Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0900-2014

for

PR/SM for IBM zEnterprise EC12 GA2 and BC12 GA1
Driver Level D15F

from

IBM Corporation

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-0900-2014

Server Applications: Virtualization

PR/SM for IBM zEnterprise EC12 GA2 and BC12 GA1
Driver Level D15F

from	IBM Corporation
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, AVA_VAN.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 approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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, 19 February 2014

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

SOGIS Recognition Agreement for components up to EAL 4

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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

5 Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

This evaluation contains the components ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL4 components of these assurance families are relevant.

2.2 International Recognition of CC – Certificates (CCRA)

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 September 2011 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 website: 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 by the nations listed above.

This evaluation contains the components ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, and AVA_VAN.5 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 PR/SM for IBM zEnterprise EC12 GA2 and BC12 GA1, Driver Level D15F has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0846-2013. Specific results from the evaluation process BSI-DSZ-CC-0846-2013 were re-used.

The evaluation of the product PR/SM for IBM zEnterprise EC12 GA2 and BC12 GA1, Driver Level D15F was conducted by atsec information security GmbH. The evaluation was completed on 18 February 2014. atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: IBM Corporation.

The product was developed by: IBM Corporation.

[6] Information Technology Security Evaluation Facility

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, as specified in the following report and in the Security Target.

For the meaning of the assurance levels 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 evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual 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 PR/SM for IBM zEnterprise EC12 GA2 and BC12 GA1, Driver Level D15F has been included in the BSI list of certified products, which is published regularly (see also Internet: https://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] IBM Corporation
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 PR/SM for IBM zEnterprise EC12 GA2 and BC12 GA1, Driver Level D15F.

PR/SM is a hardware facility running on IBM System zEnterprise 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™, z/VSE, z/TPF™ or Linux for System z. These operating systems run unmodified in a PR/SM partition.

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 augmented by ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
Identification and Authentication	The TOE supports identification and authentication of users by means of • Unique identification via zone numbers assigned to each logical partition • Unique user IDs assigned to each user of the HMC/SE
Access Control and Information Flow Control	The TOE supports access control between users and resources by means of: The TOE implements LPAR Security Controls which define a partition's access to IOCDSs, performance data, cryptographic hardware, the channel reconfiguration process, and the authority to reset or shutdown other partitions. The TOE allows access to specific control units and devices on non-dedicated channels to be restricted. The TOE ensures that dedicated channels, storage and physical CPs are never shared. The TOE will prevent the transfer of any message between a logical partition and any resource not explicitly allocated to it. The TOE implements management access controls to define configurable role-based authorized administrator access to the TOE's management functions.
Auditing	The TOE supports auditing of relevant events by means of a security log with the following characteristics: • All security relevant events are recorded in the security log. This auditing mechanism cannot be bypassed.

TOE Security Functionality	Addressed issue
	• The security log is protected from unauthorized deletions or modifications. • Applications in logical partitions cannot read the security log. • The security log can be offloaded for archival purposes.
Authorized Administration and Operation	The HMC/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. In addition to a set of five 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 users (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.
Object Reuse	The TOE supports object reuse by means of: • Clearing of all storage prior to allocation or re-allocation. • Resetting all information in physical processors before dispatching the processor to a new logical partition. • Resetting non-shared channel paths and attached I/O devices prior to allocation to a logical partition.
Reliability of Service	The TOE supports the control of the processor running time and wait completion processor parameters. 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.
TSF Protection	The TOE supports TSF protection by means of: • Self test whenever the TOE is loaded and started and periodically during the TOE's operation. • The PR/SM kernel is loaded into a protected area of central storage where it is inaccessible by any users, operating systems or applications. • An alternate (backup) SE operates to provide real time mirroring of relevant system data: IOCDSs, audit log, image profiles.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 1.5.2.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapters 3.1, 3.2, and 3.3.

This certification covers the configurations of the TOE as outlined in 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:

PR/SM for IBM zEnterprise EC12 GA2 and BC12 GA1, Driver Level D15F

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	LPAR Licensed Internal Code (LIC)	D15F	n/a[8]
2	SW	HMC/SE Licensed Internal Code (LIC)	D15F	n/a[9]
3	DOC	Processor Resource/Systems Manager Planning Guide	SB10-7156-01 Level 00a	DVD
4	DOC	Hardware Management Console Operations Guide	2.12.1	Pre-installed as integral part of the HMC help system
5	DOC	Support Element Operations Guide	2.12.1	Pre-installed as integral part of the SE help system
6	DOC	Input/Output Configuration Program User's Guide for ICP IOCP	SB10-7037-11	DVD
7	DOC	Stand-Alone Input/Output Configuration Program User's Guide	SB10-7152-07	DVD
8	DOC	zEnterprise EC12 Service Guide	GC28-6915-01	DVD (for zEC12 only)
9	DOC	zEnterprise EC12 Installation Manual for Physical Planning 2827	GC28-6914-01	DVD (for zEC12 only)
10	DOC	zEnterprise BC12 Service Guide	GC28-6924-00	DVD (for zBC12 only)
11	DOC	zEnterprise BC12 Installation Manual for Physical Planning 2828	GC28-6923-00	DVD (for zBC12 only)

Table 2: Deliverables of the TOE

Note that the guidance documents listed in the above table as items 4 and 5 are also available online on the Internet via the IBM System z HMC and SE (Version 2.12.1) Information Center. However, the Processor Resource/Systems Manager Planning Guide

[8]Note that the customer is not provided with a media that contains the installable LIC. All LIC is installed at the customer's site by IBM personnel and tested before the system is handed over.

[9]Also the HMC/SE LIC is installed and tested by IBM service personnel prior to actually handing over the TOE to the customer.

[9] listed as item 3 in the table clearly states in its Appendix C that the pre-installed versions of those documents take precedence over their respective Information Center versions.

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:

- Identification and Authentication
- Access Control and Information Flow Control
- Auditing
- Authorized Administration and Operation
- Object Reuse
- Reliability of Service
- TSF Protection

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:

- Security log data stored off of the TOE must be controlled for confidentiality and integrity according to the owner's needs.
- Personnel working as administrators or other privileged positions must be carefully selected and trained.
- The TOE must be protected during the setup phase.
- Physical access and remote access to the HMC and zEC12 / zBC12 must be restricted only to authorized and approved users.
- 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.
- The underlying physical I/O LIC must provide separation mechanisms that can be used by the TOE to restrict access of one partition to authorized logical I/O resources.

Details can be found in the Security Target [6], chapter 4.2. Those are also outlined following an SFR-like notation in the Security Targer [6], chapter 6.

5 Architectural Information

The TOE is the PR/SM Licensed Internal Code (LIC) kernel running on the zEC12 GA2 and zBC12 GA1. The kernel provides the capability to initialize the zEC12 GA2 and zBC12 GA1 in LPAR mode, which is the only mode of operation. 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:

1. The LPAR LIC running on the Central Processing Complex (CPC) as hypervisor responsible for maintaining the isolation of logical partitions maintained and controlled by the TOE.
2. HMC LIC running on the Hardware Management Console (HMC) providing remote system administration functions to maintain the current configuration. The HMC is connected over internal network with one or more Support Elements.
3. SE LIC running on the Support Element (SE) physically located in the CPC cabinet and connected to the CPC. The SE also provides system administration functions to maintain the current configuration and can be used independently from an HMC connected to it.

PR/SM LIC provides the security administrator with the ability to define a completely secure system configuration. When the system is defined in such a manner, total separation of the logical partitions is achieved, thereby preventing a partition from gaining any knowledge of another partition's operation.

Only functions related to logical partition isolation, physical resource allocation, access control and audit are the subject of the Security Target. Additional functions of PR/SM related to normal operations and maintenance of the system are not considered as security enforcing functions, because the TOE will be configured to provide a configuration consistent with secure isolation such that these operations cannot be in conflict with the security policy of PR/SM.

The other functions are therefore not evaluated for correctness and no vulnerability analysis for those functions is performed.

The address space of the TSF is isolated from the address space of the partitions by hardware protection mechanisms (the "start interpretive execution" (SIE) instruction provided by the underlying processor as described below), and by the provision of separate hardware for the SE 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 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 an 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 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 IOCDSs, defining 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 z/Architecture® and ESA/390® architecture supports 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 instructions 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 and ESA/390 architectural mode. The SCP can define whether it is running in z/Architecture mode or ESA/390 mode by a use of a SIGP instruction. Typically, if the SCP understands z/Architecture mode, it gets into z/Architecture mode immediately and remains in that mode. But z/OS will switch back to ESA/390 if it needs to load the standalone dump program.

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.

The zEC12 GA2 and zBC12 GA1 provide 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 ensures 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 ESA/390 architecture (which includes the functions of ESA/370 Architecture), these models have problem-program compatibility with S/360TM, S/370TM, and 4300 processors. They can access virtual storage in multiple address spaces and data spaces. This extends addressability for system, sub-system, and application functions that use z/Architecture or ESA/390 architecture.

The Security Features are outlined in the following table.

TOE Security Functionality	Addressed issue
Identification and Authentication	The TOE supports identification and authentication of users by means of • Unique identification via zone numbers assigned to each logical partition • Unique user IDs assigned to each user of the HMC/SE For the logical partitions, there is no specific password. The logical partition is authenticated by its existence in the I/O Configuration Dataset (IOCDS) definition when activation occurs. The zone number is used to mediate access between the logical partition and the physical resources of the processor assigned to that logical partition. For the HMC/SE user, the required passwords are assigned by the security administrator. The use of the user ID and password allows the user of the HMC/SE to invoke the various functions that are defined as being allowed for that user ID.
Access Control and Information Flow Control	The TOE supports access control between users and resources by means of: • The TOE implements LPAR Security Controls which define a partition's access to IOCDSs, performance data, cryptographic hardware, the channel reconfiguration process, and the authority to reset or shutdown other partitions. • The TOE allows access to specific control units and devices on non-dedicated channels to be restricted. • The TOE ensures that dedicated channels, storage and physical CPs are never shared. • The TOE will prevent the transfer of any message between a logical partition and any resource not explicitly allocated to it. • The TOE implements management access controls to define configurable role-based authorized administrator access to the management functions of the TOE.
Auditing	The TOE supports auditing of relevant events by means of a security log with the following characteristics: • All security relevant events are recorded in the security log. This auditing mechanism cannot be bypassed. • The security log is protected from unauthorized deletions or modifications. • Applications in logical partitions cannot read the security log. • The security log can be offloaded for archival purposes.
Authorized Administration and Operation	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 HMC/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 base HMCs/SEs. **Operator** - A person with operator authority typically performs basic system start up and shutdown operations using predefine procedures.

TOE Security Functionality	Addressed issue
	Advanced Operator - A person with advanced operator authority possesses operator authority plus the ability to perform some additional recovery and maintenance tasks. **Programmer** - A person with 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 HMC or for service mode on the support element. A user profile consists of 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. 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 users (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. The following general definitions can be established: ***Administrator*** The Administrator is defined to be any user(s) with access to the HMC/SE workplace. ***Security Administrator*** Any administrator authorized to perform all of the following tasks: • Archive Security Logs • Change LPAR Controls • Change LPAR Group Controls • Change LPAR I/O Priority Queuing • Change LPAR Security • Customize/Delete Activation Profiles • Customize User Controls • Input/Output (I/O) Configuration • Logical Processor Add • Manage Users Wizard • Reassign Channel Path • User Profiles • View Security Logs A detailed list of the console actions authorized for each predefined role is contained in the Hardware Management Console Operations Guide [8].
Object Reuse	The TOE supports object reuse by means of:

TOE Security Functionality	Addressed issue
	• Clearing of all storage prior to allocation or re-allocation. • Resetting all information in physical processors before dispatching the processor to a new logical partition. • Resetting non-shared channel paths and attached I/O devices prior to allocation to a logical partition.
Reliability of Service	The TOE supports the control of the processor running time and wait completion processor parameters. 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
TSF Protection	The TOE supports TSF protection by means of: • Self test whenever the TOE is loaded and started and periodically during operation. • The PR/SM kernel is loaded into a protected area of central storage where it is inaccessible by any users, operating systems or applications. • An alternate (backup) SE operates to provide real time mirroring of relevant system data: IOCDSs, audit log, image profiles.

Table 3: Summary of security features

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. Please note that the evaluated guide is being shipped with the TOE, additional available documentation has not been part of the assessment.

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

7.1 Test Configuration

With respect to the underlying hardware used, the test configuration is identical to the evaluated configuration of the TOE. However, some of the configuration requirements mandated by the Processor Resource/Systems Manager Planning Guide [9] do not fully apply to the test configuration as they refer to secure operation of the TOE at the customer's site. Moreover, in some cases overriding safeguards mandated for the TOE, like, for instance, security authorities settings for partitions, was required to actually perform tests related to that safeguard, i.e. to verify that with an authority enabled, a logical partition in fact may perform actions but cannot do so with that authority removed.

The evaluator assessed the configuration deviations identified during his analysis of developer test cases and test approach and concluded that the configuration tested by the developer was consistent with the evaluated configuration of the TOE. When performing his independent tests, the evaluator deliberately invalidated the configuration requirements in order to observe the behaviour of the TOE, which he also considered a valid and acceptable approach. At any time during his testing, the evaluator considered the TOE to be in its evaluated configuration.

7.2 Developer Testing

For security-specific testing the evaluator identified the following developer testing effort:

- The security test suite is run for any major driver change.
- A random subset of the security test suite must be included in the driver regression testing

This ensures that changes to the driver do not affect the security functions of the TOE.

There is significantly more effort spent by the developer in addition to the security-specific testing:

- New features that are implemented in the TOE have to follow the strict development procedures. This includes, that in parallel to the design, test cases need to be written. This is done by creating test variation lists, i.e. checking what variations of inputs, configurations etc. need to be tested, and writing test cases. The whole process is shadowed by review cycles ensuring a broad agreement, and coverage of all necessary test scenarios. If the design documentation points out that other parts of the system may be affected by the new feature, test cases are written to verify that there is no negative impact. Tests must complete successfully before the new feature is approved.
- If errors are reported, the TOE gets fixed by the developer. After fixing the bug and informal testing by the developer, the newly built driver is tested to verify that the bug is fixed. Normal regression tests ensure that the TOE as a whole is still functional.
- New drivers are tested using an internal proprietary test program, which is also included in the test suite. The internal proprietary test program is used for rigorous and continuous testing of the TOE. It provides a pseudo-random stream of instructions from a customizable set of instructions that are issued to a logical partition, thus simulating a running application. The tool would reveal unexpected system behavior during the intense test runs on the TOE, e.g. if some processor instructions are not properly simulated by the TOE. Running the internal proprietary test program successfully for a long period without crash and without detecting unexpected behaviour, gives a rather good confidence that the TOE is working correctly.

There are no specific configuration requirements for the TOE to be tested in its evaluated configuration apart from running the tests on one of the hardware platforms listed in the ST using the appropriate version of the TOE (i.e. the driver level D15F) and configuring the separation conditions as required by assumption A.Sep_Strength and Appendix C of [9].

Additional requirements and assumptions from the ST may be neglected for testing since they have been considered to have no impact on the testing itself nor do they impact the security functionality of the TOE.

The evaluator concluded that the configuration chosen for developer testing was in accordance with the evaluated configuration as defined by the ST.

The tests performed by the developer were at the level of the modules of the TOE design.

The actual test results obtained by the developer during the developer testing performed in September 2013 matched the expected test results laid down in the test documentation. Also, the internal proprietary test program did not return any deviation from the z/Architecture definition.

7.3 Evaluator Testing Effort

The following testing was performed by the evaluator:

a) TOE test configurations:

The tests were performed on the following system:

- IBM System zEC12 server H43 model and zBC12 server H13 model at microcode driver level D15F. This configuration is consistent with the platform configuration given in the ST.

The correct driver level was confirmed by the evaluator using the System Information Panel on the Support Element logged on in SERVICE mode. The System Information Panel stated driver level D15F, which matches the TOE version stated in the ST.

The general machine configuration was modified on a test-specific basis (e.g. by defining specific IOCDS) to adapt the machine configuration to the test purpose. No external connectivity was enabled throughout the tests. As a result of this setup, the TOE at any time was in its evaluated configuration when performing the evaluator tests.

b) Subset of independently repeated developer tests

The evaluator performed a subset of the developer test suite, deliberately skipping the internal proprietary test program, which has already been confirmed to be effective by multiple evaluations. The sampled subset chosen was considered appropriate in size and coverage.

The following security functions as stated in the ST were subject to testing:

1. Identification and Authentication
2. Access Control and Information Flow Control
3. Auditing
4. Authorized Administration
5. Authorized Operation
6. Reliability of Service
7. TSF Protection (Self Test)

As a result of testing the above-mentioned security functions, the following interfaces (TSFI) have been included in the evaluator testing:

1. GUI as part of testing of all security functions

2. z/Architecture as part of tests related to security function Authorized Operation
3. Proprietary internal interfaces as part of tests related to all tested security functions except Self Test
4. CHSC as part of tests related to security functions Authorized Operations and Object Reuse
5. IOCP as part of tests related to security function Access Control and Information Flow Control
6. SIE as part of all tests that involve running LPARs[10]

The subset chosen by the evaluator covers all interfaces to the TOE security functions.

In addition to repetition of developer tests, the evaluator applied variations to the test steps and input data and observed the deviating results of the TOE.

c) Verdict for the activity:

The overall judgement on the results of testing during the evaluation is that all security tests passed, i.e. the actual results achieved by the evaluator either exactly matched the expected results, or, in case of test variations, matched the expectation of the evaluator.

By using developer tests as a base for independent testing, the evaluator achieved the same test depth as the developer when performing the developer tests. Therefore, the tests performed by the evaluator were at the level of the modules of the TOE design.

There were no failed tests that were caused by TOE behaviour different from the expected behavior or violating requirements stated in ST.

7.4 Evaluator Penetration Testing

The evaluator did neither devise nor conduct additional penetration testing apart from his source code analysis performed with respect to an identified potential vulnerability. That analysis at level of the LPAR LIC source code was based on an assumed misuse of a proprietary internal interface in order to gain unauthorized access to storage areas actually allocated to partitions other than the partition using that proprietary internal interface. Examination of the implementation revealed that no such penetration is feasible.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The Target of Evaluation is PR/SM for IBM System zEC12 GA2 and zBC12 GA1 at driver level D15F. The TOE is firmware only and is accompanied by guidance documentation. The items listed in table 2 of this report represent the TOE.

The TOE can be run on a number of hardware models all belonging to the IBM zEC12 GA2 and zBC12 GA1 server families. The various machine models are not part of the TOE but provide the underlying abstract machine for TOE operation. The supported machine

[10]Note that SIE is a TSFI not accessible from the outside but invoked whenever a logical partition is operative.

models differ with respect to the number of available central processors. However, those differences have no impact on the validity of the evaluation activities performed.

A detailed list of supported machine models is given in section 1.5.3 of the ST [6], which is the base for evaluation.

The evaluated configuration of the TOE is defined by the mandatory configuration requirements to be met as stated in section "Trusted Configuration" in Appendix C of [9]. The ST [6] directly redirects readers to this document, which is part of the deliverables as listed in table 2.

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 EAL5 extended by advice of the Certification Body for components beyond EAL 5 [4] (AIS 34).

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

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0846-2013, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the new suppported hardware and feature refinements.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, AVA_VAN.5

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 cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

10 Obligations and Notes for the Usage of the TOE

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

Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

AIS Application Notes and Interpretations of the Scheme

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

LIC Licensed Internal Code

LPAR Logical Partition

PP Protection Profile

PR/SM Processor Resource/Systems Manager™

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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.

I/O Configuration Data Set - This is a system file that defines the available logical partitions, and the allocation of the available the I/O devices to the defined logical partitions.

Informal - Expressed in natural language.

Logical Partition - A virtual machine which runs on the host system. It has a unique identifier (the zone number) and name. A logical partition can be both an object and a user of the system. A logical partition has attributes determining whether the logical partition is authorized for various actions. Other attributes define the amount of logical processor and storage resources to be allocated to the partition, and the scheduling parameters for the partition's processors. The possible logical partitions are defined in the current configuration object. Only activated logical partitions may use the system.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[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), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0900-2014, Version 13.5, 17 February 2014, Security Target for PR/SM for IBM zEnterprise EC12® (zEC12) GA2 and BC12® (zBC12) GA1, IBM Corporation

[7] Evaluation Technical Report, Version 2, 18 February 2014, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] Hardware Management Console Operations Guide, Version 2.12.1, September 2013

[9] Processor Resource/Systems Manager Planning Guide, Version SB10-7156-01 Level 00a, 14 February 2014

[11] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 38, Version 2, Reuse of evaluation results

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC 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 augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.