Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0481-2008

for

Oracle Enterprise Linux
Version 5 Update 1

from

Oracle Corporation

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0481-2008

Operating System

Oracle Enterprise Linux
Version 5 Update 1

from	Oracle Corporation
PP Conformance:	Controlled Access Protection Profile (CAPP) Version 1.d Information Systems Security Organization and Labeled Security Protection Profile (LSPP) Version 1.b Information Systems Security Organisation
Functionality:	PP conformant plus product specific extensions; Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

Common Criteria Recognition Arrangement

Common Criteria

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

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

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

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

Bonn, 15 October 2008
For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 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 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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

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

---

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

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

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

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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became effective on 3 March 1998.

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

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

2.2 International Recognition of CC - Certificates

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

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

This evaluation contains the component ALC_FLR.3 which is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 components of these assurance families are relevant.

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 5 Update 1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0427-2007. Specific results from the evaluation process BSI-DSZ-CC-0427-2007 were re-used.

The evaluation of the product Oracle Enterprise Linux Version 5 Update 1 was conducted by atsec information security GmbH. The evaluation was completed on 1 October 2008. 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 and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

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

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

5 Publication

The product Oracle Enterprise Linux Version 5 Update 1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] Oracle Corporation
520 Oracle Parkway
Thames Valley Park, Reading
Berkshire, RG6 1RA
U.K.

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 Oracle Enterprise Linux Version 5 Update 1 (Oracle Enterprise Linux operating system) with the capp-lspp-config-oracle package.

Oracle Enterprise Linux is a highly-configurable Linux-based operating system which has been developed to provide a good level of security as required in commercial environments. It also meets all of the requirements of the Controlled Access Protection Profile (CAPP) and the Labeled Security Protection Profile (LSPP) developed by the Information Systems Security Organization within the National Security Agency.

The TOE can operate in two different modes of operation called “CAPP mode” and “LSPP mode”:

- In CAPP mode the SELinux security module does not enforce a mandatory access control policy and does not recognize sensitivity labels of subjects and objects. SELinux can either be disabled completely, or enabled with a non-MLS policy such as the “targeted” or “strict” policies which only add additional restrictions to the CAPP requirements without interfering with the “root” administrator role. In this mode the TOE enforces all security requirements of CAPP but does not enforce the requirements of LSPP.
- In LSPP mode the SELinux security module is configured to enforce the mandatory access control policy based on the labels of subjects and objects as required by LSPP.

Several servers running Oracle Enterprise Linux can be connected to form a networked system. The communication aspects within Oracle Enterprise Linux used for this connection are also part of the TOE. Communication links can be protected against loss of confidentiality and integrity based on cryptographic protection mechanisms.

The TOE focuses on usage as a server or a network of servers. Therefore a graphical user interface has not been included as part of the evaluation. In addition it is assumed, that the the network of servers is being operated in a non-hostile environment.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profiles Controlled Access Protection Profile (CAPP) Version 1.d Information Systems Security Organization and Labeled Security Protection Profile (LSPP) Version 1.b Information Systems Security Organisation [9], [10].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL4 augmented by ALC_FLR.3 - Systematic flaw remidiation.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target, chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.3.

The TOE Security Functional Requirements are implemented by the following 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 and Role Changing
IA.5	Login Processing
IA.6	TOE access
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 supported by the TOE
DA.4	Discretionary Access Control: IPC Objects
Role-Based Access Control (LSPP mode only)	
RA.1	Role-Based Access Control
Mandantory Access Control (LSPP mode only)	
MA.1	Information Flow Control
MA.2	Import/Export of labeled data
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

TOE Security Function	Addressed issue
TP.4	Trusted Processes
TP.5	TSF Databases
TP.6	Internal TOE Protection Mechanisms
TP.7	Testing the TOE Protection Mechanisms
TP.8	Testing the TSF Mechanisms
TP.9	Secure failure state

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.2.

The claimed TOE's Strength of Functions 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 5.1.9 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1 . Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the following configurations of the TOE:

The TOE can be installed on the following hardware in a physical secure environment:

- Dell PowerEdge 1850 (EM64T)
- HP ProLiant DL380 G5 (EM64T)
- Oracle Virtual Machine (OVM) guest on HP ProLiant DL380 G5 (EM64T)

It supports the setup modes "CAPP mode" and "LSPP mode", described in the guidance manual [12]. Further details can be found in chapter 8 of this report.

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

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Oracle Enterprise Linux Version 5 Update 1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Oracle Enterprise Linux	Release 5 Update 1	5 CD ISO images, download
2	SW	RPM software packages as listed below.	na	RPM files, download

No	Type	Identifier	Release	Form of Delivery
3	DOC	Common Criteria LSPP EAL4+ Evaluated Configuration Guide for Oracle Enterprise Linux 5 Update 1	2.3	download

Table 2: 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:

- lspp-eal4-config-oracle-0.65-2.0.0.0.2.el5.noarch.rpm
- kernel-2.6.18-53.1.19.0.1.el5.x86_64.rpm
- kernel-devel-2.6.18-53.1.19.0.1.el5.x86_64.rpm
- mcstrans-0.2.6-1.el5_1.1.x86_64.rpm
- selinux-policy-2.4.6-106.el5_1.3.noarch.rpm
- selinux-policy-devel-2.4.6-106.el5_1.3.noarch.rpm
- selinux-policy-mls-2.4.6-106.el5_1.3.noarch.rpm
- selinux-policy-strict-2.4.6-106.el5_1.3.noarch.rpm
- selinux-policy-targeted-2.4.6-106.el5_1.3.noarch.rpm
- cups-1.2.4-11.14.el5_1.6.x86_64.rpm
- cups-libs-1.2.4-11.14.el5_1.6.i386.rpm
- cupslibs-1.2.4-11.14.el5_1.6.x86_64.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 [12]. 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 is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues, as stated in [6], chapter 6.1.5:

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:

- The Oracle Enterprise Linux kernel is running on each computer in the networked system.
- Identification and authentication (I&A) is performed locally by each 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) or use ftp. 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), role-based access control and mandatory access control (when operated in LSPP mode) is performed locally by each of the host computers and is based on user identity, group membership, user roles and the object attribute on this host. Each process has an identity (the user on whose behalf it is operating), belongs to one or more groups and operates with a role. All named objects have an owning user, an owning group, DAC attributes, 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.
- When operated in LSPP mode, Role-based access control (RBAC) is implemented as part of the SELinux policy. This allows defining a set of roles that can be assigned to users and a set of domains a user in a role can switch to. The TOE includes a policy that defines a hierarchical set of roles with general system administration, security administration and audit configuration assigned to different roles.
- When operated in LSPP mode, the security context assigned to each object and process also contains the sensitivity label of the object or process. Processes get a security context from the user that initiated them. On every access of a process to a protected resource the TOE will evaluate the sensitivity labels of the subject and the object and check if access is allowed according to the rules of the mandatory access control.
- 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 user identity and user role.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: competence and trustworthiness of TOE administration, handling of authentication data, procedures for secure installation, physical safety the TOE, protection of information by users, preventative maintenance, security of recovery procedures, secure configuration to prevent installation of insecure software, procedures for serial login devices, hardware measures to protect TSF and TSF data, secure connections between servers. Details can be found in the Security Target [6] chapter 4.2.

5 Architectural Information

General overview

Oracle Enterprise Linux 5 (OEL5) Update 1 is a general-purpose, multi-user, multi-tasking Linux based operating systems. 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 OEL5. The hardware platforms selected for the evaluation consist of machines which are available when the evaluation has completed and are intended to remain available for a substantial period of time afterwards.

The TOE Security Functions (TSF) consist of functions of OEL5 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 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 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. In addition, the IPSec mechanism and the CIPSO implementation are used to provide labeled networking.
- **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.

- **SELinux Subsystem**
  The SELinux subsystem provides the framework for enforcing a loadable policy for various access control checks. The TOE provides a policy providing the ruleset for multi-level security and for role-based access control.
- **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. In addition, the printing support provided by CUPS is implemented as network application.
- **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 processed 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 processed 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.
- **Mandatory Access Control**
  Mandatory access control (MAC) restricts access to file system objects, IPC objects and network objects based on labels attached to those objects as part of their security context managed by SELinux. The label is compared to the security label of the subject that attempts to access/use the object. The mandatory access control includes a fixed set of rules based on the labels of the subject and the object and the type of access attempted that determine if the subject may access the object in the attempted way. Mandatory access control checks are performed in addition to the discretionary access control checks and access is granted only if access is granted by both the mandatory and the discretionary access control policies.
- **Role-based Access Control**
  Roles in the TOE are defined via types and access to types. A “type” is a security attribute given to an object or a process. The type of a process is commonly called a “domain”. Policy rules define how domains may interact with objects and with other domains.
  Roles can be assigned to users and define which user can have access to which domain. A user may have several roles assigned to him but will always act in one role only. To change from his current role to another role that has been assigned to him he needs to use the newrole command which requires re-authentication. This prohibits that the user’s role is changed by a malicious program without the user knowing this. In addition the transition between roles may be restricted by the policy.
  The TOE has a hierarchical set of roles defined in the policy.
- **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, are 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 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

Report on the developer testing effort

Test configuration

The test results provided by the sponsor were generated on the following systems:

- Dell PowerEdge 1850 (Intel Xeon EM64T based system)
- HP ProLiant DL380 G5 (Intel Xeon EM64T based system)
- OVM guest on HP ProLiant DL380 G5 without paravirtualized I/O drivers
- OVM guest on HP ProLiant DL380 G5 with paravirtualized I/O drivers

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 [12].

Each test system was installed with OEL5 U1 to perform independent test runs on the operating system.

Testing approach

The Test Plan provided by the sponsor lists test cases by groups, which reflects the mix of sources for the test cases. The mapping provided lists the TSF/TSFI the test cases are associated with. The Test Plan is focused on the security functions of the TOE and ignores other aspects typically found in developer test plans. The test cases are mapped to the corresponding Functional Specification and HLD. The developer uses several test suites that are integrated into one test bucket, which includes automatic and manual tests to test the TOE.

Test depth

In addition to the mapping to the functional specification, the sponsor provided a mapping of test cases to subsystems of the high level design and the internal interfaces described in the high level design. This mapping shows that all subsystems and the internal interfaces are covered by test cases.

Testing results

All test results from all tested platforms show that the expected test results are identical to the actual test results, considering the expected failures stated in the developer's test plan.

Report on the 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, 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:

- OVM guest on HP ProLiant DL380 G5
  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 and depth

The evaluator joined the developer during his testing and observed the steps for executing the testing. Also, the evaluator saw the test cases running. The evaluator testing effort consists of two parts. The first one is the re-run of the developer test cases and the second is the execution of the tests created by the evaluator.

For devising a test subset, the evaluator considered the following issues identified during other phases of the evaluation:

- The evaluator test cases examine some TOE functionality in more detail than the test cases provided by the sponsor (such as object reuse, password quality, DAC enforcement).
- Evaluator test cases cover aspects which are not included in the developer testing (ACL support verification in the backup tool, DAC enforcement on file descriptors).

- The developer tests cover already a very large set of functionality with a large number of different permutations of input values. Therefore, the evaluator testing is rather small. Moreover, the evaluator concentrated on source code analysis as outlined in the evaluation report on low-level design and implementation representation as well as in the evaluation report on vulnerability analysis to validate the functionality of the system.

Testing results

All the test results conformed to 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 and analysis of the TOE source code.

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

This certification covers the following configurations of the TOE:

The TOE configuration covers one or more systems running Oracle Enterprise Linux, networked in a non-hostile network, with a well-managed and non-hostile user community. It is not intended to address the needs of a directly Internet-connected server, or the case where services are to be provided to potentially hostile users.

It can be installed on the following hardware in a physical secure environment:

- Dell PowerEdge 1850 (EM64T)
- HP ProLiant DL380 G5 (EM64T)
- Oracle Virtual Machine (OVM) guest on HP ProLiant DL380 G5 (EM64T)

Only the software listed in chapter 2 of this report is to be installed. The setup procedures described in the guidance [12] have to be followed. The TOE supports the setup modes “CAPP mode” and “LSPP mode”, described in the guidance manual.

9 Results of the Evaluation

9.1 CC specific results

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

The Evaluation Methodology CEM [2] was used for those components up to EAL4 [4] (AIS 34).

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

- All components of the class ASE
- All components of the EAL4 package as defined in the CC (see also part C of this report)

- The components ALC_FLR.3 - Systematic flaw remidiation augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0427-2007, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was mainly on the updated version of the TOE and the requirements resulting from the LSPP conformance.

The evaluation has confirmed:

- PP Conformance: Controlled Access Protection Profile (CAPP) Version 1.d Information Systems Security Organization and Labeled Security Protection Profile (LSPP) Version 1.b Information Systems Security Organisation [9], [10]
- for the Functionality: PP conformant plus product specific extensions; Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3
- The following TOE Security Function fulfils the claimed Strength of Function: medium IA.1 (Common Authentication Mechanism)

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 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 TOE Security Function SC.1 (Secure Protocols, using RSA, RC4, 3DES, AES) and
- for other usage of encryption and decryption within the TOE.

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, the additional packages have to be installed as stated in chapter 2.

To ensure the proper operation of the TOE, administrators and users must not create directories with the SGID bit set which allow other users not being a member of the owning group of the directory to write into it.

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

CAPP Controlled Access Protection Profile

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

EAL Evaluation Assurance Level

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

LSPP Labeled Security Protection Profile

PP Protection Profile

RPM RPM Package Manager

SF Security Function

SFP Security Function Policy

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

Package - An (RPM) package is an archive file containing software and additional data for its installation.

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

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

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

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

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

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

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

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

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

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

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

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

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

13 Bibliography

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

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

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

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

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

[6] Security Target BSI-DSZ-0481-2008, Version 1.6, 19 September 2008, Oracle Enterprise Linux Version 5 Update 1 Security Target for CAPP and LSPP Compliance

[7] Evaluation Technical Report, Release 3, 10 October 2008, Evaluation Technical Report Oracle Enterprise Linux 5 Update 1, atsec information security GmbH (confidential document)

[8] Configuration list for the TOE, 7 July 2008, SVN logs for EL 5.1 x86-64 security evaluation (confidential document)

[9] Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999, developed by: Information Systems Security Organisation, National Security Agency

[10] Labeled Security Protection Profile (LSPP), Version 1.b, 8 October 1999, developed by: Information Systems Security Organisation, National Security Agency

[11] Certification Report BSI-DSZ-CC-0427-2007 Oracle Enterprise Linux Version 4 Update 4, 19 July 2007

[12] Guidance documentation for the TOE, V2.3, 1 July 2008, Common Criteria LSPP EAL4+ Evaluated Configuration Guide for Oracle Enterprise Linux 5 Update 1

[8] specifically

- AIS 14, Version 1, 2 April 2007, Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC
- AIS19, Version 1, 2 April 2007, Gliederung des ETR
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

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

plus one of the following:

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

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

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

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

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

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

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

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

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

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

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.