Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0371-2006

for

SUSE Linux Enterprise Server V 8
with Service Pack 3

from

SUSE Linux Products GmbH

sponsored by

IBM Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-5455, Infoline +49 228 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0371-2006

SUSE Linux Enterprise Server V 8 with Service Pack 3

from

SUSE Linux Products GmbH

sponsored by

IBM Corporation

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, Part 1 Version 0.6*, *Part 2 Version 1.0* extended by CEM supplementation "ALC_FLR – Flaw remediation" for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

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** **EAL3 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, 06th June 2006

The President of the Federal Office
for Information Security

IT Security Certified

Hange L.S. SOGIS-MRA

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, Infoline +49 (0)3018 9582-111, Telefax +49 (0)3018 9582-455

The rating of the strength of functions does not include the cryptographic algorithms 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 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- CEM supplementation on “ALC_FLR – Flaw remediation”, Version 1.1, February 2002

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

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 7 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 22nd September 2000 in the Bundesanzeiger p. 19445

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 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of 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 levels (EAL 1 – EAL 7).

2.2 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 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

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 SUSE Linux Enterprise Server V 8 with Service Pack 3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0327-2005.

The evaluation of the product SUSE Linux Enterprise Server V 8 with Service Pack 3 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor is:

IBM Italia, Communications Sector
Responsabile Relazioni Commerciali- Account Manager
Via Sciangai 53, 00144 Rome - Italy

The vendor and distributor is:

SUSE Linux Products GmbH
Maxfeldstraße 5
90409 Nuernberg, Germany

The certification is concluded with

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

This work was completed by the BSI on 06.06.2006.

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-42.

The product SUSE Linux Enterprise Server V 8 with Service Pack 3 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] SUSE Linux Products GmbH
Maxfeldstraße 5
90409 Nuernberg, Germany

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 SUSE Linux Enterprise Server V 8 with Service Pack 3 (also named SLES in short).

It is a general purpose, multi-user, multitasking Linux based operating system. It provides a platform for a variety of applications in the governmental and commercial environment. SLES is available on a broad range of computer systems, ranging from departmental servers to multi-processor enterprise servers. The SLES evaluation covers a potentially distributed, but closed network of IBM xSeries servers running the evaluated version of SLES.

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 IBM xSeries x346 platform. For a detailed description of the systems the tests were performed on, please refer to chapter 7 of this report.

The product SUSE Linux Enterprise Server V 8 is delivered by SUSE Linux Products GmbH on a CD-ROM or DVD. In addition to the software delivered on CD-ROM/DVD the Service Pack 3, Release Candidate 4 (RC4) and additional packages have to be installed. The ISO images of the service pack and the additional packages can be downloaded from the SUSE ftp-server.

During the installation process the user has to verify the integrity and authenticity of the downloaded software as described in the Security Guide [10]. The base software installed from the CD/DVD allows the user to perform this verification by checking the digital signatures of the ISO images and the additional packages.

For a precise listing of packages making up the TOE please refer either to chapter 2.3 of the Security Target [7] or 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 TOE Security Functional Requirements (SFR) used in the Security Target are Common Criteria Part 2 extended as shown in the following table:

Security Functional Requirement	Identifier
SFRs from CC Part 2, contained in CAPP	
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	Protected Audit Trail Storage
FAU_STG.3	Action in Case of Possible Audit Data Loss
FAU_STG.4	Prevention of Audit Data Loss
FDP_ACC.1	Discretionary Access Control Policy
FDP_ACF.1	Discretionary Access Control Functions
FDP_RIP.2	Full Residual Information Protection
FIA_ATD.1	User Attribute Definition
FIA_SOS.1	Verification of Secrets
FIA_UAU.7	Protected Authentication Feedback
FIA_USB.1	User-Subject Binding
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of TSF Data
FMT_REV.1	Revocation
FMT_SMR.1	Security Roles
FPT_AMT.1	Abstract Machine Testing
FPT_RVM.1	Reference Mediation
FPT_SEP.1	Domain Separation
FPT_STM.1	Reliable Time Stamps

Security Functional Requirement	Identifier
SFRs from CC Part 2, contained in CAPP, substituted by hierarchical higher ones in the ST	
FIA_UAU.2	User Authentication before any Action
FIA_UID.2	User Identification before any Action
SFRs not in CC Part 2 (Part 2 extended), contained in CAPP	
„Note1“ (as in [9], chapter 5.2.4)	Subject Residual Information Protection
SFRs from CC Part 2, not contained in CAPP	
FMT_SMF.1[8]	Specification of Management Functions
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Distribution
FCS_COP.1	Cryptographic Operation
FDP_UCT.1	Basic Data Exchange Confidentiality
FDP_UIT.1	Data Exchange Integrity
FMT_MSA.2	Secure Security Attributes
FTP_ITC.1	Inter-TSF Trusted Channel

Table 1: TOE Security Functional Requirements

Note that some of the SFRs have been iterated in the Security Target. For details on the iteration and the required security functionality please refer to [7], chapter 5.1.

The TOE SUSE Linux Enterprise Server V 8 with Service Pack 3 was evaluated by atsec information security GmbH.

The evaluation was completed on 20.04.2006. The atsec information security GmbH is an evaluation facility (ITSEF)[9] recognised by BSI.

The sponsor is:

IBM Italia, Communications Sector
Responsabile Relazioni Commerciali- Account Manager
Via Sciangai 53, 00144 Rome - Italy

[8] Added because of AIS32, Final Interpretation 065

[9] Information Technology Security Evaluation Facility

The vendor and distributor is:

SUSE Linux Products GmbH
Maxfeldstraße 5
90409 Nuernberg, Germany

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 part C of this report, or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL3+ (Evaluation Assurance Level 3 augmented).

The assurance level is augmented by: ALC_FLR.3 – Systematic flaw remediation. For the evaluation of the CC component ALC_FLR.3 the mutually recognised CEM supplementation “ALC_FLR – Flaw remediation”, Version 1.1, February 2002 ([5]) was used.

1.2 Functionality

The TOE SUSE Linux Enterprise Server V 8 with Service Pack 3 provides the following Security Functions:

Name	Function
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

Name	Function
DA.3	Access Control Lists supported by SLES
DA.4	Discretionary Access Control: IPC Objects
Object Reuse (OR)	
OR.1	Object Reuse: File System Objects
OR.2	Object Reuse: IPC Objects
OR.3	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
TP.6	Internal TOE Protection Mechanisms
TP.7	Testing the TOE Protection Mechanisms

Table 2: TOE Security Functions

Note: Only the acronyms and the titles of the SFs are provided here because they are very granular and almost self-explanatory. Please refer for a precise definition of the SF to the Security Target of the TOE ([7], chapter 6.2)

1.3 Strength of Function

The TOE's strength of function is rated 'SOF-medium' only for the authentication function (IA) using passwords (refer to [7], chapter 6.5).

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

The following threats as defined in [7], chapter 3.2.1 are averted by the TOE:

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.

The TOE has to comply to the following Organisational Security Policies (OSPs) as defined in the Security Target [7], chapter 3.2.3:

P.AUTHORISED_USERS

Only those users who have been authorized to access the information within the system may access the system.

P.NEED_TO_KNOW

The organization must define a discretionary access control policy on a need-to-know basis which can be modeled based on: (i) the owner of the object; and (ii) the identity of the subject attempting the access; and (iii) the implicit and explicit access rights to the object granted to the subject by the object owner or an administrative user.

P.ACCOUNTABILITY

The users of the system shall be held accountable for their actions within the system.

1.5 Special configuration requirements

The configuration requirements for the TOE are defined in chapter 2.4 and subsequent chapters of the Security Target [7] 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 Security Guide [10] and installed accordingly;
- SLES 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 workstation and requires the same physical protection as the workstation;
- The TOE comprises a single server machine (and optional peripherals) running the allowed system software (refer to list of allowed packages). A server running the allowed software is referred to as a “TOE server” in the following. Details on the allowed peripherals can be found in [7], chapter 2.4.2.
- Several TOE servers may be interlinked by a LAN, which may be joined by bridges/routers or by TOE workstations which act as routers / gateways.
- Each TOE server within this network implements its own security policy. No synchronisation function for those policies exists.
- If other systems are connected to the network they need to be configured and managed by the same authority using an appropriate security policy not conflicting with the security policy of the TOE.
- The following file systems are supported: the Ext3 journaling filesystem, the ISO 9660 file system for CD-ROM drives and the process file system, procfs, the devpts virtual file system used to provide pseudo terminal support, the shmfs virtual file system used for nonpersistent memory-backed storage.

Note:

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.

1.6 Assumptions about the operating environment

The following constraints concerning the allowed hardware and peripherals are made in the Security Target (refer to [7], chapter 2.4.2):

Hardware Platform:

IBM xSeries x346 (Intel Xeon based multi processor server)

Peripherals:

All terminals and printers supported by the TOE
(except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces)

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: The peripherals are physical peripherals. Logical partitioning is not supported on the above listed hardware platforms. Excluding hot pluggable devices connected via USB does not exclude all USB devices. USB 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 [7], chapter 3.3:

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 well enough 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.

A.NET_COMP

All network components (like 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.

The following constraints are based on Security Objectives which have to be met by the TOE environment. They are defined in [7], chapter 4.2:

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 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. IBM 3151 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 protocols and if protection against interruption of communication is required, adequate protection in the TOE environment has to be established for all communication links!).

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 is called:

SUSE Linux Enterprise Server V 8
with Service Pack 3

The product SUSE Linux Enterprise Server V 8 is delivered by SUSE Linux Products GmbH on a CD-ROM or DVD. In addition to the software delivered on CD-ROM/DVD the Service Pack 3, Release Candidate 4 (RC4) and additional packages have to be installed. The ISO images of the service pack and the additional packages can be downloaded from the SUSE ftp-server.

During the installation process the user has to verify the integrity and authenticity of the downloaded software as described in the Security Guide [10]. The base software installed from the CD/DVD allows the user to perform this verification by checking the digital signatures of the ISO images and the additional packages.

The following packages (rpm) make up the evaluated version of theTOE:

Package name	Version Number
UnitedLinux-build-key	1.0-23
aaa_base	2003.3.27-78
aaa_skel	2002.10.14-1
acl	2.0.19-88
amtu	0.1-5
ash	0.2-641
at	3.1.8-806
attr	2.4.2-55
attr-devel	2.4.2-55
bash	2.05b-50
bc	1.06-498
binutils	2.12.90.0.15-50
bzip2	1.0.2-51
certification-sles-eal3	1.2-5
cpio	2.5-54
cpp	3.2.2-38
cracklib	2.7-716
cron	3.0.1-839
curl	7.9.8-54
cyrus-sasl	1.5.27-280
db	4.0.14-194
devs	2006.1.10-2
dialog	0.62-618
diffutils	2.8.1-49
e2fsprogs	1.28-30
ed	0.2-611
expect	5.34-192
file	3.37-311
filesystem	2002.9.2-56
fileutils	4.1.11-107
fillup	1.10-32
findutils	4.1.7-435
flex	2.5.4a-48

Package name	Version Number
freetype2	2.0.9-87
gawk	3.1.1-327
gcc	3.2.2-38
gcc-c++	3.2.2-38
gdbm	1.8.0-689
glibc	2.2.5-235
glibc-devel	2.2.5-235
glibc-locale	2.2.5-235
gpg	1.0.7-183
gpm	1.20.1-47
grep	2.5.1-84
groff	1.17.2-403
grub	0.93-407
gzip	1.3-326
hdparm	5.2-33
heimdal-lib	0.4e-207
howtoenh	2002.9.6-6
hwinfo	5.62-1
iproute2	2.4.7-495
iputils	ss020124-457
isapnp	1.26-235
k_smp	2.4.21-306
kbd	1.06-169
kernel-source	2.4.21-306
ksymoops	2.4.5-68
l2h-pngicons	99.2beta8-540
laus	0.1-59
laus-devel	0.1-55
less	376-127
libgcc	3.2.2-54
libstdc++	3.2.2-54
libstdc++-devel	3.2.2-38
libxcrypt	1.1-54
libxml2	2.4.23-117
liby2util	2.6.24-4
lilo	22.3.2-57
logrotate	3.5.9-198
lprng	3.8.12-46
lsb-runtime	1.2-105
lukemftp	1.5-330
m4	1.4o-286
mailx	8.1.1-603
make	3.79.1-407
man	2.3.19deb4.0-712
man-pages	1.53-32
mktemp	1.5-482
modutils	2.4.25-53
ncurses	5.2-402
net-tools	1.60-568
netcat	1.10-612
netcfg	2002.9.4-13
openldap2-client	2.1.4-70
openssh	3.4p1-270
openssl	0.9.6g-132
openssl-devel	0.9.6g-132
pam	0.76-109
pam-laus	0.76-46
pam-modules	2002.8.29-12
parted	1.6.6-40
pciutils	2.1.10-99
pcre	3.9-267
perl	5.8.0-204
permissions	2005.10.20-3
popt	1.6-282

Package name	Version Number
postfix	1.1.12-12
ps	2003.10.7-1
readline	4.3-53
rpm	3.0.6-418
sed	3.02.80-53
sh-utils	2.0-377
shadow	4.0.2-410
sitar	0.7.2-29
sles-admin-x86+x86-64_en	8.1.0.2-5
sles-inst-x86+x86-64_en	8.1.0.2-5
sles-release	8-7
star	1.4.2-2
stunnel	3.14-411
SUSE-build-key	1.0-198
sysconfig	0.23.22-66
syslogd	1.4.1-340
sysvinit	2.82-364
tar	1.13.25-328
tcl	8.4-60
telnet	1.0-306
terminfo	5.2-402
texinfo	4.2-48
textutils	2.1-39
timezone	2.2.5-213
tk	8.4-60
unitedlinux-release	1.0-218
utempter	0.5.2-391
util-linux	2.11u-134
vim	6.1-194
vsftpd	1.1.0-31
w3m	0.3.1-105
wget	1.8.2-233
xinetd	2.3.11-26
xshared	4.2.0-213
yast2	2.6.40-6
yast2-bootloader	2.6.77-2
yast2-core	2.6.56-3
yast2-country	2.6.35-1
yast2-installation	2.6.136-1
yast2-mouse	2.6.21-5
yast2-ncurses	2.6.24-19
yast2-network	2.6.39.1-2
yast2-online-update	2.6.17-59
yast2-packagemanager	2.6.51-49
yast2-packager	2.6.78-0
yast2-pam	2.6.5-64
yast2-runlevel	2.6.16-20
yast2-security	2.6.10-85
yast2-storage	2.6.69-2
yast2-sysconfig	2.6.14-20
yast2-theme-SUSELinux	2.6.8-0
yast2-theme-UnitedLinux	2.6.8-0
yast2-trans-en_US	2.6.7-1
yast2-transfer	2.6.1-149
yast2-update	2.6.23-2
yast2-users	2.6.37-7
yast2-xml	2.6.8-79
zlib	1.1.4-51

Table 3: Packages used in the TOE

The following guidance documents are supplied together with the TOE. The guidance documents have to be followed to ensure an certification conformant operation of the TOE:

- SLES Security Guide [10]
- SUSE Linux Enterprise Server 8. Administration [11]
- SUSE Linux Enterprise Server 8 – Installation Manuals for the individual platforms [12]

Please refer to chapter 6 for a more detailed listing of the guidance documents.

3 Security Policy

The TOE is a Linux based multi-user multi-tasking operating system. The TOE may provide services to several users at the same time. After successful login, the users have access to a general computing environment, allowing the start-up of user applications, issuing user commands at shell level, creating and accessing files. The TOE provides adequate mechanisms to separate the users and protect their data. Privileged commands are restricted to administrative users.

The TOE uses the standard Unix model of normal (unprivileged) users and administrative users that have the capability to get full root privileges.

The TOE is intended to operate in a networked environment with other instantiations of the TOE as well as other well-behaved client systems operating within the same management domain (refer to [7], chapter 6.1.5 for more details). All those systems need to be configured in accordance with a defined common security policy.

The TOE permits processors and attached peripheral and storage devices to be used by multiple users to perform a variety of functions requiring controlled shared access to the data stored on the system. Such installations are typical for workgroup or enterprise computing systems accessed by users local to, or with otherwise protected access to, the computer system.

It is assumed that responsibility for the safeguarding of the data protected by the TOE can be delegated to the TOE users.

All data is under the control of the TOE. The data is stored in named objects, and the TOE can associate with each controlled object a description of the access rights to that object.

All individual users are assigned a unique user identifier within the single host system that forms the TOE. This user identifier is used as the basis for access control decisions. The TOE authenticates the claimed identity of the user before allowing the user to perform any further actions.

The TOE enforces controls such that access to data objects can only take place in accordance with the access restrictions placed on that object by its owner or administrative users. Ownership of named objects may be transferred under the control of the access control policy.

Access rights (e.g. read, write, execute) can be assigned to data objects with respect to subjects (users). Once a subject is granted access to an object, the content of that object may be freely used to influence other objects accessible to this subject.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the personnel assumptions the following usage conditions exist. Refer to [7], chapter 3.3.2 or chapter 1.6 of this report for more details:

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

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 [7], chapter 3.3.1 and 3.3.3 or chapter 1.6 of this report):

- 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 (see also Security Target [7]).

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.

5 Architectural Information

General Overview

SUSE Linux Enterprise Server V 8 with Service Pack 3 (also called SLES in short) is a general purpose, multi-user, multitasking Linux based operating system. It provides a platform for a variety of applications in the governmental and commercial environment. SLES is available on a broad range of computer systems, ranging from departmental servers to multi-processor enterprise servers.

The SLES evaluation covers a potentially distributed, but closed network of IBM servers (xSeries) running the evaluated version of SLES.

The TOE Security Functions (TSF) consist of functions of SLES 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 they are not considered to be part of this TSF.

The TOE includes installation from CDROM and from a local hard disk partition.

The TOE includes standard networking applications, such as ftp and ssh. xinetd is 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.

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 use by calling kernel services via the system call interface). Direct access to the underlying abstract machine (hardware or partitioned environment) 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 includes 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.

This structure is shown in the following figure:

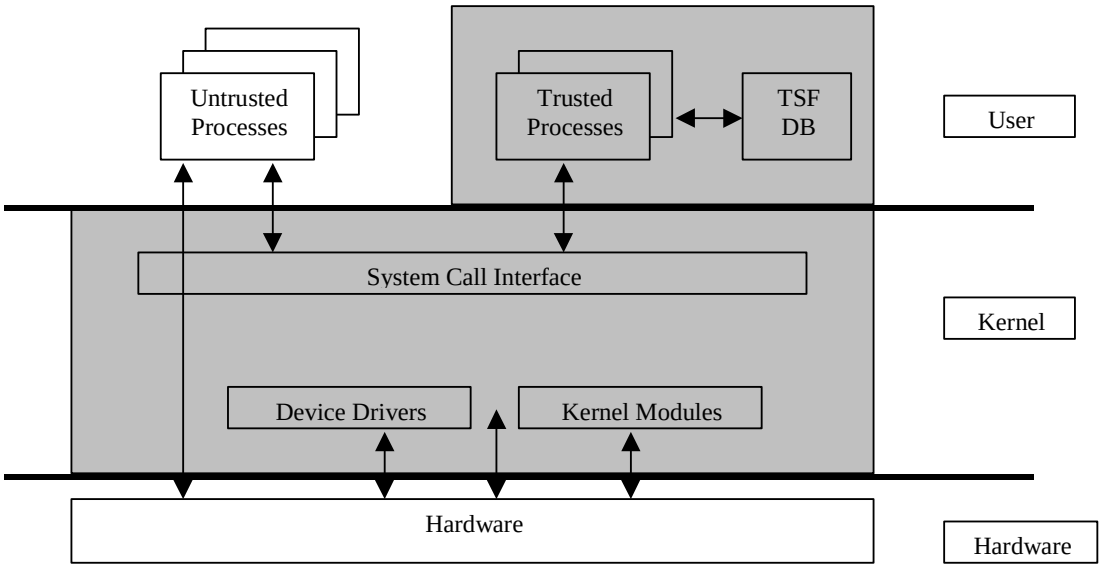

Figure 1: Overall sttructure of the TOE

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
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 synchronise 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
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 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 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 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 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 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 initialisation 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 initialised and in a secure state.

Security Functions

The following security functions of the TOE are defined by the Security Target. Please note that only a short summary for each function is provided here. For a complete description please refer to [7], chapter 6.2:

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 SLES.

Other authentication methods (e. g. Kerberos authentication, token based authentication) that are supported by SLES as pluggable authentication modules are not part of the evaluated configuration.

Functions to 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 a configurable number of audit bin files. When one of those files is full, the TOE switches to the next bin file and starts an administrator defined program to process the audit records in the bin file that just has been filled. The TOE provides a program for this purpose that converts the audit records into a human readable format and writes them to a sequential file or to a printer. The output could also be redirected to a program that transfers the audit records to another machine via a network connection.
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 unauthorised access.
The TOE includes the ext3 file system, which supports POSIX ACLs. This allows you to define 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 SLES 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 unauthorised 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 unauthorised 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:

- SLES Security Guide, Version 2.38, April 3, 2006 [10]
- SUSE Linux Enterprise Server 8. Administration. Books delivered in PDF format as part of the following (platform specific) packages: sles-admin-x86+x86-64_en 8.1.0.2-5 [11]
- SUSE Linux Enterprise Server 8 – Installation Manuals for the individual platforms. Books delivered in PDF format as part of the following package: sles-inst-x86+x86-64_en 8.1.0.2-5 [12]

A full description of the installation and configuration process to get the evaluated configuration of the TOE can be found in [10]. The user will need [11] and [12] just to obtain information on the use of the YaST user interface. All steps required to install and configure the TOE for the evaluated configuration are contained in [10].

7 IT Product Testing

Test configuration

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

- IBM xSeries, model x346

Tests have been performed on the following systems:

- **IBM xSeries model 346**: 2x Intel Xeon 2 GHz with Hyperthreading

The test system has been installed and configured following the information provided in the Security Guide [10] with additional software packages required for the test suite.

Depth/Coverage of Testing

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

Summary of Developer Testing Effort

Test configuration:

The sponsor/developer has performed the tests on the hardware platform defined above. 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. It was argued by the developer's Test Plan that 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 of which the sponsor is a member.

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 had the same machine available as the developer. Test have been carried out on the IBM x346 platform. The machine was conformant to the Security Target requirements and has been set up according to the Security Guide [10].

Testing approach:

Since the this evaluation is a re-evaluation of a previous evaluation of the TOE without changed security functionality the evaluator repeated all automated developer tests on the hardware platform listed above. In addition the evaluator attended the developer testing on all other platforms. Additional tests were defined and executed by the evaluation facility in the following areas:

- Identification & Authentication
- Audit
- Access Control
- TSF Protection
- Object Reuse

Testing results:

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

Evaluator penetration testing:

The evaluators have 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 addressed the following security functions:
- Audit
- Discretionary Access Control

- TSF Protection

with some emphasis on the TSF Protection.

The penetration testing showed the existence of vulnerabilities but none of the vulnerabilities were exploitable in the intended environment of the TOE and/or the attack potential assumed for EAL3 (AVA_VLA.1).

Expansion of the results on other hardware platforms

The Security Target [7] defines the IBM xSeries model x346 with a set of supported peripherals as the hardware base for the TOE.

The IBM xSeries models are multi-processor system using Intel XEON processors with Hyperthreading technology. The tests have been performed only using multi-processor version of the kernel.

8 Evaluated Configuration

According to the Security Target the evaluated configuration of the TOE (as specified in chapter 2 of this report) is defined as follows (refer also to the Security Target [7]):

The TOE “SUSE Linux Enterprise Server V 8 with Service Pack 3” is delivered by SUSE Linux Products GmbH a CD-ROM or DVD and via the internet. In addition to the packages delivered on CD-ROM/DVD (SUSE Linux Enterprise Server 8) the Release Candidate 4 of Service Pack 3 and additional packages (refer to chapter 2 for a complete package listing) have to be downloaded from the SUSE ftp-server. The integrity and authenticity of this software has to be verified during the installation process. The packages (rpm) as specified in chapter 2 make up the evaluated version of the TOE.

The configuration requirements for the TOE are defined in chapter 2.4 and subsequent chapters of the Security Target [7] 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 Security Guide [10] and installed accordingly;
- SLES 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 workstation and requires the same physical protection as the workstation;
- The TOE comprises a single server machine (and optional peripherals) running the allowed system software (refer to list of allowed packages). A server running the allowed software is referred to as a “TOE server” in the following. Details on the allowed peripherals can be found in [7], chapter 2.4.2.
- Several TOE servers may be interlinked by a LAN, which may be joined by bridges/routers or by TOE workstations which act as routers / gateways.
- Each TOE server within this network implements its own security policy. No synchronisation function for those policies exists.

- If other systems are connected to the network they need to be configured and managed by the same authority using an appropriate security policy not conflicting with the security policy of the TOE.
- The following file systems are supported: the Ext3 journaling filesystem, the ISO 9660 file system for CD-ROM drives and the process file system, procfs, the devpts virtual file system used to provide pseudo terminal support, the shmfs virtual file system used for nonpersistent memory-backed storage.

Note:

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.

For setting up / configuring the TOE all guidance documents (refer to chapter 6 of this report) especially document [10] has to be followed.

The following constraints concerning the allowed hardware and peripherals are made in the Security Target (refer to [7], chapter 2.4.2):

Hardware Platform:

IBM xSeries x346 (Intel Xeon based multi processor server)

Peripherals:

All terminals and printers supported by the TOE
(except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces)

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: The peripherals are physical peripherals. Logical partitioning is not supported on the above listed hardware platforms. Excluding hot pluggable devices connected via USB does not exclude all USB devices. USB keyboards and mice may be attached provided they are connected before booting the operating system.

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [8] 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 identical with EAL3. For the component ALC_FLR.3 (Systematic flaw remediation) the CEM supplementation on “ALC_FLR – Flaw remediation”, Version 1.1, February 2002 has been used.

The verdicts for the CC, Part 3 assurance components (according to EAL3 augmented by ALC_FLR.3 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance Classes and Components		**Verdict**
Security Target	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
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and Operation	CC Class ADO	PASS
Delivery Procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.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 remediaton	ALC_FLR.3	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

Assurance Classes and Components		Verdict
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

The current certification is a re-certification of BSI-DSZ-CC-0327-2005. There have been no changes in the security functions of the TOE. Security updates and patches have been applied and a different hardware platform has been used in this certification.

The evaluation has shown that:

- the TOE is conform to the Protection Profile “Controlled Access Protection Profile (CAPP), Issue 1.d, 08.10.1999” [9]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL3 augmented by ALC_FLR.3 Systematic flaw remediation
- The following TOE Security Functions fulfil the claimed Strength of Function: The authentication function (IA) using passwords

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

(i) the security function Secure Communication (SC) and

(ii) Random number generation as part of the security function SC.

The results of the evaluation are only applicable to the SUSE Linux Enterprise Server V 8 with Service Pack 3 in the evaluated configuration (list of packages 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 guidance documents as listed in chapter 6 of this report and the Security Target [7] contain 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 [7] of the Target of Evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

ACL	Access Control List
AMD	Advanced Micro Devices, Inc.
AU	Audit
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria for IT Security Evaluation
CCRA	Common Criteria Recognition Arrangement
DA/DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
HTTP	Hyper Text Transfer Protocol
IA	Identification and Authentication
IPC	Interprocess Communication
ISO	International Organisation for Standardisation
IEEE	Institute of Electrical & Electronics Engineers
IT	Information Technology
LTP	Linux Test Project
OSP	Organisational Security Policy
OR	Object Reuse
PAM	Password authentication module
PCMCIA	Personal Computer Memory Card International Association
PP	Protection Profile
RPM	Red Hat Package Manager
SC	Secure Communication
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SM	Security Management
SLES	SUSE Linux Enterprise Server
SSH	Secure Shell

SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TP	TSF Protection
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TST	TST mode of the DEP/PCI
USB	Universal Serial Bus
YaST	Yet Another Setup Tool

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 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

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

[5] Applicaton Notes and Interpretations of the Scheme AIS33, Version 2 – “Methodologie zur Fehlerbehebung – Flaw Remediation”, 26.07.2002

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

[7] Security Target BSI-DSZ-CC-0371, Version 2.11, 31.03.2006, SUSE Linux Enterprise Server V 8 with Service Pack 3 Security Target for CAPP Compliance, SUSE Linux Products GmbH, IBM Corporation

[8] Evaluation Technical Report BSI-DSZ-CC-0371, Version 2.0, 19.04.2006, atsec information security GmbH (confidential document)

[9] Controlled Access Protection Profile (CAPP), Version 1.d National Security Agency, 1999-10-08

User Guidance Documentation:

[10] SLES Security Guide, Version 2.38, April 3, 2006

[11] SUSE Linux Enterprise Server 8. Administration. Books delivered in PDF format as part of the following (platform specific) packages: sles-admin-x86+x86-64_en 8.1.0.2-5 (for xSeries)

[12] SUSE Linux Enterprise Server 8 – Installation Manuals for the individual platforms. Books delivered in PDF format as part of the following package: sles-inst-x86+x86-64_en 8.1.0.2-5

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class 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
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	MiSUSE	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 4: Assurance family breakdown and mapping

Evaluation assurance levels (chapter 6)

„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 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 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in chapter 2 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 CC 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 5: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„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 6.2.2)

„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 6.2.3)

„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 6.2.4)

„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 6.2.5)

„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 6.2.6)

„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 6.2.7)

„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 14.3)

AVA_SOF Strength of TOE security functions

„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 14.4)

AVA_VLA Vulnerability analysis

„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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

This page is intentionally left blank.