapter 2 of this report.

For a detailed listing of guidance documents to be followed by a user of the TOE refer to chapter 6 of this report.

The IT product Oracle Enterprise Linux Version 4 Update 4 (with the capp-eal4-config-oracle package) was evaluated by atsec information security GmbH. The

evaluation was completed on 13. July 2007. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

Oracle Corporation UK Limited
520 Oracle Parkway, Thames Valley Park
Reading, Berkshire, RG6 1RA, UK

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4 (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: ALC_FLR.3	Life cycle support – Systematic flaw remediation

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
FAU	**Security audit**
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective Audit
FAU_STG.1	Guarantees of Audit Data Availability
FAU_STG.3	Action in Case of Possible Audit Data Loss
FAU_STG.4	Prevention of Audit Data Loss

[8] Information Technology Security Evaluation Facility

Security Functional Requirement	Addressed issue
FCS	**Cryptographic support**
FCS_CKM.1(1)	Cryptographic key generation (SSL: Symmetric algorithms)
FCS_CKM.1(2)	Cryptographic key generation (SSH: Symmetric algorithms)
FCS_CKM.1(3)	Cryptographic key generation (SSL: RSA)
FCS_CKM.2(1)	Cryptographic key distribution (SSL: RSA public keys)
FCS_CKM.2(2)	Cryptographic key distribution (SSH: DiffieHellman key negotiation)
FCS_CKM.2(3)	Cryptographic key distribution (SSH: DSS public keys)
FCS_CKM.2(4)	Cryptographic key distribution (SSL: Symmetric keys)
FCS_COP.1(1)	Cryptographic operation (SSL: RSA)
FCS_COP.1(2)	Cryptographic operation (SSL: Symmetric operations)
FCS_COP.1(3)	Cryptographic operation (SSH: Symmetric operations)
FDP	**User data protection**
FDP_ACC.1	Discretionary Access Control Policy
FDP_ACF.1	Discretionary Access Control Functions
FDP_RIP.2	Object Residual Information Protection
FDP_UCT.1	Basic data exchange confidentiality
FDP_UIT.1	Data exchange integrity
FIA	**Identification and authentication**
FIA_ATD.1	User Attribute Definition
FIA_SOS.1	Strength of Authentication Data
FIA_UAU.2	Authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.2	Identification
FIA_USB.1	User Subject Binding
FMT	**Security Management**
FMT_MSA.1	Management of Object Security Attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static Attribute Initialization
FMT_MTD.1	Management of the Audit Trail
FMT_MTD.1	Management of Audited Events
FMT_MTD.1	Management of User Attributes
FMT_MTD.1	Management of Authentication Data

Security Functional Requirement	Addressed issue
FMT_REV.1	Revocation of User Attributes
FMT_REV.1	Revocation of Object Attributes
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Management Roles
FPT	**Protection of the TOE Security Functions**
FPT_AMT.1	Abstract Machine Testing
FPT_RVM.1	Reference Mediation
FPT_SEP.1	Domain Separation
FPT_STM.1	Reliable Time Stamps
FTP	**Truted path/channels**
FTP_ITC.1	Inter-TSF trusted channel

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Addressed issue
FDP	**User data protection**
Note 1	Subject Residual Information Protection

Table 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FMT	**Security Management**
FMT_MSA.3	Static attribute initialisation

Table 4: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.3.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
Identification and Authentication (IA)	
IA.1	User Identification and Authentication Data Management
IA.2	Common Authentication Mechanism
IA.3	Interactive Login and Related Mechanisms
IA.4	User Identity Changing
IA.5	Login Processing
Audit (AU)	
AU.1	Audit Configuration
AU.2	Audit Processing
AU.3	Audit Record Format
AU.4	Audit Post-Processing
Discretionary Access Control (DA)	
DA.1	General DAC Policy
DA.2	Permission Bits
DA.3	Access Control Lists
DA.4	Discretionary Access Control: IPC Objects
Object Reuse (OR)	
OR.1	Object Reuse: File System Objects
OR.2	Object Reuse: IPC Objects
OR.4	Object Reuse: Memory Objects
Security Management (SM)	
SM.1	Roles
SM.2	Access Control Configuration and Management
SM.3	Management of User, Group and Authentication Data
SM.4	Management of Audit Configuration
SM.5	Reliable Time Stamps
Secure Communication (SC)	
SC.1	Secure Protocols
TSF Protection (TP)	
TP.1	TSF Invocation Guarantees
TP.2	Kernel
TP.3	Kernel Modules
TP.4	Trusted Processes
TP.5	TSF Databases

TOE Security Function	Addressed issue
TP.6	Internal TOE Protection Mechanisms
TP.7	Testing the TOE Protection Mechanisms

Table 5: Security Functions

Please note that only the titles of the Security Functions have been provided here. For more details please refer to the Security Target [6], chapter 6.2.

1.3 Strength of Function

The TOE's strength of functions is claimed 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 6.5.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The TOE has to avert the following threats. They are cited from the Security Target [6], chapter 3.2.1:

Threats	Addressed issue
T.UAUSER	An attacker (possibly, but not necessarily, an unauthorized user of the TOE) may impersonate an authorized user of the TOE. This includes the threat of an authorized user that tries to impersonate as another authorized user without knowing the authentication information.
T.UAACCESS	An authorized user of the TOE may access information resources without having permission from the person who owns, or is responsible for, the information resource for the type of access.
T.COMPROT	An attacker (possibly, but not necessarily, an unauthorized user of the TOE) may intercept a communication link between the TOE and another trusted IT product to intercept or modify information transferred between the TOE and the other trusted IT product (which may be another instantiation of the TOE) using defined protocols (SSH or SSL) in a way that can not be detected by the TOE or the other trusted IT product.

Table 6: Threats addressed by the TOE

The TOE has to comply to the following Organisational Security Policies (OSPs). They are defined in the Security Target [6], chapter 3.3 and summarised here:

Organisational Security Policy	Addressed issue
P.AUTHORISED_USERS	Only users who have been authorised to access information within the system may access the system.
P.NEED_TO_KNOW	The organisation using the TOE must define a discretionary access control policy on a need-to-know basis. The rules of this access control policy should be based on the attributes (i) owner of object, (ii) identity of subject attempting access to an object and (iii) access rights (of a subject for the accessed object).
P.ACCOUNTABILITY	The users of the system shall be held accountable for their actions.

Table 7: Organisational Security Policies defined in the ST

1.5 Special configuration requirements

The configuration requirements for the TOE are defined in chapter 2.4 and subsequent chapters of the Security Target [6] and are summarised here (please refer to the Security Target for the precise and more detailed description):

- The CC evaluated package set must be selected at install time in accordance with the description provided in the Evaluated Configuration Guide and installed accordingly.
- The operating system supports the use of IPv4 and IPv6, only IPv4 is included within the TOE.
- Both installation from CD and installation from a defined disk partition are supported.
- The default configuration for identification and authentication are the defined password based PAM modules. Support for other authentication options e.g. smartcard authentication, is not included in the evaluation configuration.
- If the system console is used, it must be connected directly to the system and afforded the same physical protection as the server.
- The TOE comprises a single server machine (and optional peripherals) as listed in section 2.4.2 of the Security Target [6] running the system software listed in the package list in section 2.3 of the ST (a server running the above listed software is referred to as a “TOE server” in the following).

The evaluated configuration supports multiple following file system types.

- Filesystems using physical media (hard disk, CD-ROM or DVD-ROM):
  - ext3 journaling filesystem,
  - ocfs2, the Oracle Cluster File System,

  - the read-only ISO 9660 filesystem for CD-ROM and DVD-ROM drives,
- RAM based nonpersistent file systems:
  - The temporary filesystem (tmpfs) used as a temporary RAM based file system. This file system is not persistent across boots of the operating system,
  - dlmfs, the Distributed Lock Manager File System
- Pseudo file systems that are used as configuration or monitoring interfaces to the kernel in a running system, and that do not support arbitrary data storage:
  - The process file system, procfs (/proc), provides access to the process image of each process on the machine as if the process were a “file”. Process access decisions are enforced by DAC attributes inferred from the underlying process’ DAC attributes. Additional restrictions apply for specific objects in this file system.
  - The sysfs filesystem (sysfs) used to export and handle non-process related kernel information such as driver specific information. Access to objects there can be restricted using the DAC mechanism (which are the permission bits only).
  - The kernel configuration filesystem (configfs) which supports an administrative interface to kernel data objects.
- The pseudo terminal device file system (devpts) used to provide pseudo terminal support.
- The miscellaneous binary file format registration file system (binfmt_misc) used to configure interpreters for executing binary files based on file header information. For example, this enables direct execution of Java files using the execve system call instead of the traditional invocation of the java interpreter with the Java file provided as an argument.
- The virtual root file system (rootfs) used temporarily during system startup.
- The Security Enhanced Linux file system (selinuxfs) used for configuring the selinux system. SELinux adds additional restrictions to access checks and is beyond the scope of the TOE.

Note: This evaluation focuses on the use of the TOE as a server or a network of servers. Therefore a graphical user interface has not been included as part of the evaluation. In addition the evaluation assumes the operation of the network of servers in a non-hostile environment.

1.6 Assumptions about the operating environment

The constraints concerning the allowed hardware and peripherals are made in the Security Target (refer to [6], chapter 2.4.2).

Hardware platforms:

- Dell PowerEdge 1850 (EM64T) RHEL 4 Server Certified (described in [9])
- HP ProLiant DL380 G5 (EM64T) RHEL 4 Server Certified (described in [10])

Peripherals:

- all terminals supported by the TOE (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces).
- printers compatible with PostScript level 1 or PCL 4 attached via parallel port, USB, or Ethernet.
- all storage devices and backup devices supported by the TOE (hard disks, CDROM drives, streamer drives, floppy disk drives) (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces)
- all Ethernet and Token-Ring network adapters supported by the TOE

Note: peripheral devices are part of the TOE environment.

Note: Excluding hot pluggable devices connected via USB does not exclude all USB devices. USB printers, keyboards and mice may be attached provided they are connected before booting the operating system.

The following constraints concerning the operating environment are made in the Security Target. The constraints are based on the assumptions defined in [6], chapter 3.4 and are repeated in the following table:

Assumption	Addressed issue
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.MANAGE	It is assumed that there are one or more competent individuals who are assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL_ADMIN	The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
A.COOP	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
A.UTRAIN	Users are trained to use the security functionality provided by the system appropriately.
A.UTRUST	Users are trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their data.

Assumption	Addressed issue
A.NET_COMP	All network components (such as bridges and routers) are assumed to correctly pass data without modification.
A.PEER	Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. There are no security requirements which address the need to trust external systems or the communications links to such systems.
A.CONNECT	All connections to peripheral devices and all network connections not using the secured protocols SSH v2 or SSL v3 reside within the controlled access facilities. Internal communication paths to access points such as terminals or other systems are assumed to be adequately protected.

Table 8: Assumptions defined in the Security Target

The following constraints are based on Security Objectives which have to be met by the TOE environment. Theses objectives are defined in [6], chapter 4.2 and are repeated here:

Security Objective	Addressed issue
OE.ADMIN	Those responsible for the administration of the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
OE.CREDEN	Those responsible for the TOE must ensure that user authentication data is stored securely and not disclosed to unauthorized individuals. In particular: Procedures must be established to ensure that user passwords generated by an administrator during user account creation or modification are distributed in a secure manner, as appropriate for the purpose of the system. The media on which authentication data is stored must not be physically removable from the system by other than administrative users. Users must not disclose their passwords to other individuals.
OE.INSTALL	Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected

Security Objective	Addressed issue
	from physical attack which might compromise IT security objectives.
OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: DAC protections on security critical files (such as configuration files and authentication databases) shall always be set up correctly. Network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted unless one of the secure protocols provided by the TOE is used for the communication with another trusted entity. This requires that users are trained to perform those tasks properly and trustworthy to not deliberately misuse their access to information and pass it on to somebody that does not have the right to access the information.
OE.MAINTENANCE	Administrative users of the TOE must ensure that any diagnostics facilities provided by the product are invoked at every scheduled preventative maintenance period.
OE.RECOVER	Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that, after system failure or other discontinuity, recovery without a protection (i.e., security) compromise is obtained.
OE.SOFTWARE_IN	Those responsible for the TOE shall ensure that the system shall be configured so that only an administrative user can introduce new trusted software into the system.
OE.SERIAL_LOGIN	Those responsible for the TOE shall implement procedures to ensure that users clear the screen before logging off where serial login devices (e.g. VT100 terminals) are used.
OE.HW_SEP	The underlying hardware must provide separation mechanism that can be used by the TOE to protect the TSF and TSF data from unauthorized access and modification.
OE.PROTECT	Those responsible for the TOE must ensure that procedures and/or mechanisms exist to ensure that data transferred between servers is secured from disclosure, interruption or tampering (when using communication links not protected by the use of the SSL or SSH protocols. Note that interruption of communication is not prevented by the use of those

Security Objective	Addressed issue
	protocols and if protection against interruption of communication is required, adequate protection in the TOE environment has to be established for all communication links).

Table 9: Security Objectives for the TOE environment

1.7 Disclaimers

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 Linux Version 4 Update 4

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Oracle Enterprise Linux	Version 4 Update 4	CD ISO Images, Download
2	SW	RPM software packages as listed below.	na	Download
3	DOC	CAPP EAL4 Evaluated Configuration Guide for Oracle Enterprise Linux 4 U4 and U5	1.3	Download

Table 10: Deliverables of the TOE

In addition to the CD ISO images the following additional packages have to be downloaded from Oracle through their internet representation. The user has to ensure the integrity of the downloaded software before using the packages:

- kernel-2.6.9-55.0.0.0.2.EL.x86_64.rpm
- kernel-devel-2.6.9-55.0.0.0.2.EL.x86_64.rpm
- kernel-smp-2.6.9-55.0.0.0.2.EL.x86_64.rpm
- kernel-smp-devel-2.6.9-55.0.0.0.2.EL.x86_64.rpm
- audit-libs-1.0.14-1.EL4.i386.rpm

- audit-libs-devel-1.0.14-1.EL4.i386.rpm
- capp-eal4-config-oracle-1.0-1.EL4.noarch.rpm

Installing no 1 and 2 of the table above results in a system which has the software packages as listed in [6], chapter 2.3 in place.

To install and configure the TOE such that it matches the configuration described in the Security Target the user has to follow the guidance provided in [11]. The Evaluated Configuration Guide provides all information on how to install and configure the TOE in accordance with the Security Target.

3 Security Policy

The Security Policy which is implemented by the TOE is defined in [6], chapter 6.1.5. This policy is refined by an extensive Security Policy Model document (confidential) that has been subject to analysis under the assurance component ADV_SPM.1 as required by EAL4. An overview as given in the ST is provided here:

The TOE is a single Oracle Enterprise Linux system running on one machine. Several of those systems may be interconnected via a local area network and exchange information using the network services. But one should keep in mind that the following statements hold:

- Each host computer in the networked system runs the Oracle Enterprise Linux kernel.
- Identification and authentication (I&A) is performed locally by each host computer. Each user is required to Login with a valid password and user identifier combination at the local system and also at any remote computer where the user can enter commands to a shell program (using ssh). User ID and password for one human user may be different on different hosts. User ID and password on one host system are not known to other host systems on the network and therefore a user ID is relevant only for the host where it is defined.
- Discretionary access control (DAC) is performed locally by each of the host computers and is based on user identity and group membership on this host. Each process has an identity (the user on whose behalf it is operating) and belongs to one or more groups. All named objects have an owning user, an owning group and a DAC attribute, which is a set of permission bits. In addition, file system objects optionally have extended permissions also known as an Access Control List (ACL). The ACL mechanism is a significant enhancement beyond traditional UNIX systems, and permits control of access based on lists of users and/or groups to whom specific permissions may be individually granted or denied.
- Object reuse is performed locally, without respect to other hosts.
- Interrupt handling is performed locally, without respect to other hosts.

- Privilege is based on the root identity. All privileged processes (setuid root programs and programs run under the root identity) start as processes with all privileges enabled. Unprivileged processes, which include setgid trusted processes, start and end with no privileges enabled.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the personnel assumptions the following usage conditions exist. Refer to [6], chapter 3.4.2 for more details:

- A.MANAGE
- A.NO_EVIL_ADMIN
- A.COOP
- A.UTRAIN
- A.UTRUST

Please note that only the names have been listed here. The details can be found either in the ST or in chapter 1.6 of this report.

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [6], chapter 3.4.1 and 3.4.3):

- A.LOCATE
- A.PROTECT
- A.NET_COMP
- A.PEER
- A.CONNECT

Please consider also the requirements for the evaluated configuration specified in chapter 8 of this report.

4.3 Clarification of scope

The threats listed below have to be averted in order to support the TOE security capabilities but are not addressed by the TOE itself. They have to be addressed by the operating environment of the TOE (for detailed information about the threats and how the environment may cover them refer to the Security Target [6]).

Environmental Threat	Addressed issue
TE.HWMF	An attacker with legitimate physical access to the hardware of the TOE (examples are maintenance personnel or legitimate users) or environmental conditions may cause a hardware malfunction with the effect that a user (normal or administrative) is losing stored data due to this hardware malfunction. An attacker may cause such a hardware malfunction either by having physical access to the hardware the TOE is running on or by executing software that capable of causing hardware malfunction. Note that such a hardware malfunction may be caused accidentally without malicious intent by persons having physical access to the TOE.
TE.COR_FILE	An attacker (possibly, but not necessarily, an unauthorized user of the TOE) or environmental conditions like a hardware malfunction may intentionally or accidentally modify or corrupt security enforcing or relevant files of the TOE without an administrative user being able to detect this. An attacker may corrupt such files either by having physical access to the hardware the TOE is running on, by booting other software than the TOE in its evaluated configuration or by modifying or corrupting files on backup media. Note that such a corruption may be caused accidentally without malicious intent by persons having legitimate access to media where such data is stored.
TE.HW_SEP	An attacker (possibly, but not necessarily, an unauthorized user of the TOE) with legitimate physical access to the hardware the TOE is running on or environmental conditions may cause the underlying hardware functions of the hardware the TOE is running on to not provide sufficient capabilities to support the self-protection of the TSF from unauthorized programs. Note that this also covers persons with legitimate access to the TOE hardware causing such a problem accidentally without malicious intent.

Table 11: Threats to be averted by the TOE environment

5 Architectural Information

General overview:

Oracle Enterprise Linux Version 4 Update 4 (OEL) is a general-purpose, multi-user, multi-tasking Linux based operating system. The version provides a platform for a variety of applications in the governmental and commercial environment.

The evaluation covers a potentially distributed, but closed network (which may contain a router connecting to other networks) of the hardware systems listed in section 2.4.2 in the ST running the evaluated version of OEL. The hardware platforms selected for the evaluation consist of machines which are available when the evaluation was completed and are intended to remain available for a substantial period of time afterwards.

The TOE Security Functions (TSF) consist of functions of OEL that run in kernel mode plus some trusted processes. These are the functions that enforce the security policy as defined in this Security Target. Tools and commands executed in user mode that are used by an administrative user need also to be trusted to manage the system in a secure way. But as with other operating system evaluations they are not considered to be part of this TSF.

Also the hardware and the BootProm firmware are not considered to be part of the TOE.

The TOE includes installation from CD-ROM and from a local hard disk partition. Installation from the local hard disk partition is required when the TOE is installed on a real or virtual system without a CD-ROM.

The TOE includes standard networking applications, such as ftp and ssh. It also includes the stunnel client and server program that allows to set up a trusted channel using the SSL v3 protocol. xinetd can be used to protect network applications which might otherwise have security exposures.

System administration tools include the standard commands. A graphical user interface for system administration or any other operation is not included in the evaluated configuration.

The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services. For example a HTTP server using a port above 1024 (e. g. on port 8080) may be used as a normal application running without root privileges on top of the TOE. If this server should be accessed via a SSL protected connection only, stunnel as part of the TSF can be used to provide this trusted channel.

Major structural units of the TOE

The TOE is structured in much the same way as many other operating systems, especially Unix-type operating systems. It consists of a kernel, which runs in the privileged state of the processor and provides services to applications (which those can be used by calling kernel services via the system call interface).

Direct access to the hardware is restricted to the kernel, so whenever an application wants to access hardware like disk drives, network interfaces or other peripheral devices, it has to call kernel services. The kernel then checks if the application has the required access rights and privileges and either performs the service or rejects the request.

The kernel is also responsible to separate the different user processes. This is done by the management of the virtual and real memory of the TOE which ensures that processes executing with different attributes can not directly access memory areas of other processes but have to do so using the inter-process communication mechanism provided by the kernel as part of its system call interface.

The TSF of the TOE also include a set of trusted processes, which when initiated by a user with a system call operate with extended privileges. The programs that represent those trusted processes on the file system are protected by the file system discretionary access control security function enforced by the kernel.

In addition the execution of the TOE is controlled by a set of configuration files, which are also called the TSF database. Also those configuration files are protected by the file system discretionary access control security function enforced by the kernel.

Normal users – after they have been successfully authenticated by a defined trusted process – can start untrusted applications where the kernel enforces the security policy of the TOE when those applications request services from the kernel via the system call interface.

The kernel itself is structured into a number of subsystems which are explained in detail in the high level design of the TOE. Those are:

File and I/O Subsystem
Implements all file system object related functions. Functions include those that allow a process to create, maintain, interact and delete file-system objects, such as regular files, directories, symbolic links, hard links, device special files, named pipes, and sockets.

Process Control Subsystem
Implements functions related to process and thread management. Functions include those that allow the creation, scheduling, execution, and deletion of process and thread subjects.

Memory Management Subsystem
Implements functions related to the management of a system's memory resources. Functions include those that create and manage virtual memory, including management of page tables and paging algorithms.

Networking Subsystem
This subsystem implements UNIX and internet domain sockets as well as algorithms for scheduling network packets.

IPC Subsystem
Implements functions related to inter-process communication mechanisms. Functions include those that facilitate controlled sharing of information between processes, allowing them to share data and synchronize their execution in order to interact with a common resource.

Audit Subsystem
Implements the kernel functions required to intercept system calls and audit them in accordance with the auditing policy defined by the system administrator.

Kernel Modules Subsystem
This subsystem implements an infrastructure to support loadable modules. Functions include those that load and unload kernel modules.

Device Driver Subsystem
Implements support for various hardware devices through common, device independent interface.

The trusted processes include the following subsystems:

Identification and Authentication
This subsystem includes all the processes that require to identify and authenticate users. All those processes share a common set of functions (pluggable authentication modules (PAM)) that ensure the same policy to be enforced with respect to identification and authentication of users. Successful as well as unsuccessful authentication attempts can be audited.

Network Applications
This subsystem includes the trusted processes implementing networking functions. The TOE supports FTP and SSH v2 as well as setting up a secure channel to another trusted system via the stunnel client and server processes using the SSL v3 protocol. The secure configuration as defined in the Security Target restricts the cipher suites that can be used for secure communication.

System Management
This subsystem includes the trusted commands a system administrator can use to manage users and groups, set the time and date and check the integrity of the underlying abstract machine.

Batch Processing
This subsystem includes the cron and at trusted processes that allow to execute user programs at predefined time schedules. They ensure that the users are restricted to the same security policy restrictions that also apply when they start programs interactively.

User Level Audit
This subsystem includes all the trusted processes and commands outside of the kernel required to collect, store and process audit records.

In addition to those functions the TOE includes a secure system initialization function which brings the TOE into a secure state after it is powered on or after a reset. This function ensures that user interaction with the TOE can only occur after the TOE is securely initialized and in a secure state.

Security Functions

The security functions of the TOE defined in the Security Target are:

Identification and Authentication

The TOE provides identification and authentication using pluggable authentication modules (PAM) based upon user passwords. The quality of the passwords used can be enforced through configuration options controlled by the TOE. Other authentication methods (e. g. Kerberos authentication, token based authentication) that are supported by the TOE as pluggable authentication modules are not part of the evaluated configuration. Functions ensure a basic password strength and limit the use of the su command and restrict root login to specific terminals are also included.

Audit

The TOE provides the capability to audit a large number of events including individual system calls as well as events generated by trusted processes. Audit data is collected in regular files in ASCII format. The TOE provides a program for the purpose of searching the audit records.

The system administrator can define a rule base to restrict auditing to the events he is interested in. This includes the ability to restrict auditing to specific events, specific users, specific objects or a combination of all of this.

Discretionary Access Control

Discretionary Access Control (DAC) restricts access to file system objects based on Access Control Lists (ACLs) that include the standard UNIX permissions for user, group and others. Access control mechanisms also protect IPC objects from unauthorized access.

The TOE includes the ext3 file system, which supports POSIX ACLs. This allows defining access rights to files within this type of file system down to the granularity of a single user.

Object Reuse

File system objects as well as memory and IPC objects will be cleared before they can be reused by a process belonging to a different user.

Security Management

The management of the security critical parameters of the TOE is performed by administrative users. A set of commands that require root privileges is used for system management. Security parameters are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorized access by users that are not administrative users.

Secure Communication

The TOE supports the definition of trusted channels using either the SSH v2 or the SSL v3 protocol. In the case of SSH the TOE includes the SSH server and client functions. Password based authentication is supported.

To use the SSL v3 protocol the TOE provides the stunnel client and server functions.

Only a restricted number of cipher suites are supported for those protocols in the evaluated configuration. They are listed in the Security Target.

TSF Protection

While in operation, the kernel software and data are protected by the hardware memory protection mechanisms. The memory and process management components of the kernel ensure a user process cannot access kernel storage or storage belonging to other processes.

Non-kernel TSF software and data are protected by DAC and process isolation mechanisms. In the evaluated configuration, the reserved user ID root owns the directories and files that define the TSF configuration. In general, files and directories containing internal TSF data (e.g., configuration files, batch job queues) are also protected from reading by DAC permissions.

The TOE and the hardware and firmware components are required to be physically protected from unauthorized access. The system kernel mediates all access to the hardware mechanisms themselves, other than program visible CPU instruction functions.

6 Documentation

The following documentation is provided with the product by the developer to the customer:

> CAPP EAL4 Evaluated Configuration Guide for Oracle Enterprise Linux 4 U4 and U5, Version 1.3, 2007-06-20, Orcale Corporation, [11]

Document [11] contains a full description of the installation and configuration process to get the evaluated configuration of the TOE. Please note that it is the central document providing administrator guidance to the secure administration of the TOE. This guide has been developed to address all security issues related to the TOE and its security functions as described in the Security Target. Advice given in this guide takes precedence over any other guidance document.

7 IT Product Testing

Test configuration

The Security Target defines the following hardware platforms for the TOE:

- Dell PowerEdge 1850 (EM64T) RHEL 4 Server Certified
- HP ProLiant DL380 G5 (EM64T) RHEL 4 Server Certified

The sponsor has performed his tests on the above listed hardware platforms. The software was installed and configured as defined in the Evaluated Configuration Guide [11].

Depth/Coverage of Testing

The developer has done substantial functional testing of all externally visible interfaces (TSFI). Internal interfaces of the High-level design have been covered by direct and indirect testing. The evaluators repeated the developer tests (because of the highly automated testing approach of the developer) and conducted additional independent tests and penetrations tests.

Summary of Developer Testing Effort

Test configuration:

The sponsor/developer has performed the tests on the following hardware platform:

- Dell PowerEdge 1850 (Intel Xeon EM64T based system)
- HP ProLiant DL380 G5 (Intel Xeon EM64T based system)

The software was installed and configured as in the Guidance Documents (refer to chapter 6). Additional software was installed on the system to perform the tests. A rationale was given why this additional software was within the boundary defined by the Security Target and did not constitute a violation of the evaluated configuration.

Testing approach:

The sponsor/developer used several test suites and manual tests to test the TOE. One of the test suites used was the LTP test suite. It is an adapted version of tests from the Linux Test Project. The tests have a common framework in which individual test cases adhere to a common structure for setup execution and cleanup of tests. Each test case may contain several tests of the same function, stressing different parts (for example, base functionality, behaviour with illegal parameters and reaction to missing privileges). Each test within a test case reports PASS respectively OK or FAIL and the test case summary in batch mode reports PASS if all the tests within the test case passed, otherwise FAIL. Tests can be executed either manually by running the individual test case files or run in batch mode by running an overall script.

Testing results:

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

Summary of Evaluator Testing Effort

Test configuration:

The evaluator was provided with a test system that was pre-installed with the evaluated configuration. To verify that the system's configuration is consistent with the evaluated configuration set forth in the Evaluated Configuration Guide [11], the evaluator verified that the resulting system configuration of each installation and configuration step outlined in the guide is present.

The evaluator used the following test system:

- Dell PowerEdge 1850

The system was located in the Oracle facility in Redwood Shores, CA. This system was used by the sponsor to perform the developer testing of the TOE.

Testing approach:

Since the developer tests are highly automated the evaluation facility decided to re-run all automated developer tests but on a 64-bit platform only. In addition evaluator tests were defined and executed by the evaluation facility.

Testing results:

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

Evaluator penetration testing:

The evaluators devised a set of penetration tests based on

- common sources for vulnerabilities of the Linux Operating System,
- findings of their evaluation work examination.

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

8 Evaluated Configuration

According to the Security Target the evaluated configuration of the TOE is defined as follows (refer also to the Security Target [6]):

The TOE Oracle Enterprise Linux Version 4 Update 4 is delivered via electronic download. The TOE contains a set of CD ISO images and the following additional packages:

- kernel-2.6.9-55.0.0.0.2.EL.x86_64.rpm
- kernel-devel-2.6.9-55.0.0.0.2.EL.x86_64.rpm
- kernel-smp-2.6.9-55.0.0.0.2.EL.x86_64.rpm
- kernel-smp-devel-2.6.9-55.0.0.0.2.EL.x86_64.rpm
- audit-libs-1.0.14-1.EL4.i386.rpm
- audit-libs-devel-1.0.14-1.EL4.i386.rpm

- capp-eal4-config-oracle-1.0-1.EL4.noarch.rpm

The integrity and authenticity of the downloaded software has to be verified before the installation process.

For a precise listing of all the packages please that make up the evaluated configuration of the TOE please refer to [6], chapter 2.3.

The configuration requirements for the TOE are defined in chapter 2.4 and subsequent chapters of the Security Target [6] and are also summarised in the chapters 1.5 and 1.6 of this report.

9 Results of the Evaluation

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 verdicts for the CC, Part 3 assurance components (according to EAL4 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS

Assurance classes and components		Verdict
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Systematic flaw remediation	ALC_FLR.3	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Independent vulnerability analysis	AVA_VLA.2	PASS

Table 12: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conform to the PP Controlled Access Protection Profile, Issue 1.d, 8 October 1999, [8]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by ALC_FLR.3 – Systematic flaw remediation.
- The following TOE Security Function fulfils the claimed Strength of Function: User authentication based on passwords (IA).

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for the Security Function SC (Secure Communication).

The results of the evaluation are only applicable to the operating system Oracle Enterprise Linux Version 4 Update 4 as outlined in chapter 2 of this report.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational document [11] contains necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

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

13.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Bibliography

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

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

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

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

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

[6] Security Target BSI-DSZ-0427-2007, Version 1.6, 2007-07-12, "Oracle Enterprise Linux Version 4 Update 4 Security Target for CAPP Compliance", Oracle Corporation UK Limited

[7] Evaluation Technical Report BSI-DSZ-CC-0427-2007, Version 2, 2007-07-12, atsec information security GmbH (confidential document)

[8] Controlled Access Protection Profile, Issue 1.d, 8 October 1999

[9] Dell PowerEdge 1850 spec sheet, http://www.dell.com/downloads/-global/products/pedge/en/1850_specs.pdf

[10] QuickSpecs HP ProLiant DL380 G5 Storage Server, http://h18000.www1.hp.com/products/quickspecs/12559_na/-12559_na.pdf

[11] CAPP EAL4 Evaluated Configuration Guide for Oracle Enterprise Linux 4 U4 and U5, Version 1.3, 2007-06-20, Orcale Corporation

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

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

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

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

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

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

CC Part 3:

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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