Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0557-2009

for

Processor Resource / Systems Manager (PR/SM) for the IBM z10 EC GA2 and z10 BC GA1

from

International Business Machines Corporation (IBM)

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0557-2009

Processor Resource / Systems Manager (PR/SM)
for the IBM z10 EC GA2 and z10 BC GA1

from	International Business Machines Corporation (IBM)
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 5

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

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 extended by advice of the Certification Body for components beyond EAL 4 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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.

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.

Bonn, 4 May 2009
For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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 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 3 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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

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 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 Processor Resource / Systems Manager (PR/SM) for the IBM z10 EC GA2 and z10 BC GA1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0460-2008. Specific results from the evaluation process BSI-DSZ-CC-0460-2008 were re-used.

The evaluation of the product Processor Resource / Systems Manager (PR/SM) for the IBM z10 EC GA2 and z10 BC GA1 was conducted by atsec information security GmbH. The evaluation was completed on 6 April 2009. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

[6] Information Technology Security Evaluation Facility

For this certification procedure the sponsor and applicant is: International Business Machines Corporation (IBM)

The product was developed by: International Business Machines Corporation (IBM)

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. 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 and in the Security Target.

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.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product Processor Resource / Systems Manager (PR/SM) for the IBM z10 EC GA2 and z10 BC GA1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] International Business Machines Corporation (IBM)
2455 South Road
P329, Poughkeepsie
NY 12601
USA

This page is intentionally left blank.

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.

1 Executive Summary

The Target of Evaluation (TOE) is the Licensed Internal Code (LIC) kernel of the Processor Resource / System Manager (PR/SM) running on the IBM hardware platform z10[8]. LIC is microcode licensed by IBM.

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. 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 differing national security classifications must be isolated.

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 z/OS, z/VM, VIF, VM/ESA, VSE/ESA, TPF or Linux. These operating systems run in a PR/SM partition.

The TOE assures the separation of logical partitions. The separation policy can be configured. For instance, there can be an authorised partition, sending service calls (i.e. for changing the configuration) to other partitions.

The TOE is implemented in LIC. 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.

The Hardware Management Console (HMC) / Support Element (SE) workplace is the window from where users start tasks for monitoring and operating the CPC (central processor complex). User profiles determine which tasks and controls users can use on the workplace. Not all tasks are available for each user.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 5.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant .

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6] and [9], chapter 5.2.

---

[8] HiperSockets, IBM®, Processor Resource/Systems Manager, PR/SM, S/390®, System z, System z10, System z10 BC, System z10 EC, VM/ESA®, VSE/ESA, z10 BC, z10 EC, z/OS®, z/VM® are trademarks or registered trademarks of the International Business Corporation in the United States, other countries, or both.
Linux is a registered trademark of Linus Torvalds.

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

TOE Security Function	Addressed issue
Logical Partition Identity	The TOE implemented 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 specified when defining a new user determines the tasks made available to that user. This capability allows an authorized administrator to effectively manage the TOE and its security functions.
Authorized Operations	The authority level specified when defining a new user determines the tasks made available to that user. This capability allows an authorized administrator to effectively operate the TOE and its security functions
Audit and Accountability	The TOE implemented a Security Log that is always enabled and contains a record of security relevant events. The log data assists an administrator in detection of potential attack or misconfiguration of the TOE security features.
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 implemented 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 implemented a set of self-test functions that are executed when the TOE is started or reset, and periodically during normal execution. These functions ensure that critical hardware functions work properly and that the TOE has not been tampered with when it was powered off.
Alternate Support Element	The TOE implemented 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 SE to the alternate SE. The Support Elements communicate using TCP/IP over a private Ethernet network that connects cage controllers and support elements.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 6.3.

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

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapters 3.2, 3.3 and 3.4.

This certification covers the following configurations of the TOE: Driver Level D73 Control Level 3 running on the IBM z10 EC or IBM z10 BC hardware platforms. For details refer to chapter 8.

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:

Processor Resource / Systems Manager (PR/SM) for the IBM z10 EC GA2 and z10 BC GA1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	IBM PR/SM for IBM z10 EC / BC hardware platforms including: ● LPAR kernel LIC ● Support Element (SE) LIC ● Hardware Management Console (HMC) LIC	Driver D76 Control Level 3	Delivered with IBM z10 EC / BC hardware
2	DOC	System z Hardware Management Console Operations Guide	First Edition, October 2008	Delivered with IBM z10 EC / BC hardware
3	DOC	System z Input/Output Configuration Program User's Guide for ICP IOCP	Eighth Edition, October 2008	Delivered with IBM z10 EC / BC hardware
4	DOC	System z10 Enterprise Class Processor Resource/Systems Manager Planning Guide	Second Edition, October 2008	Delivered with IBM z10 EC / BC hardware
5	DOC	System z10 and System z9 Stand-Alone Input/Output Configuration Program User's Guide	Fourth Edition, October 2008	Delivered with IBM z10 EC / BC hardware
6	DOC	System z10 Support Element Operations Guide	First Edition, October 2008	Delivered with IBM z10 EC / BC hardware
7	DOC	System z10 Enterprise Class Service Guide	Third Edition, October 2008	Delivered with IBM z10 EC hardware
8	DOC	System z10 Business Class Service Guide	First Edition, October 2008	Delivered with IBM z10 BC hardware
9	DOC	System z10 Enterprise Class Installation Manual for Physical Planning	Fourth Edition, October 2008	Delivered with IBM z10 EC hardware
10	DOC	System z10 Business Class Installation Manual for Physical Planning	First Edition, October 2008	Delivered with IBM z10 BC hardware

Table 2: Deliverables of the TOE

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”. The TOE can be run only on a special hardware. Thus, an IBM technician delivers the TOE personally either as part of installation of new hardware or by upgrading the the Licensed Internal Code and HMC/SE. The TOE is delivered with IBM z10 EC and IBM z10 BC hardware platforms.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

TOE Security Function Policy	Addressed issue
Access Control	The TOE implements an access control policy between subjects (users) and objects. The subjects or users are logical partitions and the System Administrator. The objects are the physical resources of the processor (CPs, storage, CHPIDS, audit data, performance data, IOCDSs, profiles, …). Access to objects by subjects will be mediated by this policy to insure that subjects are only able to gain access to authorized objects.
Information Flow Control	The TOE implements an information flow control policy between subjects (users) and objects, and between objects and objects. The subjects or users are logical partitions and the System Administrator. The objects are the physical resources of the processor (CPs, storage, CHPIDS, audit data, performance data, IOCDSs, profiles, …) 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 insure that information flow is only possible when subjects and objects are associated with the same logical partition.

Table 3: TOE Security Function Policies

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- It is the customer’s responsibility to back-up the audit log prior to the log reaching capacity. Physical access of archived audit log data is also the responsibility of the customer.
- Physical protection of processor, I/O (including LAN) and HMC is required.
- The remote support facility must be disabled.
- 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 any partition other than the partition to be isolated (although they may be accessible by more than one channel path).

2. Each I/O (physical) control unit must be allocated only to an isolated partition in the current configuration.
3. The Security Administrator must not reconfigure a channel path owned by an isolated partition 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 owned by an isolated partition are reset before the path is allocated to another partition.
5. No channel paths may be shared between an isolated partition and any other partition(s).
6. The System Administrator must ensure that the number of processors dedicated to activated partitions is less than the total number available.
7. Dynamic I/O configuration changes must be disabled.
8. If I/O Priority Queuing is enabled for the system an isolated partition's minimum and maximum I/O Priority values must be equal.
9. For isolated partitions, Workload Manager must be disabled so that CPU and I/O resources are not managed across partitions.
10. An isolated partition must not be configured to enable hipersockets (Internal Queued Direct I/O).
11. Partitions must be prevented from receiving performance data from resources that are not allocated to them (global performance data control authority must be disabled).
12. 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).
13. 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).
14. 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).
15. No partition may have cross-partition control authority (i.e. no partition should be able to reset or deactivate another partition).
16. No isolated partition may have coupling facility channels that would allow communication to a Coupling Facility partition.
17. The 'Use dynamically changed address' and 'Use dynamically changed parameter' checkboxes must not be selected in the Image or Load profile.
18. No Isolated partition should have the following Counter Facility Security Options enabled:
    - Crypto activity counter set authorization control
    - Coprocessor group counter sets authorization control

Disabling these options will ensure that its crypto and coprocessor activities are not visible to any other partitions.

- The hardware of a Central Electronics Complex must be partitionable into several independent partitions.

Details can be found in the Security Target [6] and [9] chapters 3.2 and 3.4.

5 Architectural Information

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 z/OS, z/VM, VIF, VM/ESA, VSE/ESA, TPF or Linux. These operating systems run in a PR/SM partition.

The TOE is implemented in LIC. 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.

The Hardware Management Console (HMC) / Support Element (SE) workplace is the window from where users start tasks for monitoring and operating the CPC (central processor complex). A user profile determines which tasks and controls users can use on the workplace. Not all tasks are available for each user.

The following predefined default user IDs are established as part of a base Hardware Management Console:

User ID	Description
Operator	A person with Operator authority typically performs basic system startup and shutdown operations using predefined 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 on the Hardware Management Console or for service mode on the support element. A user profile consists of a user identification, a password, managed resource roles and task roles
Service Representative	A person with Service Representative authority has access to tasks related to the repair and maintenance of the system.

Table 4: User IDs

In addition to the predefined user roles supplied with the console the ability to define customized user roles is also provided. A user role is a collection of authorizations. A user role can be created to define the set of tasks allowed for a given class of user (task roles) or it can be created to define the set of managed objects that are manageable for a user (managed resource roles). A customized user role is based on one of the predefined user roles from which objects or tasks are removed. Once user roles are defined or customized

they can be used to create new users with their own permissions. A user can be created with one or more user roles.

A table identifying all specific tasks allowed for each of the 5 user IDs is provided in [6] resp. [9], chapter 2.2.

The address space of the TSF is isolated from the address space of the partitions by hardware protection mechanisms (the SIE instruction provided by the underlying processor as described below), and by the provision of separate hardware for the Support Element and I/O (SAP) processors. The TSF LIC and data is therefore protected from modification or tampering.

The Security Administrator uses an I/O configuration utility (IOCP) to define an Input/Output configuration data set (IOCDS) of the I/O resources and their allocation to specific logical partitions. The IOCDS should 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 among a defined set of partitions, or shared by a defined set of partitions. When a System Administrator wishes to activate a partition, the activation request is initiated from the HMC. LPAR will receive an external interrupt and issue an 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.

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 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.

The zArchitecture 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 System z and 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 System z10 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.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

The TOE is available on different models of the System z10 server family. All models possess the common z/Architecture, system software, applications, channel I/O and operational environment. Therefore, the identical LIC for the TOE can be run without any modification on each model that is part of that family of servers. For a list of supported models see the tables provided in chapter 8.

Developer tests have been performed on those platforms. It should be noted that it was not deemed necessary by the evaluator to test on all possible platforms from the lists provided, since the models listed for each of the server families only differ in the total amount of processors available.

Evaluator tests were executed on a System z10 EC server and a System z10 BC server. The machines were made available to the evaluator by the developer during the evaluator’s visit at the IBM development site in Poughkeepsie, NY.

Developer Tests

Test configuration and approach

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 security functionality of the TOE was tested at a level of SFR. The security relevant test cases are combined in a specific security test suite.

Test results

The developer testing was performed successfully on the evaluated configuration of the TOE as listed above. Actual test results are kept under configuration control. The actual test results matched the expected results for the respective test case as documented in the developer test documentation.

Test coverage

The security functionality of the TOE was covered by the developer's security test suite and the executed tests. As for the TSFI as detailed in the Functional Specification they are completely covered by the security test suite.

Test depth

The evaluator verified that developer tests provide for a sufficient depth as required by EAL5. The security test suite provided by the developer covers the subsystems as defined in the high-level design documentation of the TOE as well as the modules as defined in the low-level design.

The overall test depth of the developer tests comprises the low-level design modules, the high-level design subsystems and the internal interfaces of those subsystems and modules as required for the assurance level of the evaluation.

Evaluator Tests

Test configuration and approach

The evaluator performed independent evaluator tests at the developer site in Poughkeepsie, NY.

The evaluator testing effort comprised two major test sessions: Both sessions concentrated on repeating selected test of the security test suite provided by the developer. There was a test session designated to each of the IBM System z10 server families, with a specific focus on the newly introduced System z10 BC server. During the test sessions the evaluator applied variations on the test case. The objective of those variations was to determine whether TOE security mechanisms can be disabled, circumvented, or behave differently.

The sessions were performed on a System z10 EC server as well as on a System z10 BC server. The driver levels of the machines used for independent testing were identified by the evaluator as being the TOE as defined in chapter 8.

Prior to testing on either machines, the evaluator verified the driver level and the machine type and set up the TOE according to the Security Target and all relevant guidance, ensuring that all evaluator tests were performed on the evaluated configuration of the TOE.

Developer tests performed

The evaluator successfully performed a set of selected developer tests from the security test suite. The actual test results achieved by the evaluator matched the expected results as documented by the developer in the developer test documentation.

Additional evaluator tests

The evaluator devised tests additional to the developer tests, as suggested by the CEM. Those test cases were derived by variation of the developer test cases. The evaluator identified one potential vulnerability with an attack potential rated low. As for the corresponding attack paths, the evaluator performed a source code analysis rather than actual penetration tests. That source code analysis revealed that the identified attack paths do not exist; therefore the identified vulnerability is not exploitable.

Since no other vulnerabilities with a low or moderate attack potential were discovered during the vulnerability assessment, no additional penetration tests were performed by the evaluator.

8 Evaluated Configuration

The TOE, as stated in table 2, uses Driver D76 Control Level 3.

This certification covers the following configurations of the TOE:

z10 EC Model Number	Feature Codes	CPs (depending on Feature Code)
E12	6700 – 6712	0[9] – 12
E26	6713 – 6726	13 – 26
E40	6727 – 6740	27 – 40
E56	6741 – 6756	41 – 56
E64	6757 – 6764	57 – 64

Table 5: Supported z10 EC hardware (not part of the TOE)

z10 BC Model Number	Feature Codes	Model Capacity ID	CPs (depending on Feature Code)
E10	5013 – 5018	A00 – A05	0[10] – 5
E10	5019 – 5023	B01 – B05	1 – 5
E10	5024 – 5028	C01 – C05	1 – 5
E10	5029 – 5033	D01 – D05	1 – 5
E10	5034 – 5038	E01 – E05	1 – 5
E10	5039 – 5043	F01 – F05	1 – 5
E10	5044 – 5048	G01 – G05	1 – 5
E10	5049 – 5053	H01 – H05	1 – 5
E10	5054 – 5058	I01 – I05	1 – 5
E10	5059 – 5063	J01 – J05	1 – 5
E10	5064 – 5068	K01 – K05	1 – 5
E10	5069 – 5073	L01 – L05	1 – 5
E10	5074 – 5078	M01 – M05	1 – 5
E10	5079 – 5083	N01 – N05	1 – 5
E10	5084 – 5088	O01 – O05	1 – 5
E10	5089 – 5093	P01 – P05	1 – 5
E10	5094 – 5098	Q01 – Q05	1 – 5
E10	5099 – 5103	R01 – R05	1 – 5
E10	5104 – 5108	S01 – S05	1 – 5

[9] Model z10 EC E12 ordered with 0 CPs has no central processors but could be all IFLs or all ICFs (see [6] resp. [9], Appendix B.2 “Processor Unit” for details).

[10] Model z10 BC E10 ordered with 0 CPs has no central processors but could be all IFLs or all ICFs (see [6] resp. [9], Appendix B.2 “Processor Unit” for details).

z10 BC Model Number	Feature Codes	Model Capacity ID	CPs (depending on Feature Code)
E10	5109 – 5113	T01 – T05	1 – 5
E10	5114 – 5118	U01 – U05	1 – 5
E10	5119 – 5123	V01 – V05	1 – 5
E10	5124 – 5128	W01 – W05	1 – 5
E10	5129 – 5133	X01 – X05	1 – 5
E10	5134 – 5138	Y01 – Y05	1 – 5
E10	5139 – 5143	Z01 – Z05	1 – 5

Table 6: Supported z10 BC hardware (not part of the TOE)

The assumptions outlined in chapter 4 of this report, especially those concerning configurations, have to be considered.

9 Results of the Evaluation

9.1 CC specific results

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

The Evaluation Methodology CEM [2] was used for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 [4] (AIS 34).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 5 package as defined in the CC (see also part C of this report)

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0460-2008, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the added underlying hardware platform System z10 BC.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
EAL 5

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

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The TOE does not include crypto algorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CP	Central Processor
EAL	Evaluation Assurance Level
HMC	Hardware Management Console
IOCDS	Input/Output configuration data set
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LIC	Licensed Internal Code
LPAR	Logical Partition
PP	Protection Profile
PR/SM	Processor Resource / System Manager
SE	Support Element
SF	Security Function
SFP	Security Function Policy
SIE	Start Interpretive Execution
SOF	Strength of Function
ST	Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

12.2 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.

13 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.[11]

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

[6] Security Target BSI-DSZ-CC-0557, Version 8.3, January 29, 2009, Security Target for PR/SM for the IBM System z10 Enterprise Class and IBM System z10 Business Class, IBM Corporation (confidential document)

[7] Evaluation Technical Report, Version 2.0, April 6, 2009, Evaluation Technical Report PR/SM for the IBM System z10 at Driver D76 Control Level 3, atsec information security GmbH (confidential document)

[8] Configuration lists for the TOE (confidential documents):
July 03, 2008, HMC Configuration List ZHMC
July 03, 2008, SE Configuration List ZSE
February 02, 2009, zSeries z10 EC GA2 and z10 MR GA2 (D76) LPAR Module List
December 18, 2008, RPM Configuration Mgmt Report
October 28, 2008, z10 EC and z10 BC publications: by Title
March 13, 2008, ODTs Solved or Dropped in z10EC GA2 - z10BC GA1

[9] Public Version of the Security Target BSI-DSZ-CC-0557, Version 8.3, January 29, 2009, Security Target for PR/SM for the IBM System z10 Enterprise Class and IBM System z10 Business Class, IBM Corporation (sanitised public document)

[10] Guidance documentation for the TOE, First Edition, October 2008, System z Hardware Management Console Operations Guide

[11] Guidance documentation for the TOE, Eighth Edition, October 2008, System z Input/Output Configuration Program User's Guide for ICP IOCP

[12] Guidance documentation for the TOE, Second Edition, October 2008, System z10 Processor Resource/Systems Manager Planning Guide

[13] Guidance documentation for the TOE, Fourth Edition, October 2008, System z10 and System z9 Stand-Alone Input/Output Configuration Program User's Guide

---

[11] specifically

- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 2.00, 24 October 2008, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document resp. CC Supporting Document and CCRA policies
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[14] Guidance documentation for the TOE, Fifth Edition, October 2008, System z10 Enterprise Class Installation Manual

[15] Guidance documentation for the TOE, First Edition, October 2008, System z10 Business Class Installation Manual

[16] Guidance documentation for the TOE, First Edition, October 2008, System z10 Enterprise Class Support Element Operations Guide

[17] Guidance documentation for the TOE, Third Edition, October 2008, System z10 Enterprise Class Service Guide

[18] Guidance documentation for the TOE, First Edition, October 2008, System z10 Business Class Service Guide

[19] Guidance documentation for the TOE, Fourth Edition, October 2008, System z10 Enterprise Class Installation Manual for Physical Planning

[20] Guidance documentation for the TOE, First Edition, October 2008, System z10 Business Class Installation Manual for Physical Planning

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:

- **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.
- **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:

- **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.
- **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:

- **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:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

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.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.