Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0194-2002

for

AIX 5L for POWER V5.2
Program Number 5765-E62

from

IBM Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0194-2002

AIX 5L for POWER V5.2

Program Number 5765-E62

from

IBM Corporation

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an recognised 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", Version 1.1, February 2002 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)*.

Evaluation Results:

PP Conformance:	**Controlled Access Protection Profile, Issue 1.d, 8 October 1999**
Functionality:	**Controlled Access Protection Profile conformant plus product specific extensions** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 augmented by** ALC_FLR.1 (Life cycle support - Basic 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 Bundesamt für Sicherheit in der Informationstechnik 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, 04. November 2002

The Vice President of the Bundesamt für
Sicherheit in der Informationstechnik

IT Security Certified

SOGIS-MRA

Hange

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

This certificate is not an endorsement of the IT product by the Bundesamt für Sicherheit in der Informationstechnik or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by Bundesamt für Sicherheit in der Informationstechnik 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 Bundesamt für Sicherheit in der Informationstechnik (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 Bundesamt für Sicherheit in der Informationstechnik (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)

---

[2] Act setting up the Bundesamt für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Bundesamt für Sicherheit in der Informationstechnik (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 29th October 1992, Bundesgesetzblatt I p. 1838

[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 based on the CC 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.

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 AIX 5L for POWER V5.2 Program Number 5765-E62 has undergone the certification procedure at BSI.

The evaluation of the product AIX 5L for POWER V5.2 Program Number 5765-E62 was conducted by atsec Information Security GmbH which is an evaluation facility recognised by BSI (ITSEF)[6].

The sponsor is:

IBM Deutschland GmbH
Pascal Straße 100
70569 Stuttgart.

The developer is:

IBM Corporation, Austin
11400 Burnet Road
Austin, TX 78758
USA.

The certification is concluded with

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

This work was completed by the BSI on 17 October 2002.

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-34.

The product AIX 5L for POWER V5.2 Program Number 5765-E62 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 0228/9582-111.

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

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 AIX 5L for POWER V5.2 Program Number 5765-E62 (also named AIX, Version 5.2 in short). It is a UNIX-based Operating System which has been developed to meet the requirements of the Controlled Access Protection Profile (CAPP), Issue 1.d, 8 October 1999. By being compliant to the CAPP the TOE fulfils the requirements of the C2 class of the U.S. Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) (see [9], chapter 1.2). This includes the fulfilment of the requirements for Identification and Authentication, Audit, Object Reuse and Access Control including the use of Access Control Lists.

The TOE can be used on one or more servers running the evaluated version of AIX which are connected to form a distributed system. The communication aspects used for this connection are also part of the evaluation. The communication links themselves are protected against interception and manipulation by measures which are outside the scope of the evaluation.

The TOE and a various set of user guidance for the TOE is delivered on CD-ROM (for details refer to chapter 6 of this report). The following Licensed Product Packages (LPPs) are allowed to be used for the evaluated configuration of the TOE:

LPP Name	Description
bos	AIX Base Operating System
devices	AIX supported devices
sysmgt	System management tools.
Adobe	Formats PDF files for on-screen viewing in an X-Window display.
Java	Various libraries, commands and classes associated with Java.
Netscape	Netscape browser and other client applications
X11	X-Windows server, libraries and applications

The TOE uses the following hardware:

- IBM pSeries Systems using Power3-II CPUs (p610)
- IBM pSeries Systems using RS 64 (III or IV) CPUs (p660)
- IBM pSeries Symmetric Multiprocessor (SMP) Systems, using Power4 CPUs (p690)

The hardware is not part of the TOE but supports TSF by providing a separation mechanism. The BootPROM firmware is not part of the TOE either.

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	Guarantees of Audit Data Availability
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	Object Residual Information Protection
FIA_ATD.1	User Attribute Definition
FIA_SOS.1	Strength of Authentication Data
FIA_UAU.7	Protected Authentication Feedback
FIA_USB.1	User-Subject Binding
FMT_MSA.1	Management of Object Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of the Audit Trail
FMT_MTD.1	Management of Audited Events
FMT_MTD.1	Management of User Attributes
FMT_MTD.1	Management of Authentication Data
FMT_REV.1	Revocation of User Attributes
FMT_REV.1	Revocation of Object Attributes
FMT_SMR.1	Security Management Roles
FPT_AMT.1	Abstract Machine Testing
FPT_RVM.1	Reference Mediation
FPT_SEP.1	Domain Separation
FPT_STM.1	Reliable Time Stamps
SFRs from CC Part 2, contained in CAPP, substituted by hierarchical higher ones in the ST	
FIA_UAU.2	Authentication
FIA_UID.2	Identification

Security Functional Requirement	Identifier
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[7]	Specification of Management Functions

The TOE AIX, Version 5.2 was evaluated by:

atsec Information Security GmbH
Steinstraße 68
D-81667 München.

The evaluation was completed on 17 October 2002. The atsec Information Security GmbH is an evaluation facility recognised by BSI (ITSEF)[8].

The sponsor is:

IBM Deutschland GmbH
Pascal Straße 100
70569 Stuttgart

The developer is:

IBM Corporation, Austin
11400 Burnet Road
Austin, TX 78758
USA

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 EAL4+ (Evaluation Assurance Level 4 augmented). The assurance level 4 is augmented by: ALC_FLR.1 – Basic Flaw Remediation. For the evaluation of the CC component ALC_FLR.1 the mutually regognised CEM supplementation “ALC_FLR – Flaw remediation”, Version 1.1, February 2002 ([5]) had been used.

---

[7] Added because of AIS32, Final Interpretation 065

[8] Information Technology Security Evaluation Facility

The evaluation assurance level named in the Protection Profile is EAL3 with no augmentation. The Security Target of the TOE claims an evaluation assurance level of EAL4 augmented by ALC_FLR.1. Since EAL4 is hierarchical to EAL3 conformance to the assurance requirements of the Protection Profile is given.

1.2 Functionality

The TOE AIX, Version 5.2 provides the following Security Functions:

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

IA.6 – Logoff Processing

Auditing (AU)

AU.1 – Audit Record Format

AU.2 – Audit Record Generation

AU.3 – Audit Record Processing

AU.4 – Audit Review

AU.5 – Audit File Protection

AU.6 – Audit Record Loss Prevention

Discretionary Access Control (DA)

DA.1 – Permission Bits

DA.2 – Extended Permissions

DA.3 – Discretionary Access Control: File System Objects

DA.4 – Discretionary Access Control: TCP Connections

DA.5 – 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: Queuing System Objects

OR.4 – Object Reuse: Miscellaneous Objects

Security Management (SM)

SM.1 – Roles

SM.2 – Audit Configuration and Management

SM.3 – Access Control Configuration and Management

SM.4 – Management of User, Group and Authentication Data

SM.5 – Time Management

TSF Protection (TP)

TP.1 – TSF Invocation Guarantees

TP.2 – Kernel

TP.3 – Kernel Extensions

TP.4 – Trusted Processes

TP.5 – TSF Databases

TP.6 – Internal TOE Protection Mechanisms

TP.7 – Diagnosis

Only the titles of the SF are provided here because they are very granular and almost self-explanatory. Please refer for a precise definition and description of the SF to the TOE Summary Specification of the Security Target ([7], chapter 6)

1.3 Strength of Function

The TOE's strength of functions is rated 'medium' (SOF-medium) for the identification and authentication function **IA.1** (refer to Security Target [7], chapter 6.5).

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

Since the Security Target claims conformance to the CAPP, the OSPs defined there (refer to [9], chapter 3.2) are applied for the TOE as well.

Because all security objectives of the CAPP are derived from OSPs, no specific threats have been defined in the Protection Profile. In addition to the PP, the Security Target adds the following threats T.UAUSER (impersonation of an attacker as authorised user), T.UAACCESS (access to information by an unauthorised user) and T.UAACTION (attacker performing unauthorised actions) which are averted by the TOE (for detailed information on additional threats please refer to Security Target [7], chapter 3.2.1). Note that also threats to be averted by the TOEs environment have been defined (refer to Security Target [7], chapter 3.2.2).

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 (for the complete information please refer to the Security Target):

- The CC evaluated file set must be selected at install time.
- If a windowing environment is to be used, the CDE file set must be selected at install time.
- The role based system administration features of AIX 5.2 are not included.
- AIX 5.2 supports the use of IPv4 and IPv6, only IPv4 is included in the evaluated configuration .
- Only 64 bit architectures are included.
- Web Based Systems Management (WebSM) is not included.
- Both network (NIM, Network Install Manager) and CD installations are supported.
- The default configuration for identification and authentication is to be used only. Support for other authentication options e.g. smartcard authentication, is not included in the evaluated configuration.
- If the system console is used, it must be connected directly to the workstation and the same physical protection as for the workstation is needed.
- More than one server machine (running AIX 5.2 in the evaluated configuration) can be used. If more than one so called TOE server is used they are linked by LAN which may be joined by bridges/routers or TOE server acting as routers/gateways. No other systems may be connected to the network.
- Support of the following files systems: AIX journaling file system (jfs2), network file system (nfs v3), file system for CD-ROM drives (*cdrfsisof*s) and the process file system (procfs)

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 pSeries Systems using Power3-II CPUs (p610)
- IBM pSeries Systems using RS 64 (III or IV) CPUs (p660)
- IBM pSeries Symmetric Multiprocessor (SMP) Systems, using Power4 CPUs (p690)

Peripherals:

- all terminals and printers supported by the TOE
- all storage devices and backup devices supported by the TOE (hard disks, CD-ROM drives,streamer drives, floppy disk drives)
- all Ethernet and Token-Ring network adapters supported by the TOE (supporting TCP/IP services over the TCP/IP protocol stack)
- all printer devices supported by the TOE

Since the Security Target claims conformance to the CAPP Protection Profile, the assumptions defined there on physical, personnel and connectivity aspects are also valid for the TOE (refer to [9], chapter 3.3). Additionally the Security Target defines the assumptions A.UTRAIN and A.UTRUST (which are both personnel assumption) and the assumption A.NET_COMP (concerned with connectivity aspects). For a detailed description refer to the Security Target [7], chapter 3.4.2 and 3.4.3.

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 Bundesamt für Sicherheit in der Informationstechnik (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:

AIX 5L for POWER V5.2
Program Number 5765-E62

The TOE documentation is supplied on CD-ROM (see chapter 14 of this report documents [10] to [30]). The documents [24] (Release Notes) and [25] (Security Guide) are used as a starting point for an evaluation conformant usage of the TOE.

The following table contains a list of Licensed Product Packages (LPPs) / File Sets which are allowed to be installed in the evaluated configuration of the TOE:

LPP Name	Description
bos	AIX Base Operating System
devices	AIX supported devices
sysmgt	System management tools.
Adobe	Formats PDF files for on-screen viewing in an X-Window display.
Java	Various libraries, commands and classes associated with Java.
Netscape	Netscape browser and other client applications
X11	X-Windows server, libraries and applications

3 Security Policy

The TOE is a UNIX based multi-user multi-tasking operating system, thus providing service 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 the system administrator role (root).

The TOE provides facilities for on-line interaction with users. Networking is covered only to the extent to which the TOE can be considered to be part of a centrally-managed system that meets a common set of security requirements (refer to the Security Target [7] for the constraints).

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. This user identifier supports individual accountability. 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 other suitably authorised user. 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.

A detailed description/definition of the Security Policy enforced by the TOE is given in the Security Target [7] and with even more detail in the developer document of the security policy model.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the Organisational Security Policies to which the TOE complies the following usage assumptions arise:

- Only those users who have been authorised to access the information within the system may access the system (P.AUTHORIZED_-USERS).
- Implicit and explicit access rights to an object are granted by the object owner (P.NEED_TO_KNOW).
- The users of the system shall be held accountable for their actions within the system (P.ACCOUNTABLE).

Based on the personnel assumptions the following usage conditions consist:

- The TOE and the security of information have to be managed by one or more competent individuals (A.MANAGE).
- The system administrative personnel are not careless, malicious and abide the instruction provided by the TOE documentation (A.NO_EVIL_ADMIN).
- TOE users are expected to act in a co-operating manner in a benign environment (A.COOP).
- TOE users are trained well enough to be able to use the security functionality appropriately (A.UTRAIN).
- TOE users are trusted to some task or group of tasks within a secure IT environment by exercising complete control over their data (A.UTRUST).

For a detailed description of the usage assumptions refer to the Security Target [7], especially chapter 3.3 and 3.4

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 3.4.1 and 3.4.2):

- It is assumed that the processing resources of the TOE are located within controlled access facilities which will prevent unauthorised physical access (A.LOCATE).

- It is assumed that TOE hardware and software (critical to security policy enforcement) is protected from unauthorised physical modification (A.PROTECT).
- All network components (like bridges and routers) are assumed to correctly pass data without modification (A.NET_COMP).
- Any other system with which the TOE communicates is assumed to be under the same management control and operates under the same security policy constraints. There are no security requirements which address the need to trust external systems or the communication links to such systems (A.PEER).
- It is assumed that all connections to peripheral devices and all network connections reside within the controlled access facilities. Internal communication paths to access points such as terminals or other systems are assumed to be adequately protected (A.CONNECT).

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

4.3 Clarification of scope

The threats listed below have to be averted in order to support the TOE security capabilities but are not addressed by the TOE itself. They have to be addressed by the operating environment of the TOE (for detailed information about the threats and how the environment may cover them refer to the Security Target [7]).

- A unprivileged user or the privileged system administrator is losing stored data due to hardware malfunction (TE.HWMF).
- Security enforcing or relevant files of the TOE are manipulated or accidentally corrupted without the system administrator being able to detect this (TE.COR_FILE).
- The underlying hardware functions of the hardware the TOE is running on does not provide sufficient capabilities to support the self-protection of the TSF from unauthorised programs (TE.HW_SEP).

5 Architectural Information

General Overview:

The target of evaluation (TOE) is the operating system AIX Version 5.2. AIX is a general purpose, multi-user, multi-tasking operating system. It is compliant with all major international standards for UNIX systems, such as the POSIX standards, X/Open XPG 4, Spec 1170, and FIPS Pub 180. It provides a platform for a variety of applications in the governmental and commercial environment. AIX is available on a broad range of computer systems from IBM, ranging from departmental servers to multi-processor enterprise servers.

The evaluated configuration of AIX 5.2 consist of a distributed, closed network of high-end, mid-range and low-end IBM pSeries servers running the TOE. The servers may be either a p610, p660 or p690 system with hardware components as defined in the Security Target.

The network links and cabling are assumed to be physically protected against eavesdropping and tampering. All hosts within the network must run the evaluated version of the TOE software and must be configured in accordance with the requirements as described in the AIX Security Guide [25] for the operation of the TOE as CAPP/EAL4 system.

The TOE Security Functions (TSF) consists of those parts of AIX that run in kernel mode plus some defined trusted processes. These together are the functions that enforce the security policy as defined in the Security Target. Tools and commands executed in user mode that are used by the system administrator 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.

The hardware and the BootProm firmware are considered not to be part of the TOE but part of the TOE environment.

The TOE includes installation from CDROM and from the network.

The TOE includes standard networking applications, such as ftp, rlogin, rsh and NFS. Configuration of those network applications has to be performed in accordance with the guidance provided in [25] and [24] for a CAPP/EAL4+ conformant configuration.

The TOE includes the X-Window graphical interface and X-Window applications.

System administration tools include the *smitty* non-graphical system management tool.

The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services, for example the Netscape browser or the Adobe Acrobat Reader to access the supplied online

documentation (which is provided in HTML and PDF formats). No HTTP server is included in the evaluated configuration.

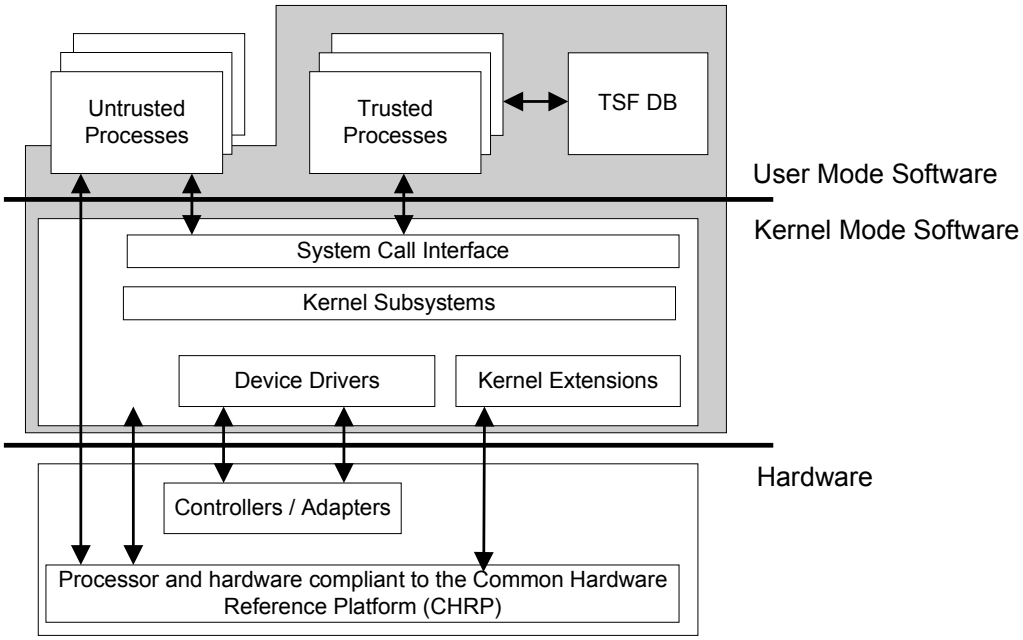
Major structural units of the TOE:

The TOE contains the following structural units:

- The kernel, which executes in system mode
- A set of trusted processes that execute in user mode but with root privileges. They also provide some of the security functions of the TOE.

A set of configuration files that define the system configuration. Those files are named the “TSF database” and need to be protected by the access control mechanisms of the TOE such that they can only be modified by the system administrator. The document [20] provides the detailed specification of those files and also defines the access modes for each file.

The following figure provides a general overview of the TOE with parts in the grey shaded area indicating the parts that implement the TSF:



Security Functions:

The security functions that have been evaluated include (please refer to the Security Target [7] for a complete listing and precise definition):

- **Identification and Authentication.**

  The TOE requires users to authenticate themselves before they can work with the TOE. The mechanism used for authentication is a userid/password combination. The system administrator has a variety of configuration parameter he can use to enforce users to select

passwords that are hard to guess. In addition the system administrator can define the maximum and minimum life-time of passwords.

Users need to authenticate themselves when they log in but also when they change their identity using the su command or when using network applications like rlogin, telnet, ftp. To avoid that normal users can login as root when they for some reason get hold of the password for root, direct login as root is prohibited. A system administrator has to log in under his id using his password and then get root using the su command. Since the use of the su command to get root can be restricted to defined users that act as system administrators, any user without this permission can not log in as root even when he knows the root password.

- **Auditing.**

  The TOE includes the possibility to audit a large number of events. The system administrator can configure which events are audited and is also able to define such events on a per file system object basis, define audit classes and assign them individually to users. This allows for a great flexibility in the configuration of the events that are audited.

  For the minimal set of events to be audited in the evaluated configration refer to the Security Target [7], chapter 5.2.

  The evaluated configuration supports bin mode auditing only.

- **Discretionary Access Control**

  The TOE supports discretionary access control for three different types of objects:

  - The discretionary access control for file system objects
    The discretionary access control for file system objects in the TOE supports the standard Unix permission bits extended by access control lists that allow the system administrator and the owner of the file system object to allow or restrict the access to the file system object down to the granularity of a single user.
  - The discretionary access control for IPC objects
    The TOE supports discretionary access control based on Unix permission bits for semaphore, shared memory segments and message queues.
  - The discretionary access control for TCP ports
    The TOE includes a unique access control feature for TCP ports allowing the system administrator to restrict the use of TCP ports (binding to this port) to defined users. This feature also allows to define TCP ports with numbers higher than 1024 to be privileged ports (i. e. only a process with root authority can bind to this port).

This feature allows to eliminate some known vulnerabilities for network programs using port numbers higher than 1024.

- **Object Reuse**

  The TOE ensures that objects are cleared before they are reassigned to and reused by other subjects. This applies to memory and file system objects as well as to a number of other objects that could transmit information a user might not want to be transmitted to other users.

- **System management**

  The TOE supports only two roles: System administrator and normal users. Additional privileges that exist within the TOE are not used in the evaluated configuration.

  System management within the TOE is restricted to the system administrator. He may either use the commands provided for system management or the “smitty” tool, which provides a non-graphical interface. The tool will generate scripts using the system management commands.

- **TOE Protection**

  The TOE protects itself from tampering by untrusted subjects in a variety of ways. The kernel operates in its own protected address space, which can not be modified or read by untrusted processes. The kernel also prohibits any direct access of untrusted processes to hardware. All non-kernel processes have to use the system call interface to get access to objects in the file system, inter-process communication objects or network objects. The kernel controls access to those objects based on the access control policy for those objects and the access rights defined for the individual users. There is also a number of system calls where the use is restricted to the system administrator. Other system calls have specific parameters that are restricted to system administrators.

  In addition the TOE uses trusted processes which run with system administrator privileges to implement some of the TOE security functions. Those trusted processes are separated by the kernel from untrusted processes. Also the configuration files used by the TSF are protected by the discretionary access control functions of the TOE from unauthorized access by untrusted users.

6 Documentation

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

[10] "System Management Concepts: Operating System and Devices", version AIX 5L 5.2, as of October 2002 (admconc.pdf)

[11] "Technical Reference: Communications, Volume 1", version AIX 5L 5.2, as of October 2002 (commtrf1.pdf)

[12] "Technical Reference: Communications, Volume 2", version AIX 5L 5.2, as of October 2002 (commtrf2.pdf)

[13] "Commands Reference, Volume 1", version AIX 5L 5.2, as of October 2002 (aixcmds1.pdf)

[14] "Commands Reference, Volume 2", version AIX 5L 5.2, as of October 2002 (aixcmds2.pdf)

[15] "Commands Reference, Volume 3", version AIX 5L 5.2, as of October 2002 (aixcmds3.pdf)

[16] "Commands Reference, Volume 4", version AIX 5L 5.2, as of October 2002 (aixcmds4.pdf)

[17] "Commands Reference, Volume 5", version AIX 5L 5.2, as of October 2002 (aixcmds5.pdf)

[18] "Commands Reference, Volume 6", version AIX 5L 5.2, as of October 2002 (aixcmds6.pdf)

[19] "Understanding the Diagnostic Subsystem for AIX", version AIX 5L 5.2, as of October 2002 (diagunsd.pdf)

[20] "Files Reference", version AIX 5L 5.2, as of October 2002 (aixfiles.pdf)

[21] "General Programming Concepts: Writing and Debugging Programs", version AIX 5L 5.2, as of October 2002 (genprogc.pdf)

[22] "System Management Guide: Operating System and Devices", version AIX 5L 5.2, as of October 2002 (baseadmn.pdf)

[23] "System Management Concepts: Operating Systems and Devices", version AIX 5L 5.2, as of October 2002 (admnconc.pdf)

[24] "AIX 5.2 Release Notes", version AIX 5L 5.2, as of October 2002 (10079300.html)

[25] "Security Guide", version AIX 5L 5.2, as of October 2002 (security.pdf)

[26] "System Management Guide: Communications and Networks", version AIX 5L 5.2, as of October 2002 (commadmn.pdf)

[27] "System User's Guide: Communication and Networks", version AIX 5L 5.2, as of October 2002 (usrcomm.pdf)

[28] "System User's Guide: Operating System and Devices", version AIX 5L 5.2, as of October 2002 (usrosdev.pdf)

[29] "Technical Reference: Base Operating System and Extensions, Volume 1", version AIX 5L 5.2, as of October 2002 (basetrf1.pdf)

[30] "Technical Reference: Base Operating System and Extensions, Volume 2", version AIX 5L 5.2, as of October 2002 (basetrf2.pdf)

The administrator/user is recommended to use the documents:

- "AIX 5.2 Release Notes", version AIX 5L 5.2, as of October 2002 (10079300.html), [24] and
- "Security Guide", version AIX 5L 5.2, as of October 2002 (security.pdf), [25]

as a starting point for an evaluation conformant usage of the TOE.

7 IT Product Testing

Test Schedule

Prior to the final developer and evaluator testing several runs of all test cases on pre-releases of the product have been performed. Those tests have started when the evaluators conducted tests on a p610, p660 and p690 machine at IBM in Austin, Texas. Later on the developers conducted the full tests on the last three pre-releases before the „GOLD“ release to identify remaining potential problems.

The developer and evaluator did a re-run of the tests after the final release of the TOE was available.

Test hardware configuration

The Security Target defines three different machine types for the TOE: p610, p660 and p690.

Tests have been performed on all three machines types using the following hardware configurations:

p610

- 2 POWER3 CPUs
- 8 GB Main Memory
- ISA Bus Diskette Drive
- Wide/Ultra-3 SCSI I/O Controller
- PCI 4-Channel Ultra3 SCSI RAID Adapter
- 5 SCSI disk drives (hdisk0: 18 GB, hdisk1 to hdisk4: 36 GB each, all manufactured by IBM)
- SCSI 4 mm tape drive (20 GB), manufactured by HP
- SCSI DVD-RAM drive, manufactured by IBM
- 3 IBM 10/100 Mbits Ethernet PCI adapter
- 1 IBM PCI Token Ring Adapter
- GXT135P 2D Graphics Adapter, manufactured by Matrox
- PS/2 Keyboard
- Three Button Mouse

p660

- 4 RS64-IV CPUs
- 8 GB Main Memory

- ISA Bus Diskette Drive
- Wide/Ultra-2 SCSI I/O Controller
- 2 LVD SCSI Disk Drive (18200 MB), manufactured by IBM
- 1 SCSI Multimedia CD-ROM Drive, manufactured by IBM
- 1 IBM 10/100 Mbits Ethernet PCI adapter
- Asynchronous Terminal
- Standard I/O Serial Port

p690

- 8 POWER4 CPUs
- 8 GB Main Memory
- ISA Bus Diskette Drive
- Wide/Fast-20 SCSI I/O Controller
- Wide/Ultra-3 SCSI I/O Controller
- USB OHCI Adapter
- 2 LVD SCSI Disk Drive (18200 MB), manufactured by IBM
- 1 SCSI Multimedia CD-ROM Drive, manufactured by IBM
- 1 Gigabit Ethernet-SX PCI Adapter
- IBM 10/100 Mbps Ethernet PCI Adapter
- Asynchronous Terminal
- Standard I/O Serial Port

The detailed hardware configuration for each machine including the version numbers, serial numbers and additional details have been extracted and stored in a log file. These log files have been provided during the evaluation.

Summary of Developer Testing Effort

Test configuration:

All the tests have been performed on the configurations defined above.

Testing approach:

IBM has a large number of different test suites and test cases for each component. Several of the test suites are driven by similar frameworks. This means, the test suite provides some user space application for building (compiling, assembling) executables out of the test case files and executing the test cases. In addition to the user space applications, a library for binary test programs and several functions for shell code test programs are provided by the the testing framework. These functions are invoked by the test cases during their run when the positive or negative result of a test unit is determined.

The test case files of the framework consist of one or more test units, which are the individual tests. One test case is aimed to check one particular security function (although it tests some others indirectly), the test units of one test case in turn check different aspects of a security function. The framework can be used in batch mode or manually. In manual mode, the test case files have to be build and executed one by one by the tester. In batch mode, one user space tool is configured to build and/or execute one or more test case automatically.

Testing results:

The developer performed the testing of the final product on all three platforms (p610, p660 and p690). The developer has installed the TOE in accordance with the guidance provided in [25] and [24] for the CAPP/EAL4 configuration. The results of the tests are that all test cases show the expected behaviour in the evaluated configuration.

Summary of Evaluator Testing Effort

Test configuration

The evaluator performed his test on a p610 system located at the IBM office in Munich as well as on the same systems the developer has used for his testing in Austin.

Testing approach:

The evaluator testing effort consists of two parts. The first one is the complete rerun of the developer test cases and the second is the execution of the tests created by the evaluator.

The testing were carried out at the IBM lab in Austin and at the IBM facility in Munich. The test environment in Austin consisted of a p610, a p660 and a p690 systems connected to each other via Ethernet. In contrast, the IBM facility in Munich provided a p610 and an additional server. The additional server was used to have the p610 being part of a real network while all test cases where executed for the software running on the p610.

The evaluator performed all the developer tests and his own test cases on the TOE he has installed in conformance with the Security Target and the developer's guidance documentation. The evaluator has verified that all test cases produced the results that where expected.

Evaluator penetration testing:

The evaluators have devised a set of penetration tests based on the developer's vulnerability analysis and based on the evaluator's knowledge of the TOE gained by the other evaluation activities. All penetration tests have been designed to require only a low attack potential as defined in AVA_VLA.2. The evaluators conducted those tests and did not find any test that resulted in a successful penetration of the TOE with low attack potential.

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 to Security Target [7]):

General Aspects:

- The CC evaluated file set must be selected at install time (refer to chapter 2 of this report)
- If a windowing environment is to be used, the CDE file set must be selected at install time.
- The role based system administration features of AIX 5.2 are not included.
- AIX 5.2 supports the use of IPv4 and IPv6, only IPv4 is included.
- Only 64 bit architectures are included.
- Web Based Systems Management (WebSM) is not included.
- Both network (NIM, Network Install Manager) and CD installations are supported.
- The default configuration for identification and authentication is to be used only. 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 the same physical protection as for the workstation is needed.

Networking Aspects:

- The TOE can be run on one or more server machines (called „TOE server“ in [7]). If the product is configured with more than one TOE server, they are linked by LANs, which may be joined by bridges/routers or by TOE workstations which act as routers/gateways.
- No other systems may be connected to the network.
- The following file system types are supported:
  - the AIX journaling file system, jfs2;
  - the standard remote file system access protocol, nfs (V3);
  - the High Sierra file system for CD-ROM drives, cdrfsisofs;
  - the process file system, procfs (/proc);

Technical Aspects:

- The TOE is running on the following hardware platforms:
  - IBM pSeries Systems using Power3-II CPUs (p610)
  - IBM pSeries Systems using RS 64 (III or IV) CPUs (p660)
  - IBM pSeries Symmetric Multiprocessor (SMP) Systems, using Power4 CPUs (p690)
- The following peripherals can be run with the TOE:
  - all terminals and printers supported by the TOE
  - all storage devices and backup devices supported by the TOE (hard disks, CD-ROM drives,streamer drives, floppy disk drives)
  - all Ethernet and Token-Ring network adapters supported by the TOE
  - all printer devices supported by the TOE
- Network connectors supported by the TOE (e.g. Ethernet, Token Ring, etc.) supporting TCP/IP services over the TCP/IP protocol stack.

For setting up / configuring the TOE all guidance documents especially the documents [24] and [25] have to be followed (refer to chapter 6 of this report).

Note that LPAR is not a feature in the evaluated configuration of the TOE.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Common Evaluation Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE (this includes especially the methodology for flaw remediation, [5]).

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented by ALC_FLR.1 plus 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
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Problem tracking CM coverage	ACM_SCP.2	PASS
Delivery and Operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS

Assurance Classes and Components		Verdict
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Independent vulnerability analysis	AVA_VLA.2	PASS

The evaluation has shown that the TOE fulfils the claimed strength of function for the authentication function (based on passwords).

The results of the evaluation are only applicable to the product AIX 5L for POWER V5.2 Program Number 5765-E62 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [7] and the chapters 2, 4 and 8 of this report). The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, and if the evaluation of the modified product does not reveal any security deficiencies.

10 Evaluator Comments/Recommendations

The User Guidance documentation (especially [24] and [25]) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [7] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

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

AU	Security Function Auditing
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAPP	Controlled Access Protection Profile
CC	Common Criteria for IT Security Evaluation
CDE	Common Desktop Environment
DA	Security Function Discretionary Access Control
DoD	U.S. Department of Defense
EAL	Evaluation Assurance Level
LAN	Local Area Network
LPAR	Logical partitioning
LPP	Licensed Product Package
IP	Internet Protocol
IA	Security Function Identification and Authentication
IT	Information Technology
OR	Security Function Object Reuse
OSP	Organisational Security Policy
PP	Protection Profile
PROM	Programmable read only memory
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SM	Security Function Security Management
ST	Security Target
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation
TP	TSF Protection

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

13.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, 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-0194, Version 1.2, 2002-09-25, AIX5.2 Security Target, IBM Corporation

[8] Evaluation Technical Report BSI-DSZ-CC-0194, Version 1.3, atsec Security Information GmbH, 17.10.2002 (confidential document)

[9] Controlled Access Protection Profile, Issue 1.d, 8 October 1999, National Security Agency

User Guidance Documentation:

[10] "System Management Concepts: Operating System and Devices", version AIX 5L 5.2, as of October 2002 (admconc.pdf)

[11] "Technical Reference: Communications, Volume 1", version AIX 5L 5.2, as of October 2002 (commtrf1.pdf)

[12] "Technical Reference: Communications, Volume 2", version AIX 5L 5.2, as of October 2002 (commtrf2.pdf)

[13] "Commands Reference, Volume 1", version AIX 5L 5.2, as of October 2002 (aixcmds1.pdf)

[14] "Commands Reference, Volume 2", version AIX 5L 5.2, as of October 2002 (aixcmds2.pdf)

[15] "Commands Reference, Volume 3", version AIX 5L 5.2, as of October 2002 (aixcmds3.pdf)

[16] "Commands Reference, Volume 4", version AIX 5L 5.2, as of October 2002 (aixcmds4.pdf)

[17] "Commands Reference, Volume 5", version AIX 5L 5.2, as of October 2002 (aixcmds5.pdf)

[18] "Commands Reference, Volume 6", version AIX 5L 5.2, as of October 2002 (aixcmds6.pdf)

[19] "Understanding the Diagnostic Subsystem for AIX", version AIX 5L 5.2, as of October 2002 (diagunsd.pdf)

[20] "Files Reference", version AIX 5L 5.2, as of October 2002 (aixfiles.pdf)

[21] "General Programming Concepts: Writing and Debugging Programs", version AIX 5L 5.2, as of October 2002 (genprogc.pdf)

[22] "System Management Guide: Operating System and Devices", version AIX 5L 5.2, as of October 2002 (baseadmn.pdf)

[23] "System Management Concepts: Operating Systems and Devices", version AIX 5L 5.2, as of October 2002 (admnconc.pdf)

[24] "AIX 5.2 Release Notes", version AIX 5L 5.2, as of October 2002 (10079300.html)

[25] "Security Guide", version AIX 5L 5.2, as of October 2002 (security.pdf)

[26] "System Management Guide: Communications and Networks", version AIX 5L 5.2, as of October 2002 (commadmn.pdf)

[27] "System User's Guide: Communication and Networks", version AIX 5L 5.2, as of October 2002 (usrcomm.pdf)

[28] "System User's Guide: Operating System and Devices", version AIX 5L 5.2, as of October 2002 (usrosdev.pdf)

[29] "Technical Reference: Base Operating System and Extensions, Volume 1", version AIX 5L 5.2, as of October 2002 (basetrf1.pdf)

[30] "Technical Reference: Base Operating System and Extensions, Volume 2", version AIX 5L 5.2, as of October 2002 (basetrf2.pdf)

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4)

The pass result of evaluation shall be a statement that describes the extent to which the PP or TOE can be trusted to conform to the requirements. The results shall be caveated with respect to Part 2 (functional requirements), Part 3 (assurance requirements) or directly to a PP, as listed below.

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

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

c) **Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are in the form of an **EAL** or **assurance package** that is based only upon assurance components in Part 3.

d) **Part 3 augmented** - A PP or TOE is Part 3 augmented if the assurance requirements are in the form of an **EAL** or **assurance package**, plus other assurance components in Part 3.

e) **Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements are in the form of an **EAL** associated with additional assurance requirements not in Part 3 or an **assurance package** that includes (or is entirely made up from) assurance requirements not in Part 3.

f) **Conformant to PP** - A TOE is conformant to a PP only if it is compliant with all parts of the PP.“

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 2.1 -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 6.1 - 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.“