Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0385-2006

for

IBM AIX 5L for POWER V5.3
Technology Level 5300-05-02
with optional Virtual I/O Server (VIOS),
Version 1.3

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 9582-5455, Infoline +49 (0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0385-2006

IBM AIX 5L for POWER V5.3
Technology Level 5300-05-02
with optional Virtual I/O Server (VIOS), Version 1.3

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, Version 2.3* (ISO/IEC 15408:2005) for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

PP Conformance:	**Controlled Access Protection Profile, Issue 1.d, 8 October 1999**
Functionality:	**PP conformant plus product specific extensions** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL4 augmented by ALC_FLR.3 - Systematic flaw remediation**

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

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

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

Bonn, 22 December 2006

The President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-5455 - Infoline +49 228 9582-111

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

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

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

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

---

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

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

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

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

2 Recognition Agreements

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

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product IBM AIX 5L for POWER V5.3 Technology Level 5300-05-02 with optional Virtual I/O Server (VIOS), Version 1.3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0302-2005. 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 V5.3 Technology Level 5300-05-02 with optional Virtual I/O Server (VIOS), Version 1.3 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 22 December 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-36.

The product IBM AIX 5L for POWER V5.3 Technology Level 5300-05-02 with optional Virtual I/O Server (VIOS), Version 1.3 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] 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 V5.3 Technology Level 5300-05-02 with optional Virtual I/O Server (VIOS), Version 1.3 (also refered as AIX 5300-05-02 hereafter). 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 [8]. 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). 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.

This certification is a re-certification of BSI-DSZ-CC-0302-2005. The TOE is allowed to be used in an LPAR environment (refer to [6], chapter 2.4.2.1 for more details on LPAR). The TOE includes the Virtual Input/Output Server (VIOS) which allows for the virtualization of SCSI drives and network adapters and makes use of the LPAR environment.

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 [6], chapter 2.3.

The TOE is running in an LPAR on a IBM System p5 POWER5 server.

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 V5.3 Technology Level 5300-05-02 with optional Virtual I/O Server (VIOS), Version 1.3 was evaluated by atsec information security GmbH. The evaluation was completed on 15 December 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

[8] Information Technology Security Evaluation Facility

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4 (Evaluation Assurance Level augmented augmented by ALC_FLR.3 - Systematic flaw remediation).

1.2 Functionality

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

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Addressed issue**
FAU	**Security Audit**
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective Audit
FAU_STG.1	Guarantees of Audit Data Availability
FAU_STG.3	Action in Case of Possible Audit Data Loss
FAU_STG.4	Prevention of Audit Data Loss
FCS	**Cryptographic support**
FCS_CKM.1(SYM)	Cryptographic Key Generation (SSL: Symmetric Algorithms)
FCS_CKM.2(SYM)	Cryptographic Key Distribution (SSL: Symmetric Keys)
FCS_CKM.2(KRB)	Cryptographic Key Distribution (Kerberos)
FCS_COP.1(SYM)	Cryptographic Operation (SSL: Symmetric Operations)
FCS_COP.1(RSA)	Cryptographic Operation (SSL: RSA)
FCS_COP.1(NFS)	Cryptographic Operation (NFSv4)
FCS_COP.1(KRB)	Cryptographic Operation (Kerberos)
FDP	**User data protection**
FDP_ACC.1(CAPP)	Discretionary Access Control Policy
FDP_ACC.1(VIOS)	VIOS Access Control Policy
FDP_ACF.1(CAPP)	Discretionary Access Control Functions

Security Functional Requirement	Addressed issue
FDP_ACF.1(VIOS)	VIOS Access Control Functions
FDP_RIP.2	Object Residual Information Protection
FIA	**Identification and authentication**
FIA_ATD.1	User Attribute Definition
FIA_SOS.1	Strength of Authentication Data
FIA_UAU.2	Authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_UID.2	Identification
FIA_USB.1	User-Subject Binding
FMT	**Security Management**
FMT_MSA.1(CAPP)	Management of Object Security Attributes
FMT_MSA.1(VIOS)	Management of Object Security Attributes
FMT_MSA.2	Secure Security Attributes
FMT_MSA.3 (CAPP)	Static Attribute Initialization
FMT_MSA.3(VIOS)	Static Attribute Initialization
FMT_MTD.1	Management of the Audit Trail
FMT_MTD.1	Management of Audited Events
FMT_MTD.1	Management of User Attributes
FMT_MTD.1	Management of Authentication Data
FMT_MTD.1	Management of VIOS Mappings
FMT_REV.1	Revocation of User Attributes
FMT_REV.1	Revocation of Object Attributes
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1(CAPP)	Security Management Roles
FMT_SMR.1(VIOS)	Security Roles
FPT	**Protection of the TOE Security Functions**
FPT_AMT.1	Abstract Machine Testing
FPT_RVM.1	Reference Mediation
FPT_SEP.1	Domain Separation
FPT_STM.1	Reliable Time Stamps
FTP_ITC.1	Inter-TSF Trusted Channel

Table 1: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Addressed issue
FDP	**User data protection**
Note 1 (as defined in [8])	Subject Residual Information Protection
FDP_RIP.3-AIX	Hard disk drive residual information protection
FPT	**Protection of the TOE Security Functions**
FPT_RVM.2-AIX	Stack Execution Reference Mediation

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

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.

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

Security Functional Requirement	Addressed issue
FCS	**Cryptographic support**
FCS_CKM.1(KRB)	Cryptographic Key Generation (Kerberos)
FCS_CKM.1(RSA)	Cryptographic Key Generation (SSL: RSA)
FDP	**User data protection**
FDP_ACC.1.	Subset access control
FDP_ACF.1	Security attribute based access control .
FDP_ACC.1 (LPAR)	Subset access control
FDP_ACF.1 (LPAR)	Security attribute based access control
FIA	**Identification and authentication**
FIA_UID.2	User identification before any action
FIA_SOS.1	Verification of secrets
FMT	**Security Management**
FMT_MSA.3	Static attribute initialization

Table 3: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.

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

TOE Security Function	Addressed issue
IA	Identification and Authentication AIX provides identification and authentication (I&A) based upon user passwords. The quality of the passwords used can be enforced through configuration options controlled by AIX. Configurations for I&A allowed in the evaluated configuration are: • The default configuration for authentication, which uses passwords to authenticate users. • The LDAP authentication method configured for UNIX-type authentication, which uses passwords to authenticate users. (In the UNIX-type configuration, LDAP only stores the data used for I&A. It does not perform I&A for AIX. AIX must communicate with the LDAP server across an SSL connection.)
AU	Auditing AIX can collect extensive auditing information about security related actions taken or attempted by users, ensuring that users are accountable for their actions. For the minimal set of events to be audited in the evaluated configration refer to the Security Target [6], chapter 5.2. The audit trail writtencan be analyzed to identify attempts to compromise security and determine the extent of the compromise.
DA	Discretionary Access Control Discretionary Access Control (DAC) restricts access to objects, such as files and is based on Access Control Lists (ACLs) and the standard UNIX permissions for user, group and others. Access control mechanisms also protect IPC objects from unauthorized access. In addition, AIX supports ACLs on sockets for TCP connections. Additionally, VIOS provides DAC between VIOS SCSI device drivers acting on behalf of LPAR partitions as subjects and logical/physical volumes as objects. It also provides DAC between VIOS Ethernet device drivers acting on behalf of groups of LPAR partitions sharing a virtual network and VIOS Ethernet adapter device drivers where one is the subject and the other is the object (the Ethernet packets cannot contain VLAN tags).

TOE Security Function	Addressed issue
OR	Object Reuse All resources are protected from Object Reuse (scavenging) by one of three techniques: explicit initialization, explicit clearing, or storage management. Four general techniques are used to meet this requirement: • Explicit Initialization: The resource's contents are explicitly and completely initialized to a known state before the resource is made accessible to a subject after creation. • Explicit Clearing: The resource's contents are explicitly cleared to a known state when the resource is returned for re-use. • Storage Management: The storage making up the resource is managed to ensure that uninitialized storage is never accessible. • Erase Disk: AIX offers as part of its diagnostic subsystem an Erase Disc service aid that can be invoked by the administrator to overwrite all data currently stored in user-accessible blocks of a disk with pre-defined bit patterns.
SM	Security Management The management of the security critical parameters of AIX is performed by the system administrator. A set of commands that require system administrator privileges are used for system management. Security parameters are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorized access by users that are not the system administrator. VIOS defines a separate set of roles for system management than AIX. Each VIOS role has a set of commands available to it. Security parameters are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorized access by users.
TP	TSF 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

TOE Security Function	Addressed issue
	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 unauthorised access by untrusted users. The system administrator has the ability to start a program that checks the hardware for correct operation.

Table 4: TOE Security Functions

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

1.3 Strength of Function

The TOE's strength of functions is claimed 'medium' (SOF-medium) for specific functions as indicated in the Security Target [6], chapter 5.5.2, 5.8 and 8.3.8.

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 CAPP, the OSPs defined there (refer to [8], chapter 3.2) are applicable for the TOE as well. Because all security objectives of CAPP are derived from OSPs, no specific threats have been defined in the Protection Profile.

In addition to CAPP the following OSP have been defined in [6], chapter 3.3:

- **P.STATIC:** Dynamic partitioning must not be used for the allocation and de-allocation of resources to the TOE's partition during operation of the TOE. Only "static" partitioning may be performed while the TOE is in a non-operating phase.
- **P.ERASE:** Administrators shall be able to support information compartmentalization by preventing recovery of logically deleted information from physically and logically intact SCSI hard disk drives before they are re-used within the same system. Such hard disk drives will remain within the physical and logical protection domain of the TOE and will reside within the TSC.
- **P.DIST_USERS:** When the TOE is used in a distributed environment, the administrators shall ensure that the user databases on each TOE are consistent with each other.
- **P.COMPROT:** When the TOE is used in a distributed environment, the administrator may create a trusted communications path between NFSv4 clients and servers and, for LDAP-based authentication, between the TOE and LDAP server.

Also in addition to the PP, the Security Target [6], chapter 3.2.1 adds the following threats:

- **T.UAUSER:** An attacker (possibly, but not necessarily, an unauthorized user of the TOE) may impersonate an authorized user of the TOE. This includes the threat of an authorized user A that tries to impersonate as another authorized user without knowing the authentication information.
- **T.UAACCESS:** An authorized user of the TOE may access information resources without having permission from the person who owns, or is responsible for, the information resource for the type of access.
- **T.UAACTION:** An undetected violation of the security policy may be caused as a result of an attacker (possibly, but not necessarily, an unauthorized user of the TOE) attempting to perform actions that the individual is not authorized to do.
- **T.VIOS:** A VIOS SCSI device driver acting on behalf of an LPAR partition may try to access logical volumes or physical volumes that are not assigned to the device driver. A VIOS Ethernet device driver acting on behalf of a group of LPAR partitions may try to access a VIOS Ethernet adapter device driver intended for a different VIOS Ethernet device driver (or vise versa).

Note that also threats to be averted by the TOEs environment have been defined (refer to Security Target [6], 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 [6] 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 5300-05-02 are not included.
- AIX AIX 5300-05-02 supports the use of IPv4 and IPv6. IPv4 is included in the evaluated configuration. IPv6 is also included in the evaluated configuration, but only the functional capabilities of IPv6 that are also supported by IPv4 are 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.

- Only the default mechanism for identification and authentication and the LDAP authentication method configured for “UNIX-type” authentication with an SSL connection 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.
- Dynamic Partitioning (Dynamic LPAR, DLPAR) is not supported in the evaluated configuration, i.e. the dynamic (de-) allocation of resources to a partition during operations is not allowed and must be prevented by organizational means in the IT environment.
- The TOE comprises one or more of the server machines (and optional peripherals) running the system software listed in chapter 2 of this report (a server running this software is referred to as a “TOE server” in the following).
- 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 or they connect using the Virtual Input/Output Server (VIOS).
- 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 file system, jfs2,
  - the standard remote file system access protocol, nfs (V3, V4);
  - the High Sierra file system 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 DAC attributes inferred from the underlying process’ DAC attributes).

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:

- The TOE is running in an LPAR on a System p5 POWER5 server

Periphals:

- all terminals and printers supported by the TOE

- all storage devices and backup devices supported by the TOE (hard disks, CD- and DVD-ROM drives, streamer drives, floppy disk drives) - note that the Erase Disk functionality supports SCSI hard disk drives only
- all printer devices supported by the TOE

Network:

- Network connectors supported by the TOE (e.g. Ethernet, Token Ring, etc.) supporting TCP/IP services over the TCP/IP protocol stack.
- NFSv4 supports the use of NAS v1.4 (Kerberos Version 5) for aiding in establishing a trusted channel between NFSv4 clients and servers. NAS v1.4 is part of the TOE environment. NAS v1.4 must be configured to use LDAP for its database.

Since the Security Target claims conformance to CAPP, the assumptions defined there on physical, personnel and connectivity aspects are also valid for the TOE (refer to [8], chapter 3.3). Additionally the Security Target defines the assumptions:

- **A.UTRAIN:** Users are trained well enough to use the security functionality provided by the system appropriately.
- **A.UTRUST:** Users are trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their data.
- **A.NET_COMP:** All network components (like bridges and routers) are assumed to correctly pass data without modification.
- **A.KERB_KEY:** The Kerberos KDC generates encryption keys used for encrypting the data communications between an NFSv4 client and server.
- **A.RSA_KEY:** The environment generates RSA encryption keys used by the SSL communication.
- **A.KERB_PROTECT:** The Kerberos Key Distribution Center (KDC) used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the Kerberos database.

  This includes the requirement for user-subject binding when communicating to Kerberos and the use of the Kerberos protocol to protect the communication link between Kerberos and a Kerberos client.
- **A.LDAP_PROTECT:** The LDAP server used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the LDAP server. This includes the requirement for authentication when accessing user entries and the configuration to use SSL v3 as the preferred protocol to protect the communication links.

For a detailed description refer to the Security Target [6], 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 Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation is called:

IBM AIX 5L for POWER V5.3
Technology Level 5300-05-02
with optional Virtual I/O Server (VIOS),
Version 1.3

The TOE documentation is supplied on CD-ROM (see chapter 6 of this report). The documents [24] (Release Notes) and [25] (Security Guide) are 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 [6], chapter 2.3.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	AIX 5L for POWER V5.3 with Recommended Technology Package 5300-05-02, Program Number 5765-G03	AIX 5L TL 5300-05-02	Shrink wrapped CDs, Fixes are delivered electronically
		Virtual I/O Server (VIOS) contained in IBM Advanced Power Virtualization Version 1.3, Program Number 5765-G30	VIOS version 1.3	Shrink wrapped CDs, Fixes are delivered electronically
2	DOC	Documents as listed in chapter 6 of this report	see chapter 6	Part of the CDs

Table 5: Deliverables of the TOE

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 [6] 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 [6] 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).
- 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).
- When used in a distributed environment, the administrators shall ensure that the user databases on each TOE Server are consistent with each other (P.DIST_USERS)
- When used in a distributed environment, the a trused communication path between NFSv4 clients and server and for LDAP-based authentication between the TOE and LDAP server is in the reponsibility of the administrators (P.COMPROT)

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 [6], 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 [6], 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).
- It is assumed that the Kerberos KDC generates encryption keys used for encrypting the data communications between an NFSv4 client and server (A.KERB_KEY).
- It is assumed that the environment generates RSA encryption keys used by the SSL communication (A.RSA_KEY).
- It is assumed that the Kerberos Key Distribution Center (KDC) used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the Kerberos database. This includes the requirement for user-subject binding when communicating to Kerberos and the use of the Kerberos protocol to protect the communication link between Kerberos and a Kerberos client (A.KERB_PROTECT).
- It is assumed that the LDAP server used by the TOE provides protection mechanisms against unauthorized access to TSF data stored in the LDAP server. This includes the requirement for authentication when accessing user entries and the configuration to use SSL v3 as the preferred protocol to protect the communication links (A.LDAP_PROTECT).

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 [6]).

- 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).
- An attacker (possibly, but not necessarily, an unauthorized user of the TOE) may attempt to guess the password of a Kerberos account through repeated bind attempts to Kerberos (TE.KERB_BIND).

For a detailed description of the threats covered by the TOE environment please refer to [6], chapter 3.2.2.

5 Architectural Information

General overview of AIX

The target of evaluation (TOE) is the operating system AIX 5300-05-02.

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 5300-05-02 consists of a distributed, closed network of highend, mid-range and low-end IBM Series p5 servers running the evaluated version of AIX 5300-05-02. All servers complying with the definition of System p5 POWER5 and POWER5+ with hardware components as defined in the Security Target [6] are covered by the evaluation.

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 for the operation of the TOE as CAPP/EAL4+ system [25].

The TOE Security Functions (TSF) provided by AIX consists of those parts 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 [24] and [25] 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 Mozilla 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.

General overview of VIOS

In addition to the AIX OS, VIOS is part of the TOE as well to provide access to shared SCSI and Ethernet resources.

Conceptually, VIOS resides as a layer between the AIX OS and the physical hardware. Access to the shared resources is restricted based on the VIOS configuration performed by the administrator.

VIOS provides discretionary access control between VIOS SCSI device drivers behavior on behalf of LPAR partitions and logical or physical volumes. In addition, VIOS provides discretionary access control between shared Ethernet device drivers accessing a Hypervisormaintained virtual LAN and the VIOS Ethernet adapter device driver. A VLAN setup with VLAN tags is not supported.

VIOS defines a separate set of roles compared to AIX for system management. Each VIOS role has a set of commands available to it. Security parameters are stored in specific files that are protected by the access control mechanisms. Nevertheless, access to the VIOS management interface must be restricted to authorized administrators.

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.
- VIOS providing access to shared SCSI and Ethernet resources.

Security Functions

The security functions that have been evaluated include:

- **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. The user data is either stored locally in files or remotely within an LDAP server.

  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. The evaluated configuration supports bin mode auditing only.
- **Discretionary Access Control:** The TOE supports discretionary access control for three different types of objects:

  1. The discretionary access control for file system objects: The discretionary access control for file system objects in the TOE support 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.
  2. 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.
  3. 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.

  In addition to the AIX DAC mechanisms, VIOS control access to the shared SCSI and Ethernet resources. This access mediation is subject to the discretion of the administrator.
- **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 AIX part of 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.

  VIOS provides support for different roles for administrative purposes. As only trusted administrators are allowed to access the management interface of VIOS, these roles are provided for convenience for a group of administrators.

6 Documentation

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

- Technical Reference: Communications, Volume 1, commtrf1.pdf, Third Edtition September 2005, [9]
- Technical Reference: Communications, Volume 2, commtrf2.pdf, Third Edtition September 2005, [10]
- Commands Reference, Volume 1, aixcmds1.pdf, Third Edition September 2005, [11]
- Commands Reference, Volume 2, aixcmds2.pdf, Third Edition September 2005, [12]
- Commands Reference, Volume 3, aixcmds3.pdf, Third Edition September 2005, [13]
- Commands Reference, Volume 4, aixcmds4.pdf, Third Edition September 2005, [14]
- Commands Reference, Volume 5, aixcmds5.pdf, Third Edition September 2005, [15]
- Commands Reference, Volume 6, aixcmds6.pdf Third Edition September 2005, [16]
- Understanding the Diagnostic Subsystem for AIX, diagunsd.pdf, Sixth Edition October 2002, [17]
- Diagnostic Information for Multiple Bus Systems, 380509.pdf, Version 5.3, December 2004, [18]
- Files Reference, aixfiles.pdf, Third Edtition September 2005, [19]
- General Programming Concepts: Writing and Debugging Programs, genprogc.pdf, Third Edition September 2005, [20]
- Operating System and Device Management, baseadmndita.pdf, First Edition July 2006, [21]
- System Management Guide: Operating System and Devices, baseadmn.pdf, Thrid Edition September 2005, [22]
- System Management Concepts: Operating System and Devices, admnconc.pdf, Third Edition September 2005, [23]
- README addendunm to the AIX guidance, User_Guidance_Docs.txt, [24]
- AIX 5L Version 5.3: Security, security.pdf, Fourth Edition July 2006, [25]
- System Management Guide: Communications and Networks, commadmn.pdf, Third Edition September 2005, [26]

- Networks and Communication Management, commadmndita.pdf, First Edition July 2006, [27]
- AIX 5.3 Technical Reference: Base Operating System and Extensions, Volume 1, basetrf1.pdf, Second Edition December 2004, [28]
- AIX 5.3 Technical Reference: Base Operating System and Extensions, Volume 2, basetrf2.pdf, Second Edition December 2004, [29]
- Using the Virtual I/O Server, iphb1.pdf, Sixth Edition February 2006, [30]

The administrator/user is recommended to use the documents:

- README addendunm to the AIX guidance, User_Guidance_Docs.txt, [24]
- AIX 5L Version 5.3: Security, security.pdf, Fourth Edition July 2006, [25]

as a starting point for an evaluation conformant usage of the TOE. Please note that the information contained in the Security Target [6] also have to be taken into account.

7 IT Product Testing

Test hardware configuration

The following System p5 systems were used by the developer for the testing:

- p550: VIOS served SCSI and Ethernet resources to AIX partitions; LDAP was configured to provide the user databases
- p570: AIX standalone within an LPAR
- p575: AIX standalone within an LPAR
- p595: AIX standalone within an LPAR

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

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:

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

Testing approach:

IBM has a large number of different test suites and test cases for each component. The test suite related to the core AIX functionality is supplemented by test suites related to the NFS and VIOS. Most of the test are automatic test but some manual testing remains.

The developer performed the testing of the final product on all the platforms listed above. Correspondence of the test configuration to the configuration required by the ST and guidance documentation was ensured. Any deviations because of the test setup have been justifed. The tests cases showed the expected behaviour.

Summary of Evaluator Testing Effort

Test configuration:

The evaluator performed his test on a p5 p550 systems located in Austin.

Testing approach:

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

Since the core functinality of the TOE hasn't changed much compared to the previous evaluation the evaluator chose to concentrate his tests on the new features like VIOS.

The evaluator has verified that all test cases produced the results that where expected. 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 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 assume the the attack potential as defined in AVA_VLA.2.

The evaluator conducted those tests and did not find any test that resulted in a sucessful penetration of the TOE with the attack potential assumed for AVA_VLA.2.

8 Evaluated Configuration

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

General Aspects:

- 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 5300-05-02 are not included.
- AIX 5300-05-02 supports the use of IPv4 and IPv6. IPv4 is included in the evaluated configuration. IPv6 is also included in the evaluated configuration, but only the functional capabilities of IPv6 that are also supported by IPv4 are 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.
- Only the default mechanism for identification and authentication and the LDAP authentication method configured for “UNIX-type” authentication with an SSL connection 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.
- Dynamic Partitioning (Dynamic LPAR, DLPAR) is not supported in the evaluated configuration, i.e. the dynamic (de-) allocation of resources to a partition during operations is not allowed and must be prevented by organizational means in the IT environment.

Networking Aspects:

- The TOE comprises one or more of the server machines (and optional peripherals) running the system software listed in chapter 2 of this report.
- 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 or they connect using the Virtual Input/Output Server (VIOS).
- 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.

Technical Aspects:

- The TOE is running in an LPAR on a System p5 POWER5 server
- The following file system types are supported:
  - the AIX journaled file system, jfs2,
  - the standard remote file system access protocol, nfs (V3, V4),
  - the High Sierra file system 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 DAC attributes inferred from the underlying process’ DAC attributes).

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

9 Results of the Evaluation

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

The 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.3 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
TOE 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
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS

Assurance classes and components		Verdict
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Systematic flaw remediation	ALC_FLR.3	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: low-level design	ATE_DPT.2	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 6: Verdicts for the assurance components

This is a re-certification based on BSI-DSZ-CC-0302-2005. New functionality like VIOS, LDAP-supported I&A and NFSv4 have been subject of the re-evaluation. For details on the functionality newly integrated in the TOE please refer to [6].

The evaluation has shown that:

- the TOE is conform to the CAPP [8]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by ALC_FLR.3 - Systematic flaw remediation.
- the TOE Security Function “Identification and Authentication based on passwords” fulfil the claimed Strength of Function: SOF-medium. This strength applies for the identification and authentication of AIX as well as for the identification and authentication for VIOS.

The rating of the strength of functions does not include the cryptographic algorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for all security function related to the Security Functional Requirements from the FCS class.

The results of the evaluation are only applicable to the TOE as outlined in chapter 2 of this report.

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

10 Comments/Recommendations

The User Guidance documentation as listed in chapter 6 of this report (especially documents [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 [6] 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 [6] 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
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 2.3, August 2005

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

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

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

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

[6] Security Target BSI-DSZ-CC-0385-2006, “AIX 5L Version 5.3 Technology level 53000502 with optional Virtual I/O Server Security Target”, Version 1.3, 2006-11-27, IBM Corporation

[7] Evaluation Technical Report BSI-DSZ-CC-0385-2006, Release 2, 2006-12-14, atsec infofmation security GmbH (confidential document)

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

User Guidance Documentation:

[9] Technical Reference: Communications, Volume 1, commtrf1.pdf, Third Edtition September 2005

[10] Technical Reference: Communications, Volume 2, commtrf2.pdf, Third Edtition September 2005

[11] Commands Reference, Volume 1, aixcmds1.pdf, Third Edition September 2005

[12] Commands Reference, Volume 2, aixcmds2.pdf, Third Edition September 2005

[13] Commands Reference, Volume 3, aixcmds3.pdf, Third Edition September 2005

[14] Commands Reference, Volume 4, aixcmds4.pdf, Third Edition September 2005

[15] Commands Reference, Volume 5, aixcmds5.pdf, Third Edition September 2005

[16] Commands Reference, Volume 6, aixcmds6.pdf Third Edition September 2005

[17] Understanding the Diagnostic Subsystem for AIX, diagunsd.pdf, Sixth Edition October 2002

[18] Diagnostic Information for Multiple Bus Systems, 380509.pdf, Version 5.3, December 2004

[19] Files Reference, aixfiles.pdf, Third Edtition September 2005

[20] General Programming Concepts: Writing and Debugging Programs, genprogc.pdf, Third Edition September 2005

[21] Operating System and Device Management, baseadmndita.pdf, First Edition July 2006

[22] System Management Guide: Operating System and Devices, baseadmn.pdf, Thrid Edition September 2005

[23] System Management Concepts: Operating System and Devices, admnconc.pdf, Third Edition September 2005

[24] README addendunm to the AIX guidance, User_Guidance_Docs.txt

[25] AIX 5L Version 5.3: Security, security.pdf, Fourth Edition July 2006

[26] System Management Guide: Communications and Networks, commadmn.pdf, Third Edition September 2005

[27] Networks and Communication Management, commadmndita.pdf, First Edition July 2006

[28] AIX 5.3 Technical Reference: Base Operating System and Extensions, Volume 1, basetrf1.pdf, Second Edition December 2004

[29] AIX 5.3 Technical Reference: Base Operating System and Extensions, Volume 2, basetrf2.pdf, Second Edition December 2004

[30] Using the Virtual I/O Server, iphb1.pdf, Sixth Edition February 2006

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

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

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

plus one of the following:

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

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

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

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

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

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

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

CC Part 3:

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

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

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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