# Certification Report

**Bundesamt für Sicherheit in der Informationstechnik**

**BSI-DSZ-CC-0378-2006**

for

**PR/SM™ LPAR for the**
**IBM System z9™ Enterprise Class and the**
**IBM System z9™ Business Class**

from

**International Business Machine Corporation**
**(IBM)**

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-0378-2006**

# PR/SM™ LPAR for the IBM System z9™ Enterprise Class and the IBM System z9™ Business Class

from

## International Business Machine Corporation (IBM)

Common Criteria Arrangement
for components up to EAL4

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) extended by advice of the Certification Body for components beyond EAL4 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

**Evaluation Results:**

| | |
|---|---|
| Functionality: | **Product specific Security Target**<br>**Common Criteria Part 2 conformant** |
| Assurance Package: | **Common Criteria Part 3 conformant**<br>**EAL5** |

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, September 4th, 2006

The Vice President of the Federal Office
for Information Security

Hange

L.S.

IT Security Certified

SOGIS - MRA

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

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)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

---

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.

This evaluation contains the components ACM_SCP.3, ADV_FSP.3, ADV_HLD.3, ADV_IMP.2, ADV_INT.1, ADV_RCR.2, ADV_SPM.3, ALC_LCD.2, ALC.TAT.2, ATE_DPT.2, AVA_CCA.1 and AVA_VLA.3 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of these assurance families (if applicable) are relevant.

# 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 PR/SM LPAR for the IBM System z9 Enterprise Class (EC) and z9 Business Class (BC) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0324-2006. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0324-2006 were re-used.

The evaluation of the product PR/SM LPAR for the IBM System z9 EC and z9 BC was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The developer is:

International Business Machine Corporation (IBM)
2455 South Road, P329
Poughkeepsie, NY 12601, USA

The certification is concluded with

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

This work was completed by the BSI on September 4th, 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-26.

The product PR/SM LPAR for the IBM System z9 EC and z9 BC 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] International Business Machine Corporation (IBM)
2455 South Road, P329
Poughkeepsie, NY 12601, 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 Microcode kernel of the Processor Resource / System Manager™ (PR/SM) LPAR running on the IBM hardware platform z9 EC and z9 BC.

PR/SM is intended for use in environments where separation of workloads is a requirement, but where the use of a single hardware platform is desirable for reasons of economy, flexibility, security or management.

Leasing or purchase costs may be lower for a single large machine than for a number of smaller machines of equivalent total processing capacity. There may also be savings in operational costs resulting from lower machine room capacity and fewer operations staff.

PR/SM provides flexibility by allowing the single machine to be set up to provide a wide range of virtual machine configurations. As one workload grows, more resources can be allocated to it, providing significant advantages where the required configuration is subject to frequent change.

PR/SM provides the facility to partition a single platform to run any combination of z/OS™; z/VM™; VIF, VM/ESA®, VSE/ESA™, TPF or LINUX allowing requirements for different operating system environments to be met.

Where confidentiality is a concern, PR/SM provides separation of workloads, and prevents the flow of information between partitions. This trusted separation may be used where the separation is based on need to know, or where data at different national security classifications must be isolated.

The IT product PR/SM LPAR for the IBM System z9 EC and z9 BC was evaluated by atsec information security GmbH. The evaluation was completed on August 21st, 2006. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The developer is

International Business Machine Corporation (IBM)
2455 South Road, P329
Poughkeepsie, NY 12601, 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 Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL5 (Evaluation Assurance Level 5).

[8] Information Technology Security Evaluation Facility

## 1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 conformant 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_STG.1 | Protected Audit Trail Storage |
| FAU_STG.4 | Prevention of Audit Data Low |
| **FDP** | **User data protection** |
| FDP_ACC.2 | Complete access control |
| FDP_ACF.1 | Security attribute based access control |
| FDP_IFC.1 | Subset Information Flow Control |
| FDP_IFF.1 | Information Flow Control |
| FDP_RIP.2 | Full residual information protection. |
| **FIA** | **Identification and authentication** |
| FIA_ATD.1 | User attribute definition |
| FIA_UID.2 | User identification before any action. |
| **FMT** | **Security Management** |
| FMT_MSA.1 | Management of Security Attributes |
| FMT_MSA.3 | Static attribute initialization |
| FMT_MTD.1 | Management of TSF data |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security Roles |
| **FPT** | **Protection of the TOE Security Functions** |
| FPR_UNO.1 | Unobservability |
| FPT_AMT.1 | Abstract machine test |
| FPT_ITT.1 | Basic internal TSF data transfer protection |

| Security Functional Requirement | Addressed issue |
|---|---|
| FPT_SEP.3 | Complete reference monitor |
| FPT_STM.1 | Reliable time stamps |
| FPT_TRC.1 | Internal TSF consistency |
| FPT_TST.1 | TSF testing |
| **FRU** | **Resource Utilisation** |
| FRU_RSA.1 | Maximum quotas |
| **FTA** | **TOE access** |
| FTA_TSE.1 | TOE session establishment |

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

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.1.

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

| Security Functional Requirement | Addressed issue |
|---|---|
| **FDP** | **User data protection** |
| FDP_ACC.1 | Access control policy |
| FDP_ACF.1 | Access control functions |
| **FMT** | **Security Management** |
| FMT_MSA.3 | Static attribute initialization |

Table 2: 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 5.2.

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

**Logical Partition Identity:** The TOE implements an image profile to define the initial operational characteristics of a logical partition. In a given configuration each logical partition is uniquely named and has a corresponding image profile. One of the parameters in the image profile is the logical partition identifier (i.e. zone number). If a logical partition is in the current configuration, then the zone number uniquely identifies that partition.

**Authorized Administration:** The authority level of a subject determines which tasks are available for that subject. Subjects are System Administrators and logical partitions.

**Authorized Operations:** The TOE implements the I/O Configuration Data Set (IOCDS) used to define the logical partitions and the allocation of resources to

these logical partitions. The TOE ensures that resources are allocated to a logical partition as specified in the IOCDS.

**Audit and Accountability:** The TOE implements a Security Log that is always enabled and contains a record of security relevant events. The View Security Log task allows an administrator to view the log recorded while the Archive Security Log task allows an administrator to create an archival copy of the security log. The View Security Log task also allows an administrator to search or sort the security relevant events based on date or event criteria.

**Object Reuse:** The TOE ensures that the contents of physical processors, storage or I/O utilized by different logical partitions will be cleared of any residual information before being utilized by the receiving logical partition.

**Reliability of Service:** The TOE implements a Reset profile to define the initial operational characteristics of the physical processors. Two of the parameters in the Reset profile are the processor running time and wait completion. These parameters provide the ability to share physical processor resources on either an event-driven basis or a time-driven basis. Disabling event driven dispatching causes shared physical processor resources to be distributed on the basis of time intervals according to the weights specified to effectively prevent unauthorized denial of service.

**Self Test:** The TOE implements a set of self-test functions that are executed when the TOE is started or reset, and periodically during normal execution.

**Alternate Support Element:** The TOE implements functions that permit a quick switch to another Support Element when the primary Support Element has a hardware problem. Mirroring functions are performed on a regular basis to communicate any hard disk changes from the primary Support Element to the alternate Support Element.

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

## 1.3 Strength of Function

The strength of function claim is not applicable since no TOE security function is based on permutational or probabilistic mechanisms.

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

The assumed threats can be classified into the following two categories:

- Users may gain access to data belonging to another partition, for which they do not have clearance, specific authorization, or a need-to-know. This may be achieved either directly (for example, by reading storage allocated to another partition, or by failure to clear a resource before reallocation), or indirectly (for example, through a covert channel). Unauthorized access to audit data may lead to a false record of System Administrator actions.

- Users may gain unauthorized access to system resources (i.e. channel path, control unit, I/O device, physical or logical processor): such actions being contrary to the security or resource policy of an organization.

There have no organisational security policies been defined in the security target.

## 1.5 Special configuration requirements

There is only one configuration of the TOE.

The TOE has to be configured in accordance with the Security Target and the respective guidance documents (refer to the chapters 4 and 6 of this report). This means among other things that it is configured as strict separation virtual machine monitor (SVMM).

## 1.6 Assumptions about the operating environment

The operating environment of the TOE comprises the IBM z9 EC and z9 BC hardware.

The various models use identical but different numbers of processor chips as specified in the following table for the z9 EC.

| z9 EC Model number | Feature Code | Number of CPs |
|---|---|---|
| S08 | 4501 | 1 |
| S08 | 4502 | 2 |
| S08 | 4503 | 3 |
| S08 | 4504 | 4 |
| S08 | 4505 | 5 |
| S08 | 4506 | 6 |
| S08 | 4507 | 7 |
| S08 | 4508 | 8 |
| S18 | 4509 | 9 |
| S18 | 4510 | 10 |
| S18 | 4511 | 11 |
| S18 | 4512 | 12 |
| S18 | 4513 | 13 |
| S18 | 4514 | 14 |
| S18 | 4515 | 15 |
| S18 | 4516 | 16 |
| S28 | 4517 | 17 |
| S28 | 4518 | 18 |
| S28 | 4519 | 19 |
| S28 | 4520 | 20 |

| z9 EC Model number | Feature Code | Number of CPs |
|---|---|---|
| S28 | 4521 | 21 |
| S28 | 4522 | 22 |
| S28 | 4523 | 23 |
| S28 | 4524 | 24 |
| S38 | 4525 | 25 |
| S38 | 4526 | 26 |
| S38 | 4527 | 27 |
| S38 | 4528 | 28 |
| S38 | 4529 | 29 |
| S38 | 4530 | 30 |
| S38 | 4531 | 31 |
| S38 | 4532 | 32 |
| S54 | 4533 | 33 |
| S54 | 4534 | 34 |
| S54 | 4535 | 35 |
| S54 | 4536 | 36 |
| S54 | 4537 | 37 |
| S54 | 4538 | 38 |
| S54 | 4539 | 39 |
| S54 | 4540 | 40 |
| S54 | 4541 | 41 |
| S54 | 4542 | 42 |
| S54 | 4543 | 43 |
| S54 | 4544 | 44 |
| S54 | 4545 | 45 |
| S54 | 4546 | 46 |
| S54 | 4547 | 47 |
| S54 | 4548 | 48 |
| S54 | 4549 | 49 |
| S54 | 4550 | 50 |
| S54 | 4551 | 51 |
| S54 | 4552 | 52 |
| S54 | 4553 | 53 |
| S54 | 4554 | 54 |

Table 3: z9 EC Capabilities and number of processors

The following table specifies the possible variety for the z9 BC.

| z9 BC Model number | Feature Code | Number of CPs |
|---|---|---|
| R07 | 4901 | 1 |
| R07 | 4902 | 2 |
| R07 | 4903 | 3 |
| R07 | 4905 | 1 |
| R07 | 4906 | 2 |
| R07 | 4907 | 3 |
| R07 | 4909 | 1 |
| R07 | 4910 | 2 |
| R07 | 4911 | 3 |
| R07 | 4913 | 1 |
| R07 | 4914 | 2 |
| R07 | 4915 | 3 |
| R07 | 4917 | 1 |
| R07 | 4918 | 2 |
| R07 | 4921 | 1 |
| R07 | 4922 | 2 |
| R07 | 4925 | 1 |
| R07 | 4929 | 1 |
| R07 | 4933 | 1 |
| R07 | 4937 | 1 |
| S07 | 4944 | 4 |
| S07 | 4947 | 3 |
| S07 | 4948 | 4 |
| S07 | 4951 | 3 |
| S07 | 4952 | 4 |
| S07 | 4954 | 2 |
| S07 | 4955 | 3 |
| S07 | 4956 | 4 |
| S07 | 4958 | 2 |
| S07 | 4959 | 3 |
| S07 | 4960 | 4 |
| S07 | 4962 | 2 |
| S07 | 4963 | 3 |
| S07 | 4964 | 4 |
| S07 | 4966 | 2 |
| S07 | 4967 | 3 |
| S07 | 4968 | 4 |
| S07 | 4969 | 1 |
| S07 | 4970 | 2 |

| z9 BC Model number | Feature Code | Number of CPs |
|---|---|---|
| S07 | 4971 | 3 |
| S07 | 4972 | 4 |
| S07 | 4973 | 1 |
| S07 | 4974 | 2 |
| S07 | 4975 | 3 |
| S07 | 4976 | 4 |
| S07 | 4977 | 1 |
| S07 | 4978 | 2 |
| S07 | 4979 | 3 |
| S07 | 4980 | 4 |
| S07 | 4981 | 1 |
| S07 | 4982 | 2 |
| S07 | 4983 | 3 |
| S07 | 4984 | 4 |
| S07 | 4985 | 1 |
| S07 | 4986 | 2 |
| S07 | 4987 | 3 |
| S07 | 4988 | 4 |
| S07 | 4989 | 1 |
| S07 | 4990 | 2 |
| S07 | 4991 | 3 |
| S07 | 4992 | 4 |
| S07 | 4993 | 1 |
| S07 | 4994 | 2 |
| S07 | 4995 | 3 |
| S07 | 4996 | 4 |
| S07 | 4997 | 1 |
| S07 | 4998 | 2 |
| S07 | 4999 | 3 |
| S07 | 5000 | 4 |
| S07 | 5001 | 1 |
| S07 | 5002 | 2 |
| S07 | 5003 | 3 |
| S07 | 5004 | 4 |

Table 4: z9 BC Capabilities and number of processors

## 1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product

by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# 2 Identification of the TOE

The Target of Evaluation (TOE) is called:

**PR/SM LPAR for the IBM System z9 EC and z9 BC**

The TOE is the Microcode Driver Level D63 Date: 15 Sept 2005 at MCL bundle 22a, with the HMC support provided in Microcode Driver Level D64X, Bundle 2.

PR/SM is a hardware facility that enables the resources of a single physical machine to be divided between distinct, predefined logical machines, called “logical partitions”. Each logical partition is a domain of execution and is considered to be an object capable of running a conventional System Control Program (SCP) such as z/OS™, z/VM™, VIF, VM/ESA®, VSE/ESA™, TPF or LINUX.

The TOE is only runnable on a special hardware. Thus, an IBM technician deliveres the TOE personally either installing new hardware or upgrading the Licensed Internal Code and HMC/SE.

The following table outlines the components the TOE is delivered with. As the TOE is only runnable on a special hardware, the following table contains the configuration of hard- and software and documentation that is required for the operation of the TOE. Thus, not only the TOE but more items are included in the table. A specification of the release is only mentioned for parts of the TOE.

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1. | SW | IBM PR/SM LPAR for z9 EC and z9 BC including:<br>• all required Licensed Internal Code (LIC) at driver level D63<br>• Support Element (SE) LIC<br>• Hardware Management Console (HMC) LIC | Driver Level D63 of September 15, 2005 at MCL bundle 22a<br><br>Driver Level D64X, Bundle 2 | Delivered together with IBM z9 EC or z9 BC System Hardware |

Table 5: Deliverables of the TOE

# 3 Security Policy

The TOE implements several policies which are specified in the security functional requirements. Those policies are:

**Access Control Security Function Policy**

The TOE implements an access control policy between subjects and objects. The subjects are the logical partitions (LPAR) defined in the IOCDS and the System Administrator. The objects are the physical resources of the processor, the logical processors and the TSF data. Access to objects by subjects will be mediated by this policy to ensure that subjects are only able to gain authorized access to objects.

**Information Flow Control Security Function Policy**

The TOE implements an information flow control policy between subjects and objects, and between objects and objects. The subjects are the logical partitions (LPAR) defined in the IOCDS and the System Administrator. The objects are the physical resources of the processor and the logical processors instantiated on a physical processor on behalf of a logical partition. Flow of information between objects and subjects, and between objects and objects will be mediated by this policy to ensure that information flow is only possible when subjects and objects are associated with the same logical partition.

# 4 Assumptions and Clarification of Scope

## 4.1 Usage assumptions

The following usage assumptions are defined in the Security Target of the TOE:

**A.Sep_Mode** - Strict Separation Mode

A strict separation virtual machine monitor (SVMM) restricts the allocation of resources so that there is absolutely no sharing of objects amongst their clients. Although PR/SM may be configured as a SVMM, it may also be configured to run in a mode where sharing of some resources is permitted. To be used as a strict separation virtual machine monitor, PR/SM must be configured in the following manner:

1. Devices must be configured so that no device is accessible by more than one partition (although they may be accessible by more than one channel path);
2. Each I/O (physical) control unit must be allocated to a single partition in the current configuration;
3. The Security Administrator must not reconfigure a channel path unless all attached devices and control units are attached to that path only;
4. The Security Administrator must ensure that all devices and control units on a reconfigurable path are reset before the path is allocated to another partition;
5. No channel paths must be shared between partitions;
6. The amount of reserved storage for a partition must be zero;

7. The System Administrator must ensure that the number of processors and coprocessors dedicated to activated partitions is less than the total number available.
8. Dynamic I/O configuration changes must be disabled (i.e. changes require a power-on reset);
9. I/O Priority Queuing must be disabled.
10. Workload Manager must be disabled so that CPU and I/O resources are not managed across partitions.
11. No partition must be configured to enable hipersockets (Internal Queued Direct I/O).
12. Partitions must be prevented from receiving performance data from resources that are not allocated to them (no partition should have global performance data control authority);
13. At most one partition can have I/O configuration control authority (i.e. no more than one partition must be able to update any IOCDS) and this partition must be administered by a trustworthy administrator (i.e. the administrator of this partition is considered a System Administrator of the TOE);
14. The Security Administrator must ensure that write access is disabled for each IOCDS, unless that IOCDS is to be updated (the current IOCDS must not be updated);
15. The Security Administrator must verify any changed IOCDS after a power-on reset with that IOCDS, before any partitions have been activated (the Security Administrator may determine whether the IOCDS has been changed by inspecting the date of the IOCDS);
16. No partition should have cross-partition control authority (i.e. no partition should be able to reset or deactivate another partition);
17. No partition must have coupling facility channels that would allow communication to a Coupling Facility partition;
18. Replication of HMC Customizable Data must be disabled.

## 4.2 Environmental assumptions

The following assumptions on physical and connectivity aspects are defined in the Security Target of the TOE:

**A.Data_Secure** – Physical and/or controlled access of TOE audit log is required.

The TOE records security-relevant actions performed by the System Administrator in an audit log. The TOE will prune the audit log to two-thirds (2/3) of its capacity when the audit log has been filled. It is the customer's responsibility to back-up the audit log prior to the log reaching its capacity.

Physical access of archived audit log data is also the responsibility of the customer.

**A.Phys_Secure** – Physical protection of processor, I/O and HMC is required

The environment of the hardware is physically secured against unauthorized access. Access to I/O devices is restricted to authorized personnel. In particular the hardware management console and the Local Area Network (LAN) connecting it to the SEs must be physically protected from access other than by authorized system administrators.

**A.No_Remote** – The remote support facility must be disabled.

The phone line and modem connection to the remote support center must be disabled to prohibit unauthorized connections for remote service.

**A.Admin_Secure** – Administrative Personnel Security

Logical partitions within the System z9 EC and z9 BC can be operated from the Hardware Management Console (HMC) and the Support Element (SE). The administrator/operators of the system must be cleared for the highest security classification of work being performed on the system.

## 4.3 Clarification of scope

There are no threats defined in the Security Target which have to be averted by the TOEs IT environment.

Nevertheless the following Objectives have to be met by the environment of the TOE:

**OE.Data_Store** – Off-TOE Data Storage

Audit Log data stored off of the TOE must be controlled for confidentiality and integrity according to the owner’s needs.

**OE.Perss** – Personnel

Personnel working as System Administrators or other privileged positions must be carefully selected and trained.

**OE.Sec_Setup** – Secure Setup

The TOE must be protected during the setup phase.

**OE.Phys_Prot** – Restricted physical and remote access

Physical access and remote access to the HMC and System z9 EC and z9 BC must be restricted only to authorized and approved users.

**OE.SIE** – Memory access control

The underlying hardware must provide separation mechanism that can be used by the TOE to protect the TSF and TSF data from unauthorized access and modification.

**OE.CHANNEL** – Channel access control

The underlying physical I/O LIC must provide separation mechanism that can be used by the TOE to restrict access of one partition to authorized logical I/O resources.

# 5 Architectural Information

The TOE is implemented in LIC (licensed internal code), which is microcode licensed by IBM. The use of LIC prevents untrusted code from masquerading as part of the TOE and abusing TOE privileges. The TOE is composed of:

a) Logical partition (LPAR) LIC, which is the LIC that is responsible for maintaining the isolation of partitions;

b) Hardware Management Console/Support Element LIC, which provides the system administration, functions to maintain the current configuration;

PR/SM is a hardware facility that enables the resources of a single physical machine to be divided between distinct, predefined logical machines called "logical partitions". Each logical partition is a domain of execution, and is considered to be a subject capable of running a conventional system control program (SCP) such as such as z/OS™, z/VM™, VIF, VM/ESA®, VSE/ESA™, TPF or LINUX.

A Hardware Management Console (HMC) / Support Element (SE) workplace is used as a window to start tasks for monitoring and operating the CPC. A user ID determines which tasks and controls can be used. Not all tasks are available for each user ID. The following predefined default user IDs are available:

| User ID | Description |
|---|---|
| Operator | A person with Operator authority typically performs basic system startup and shutdown operations using predefine procedures. |
| Advanced Operator | A person with Advanced Operator authority possesses Operator authority plus the ability to perform some additional recovery and maintenance tasks. |
| System Programmer | A person with System Programmer authority has the ability to customize the system in order to determine its operation. |
| Access Administrator | A person with Access Administrator authority has the ability to create, modify, or delete user profiles for the user modes on the Hardware Management Console or for service mode on the support element. A user profile consists of a user identification, password, and user mode. |
| Service Representative | A person with Service Representative authority has access to tasks related to the repair and maintenance of the system. |

Table 6: User IDs

The following general definitions apply to the above user modes:

**Security Administrator** – any user(s) of the HMC who is defined with a user mode of System Programmer or Service Representative.

**System Administrator** – the System Administrator is defined to be any user(s) with access to the Hardware Management Console (HMC).

A table identifing all specific tasks allowed for each of the 5 user IDs is provided in [7], chapter 2.2.

The Security Administrator uses an I/O configuration program (IOCP) to define an Input/Output configuration data set (IOCDS) of the I/O resources and their allocation to specific logical partitions. The IOCDS may be verified by the Security Administrator prior to activating the partitions. PR/SM allows I/O resources to be dedicated to a single partition, relocatable amongst a defined set of partitions, or shared by a defined set of partitions[9]. When a System Administrator wishes to activate a partition, the activation request is initiated from the HMC. LPAR will receive an external interrupt identified as coming from a BFYCALL command and issue the PCCALL instruction to obtain the description of the partition the System Administrator wishes to activate. LPAR will attempt to construct the partition and will inform the HMC of the success or failure of the command via the PCCALL instruction.

Several different configurations may be stored, but only one is in effect at any time. The configuration becomes effective as part of the activation sequence.

Standard hardware resources such as a central processor, including computation and control registers, timers, clocks and optional co-processors, storage and I/O resources are objects allocated to logical partitions.

These objects are subject to a non-discretionary access control policy under which each logical partition is only permitted access to resources allocated to it. Logical partitions are logical objects that are built from existing physical objects. These logical objects fall into one of three classes:

a) Logical processor facilities, which are supported by similar physical objects. Each such logical object is represented by an internal control block that contains current state information each time context is switched to a different logical partition.

b) Logical storage, both central and expanded, is represented by the same amount of contiguous physical storage. PR/SM does not perform paging or move logical partitions once they have been placed in real storage. Physical storage can be de-allocated from one logical partition and reallocated to another. This feature can be disabled, and is subject to full object reuse control.

c) Logical I/O resources (channels) are implemented by physical resources of the same type. Such resources can be configured so that they are not shared by partitions. A channel can be de-allocated from one logical partition and reallocated to another, under the control of the Security Administrator.

---

[9] Please consider the constraints for the evaluated configuration described in chapter 4 of this report.

The z/Architecture™ and S/390® architecture support two instruction states: problem and supervisor. Problem state instructions can be executed in either problem or supervisor state. Semi-privileged instructions can be executed in supervisor state, or in problem state subject to one or more additional authorizations. Privileged instructions can be executed only in supervisor state. PR/SM exports a virtual machine including all architected instructions, and initiates the execution in supervisor state, so that all three classes of instruction can be executed within the logical partition. Thus each logical partition has both execution states available. PR/SM does not interfere with the logical partition's use of those states.

A system control program (SCP) running in a logical partition can support z/Architecture S/390® architectural mode. This is set when a partition is defined, and cannot be altered while the partition is activated. PR/SM supports and uses the "start interpretive execution" (SIE) instruction to create an interpretative execution environment in which the logical partitions execute. PR/SM begins execution in non-SIE mode. When a logical partition is to be activated PR/SM establishes the parameters for each logical processor allocated to the partition in a control block called a "state description". PR/SM executes a SIE instruction, which dispatches the logical processor in SIE mode. The PR/SM hardware executes instructions in the logical processor in SIE mode until an exception condition occurs, which causes control to return to PR/SM in non-SIE mode. The exception conditions are events that cannot be handled in interpretative mode. PR/SM receives control in non-SIE mode. PR/SM maintains a state description for each logical processor of each logical partition so that each time a logical processor is dispatched, it is in the same context as when it last had control. Since this state description is updated by the hardware, it is impossible for one logical partition to acquire control with the wrong context (i.e. the context of another logical partition). The non-SIE/SIE distinction is a powerful privilege differentiation between PR/SM and the logical partitions.

In LPAR mode, the zSeries provides support for several features that are very helpful in many customer environments. However, these features are not recommended in a secure environment. As a result, the TOE provides security related controls to disable such features assuring separation of the logical partition(s). The security related controls are outlined below:

- **Logical Partition Isolation**
  This control reserves reconfigurable unshared channel paths for the exclusive use of a logical partition. Channel paths assigned to an isolated logical partition are not available to other logical partitions and remain reserved for that LP when they are configured offline.
- **I/O Configuration Control Authority**
  This control can limit the ability of the logical partition to read or write any IOCDS in the configuration locally or remotely. Logical partitions with control authority for the I/O configuration data can read and write any non-write protected IOCDS in the configuration, and can change the I/O configuration dynamically.

- **Global Performance Data Control Authority**
  This control limits the ability of a logical partition to view central processor activity data for other logical partitions. Logical partitions with control authority for global performance data can view CP utilization data and Input/Output (IOP) busy data for all of the logical partitions in the configuration. A logical partition without control authority for the performance data can view only the CP utilization data for itself.
- **Cross-Partition Authority**
  This control can limit the capability of the logical partition to issue certain control program instructions that affect other logical partitions. Logical partitions with cross-partition authority can issue instructions to perform a system reset of another logical partition, deactivate any other logical partition, and provide support for the automatic reconfiguration facility.

In addition to the security controls mentioned above, the TOE also insures that central and expanded storage for each logical partition is isolated and cannot be shared with other logical partitions. The TOE rigidly enforces this “no sharing” rule during logical partition definition, logical partition activation, logical partition reconfiguration and during logical partition execution.

The TOE also “removes” central processors (CPs) from logical partitions by virtualizing physical CPs. Virtualized physical CPs are referred to as logical processors. Within the TOE, each logical CP is represented as a data structure that is associated with its specific logical partitions preventing the transfer of data between partitions.

Thus, when PR/SM is initialized for secure operation, one partition cannot gain access to the data within another partition nor modify any aspect of another partition.

With z/Architecture™ or S/390® architecture (which includes the functions of ESA/370 Architecture), these models have problem-program compatibility with S/360, S/370, and 4300 processors. They can access virtual storage in multiple address spaces and data spaces. This extends addressability for system, subsystem, and application functions that use z/Architecture™ or S/390® architectures.

# 6 Documentation

The following documention belongs to the TOE:

- System z Hardware Management Console Operations Guide, [9]
- System z9 Business Class and Enterprise Class and eserver® zSeries 890 and 990 Input/Output Configuration Program User’s Guide for ICP IOCP, [10]
- System z9 Processor Resource/Systems Manager Planning Guide, [11]
- System z9 Stand-Alone Input/Output Configuration Program User’s Guide, [12]

- System z9 Support Element Operations Guide, [13]
- System z9 Enterprise Class Service Guide, [14]
- System z9 Business Class Service Guide, [15]
- System z9 Enterprise Class Installation Manual for Physical Planning, [16]
- System z9 Business Class Installation Manual for Physical Planning, [17]

# 7 IT Product Testing

The test platforms were set up by the developer according to the ST and all relevant guidance, ensuring that the evaluated configuration as defined in the ST was tested. The developer testing was performed successfully on the evaluated configuration of the TOE. Complete coverage was achieved for all the TOE security functions as provided by the developer. The overall test depth of the developer tests comprises the low-level and the high-level design subsystems and the internal interfaces of those subsystems as required for the assurance level of the evaluation.

A selected subset from the security test suite have been successfully repeated by the evaluation facility. The achieved test results matched the expected results as documented by the developer in the developer test documentation. Furthermore, a set of independent tests has been performed successfully by the evaluation facility.

# 8 Evaluated Configuration

The TOE subject of this Security Target is Microcode Driver Level D63 Date: 15 Sept 2005 at at MCL bundle 22a, with the HMC support provided in Microcode Driver Level D64X, Bundle 2. All z9 EC and z9 BC models possess the common z/Architecture, system software, applications, channel I/O and operational environment. Therefore, the TOE can be used on each model that is part of these families of servers without any modification. For a list of supported models see the table provided in chapter 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 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. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4] (AIS 34).

The verdicts for the CC, part 3 assurance classes and components (according to EAL5 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 |
| Development tools CM coverage | ACM_SCP.3 | 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 |
| Semiformal functional specification | ADV_FSP.3 | PASS |
| Semiformal high-level design | ADV_HLD.3 | PASS |
| Implementation of the TSF | ADV_IMP.2 | PASS |
| Modularity | ADV_INT.1 | PASS |
| Descriptive low-level design | ADV_LLD.1 | PASS |
| Semiformal correspondence demonstration | ADV_RCR.2 | PASS |
| Formal TOE security policy model | ADV_SPM.3 | 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 |
| Standardised life-cycle model | ALC_LCD.2 | PASS |
| Compliance with implementation standards | ALC_TAT.2 | PASS |
| Tests | CC Class ATE | PASS |

| Assurance classes and components | | Verdict |
|---|---|---|
| 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 |
| Covert channel analysis | AVA_CCA.1 | PASS |
| Analysis and testing for insecure states | AVA_MSU.2 | PASS |
| Strength of TOE security function evaluation | AVA_SOF.1 | PASS |
| Moderately resistant | AVA_VLA.3 | PASS |

Table 7: Verdicts for the assurance components

A strength of function claim is not applicable since no TOE security function is based on a permutational or probabilistic mechanism.

Porting the TOE to the new hardware platform IBM z9 EC and z9 BC was the main goal of this re-evaluation.

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conformant.
- The assurance of the TOE is Common Criteria Part 3 conformant, evaluation assurance level EAL5.

The results of the evaluation are only applicable to the PR/SM LPAR for the IBM System z9 EC and z9 BC as described in chapter 2.

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

# 10 Comments/Recommendations

The operational documents as listed in chapter 6 of this report contain necessary information about the usage of the TOE and all security hints therein have to be considered.

# 11 Annexes

None.

# 12 Security Target

For the purpose of publishing, the security target [7] of the target of evaluation (TOE) is provided within a separate document. According to AIS 35 [4] it is a sanitized version of the complete security target [6] used for the evaluation performed.

# 13 Definitions

## 13.1 Acronyms

| | |
|---|---|
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security |
| **CC** | Common Criteria for IT Security Evaluation |
| **CP** | Central Processor |
| **EAL** | Evaluation Assurance Level |
| **HMC** | Hardware Management Console |
| **IOCDS** | I/O Configuration Data Set |
| **IOCP** | I/O Configuration Program |
| **IT** | Information Technology |
| **LIC** | Licensed Internal Code |
| **LPAR** | Logical Partition |
| **PP** | Protection Profile |
| **SE** | Support Element |
| **SF** | Security Function |
| **SFP** | Security Function Policy |
| **SIE** | Start Interpretive Execution |
| **SOF** | Strength of Function |
| **ST** | Security Target |
| **SVMM** | Strict Separation Virtual Machine Monitor |
| **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 2.3, 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-0378-2006, Version 6.0.4, 2006-06-21, Security Target for PR/SM for the IBM System z™ Enterprise Class (z9 EC) and IBM System z™ Business Class (z9 BC), IBM Corporation (confidential document)

[7] Security Target BSI-DSZ-0378-2006, Version 6.0.4, 2006-08-17, Security Target for PR/SM for the IBM System z™ Enterprise Class (z9 EC) and IBM System z™ Business Class (z9 BC), IBM Corporation (public document)

[8] Evaluation Technical Report BSI-DSZ-CC-0378, Version 1.0, 2006-08-17, atsec information security GmbH (confidential document)

[9] System z Hardware Management Console Operations Guide, Version 2.9.1, SC28-6857-00, First Edition (May 2006)

[10] System z9 Business Class and Enterprise Class and eserver® zSeries 890 and 990 Input/Output Configuration Program User's Guide for ICP IOCP, SB10-7037-05, Sixth Edition (May 2006)

[11] System z9 Processor Resource/Systems Manager Planning Guide, SB10-7041-01, Second Edition (April 2006)

[12] System z9 Stand-Alone Input/Output Configuration Program User's Guide, SB10-7152-01, Second Edition (May 2006)

[13] System z9 Support Element Operations Guide, Version 2.9.1, SC28-6858-00, First Edition (May 2006)

[14] System z9 Enterprise Class Service Guide, GC28-6841-02, Third Edition (May 2006)

[15] System z9 Business Class Service Guide, GC28-6853-00, First Edition (May 2006)

[16] System z9 Enterprise Class Installation Manual for Physical Planning, GC28-6844-01, Second Edition (April 2006)

[17] System z9 Business Class Installation Manual for Physical Planning, GC28-6855-00, First Edition (April 2006)

This page is intentionally left blank.

# 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.”