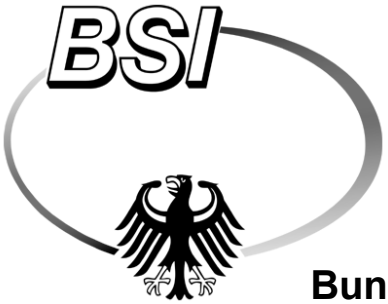


Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0225-2003

for

IBM LPAR for POWER 4
for the IBM pSeries
Firmware Releases:
3R031021 (p630), 3K031021 (p650) and 3H031021 (p690)

from

IBM Corporation

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

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0225-2003

IBM LPAR for POWER 4

for the IBM pSeries

Firmware Releases:
3R031021 (p630), 3K031021 (p650) and 3H031021 (p690)

from

Common Criteria Arrangement

IBM Corporation

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)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
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, 26. January 2004

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
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 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)
- CEM supplementation on “ALC_FLR – Flaw remediation”, Version 1.1, February 2002

---

[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 Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

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

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates 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.

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 LPAR for POWER 4 (for IBM pSeries, firmware releases 3R031021 (p630), 3K031021 (p650) and 3H031021 (p690)) has undergone the certification procedure at BSI.

The evaluation of the product IBM LPAR for POWER 4 was conducted by atsec Information Security GmbH. The atsec Information Security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor is: IBM Deutschland GmbH
Anzinger Straße 29
81671 München

The developer is: IBM Corporation
Burnet Road 11400
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 26. January 2004.

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-18.

The product IBM LPAR for POWER 4 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111.

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

[7] IBM Corporation
Burnet Road 11400
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 the logical partitioning architecture (LPAR) for POWER 4 for the IBM pSeries systems p630, p650 and p690 (firmware releases 3R031021 (p630), 3K031021 (p650) and 3H031021 (p690)). It consists of the Open Firmware, Run Time Abstraction Layer (RTAS) and the Hypervisor executing in hypervisor mode on the above mentioned hardware platforms.

The logical partitioning capable pSeries eServers p630, p650 and p690 support a logical partitioned environment that enables the pSeries systems to run multiple logical partitions concurrently.

In a logical partition, an operating system instance runs with dedicated resources: processors, memory, and I/O slots. These resources are statically assigned to the logical partition. The total amount of assignable resources is limited by the physically installed resources in the system.

The LPAR for POWER 4 is responsible for managing the separation of the partitions and allows only dedicated assignment of processors, main memory and I/O slots to individual partitions. Any sharing of those resources between different partitions is not supported by the LPAR architecture.

The separation between the different partitions in accordance with the pre-configured resource assignments is then enforced with support of the pSeries hardware.

The TOE as firmware is delivered together with the IBM pSeries eServers and has the following versions:

- For the pSeries Server p630: 3R031021
- For the pSeries Server p650: 3K031021
- For the pSeries Server p690: 3H031021

The hardware underlying the TOE and the operating systems running inside a logical partition are not part of the TOE.

The TOE Security Functional Requirements (SFR) used in the Security Target [7] are Common Criteria conformant as shown in the following table:

Security Functional Requirement	Identifier
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_RIP.1	Subset residual information protection

Security Functional Requirement	Identifier
FIA_UID.2	User identification before any action
FMT_MSA.3	Static attribute initialisation
FPT_FLS.1	Failure with preservation of secure state
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FRU_FLT.1	Degraded fault tolerance

The evaluation of the product was conducted by atsec Information Security GmbH. atsec is an evaluation facility (ITSEF)[8] recognised by BSI. The evaluation was completed on November 26th 2003.

The sponsor is: IBM Deutschland GmbH
Anzinger Straße 29
81671 München

The developer is: IBM Corporation
Burnet Road 11400
Austin, TX 78758, USA

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of this report, or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL4 (Evaluation Assurance Level 4). 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 recognised CEM supplementation “ALC_FLR – Flaw remediation”, Version 1.1, February 2002 ([3]) was used.

1.2 Functionality

The TOE IBM LPAR for POWER 4 provides the following Security Functions (please refer to the Security Target [7] for a complete listing and precise definition):

Identification (ID)

The logical partition that calls a TOE function is identified. This is done by using a partition number that is stored in a special register (LPID).

[8] Information Technology Security Evaluation Facility

Access Control (AC)

The TOE assigns processors, memory regions and I/O slots to at most one partition. This assignment is managed by a table in NVRAM, which indicates for each resource to which partition the resource is allocated. The TOE ensures that resources or part of resources are not shared between partitions.

Interference Protection (IP)

The TOE does not allow communication between software running in different partitions. No function of the TOE can be used for such communication. The TOE also ensures that none of the resources it manages is shared between partitions.

Object Reuse (OR)

On allocation of resources to a partition the TOE ensures that residual information in those resources are cleared. This applies to processors that are fully reset, memory objects that are cleared and I/O slot, which are fully reset when they are allocated to a partition.

TSF Protection (TP)

The underlying hardware of the POWER 4 processors allow the TOE to reserve areas in main memory and in NVRAM for its own operation. The TOE will not allocate those memory areas to any partition thereby protecting its own data structures and code from any type of access by software running in any partition.

1.3 Strength of Function

No security function of the TOE is based on a permutational or probabilistic algorithm. Therefore no strength of function was claimed.

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

The following threats have been claimed to be averted by the TOE.

T.UAPACCESS

A user of the TOE may get access to information in resources belonging to other partitions.

T.UATACCESS

A user of the TOE may access information resources belonging to the TOE via other than the defined TOE user functions.

T.CRASHPAR

Software running in one partition may either crash another partition or dominate resources in a way that another partition is no longer able to execute their software at an acceptable performance.

For a precise definition of the threats please refer to the Security Target [7]. Note that also threats for the TOE environment have been defined in the Security Target. They are listed in chapter 4 of this report.

1.5 Special configuration requirements

The configuration requirements for the TOE are defined in the Security Target [7] and are summarised here (for the complete information please refer to the Security Target):

- The TOE is running on the following hardware platforms:

  IBM pSeries Symmetric Multiprocessor (SMP) Systems, using POWER 4 CPUs (p630, p650 and p690)

- The following peripherals can be run with the TOE:

  All devices that are connected via the PCI bus;

  The service processor (no external device other than the HMC connected). Please note that the HMC may only be attached during configuration of the TOE, but must be detached as soon as the partitions are initialised (see [7], chapter 2.9)

  The hardware management console (not to be used when the TOE is running except for starting a partition and restarting a hanging partition)

  Floppy disk drive and CD-ROM attached to the ISA bus via a SCSI adapter.

1.6 Assumptions about the operating environment

The following constraints concerning the operating environment are made in the Security Target.

The following constraints are based on the assumptions defined in [7], chapter 3.4. The are summarised here:

Assumption	Summary
A.LOCATE	Processing resources are run in facilities with controlled access.
A.PROTECT	Protection against manipulation.
A.SP-HMC	The Service processor and the HMC work properly.
A.MANAGE	Competent personnel for management
A.NO_EVIL_ADMIN	Administrators are non-hostile
A.NOPMOD	Modification of resource assignment only after shutdown
A.CONNECT	All connections to I/O devices, the Service Processor and the HMC are within the controlled access facilities. No network connection to HMC and Service Processor.
A.NOSERVICE	No partition has Service Authority
A.PDEF	Installation and Configuration of the TOE is done correctly

Assumption	Summary
A.HW_FUNC	The underlying hardware works as specified

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 LPAR for POWER 4
for IBM pSeries

Firmware Releases
3R031021 (p630), 3K031021 (p650) and 3H031021 (p690))

The TOE is firmware operating on IBM pSeries hardware providing services for operating systems running in logical partitions. The TOE and its documentation is supplied together with the pSeries hardware and comprises the following documents [9], [10], [11] and [12] (please also refer to chapter 6 of this report).

3 Security Policy

The security policy model specified by the Security Targets SFRs and in even more detail in a separate Security Policy Model document. The following policies are enforced by the TOE:

Identification-Policy:

Each subject is uniquely identified when it is accessing objects in an LPAR environment. A subject cannot change the identification it has been assigned.

Resource-Access-Control Policy:

Each subject can only access those objects it has been assigned by the LPAR administrator. For processors and memory objects the LPAR administrator provides only the number of the objects to be assigned. The LPAR Partition Manager will then determine the object assignment within the numbers defined by the LPAR administrator.

Separation Information-Flow Control Policy:

Each subject can only access those objects it has been assigned by the LPAR administrator. For processors and memory objects the LPAR administrator provides only the number of the objects to be assigned. The LPAR Partition Manager will then determine the object assignment within the numbers defined by the LPAR administrator.

4 Assumptions and Clarification of Scope

Compliance to the following Organisational Security Policy is claimed in the Security Target:

P.PARTDEF

The organisation operating the TOE has a defined policy for the amount of processors and memory and the actual I/O slots to be allocated to the individual partitions. This policy is defined in accordance with the operational needs of the software running in the individual partitions. This policy is implemented by an administrator of the organisation using the HMC.

Based on the personnel assumptions the following usage constraints exists (for the precise definition please to [7]):

- The TOE has to be managed by competent individuals (A.MANAGE)
- The Administrators of the TOE are assumed not to be careless, willfully negligent, or hostile (A.NO_EVIL_ADMIN)
- Assignment of TOE resources will only be made after a shutdown of all partitions (A.NOPMOD)

4.1 Environmental assumptions

The following assumptions about physical, connectivity and other aspects defined by the Security Target have to be met (refer to Security Target [7], chapter 3.4.1 and 3.4.3):

- The processing resources of the TOE, the Hardware Management Console and the Service Processor are located within controlled access facilities (A.LOCATE)
- The TOE, software for policy enforcement, the Hardware Management Console and the Service Processor are secured against physical manipulation (A.PROTECT)
- The Hardware Management Console and the Service Processor work properly (A.SP-HMC)
- All direct connections to I/O devices, the Service Processor and the Hardware Management Console have to reside within controlled access facilities. No network connection is established to the Hardware Management Console or the Service Processor. (A.CONNECT)

- No Partition has Service Authority (A.NOSERVICE)
- Installation and Configuration of the TOE, the Hardware Management Console and the Service Processor is done correctly. Assignment of resources to partitions is done according to a defined policy (A.PDEF)
- The hardware underlying the TOE operates correctly in accordance with its specification. Periodical checks are performed to verify that this is the case (A.HW_FUNC)

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

4.2 Clarification of scope

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

- Data loss due to hardware malfunction (TE.HWMF)
- Unauthorised modification of NVRAM content by using the Hardware Management Console or the Service Processor (TE.MODNVRAM)
- Insufficient capabilities of the underlying hardware to support the self-protection of the TSF (TE.HW_SEP)

5 Architectural Information

General overview

The target of evaluation (TOE) is the logical partitioning architecture LPAR for POWER 4 processors. The logical partitioning capable pSeries eServers p630, p650 and p690 support a logical partitioned environment that enables the pSeries systems to run multiple logical partitions concurrently. The maximum number of partitions that can concurrently run depends on the specific partitioning-capable pSeries server model. For example, the pSeries 690 support up to 16 partitions running concurrently while the pSeries 650 supports up to 8 partitions and the pSeries 630 supports up to 4 partitions (depending on the number of interrupt controllers present in the system).

In a logical partition, an operating system instance runs with dedicated resources: processors, memory, and I/O slots. These resources are statically assigned to the logical partition. The total amount of assignable resources is limited by the physically installed resources in the system.

Because the implementation of logical partitioning is static, one has to shut down every operating system instance in all logical partitions to change the resource assignment of running logical partitions.

The logical resources that can be assigned to a partition are:

- Processors
- Main memory regions
- I/O slots

The assignment of those resources to the individual logical partitions is stored in non-volatile RAM (NVRAM). This part of the NVRAM is maintained by the service processor and cannot be read or modified directly by software running in a logical partition. The assignment itself is performed by a System Administrator, who uses a “Hardware Management Console” (HMC) to define those assignments. The HMC communicates with a “Service Processor” that accepts the commands from the HMC and sets the values to define the logical partitions in the non-volatile RAM (NVRAM) accordingly.

The TOE includes installation from using the Service Processor Menus only. The Service Authority functionality that allows update of the firmware code from a partition is disabled.

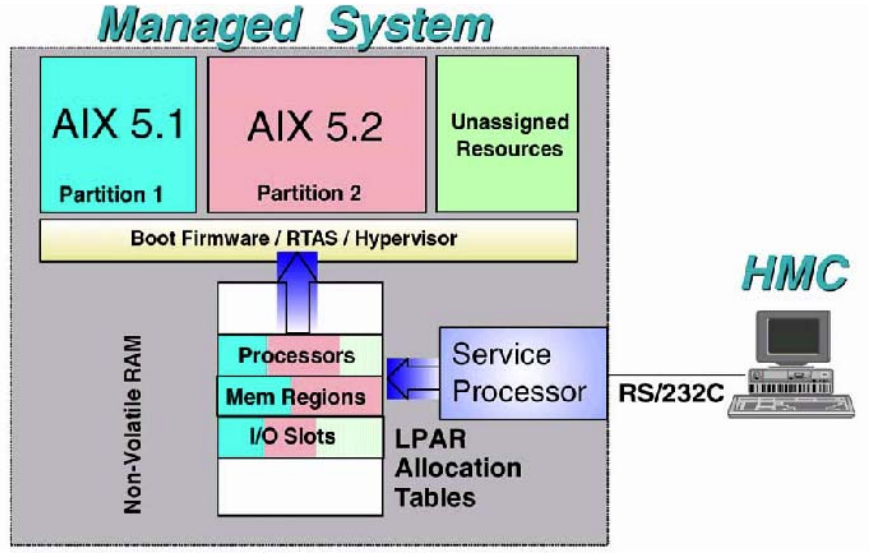
The functionality of the TOE is supported by the underlying processors, because the POWER 4 processor supplies three states: problem state, supervisor state and hypervisor state.

Major structural units of the TOE

The TOE contains the following structural units:

- The Open Firmware (boot time firmware) that initialises the hardware and the TOE
- The Hypervisor that provides controlled access to managed resources, such as page tables, TCE tables as well as virtualised hardware
- The Run-Time Abstraction Services (RTAS) that provides a common interface to the underlying system for the operating system

The following figure provides a general overview of the TOE and the interdependencies with the TOE environment:



6 Documentation

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

[9] IBM Hardware Management Console for pSeries Installation and Operations Guide, SA38-0590-05, Sixth Edition, September 2003, IBM Corporation

[10] Readme: pSeries 630 Model 6C4 and Model 6E4 Firmware Update (70286C4F.html), Version 3R031021

[11] Readme: pSeries 650 Model 6M2 Firmware Update (70386M2F.html), Version 3K031021

[12] Readme: pSeries 690 Model 681 Firmware Update (7040681F.html), Version 3H031021

7 IT Product Testing

Test Configuration

The TOE as specified in the Security Target as well as preliminary versions of the TOE have been tested on the following pSeries eServer platforms:

p630 (two different machines)

- 2 POWER 4 CPUs
- 8 GB / 16 GB Main Memory
- ISA Bus Diskette Drive

- 2 Wide/Ultra-3 SCSI I/O Controller
- Wide/Fast-20 SCSI I/O Controller
- 1 SCSI disk drives (18 GB / 4 GB) manufactured by IBM
- SCSI DVD-RAM drive, manufactured by IBM
- 2 IBM 10/100 Mbits Ethernet PCI adapter
- HMC
- PS/2 Keyboard
- Three Button Mouse

p650

- 4 POWER 4 CPUs
- 20 GB Main Memory
- ISA Bus Diskette Drive
- 2 Wide/Ultra-3 SCSI I/O Controller
- 3 Dual Channel Ultra3 SCSI Adapter
- 4 LVD SCSI Disk Drive (9100 MB, 18200 MB and two 73400 MB), manufactured by IBM
- 1 SCSI Multimedia CD-ROM Drive, manufactured by IBM
- 2 IBM 10/100 Mbits Ethernet PCI adapter
- 1 2-Port 10/100/1000 Base-TX PCI-X Adapter
- 2 2-Port Gigabit Ethernet PCI-X Adapter

p690

- 8 POWER 4 CPUs
- 16 GB Main Memory
- ISA Bus Diskette Drive
- 2 Wide/Ultra-3 SCSI I/O Controller
- 2 LVD SCSI Disk Drive (36400 MB), manufactured by IBM
- 1 SCSI Multimedia CD-ROM Drive, manufactured by IBM
- IBM 10/100 Mbps Ethernet PCI Adapter
- HMC
- Standard I/O Serial Port

Test Coverage/Depth

The developer has provided a test coverage and depth of testing analysis, demonstrating that all aspects of TSF behavior are tested.

Tests for the evaluated configuration of the TOE have been devised to test all aspects of TSF behaviour, as it has been specified throughout the functional specification and high-level design. A correspondence analysis provided by the developer shows coverage of all TSF, subsystems and interfaces that affect the security functional behaviour of the TOE. The coverage has been determined to be overall sufficient.

Summary of developer testing effort

Test Configuration

The tests have been carried out on the test configuration as described above.

Testing Approach

Because of the nature of the TOE the developer mainly used manual tests to demonstrate that all aspects of TSF behavior are tested. Detailed test instruction for each test cases have been used to ensure the tests to be repeatable.

Complete testing on all platforms underlying the TOE (p630, p650, p690) have been performed.

Testing results

The test records of the developer show that all tests on all test platforms were executed successfully, i.e. the actual test results met the expected test results.

Summary of evaluator testing effort

Test Configuration

All tests were run at the developer's sites in Austin, TX and Munich, Germany. The developer granted access to their testing environment.

The TOE was installed as required by the respective guidance documentation and the Security Target.

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.

Testing results

All evaluator test were executed successfully.

Evaluator penetration testing:

Penetration tests have been performed by the evaluation facility to assess possible vulnerabilities found during the evaluation of the different CC assurance classes. As for AVA_VLA.2 required a low attack potential was assumed. The TOE withstood the penetration efforts.

8 Evaluated Configuration

The Target of Evaluation is called **IBM LPAR for POWER 4**. The TOE is firmware operating on the IBM pSeries p630, p650 and p690 hardware.

The following firmware releases comprise the TOE:

- For the pSeries Server p630: 3R031021
- For the pSeries Server p650: 3K031021
- For the pSeries Server p690: 3H031021

The hardware underlying the TOE and the operating systems running inside a logical partition are not part of the TOE. For setting up the TOE a Service Processor and a Hardware Management Console are used which are also not part of the TOE.

For setting up and running the TOE according to the evaluated configuration all guidance documents (refer to chapter 6) and the implications given by the Security Target have to be followed. These implications can also be found in chapter 1.5 and 1.6 of this report.

9 Results of the Evaluation

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

The verdicts for the CC, Part 3 assurance components (according to EAL4 with ALC_FLR.1 augmentation and the Security Target evaluation) are summarised in the following table:

Assurance Classes and Components		**Verdict**
Security Target	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
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

Assurance Classes and Components		Verdict
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC class ADV	PASS
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
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: 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

No security function of the TOE is based on a permutational or probabilistic algorithm. Therefore no strength of function was claimed.

The TOE has no vulnerabilities which are exploitable with low attack potential in the intended operating environment.

The results of the evaluation are only applicable to the product IBM LPAR for POWER 4 (for IBM pSeries, firmware releases 3R031021 (p630), 3K031021 (p650) and 3H031021 (p690)) in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [7] and the chapters 2, 4 and 8 of this report). The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, and if the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The User Guidance documentation (refer to chapter 6 of this report) 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

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
HMC	Hardware Management Console
IT	Information Technology
LPAR	Logical Partition Architecture
LPID	Logical Partition ID
NVRAM	non-volatile RAM
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

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] CEM supplementation on “ALC_FLR – Flaw remediation”, Version 1.1, February 2002

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

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

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

[7] Security Target BSI-DSZ-0225-2003, Version 1.6, 2003-11-05, LPAR for POWER 4, IBM Corporation

[8] Evaluation Technical Report BSI-DSZ-CC-0225, Version 1.1, 2003-11-26, atsec information security GmbH (confidential document)

User Guidance Documentation:

[9] IBM Hardware Management Console for pSeries Installation and Operations Guide, SA38-0590-05, Sixth Edition, September 2003, IBM Corporation

[10] Readme: pSeries 630 Model 6C4 and Model 6E4 Firmware Update (70286C4F.html), Version 3R031021

[11] Readme: pSeries 650 Model 6M2 Firmware Update (70386M2F.html), Version 3K031021

[12] Readme: pSeries 690 Model 681 Firmware Update (7040681F.html), Version 3H031021

C Excerpts from the Criteria

CC Part 1:

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

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

The conformance result consists of one of the following:

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

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

plus one of the following:

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

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

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

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

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

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

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

CC Part 3:

Assurance categorisation (chapter 2.5)

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

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

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

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

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

Evaluation assurance level (EAL) overview (chapter 6.1)

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

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

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

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

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

Table 6.1 - Evaluation assurance level summary“

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

„Objectives

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

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

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

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

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

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

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

„Objectives

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

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

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous,

do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

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

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

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

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

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„Objectives

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

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

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

„Objectives

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

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

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

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

„Application notes

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

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