Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0303-2006

for

IBM AIX 5L for POWER V5.2
Maintenance Level 5200-05
with Innovative Security Systems PitBull Foundation
5.0

from

IBM Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-455, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0303-2006

IBM AIX 5L for POWER V5.2

Maintenance Level 5200-05
with Innovative Security Systems PitBull Foundation 5.0

from

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", Version 1.1, February 2002 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:	**Labeled Security Protection Profile (LSPP), Issue 1.b, 8 October 1999**
Functionality:	**LSPP conformant (plus product specific extensions)** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 augmented by ALC_FLR.1 – 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 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, 02 May 2006

The President of the Federal Office
for Information Security

Dr. Helmbrecht

L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

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

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

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[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)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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 07 July 1992, Bundesgesetzblatt I p. 1230

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

5 Proclamation of the Bundesministerium des Innern of 22 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 03 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 IBM AIX 5L for POWER V5.2 Maintenance Level 5200-05 with Innovative Security Systems PitBull Foundation 5.0 has undergone the certification procedure at BSI. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0302-2005 were re-used.

The evaluation of the product IBM AIX 5L for POWER V5.2 Maintenance Level 5200-05 with Innovative Security Systems PitBull Foundation 5.0 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and vendor is:

IBM Corporation
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 02 May 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-32.

The product IBM AIX 5L for POWER V5.2 Maintenance Level 5200-05 with Innovative Security Systems PitBull Foundation 5.0 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] IBM Corporation
11400 Burnet Road
Austin, TX 78758, USA

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 IBM AIX 5L for POWER V5.2 Maintenance Level 5200-05 with Innovative Security Systems PitBull Foundation 5.0 (also refered as AIX 5.2I hereafter). It is a UNIX-based Operating System which has been developed to meet the requirements of the Labeled Security Protection Profile (LSPP), Issue 1.b, 8 October 1999.

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.

This evaluation is an initial evaluation, but specific results from the evaluation process based on BSI-DSZ-CC-0302-2005 were re-used.

The TOE and a various set of user guidance for the TOE is delivered on CD-ROM (for details refer to chapters 2 and 6 of this report). The Licensed Product Packages (LPPs) which are allowed to be used for the evaluated configuration of the TOE are specified in [7], chapter 2.3.

The TOE is running on the following, LPAR enabled hardware platforms:

- IBM pSeries Symmetric Multiprocessor (SMP) Systems using Power5 CPUs (p520, p570, p595)

The hardware and LPAR are not part of the TOE but support the TSF by providing separation mechanisms. The BootPROM firmware is not part of the TOE either.

The IT product IBM AIX 5L for POWER V5.2 Maintenance Level 5200-05 with Innovative Security Systems PitBull Foundation 5.0 was evaluated by atsec information security GmbH. The evaluation was completed on 05. April 2006. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor and vendor is

IBM Corporation
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).

[8] Information Technology Security Evaluation Facility

The TOE meets the assurance requirements of assurance level EAL4 (Evaluation Assurance Level 4). 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 ([6]) was used.

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 Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following table (for clearness reasons, iterations are not listed):

Security Functional Requirement	Identifier
SFRs from CC Part 2, contained in LSPP	
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_ETC.1	Export of Unlabeled User Data
FDP_ETC.2	Export of Labeled User Data
FDP_IFC.1	Mandatory Access Control Policy
FDP_IFF.2	Mandatory Access Control Functions
FDP_ITC.1	Import of Unlabeled User Data
FDP_ITC.2	Import of Labeled User Data
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

Security Functional Requirement	Identifier
FMT_MSA.1	Management of Object Security Attributes
FMT_MSA.3	Static Attribute Initialisation
FMT_MTD.1	Management of the Audit Trail
FMT_REV.1	Revocation of User 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 LSPP, substituted by hierarchical higher ones in the ST	
FIA_UAU.2	Authentication
FIA_UID.2	Identification
SFRs not in CC Part 2 (Part 2 extended), contained in LSPP	
„Note1“ (as in [9], chapter 5.2.10)	Subject Residual Information Protection
SFRs from CC Part 2, not contained in LSPP	
FMT_SMF.19	Specification of Management Functions
FPT_TDC.1	Inter-TSF basic TSF Data Consistency
FPT_TST.1	TSF Testing
SFRs, explicitly stated	
FDP_RIP.3-AIX	Hard disk drive residual information protection

Table 1: Security Functional Requirements

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the Security Target [7], chapter 5.2 and 5.5.

9 **Added because of AIS32, Final Interpretation 065**

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

TOE Security Function	Addressed issue
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
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
AU.7	Audit System Privileges
DA.1	Discretionary Access Control: Permission Bits
DA.2	Discretionary Access Control: Extended Permissions
DA.3	Discretionary Access Control: File System Objects
DA.4	Discretionary Access Control: IPC Objects
PV.1	Identification of privileges
PV.2	Process Privilege Sets
PV.3	File Privilege Sets
AZ.1	Authorization Attributes
AZ.2	Process Authorizations
AZ.3	File Authorization Sets
AZ.4	Authorization Checks
AZ.5	Implementation
MAC	Mandatory Access Control
ASN.1	Advanced Secure Networking: Network and interface rules
ASN.2	Advanced Secure Networking: Internet Protocol Security Option
MIC.1	Mandatory Integrity Control: MIC Labels
OR.1	Object Reuse: File System Objects
OR.2	Object Reuse: IPC Objects
OR.3	Object Reuse: Queuing System Objects

TOE Security Function	Addressed issue
OR.4	Object Reuse: Miscellaneous Objects
OR.5	Object Reuse: Hard disk drives
SM.1	Security Management: Roles
SM.2	Security Management: Audit Configuration and Management
SM.3	Security Management: Access Control Configuration and Management
SM.4	Security Management: Management of User, Group and Authentication Data
SM.5	Security Management: Time Management
TP.1	TSF Protection: TSF Invocation Guarantees
TP.2	TSF Protection: Kernel
TP.3	TSF Protection: Kernel Extensions
TP.4	TSF Protection: Trusted Processes
TP.5	TSF Protection: TSF Databases
TP.6	TSF Protection: Internal TOE Protection Mechanisms
TP.7	TSF Protection: Diagnosis
TP.8	TSF Protection: Integrity Checks
TP.9	TSF Protection: File security flags

Table 2: TOE Security Functions

For more details please refer to the Security Target [7], chapter 6.2.

1.3 Strength of Function

The TOE's strength of functions is claimed medium (SOF-medium) for specific functions as indicated in the Security Target [7, chapter 8.4.3].

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

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

Since the Security Target claims conformance to the LSPP, the OSPs defined there (refer to [9], chapter 3.2) are applied for the TOE as well. Because all security objectives of the LSPP are derived from OSPs, no specific threats have been defined in the Protection Profile. In addition to LSPP the following OSPs are defined in the Security Target (see [7], chapter 3.3):

- P.DATAFLOW

- P.ERASE
- P.INTEGRITY
- P.STATIC
- P.TCBINTEGRITY

In addition to the LSPP, 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 and to chapter 4 of this report).

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 system must be installed according to the PitBull Foundation installation guide [21].
- Only the use of IPv4 is included in this evaluation.
- 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.
- Only the default mechanisms for identification and authentication are included. 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 connect directly to the workstation and afforded the same physical protection as the workstation.
- AIX 5.2 provides both a native and a Sys5 print system. Only Sys5 is supported in the evaluated configuration, as it implements the labeling requirements from LSPP.
- System security flags (or, kernel security flags) need to be configured as identified in the Security Target [7], chapter 6.2.12.1).
- The system must be configured to disable remote access for an individual user after five consecutively failed login attempts have occurred for this user.

1.6 Assumptions about the operating environment

The following assumptions about the technical environment the TOE is intended to be used in are made:

Hardware platforms:

- IBM pSeries Symmetric Multiprocessor (SMP) Systems, using Power5 CPUs (p520, p570, p595).

Periphals:

- All terminals supported by the TOE.
- All storage devices and backup devices supported by the TOE (hard disks, CDROM drives, streamer drives, floppy disk drives).
- All printer devices supported by the TOE.
- Network connectors supported by the TOE (e.g., Ethernet) supporting TCP/IP services over the TCP/IP protocol stack.

Since the Security Target claims conformance to LSPP, the assumptions defined there on physical, personnel and connectivity aspects are also valid for the TOE (refer to [9], chapter 3.3). For a detailed description of the usage assumptions, refer to the Security Target [7], chapter 3.4.

1.7 Disclaimers

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

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

IBM AIX 5L for POWER V5.2 Maintenance Level 5200-05 with Innovative Security Systems PitBull Foundation 5.0

The TOE documentation is supplied on CD-ROM (see chapter 6 of this report and documents [10] to [30]). The documents [22] (Security Features User Guide) and [23] (AIX Security Guide) can be used as a starting point for an evaluation conformant usage of the TOE.

The Licensed Product Packages (LPPs) / File Sets which are allowed to be installed in the evaluated configuration of the TOE are defined in the Security Target [7], chapter 2.3.

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 PitBull extension to the standard AIX implements all the various access control mechanisms provided by AIX: DAC, MAC, MIC, TCB, ASN, PV, AZ. This extension consists of a kernel extension for the implementation and enforcement of the access control logic as well as user space tools to manage these mechanisms.

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.ACCOUNTABILITY).
- The TOE is only to be allowed with static LPAR. Dynamic LPAR must not be used (P.STATIC).
- An administrator has to initiate the hard disk erase function of the TOE in order to prevent the recovery of the original information stored on the disk (P.ERASE).

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 3.4.3):

- 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 can 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 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).
- When running in a logical partition, software running in a different partition than the TOE is able to access resources that are assigned to the TOE (TE.LPAR).

For a detailed description of the threats covered by the TOE environment please refer to [7], chapter 3.2.2.

5 Architectural Information

The target of evaluation (TOE) is the operating system IBM AIX 5L for POWER V5.2 Maintenance Level 5200-05 with Innovative Security Systems PitBull Foundation 5.0.

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, 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 with maintenance package 5200-05 consists of a distributed, closed network of high-end, mid-range and low-end IBM pSeries servers running the evaluated version of AIX with maintenance package 5200-05. The servers may be either a p520, p570 or p595 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 configuration resulting from the initial installation the requirements as described in the guidance documentation.

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 [23] for LSPP/EAL4+ conformant configuration.

The TOE does not include 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. No HTTP server is included in the evaluated configuration.

The PitBull extension to the standard AIX implements all the various access control mechanisms provided by AIX: DAC, MAC, MIC, TCB, ASN, PV, AZ. This extension consists of a kernel extension for the implementation and enforcement of the access control logic as well as user space tools to manage these mechanisms.

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 (the “TSF database”).

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

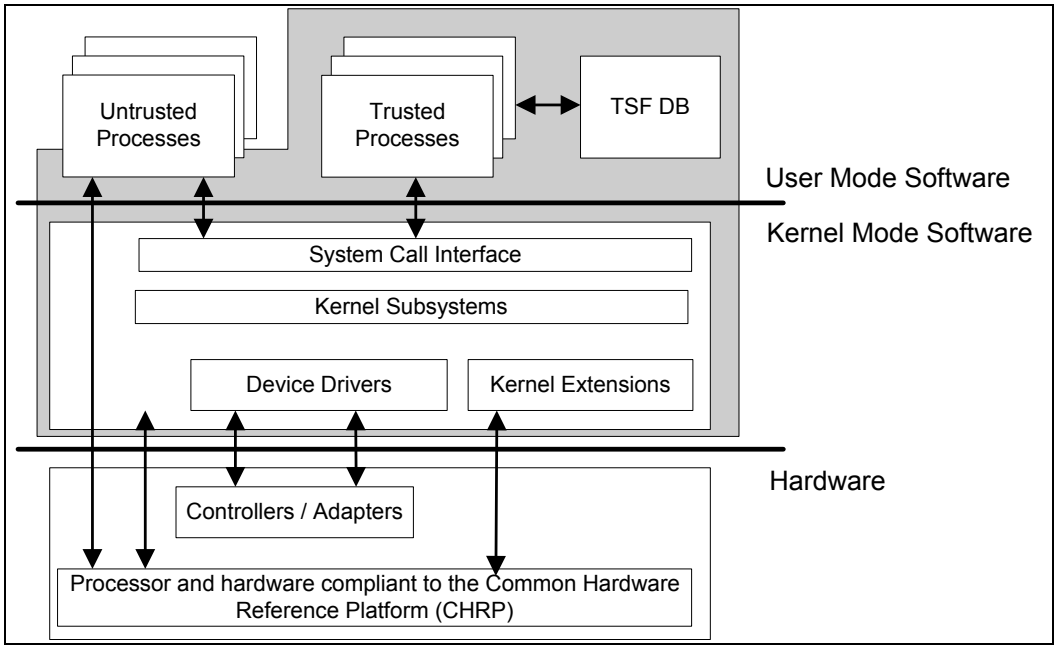

Figure 1: TOE structure

6 Documentation

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

- Technical Reference: Communications, Volume 1", Fourth edition, October 2002 [10]
- "Technical Reference: Communications, Volume 2", Fourth edition, October 2002 [11]
- "Commands Reference, Volume 1", Fifth edition, May 2003 [12]
- "Commands Reference, Volume 2", Fifth edition, May 2003 [13]
- "Commands Reference, Volume 3", Fifth edition, May 2003 [14]
- "Commands Reference, Volume 4", Fifth edition, May 2003 [15]
- "Commands Reference, Volume 5", Fifth edition, May 2003 [16]
- "Commands Reference, Volume 6", Fifth edition, May 2003 [17]
- "Understanding the Diagnostic Subsystem for AIX", Sixth edition, October 2002 [18]
- "Files Reference", Fourth edition, October 2002 [19]
- Common Criteria configuration manual for Foundation on AIX 1.1, December 2005 [20]
- PitBull Foundation and Foundation Suite Installation Guide [21]
- Security Features User Guide [22]
- “AIX 5L Version 5.2 Security Guide”, Fifth edition, May 2004 [23]
- “System User's Guide: Communication and Networks”, Third edition, October 2002 [24]
- “System User's Guide: Operating System and Devices”, Third edition, October 2002 [25]
- "Trusted Facility Manual PitBull Foundation Release 5.0”, Version 1.6 [26]
- "Technical Reference: Base Operating System and Extensions, Volume 1”, Fourth edition, October 2002 [27]
- "Technical Reference: Base Operating System and Extensions, Volume 2”, Fourth edition, October 2002 [28]
- “AIX 5.3 Technical Reference: Base Operating System and Extensions, Volume 1”, Second edition, December 2004 [29]
- “AIX 5.3 Technical Reference: Base Operating System and Extensions, Volume 2”, Second edition, December 2004 [30]

The administrator/user is recommended to use the documents:

- “Security Features User Guide”, March 2005 [22]
- "AIX 5L Version 5.2 Security Guide", Fifth edition, May 2004 [23]

as a starting point for an evaluation conformant usage of the TOE. Please note that the information contained in the Security Target also have to be taken into account.

7 IT Product Testing

Test hardware configuration

Developer testing on the TOE version in the TOE configuration as described in the Security Target was performed on the following systems:

- IBM pSeries p520
- IBM pSeries p570
- IBM pSeries p595

The configuration of the software was consistent with the PitBull installation guidance.

Evaluator testing on the TOE version with the TOE configuration as described in the Security Target was also performed on the systems mentioned above.

The tests have been performed with LPAR enabled.

Test coverage/depth

All tests were performed on external interfaces of the TSF. Internal interfaces were partially tested directly and partially indirectly. For the sufficiency of the indirect tests an argumentation was provided.

The correspondence between the tests and the functional specification was found to be accurate and complete.

Summary of Developer Testing Effort

Test configuration

The developer test was done on all hardware platforms listed in the ST. The configuration of the software was consistent with the PitBull installation guidance.

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: the TET framework. This means, the test suite provides some user space application for building (compiling, assembling) executables out of the test case files, clobbering 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 TET framework. These functions are invoked by the test cases during their run when the positive or negative result of a test unit is determined. In addition, the PitBull extension is covered with its

own test suite that is responsible for building and running the test suite and collecting the results of the test cases.

The test case files of the TET framework and the PitBull test suite 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 test some others indirectly), the test units of one test case in turn check different aspects of a security function.

Testing results:

The developer performed the testing of the final product on all three platforms (p520, p570 and p595). The developer has installed the TOE in accordance with the relevant guidance for the LSPP/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 p570 system located at the IBM office in Austin.

For testing, the developer used several test cases from the PitBull test suite. All of them are independent from each other. The evaluator decided to run all test cases out of the PitBull test suite. Since the PitBull test suite does not contain test cases for all security enforcing functions, the FVT test suite has to be used to test the standard AIX functionality.

The evaluator performed almost all the developer tests testing the TSF at its TSFI and his own test cases on the TOE he has installed in conformance with the Security Target and the developer's guidance documentation. All results from the test cases developed by the evaluator were consistent with the expected results. Therefore the evaluator has determined that the tests show that the TOE works as described in the Security Target and the developer's design documentation.

Evaluator penetration testing:

The test system for penetration testing was a p570 with the software as used for developer testing. The evaluator has 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 evaluator conducted those tests and did not find any test that resulted in a penetration of the TOE with low attack potential. Also the vulnerability analysis did not identify any vulnerability that could be exploited with low attack potential. Therefore the evaluator has determined as a result of his activities that the TOE is resistant against attacks with low attack potential.

8 Evaluated Configuration

According to the Security Target the evaluated configuration of the TOE is defined as follows (refer also to the Security Target [7]).

The evaluated configurations are defined as follows:

- The system must be installed according to the PitBull Foundation installation guide [21].
- Only IPv4 is included in this evaluation.
- 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.
- Only the default mechanisms for identification and authentication are included. 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 connect directly to the workstation and afforded the same physical protection as the workstation.
- AIX 5.2 provides both a native and a Sys5 print system. Only Sys5 is supported in the evaluated configuration, as it implements the labeling requirements from LSPP.
- System security flags (or, kernel security flags) need to be configured as identified in the Security Target [7], chapter 6.2.12.1.
- The system must be configured to disable remote access for an individual user after five consecutively failed login attempts have occurred for this user.

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.

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 system types are supported:

- The AIX journaled filesystem jfs2.
- The High Sierra filesystem for CD-ROM drives, cdrfs.
- The DVD-ROM file system, udfs.
- The process file system, procfs (/proc) , provides access to the process image of each process on the machine as if the process were a “file”. Process access decisions are enforced by MAC, MIC, and DAC attributes inferred from the underlying process’s and user security attributes.

- The Network File System, nfs.

The following assumptions about the technical environment the TOE is intended to be used in are made:

The TOE is running on the following hardware platforms:

- IBM pSeries Symmetric Multiprocessor (SMP) Systems, using Power5 CPUs (p5 520, p5 570, p5 595).

The following peripherals can be run with the TOE preserving the security functionality:

- All terminals supported by the TOE.
- All storage devices and backup devices supported by the TOE (hard disks, CDROM drives, streamer drives, floppy disk drives).
- All printer devices supported by the TOE.
- Network connectors supported by the TOE (e.g., Ethernet) supporting TCP/IP services over the TCP/IP protocol stack.

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 (this includes especially the methodology for flaw remediation, [6]).

The evaluation methodology CEM [2] was used for those components identical with EAL4.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented by ALC_FLR.1 and the class ASE for the Security Target evaluation) are summarised in the following table.

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

Assurance classes and components		Verdict
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
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Validation of analysis	AVA_MSU.2	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Independent vulnerability analysis	AVA_VLA.2	PASS

Table 3: Verdicts for the assurance components

The evaluation has shown that:

- The TOE is conform to the Labeled Security Protection Profile [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, EAL4 augmented by ALC_FLR.1.
- The following TOE Security Functions fulfil the claimed Strength of Function: SF IA.1 (User Identification and Authentication Data Management).

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).

The results of the evaluation are only applicable to the IBM AIX 5L for POWER V5.2 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 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 User Guidance documentation (especially [22] and [23]) 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 (BSI) / Federal Office for Information Security
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
FTP	File Transfer Protocol
LAN	Local Area Network
LPAR	Logical partitioning
LPP	Licensed Product Package
LSPP	Labeled Security Protection Profile
IP	Internet Protocol
IA	Security Function Identification and Authentication
IT	Information Technology
JFS	Journalled File System
NFS	Network File System
NIM	Network Install Manager
OR	Security Function Object Reuse
OSP	Organisational Security Policy
PP	Protection Profile
PROM	Programmable read only memory
RPC	Remote Procedure Call
RSH	Remote Shell
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement

SOF	Strength of Function
SM	Security Function Security Management
SMIT	System Management Interface Tool
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
VMM	Virtual Memory Manager

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

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

[6] Application Notes and Interpretations of the Scheme AIS33, Version 2 – “Methodologie zur Fehlerbehebung – Flaw Remediation” (including CEM Supplement: ALC_FLR - Flaw Remediation, Version 1.1), 26.07.2002

[7] Security Target for BSI-DSZ-CC-0303-2006, “PitBull Foundation Version 5.0 for AIX 5.2 Security Target” Version 1.0, 22. March 2006, IBM Corporation

[8] Evaluation Technical Report, Version 4, atsec security information GmbH, 05. April 2006 (confidential document)

[9] Labeled Security Protection Profile, Issue 1.b, 8 October 1999, National Security Agency

User Guidance Documentation:

[10] "Technical Reference: Communications, Volume 1", Fourth edition, October 2002

[11] "Technical Reference: Communications, Volume 2", Fourth edition, October 2002

[12] "Commands Reference, Volume 1", Fifth edition, May 2003

[13] "Commands Reference, Volume 2", Fifth edition, May 2003

[14] "Commands Reference, Volume 3", Fifth edition, May 2003

[15] "Commands Reference, Volume 4", Fifth edition, May 2003

[16] "Commands Reference, Volume 5", Fifth edition, May 2003

[17] "Commands Reference, Volume 6", Fifth edition, May 2003

[18] "Understanding the Diagnostic Subsystem for AIX", Sixth edition, October 2002

[19] "Files Reference", Fourth edition, October 2002

[20] “Common Criteria configuration manual for Foundation on AIX”, Version 1.1, December 2005

[21] “PitBull Foundation and Foundation Suite Installation Guide”, Version 1.3

[22] “Security Features User Guide”, March 2005

[23] “AIX 5L Version 5.2 Security Guide”, Fifth edition, May 2004

[24] “System User's Guide: Communication and Networks”, Third edition, October 2002

[25] “System User's Guide: Operating System and Devices”, Third edition, October 2002

[26] "Trusted Facility Manual PitBull Foundation Release 5.0”, Version 1.6

[27] "Technical Reference: Base Operating System and Extensions”, Volume 1, Fourth edition, October 2002

[28] "Technical Reference: Base Operating System and Extensions, Volume 2", Fourth edition, October 2002

[29] “AIX 5.3 Technical Reference: Base Operating System and Extensions, Volume 1”, Second edition, December 2004

[30] “AIX 5.3 Technical Reference: Base Operating System and Extensions, Volume 2”, Second edition, December 2004

This page is intentionally left blank.

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 4."

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 map

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 5 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.”