C043 Certification Report

IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088

File name: ISCB-5-RPT-C043-CR-v1b
Version: v1b
Date of document: 31 May 2013
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C043 Certification Report

IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088

31 May 2013

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines, No 7 Jalan Tasik,

The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8992 6888 Fax: +603 8992 6841

http://www.cybersecurity.my

Copyright Statement

Registered office:

Level 5, Sapura@Mines,

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Forward

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 31 May 2013, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
v1	26 April 2013	All	Final Released.
v1a	17 May 2013	Page vii, 1, 6, 12, 13	Incorporated additional comments received.
v1b	31 May 2013	Page iv	Add the date of the certificate.

Executive Summary

IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088 (hereafter referred as LPAR) from International Business Machine (IBM) Corporation is the Target of Evaluation (TOE) for Evaluation Assurance Level 4 augmented with ALC_FLR.2 (EAL4+ ALC_FLR.2) evaluation.

LPAR has been evaluated in the context of hardware models 770 (AM740_088 firmware) and 795 (AH730_087 firmware). The TOE firmware is designed to abstract and virtualise physical hardware resources to provide secure access to the underlying platform for one or more concurrent operating systems. Each virtual platform is known as a partition. The operating systems executing in the available partitions are treated as subjects of the TOE, where the TOE not only provides the necessary operational support for the hosted operating systems, but also serves to separate them from each other to ensure mutual non-interference.

While not included as part of the TOE, the TOE is configured using a connected Hardware Management Console (HMC) that provides access to the functions necessary to enable administrative personnel to effectively manage the allocation of resources (i.e., processors, memory, and I/O devices) to the configured partitions. Once the TOE is configured, the HMC must be disconnected so that it offers no interfaces while the TOE is operating in its evaluated configuration.

The security functions of the TOE that are within the scope of evaluation are user data protection, identification and authentication, security management, and protection of the TOE security function.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements.

Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

It should be noted that the scope of the TOE is purely the Hypervisor firmware of the IBM Power 770 and Power 795 server platforms. The underlying resources, including Disks, CPU, RAM, or networking, including the internal virtual switch are considered to be part of the TOE environment. It is recommended that the end customer perform their own testing of the environment that surrounds the TOE to confirm its suitability for use.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) EAL4 augmented with ALC_FLR.2. The report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the BAE Systems Detica evaluation facility (the 'BAE Systems Detica MySEF') and was completed on 25 March 2013.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangement on the Recognition of Common Criteria certificates and the product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that the LPAR meets their requirements. It is recommended that a potential user of the LPAR to refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088 (hereafter referred as LPAR), has been evaluated in the context of hardware models 770 (AM740_088 firmware) and 795 (AH730_087 firmware). The TOE firmware is designed to abstract and virtualise physical hardware resources to provide secure access to the underlying platform for one or more concurrent operating systems. Each virtual platform is known as a partition. The operating systems executing in the available partitions are treated as subjects of the TOE, where the TOE not only provides the necessary operational support for the hosted operating systems, but also serves to separate them from each other to ensure mutual non-interference.

2 While not included as part of the TOE, the TOE is configured using a connected Hardware Management Console (HMC) that provides access to the functions necessary to enable administrative personnel to effectively manage the allocation of resources (i.e., processors, memory, and I/O devices) to the configured partitions. Once the TOE is configured, the HMC must be disconnected so that it offers no interfaces while the TOE is operating in its evaluated configuration.

3 The TOE consists of the PowerVM Hypervisor which provides the virtualisation. The other components of the LPAR such as the Hardware Management Console (HMC), Flexible Service Processor (FSP), Bulk Power Assembly (BPA) and operating systems are outside the TOE scope. The underlying resources of the IBM Power 770 and Power 795 server platforms, including Disks, CPU, RAM, or networking, including the internal virtual switch are considered to be part of the TOE environment.

4 In the context of the evaluation, the TOE provides the following major security features:

a) User data protection – the TOE is designed to instantiate multiple partitions for the purpose of supporting and isolating simultaneous operating systems. As such, it implements a policy where each partition can access only those resources explicitly assigned to it. In terms of access control, the CPU, memory, and I/O devices can be assigned to a given partition and a partition can access those resources only when they are assigned to it.

b) Identification and authentication – the active entity or user of the TOE is partition, which it instantiates. Partitions are implicitly identified and authenticated by internal numerical identifiers associated with partitions (using internal data structures) as they are defined. Being implicitly identified by the TOE, partitions have no need, nor means, to identify themselves. Furthermore, the identification of a partition is guaranteed by the TOE and as such each partition is also continuously authenticated.

c) Security management – the TOE supports several management functions to configure the TOE via the dedicated physical HMC interface (out of scope for

this evaluation). Once the TOE is operational (in evaluated configuration), the TOE effectively doesn't offer any security management functions. However, the TOE serves to restrict the ability to change its own configuration nonetheless.

d) Protection of the TOE Security Function (TSF) – the components of the TOE that protect themselves using the domains provided by Power7 processors. The TOE operates in the privileged domain and the partitions operate in the unprivileged domain. This allows the TOE to protect itself as well as the resources it makes selectively available to the applicable partitions. Beyond protecting itself and its resources, the TOE is also designed such that when the hardware that supports a partition fails, the other partitions will continue uninterrupted.

1.2 TOE Identification

5 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C043
TOE Name	IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088
TOE Version	AH730_087 or AM740_088
Security Target Title	IBM Logical Partition Architecture for Power 7 Security Target
Security Target Version	v0.33
Security Target Date	8 March 2013
Assurance Level	Evaluation Assurance Level 4 augmented with ALC_FLR.2 (EAL4+ ALC_FLR.2)
Criteria	Common Criteria July 2009, Version 3.1, Revision 3
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL4 augmented with ALC_FLR.2 (EAL4+ ALC_FLR.2)
Sponsor and Developer	International Business Machine (IBM) Corporation

	3605 Hwy 52 North Rochester, MM 55901 United States
Evaluation Facility	BAE Systems Detica MySEF

1.3 Security Policy

6 The TOE is designed to instantiate multiple partitions for the purpose of supporting and isolating simultaneous operating systems. As such, it implements a policy where partitions can access only those resources explicitly assigned to it. An access control policy is defined which covers all resources as well as all operations via the HMC (out of the evaluation scope). However, the HMC will be disconnected once the TOE is operational in order to restrict the security management functions.

7 CPU, memory, and I/O device resources can be assigned to only one partition at a time. CPUs, memory, and I/O devices cannot be dynamically re-allocated, though they could be reallocated when the TOE is reconfigured while not in an operational state.

8 The TOE offers no means of direct communication among partitions, so all means of inter-partition communication within the scope of the TOE are controlled (i.e. prevented).

9 The details of these security policies are described in Section 6 of the Security Target (Ref [6]).

1.4 TOE Architecture

10 The TOE includes both logical and physical boundaries which are described in Section 2.2 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

11 The TOE security functions comprises of the following:

a) **User data protection**

The TOE is designed to instantiate multiple partitions for the purpose of supporting and isolating simultaneous operating systems. As such, it implements a policy where each partition can access only those resources explicitly assigned to it.

The TOE manages the association of CPUs, memory, and I/O devices, in a relatively static environment, with partitions containing operating system instances. CPU, memory and I/O devices are permanently assigned to a partition during configuration time via HMC interface.

The TOE also provides a mechanism where users can create LPAR groups (also referred to as eWLM groups) where a list of partitions are allowed to share the

quantity of resources (memory and processors but not I/O) between the partitions. The resource is still owned at any point in time by one and only one partition but the operating system is given the ability to remove the resource from one partition and another partition can add the resource to their partition in the same group. The TOE clears out the state of the resource before it is moved between partitions.

Partitions have no control over the resources they are assigned. The TOE receives the partition management information from the HMC when it is being configured. Once configured, the HMC is disconnected and the TOE is placed in an operational state where those assignments are continuously enforced.

b) **Identification and authentication**

The active entity or user of the TOE is partitions, which it instantiates. When partitions are defined, they are assigned unique numbers in TOE-internal data structures which are subsequently used to identify the partition and to associate resources with the partition. Once a partition is created, its number will not change except when it is deleted and recreated. Given that each partition is uniquely identified by the TOE using TOE-internal data structures, the TOE effectively ensures that each partition is authenticate on a continuous basis.

c) **Security management**

The TOE is configured via the HMC interface. Since the HMC is disconnected while the TOE is operational, the TOE effectively doesn't offer any security management functions. The resulting configuration data is pushed to the TOE prior to it being placed in an operational; evaluated configuration.

When operational, the TOE restricts the security management functions by offering no interfaces to manipulate them to its subjects (i.e., partitions). The available directly connected operator panel offer no ability to perform any security management related function. The architecture of the TOE prevents bypass and tampering of its mechanisms to ensure that inappropriate users cannot perform any security management functions.

d) **Protection of the TSF**

The components of the TOE protect themselves using the domains provided by the Power7 processors. The TOE operates in the privileged domain where full, unconstrained access to the available resources (CPUs, memory, and I/O devices) is available. Even though the TOE shares the available CPUs with its instantiated partitions, the contexts of the CPUs are saved and restored appropriately during every context switch to ensure uninterrupted operation of the TOE and the partitions.

Meanwhile, the partitions operate in the unprivileged domain where those partitions can access only resources that have been allocated for use by the associated partitions.

This allows the TOE to protect itself as well as the resources it makes selectively available to the applicable partitions. The TOE ensures that its

security mechanisms cannot be bypassed by encapsulating partitions with their assigned resources and offering only limited interfaces that are designed to ensure that partitions cannot interfere with other partitions or the TOE's own operation.

When the TOE detects a memory or I/O device failure, the TOE will shut itself down. Given that the TOE is configured and stored in firmware, it will be restored to its previous state when it is restarted. While the contents of a given partition could potentially be corrupted, the TOE itself cannot be corrupted by transient failures (such as memory errors).

1.4.2 Physical Boundaries

12 The TOE consists of a number of architectural components. The components expose a number of interfaces both externally and internally.

13 The external interfaces include the interfaces to the subject operating in a partition. These include the Hypervisor interfaces as well as the hardware instructions available to applications.

Note that when operating in the evaluated configuration, the HMC used to configure the TOE is detached and, hence, does not represent an interface. There is also an operator panel where basic, non-security related operator functions can be performed by a user with direct physical access to the TOE.

14 The internal interfaces include the FSP interface to the Hypervisor.

15 I/O represents the physical I/O slots either integrated into the hardware drawers or I/O drawers external to the server. The I/O adapters allow for the connection of disk, network, SAN, tape and other individual I/O devices.

Note that connections to a broad or public network are supported, but they would be treated as resources that can be granted to partitions for operating system use, but would not be used by TOE for its own purposes. Along these lines, while the TOE controls which devices a given partition can access, it does not control or otherwise constrain the nature of those devices. Any functions or connections of those devices are outside the scope of control of the TOE.

16 Figure 1 below describes the component of LPAR that comprises the TOE (in yellow box).

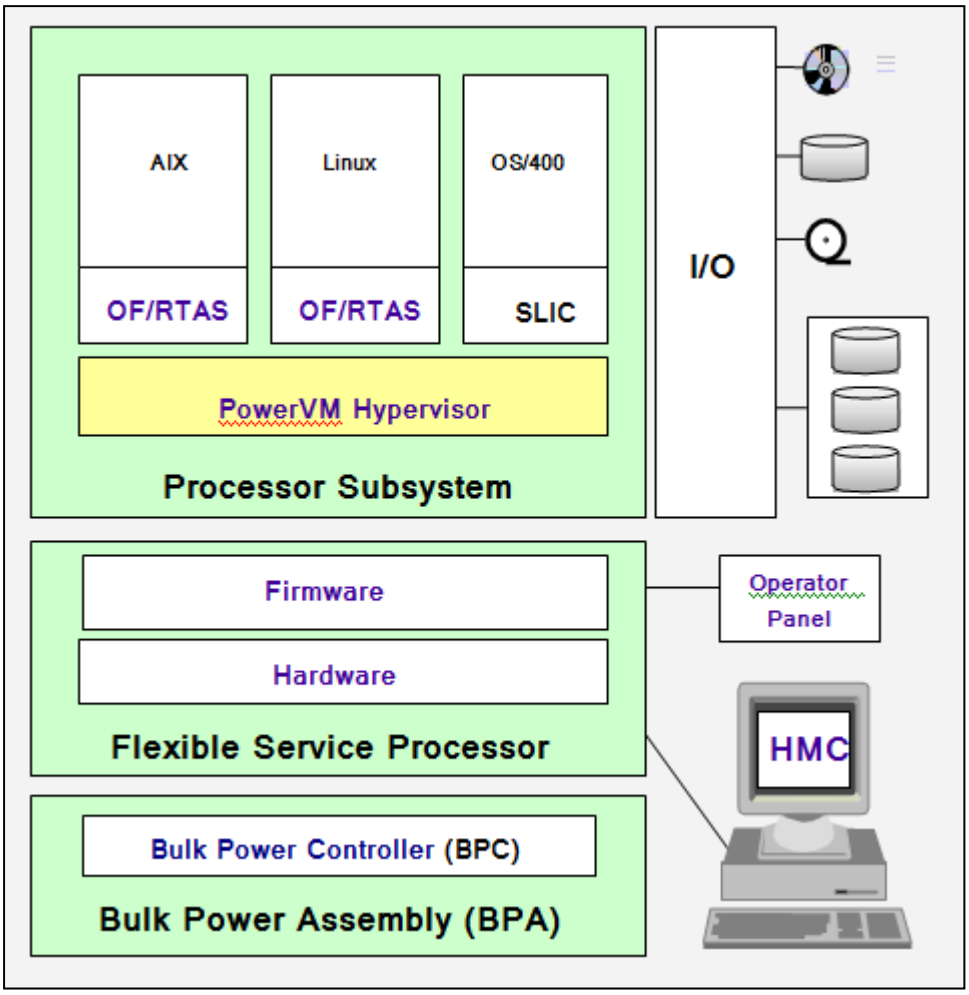

Figure 1: LPAR Architecture (TOE in yellow box)

1.5 Clarification of Scope

17 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures such as physical access protection, and secure installation and usage based on user guidance that is supplied with the product.

18 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]). The TOE consists of the PowerVM Hypervisor which provides virtualisation. The other components of the LPAR such as the Hardware Management Console (HMC), Flexible Service Processor (FSP), Bulk Power Assembly (BPA), I/O devices (including CPU, Disk, and physical and virtual networking), and operating systems are outside the scope of the evaluation.

19 Potential consumers of the TOE are advised that some functions and services of the overall product have not been tested as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

20 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE as defined in subsequent sections and in the Security Target (Ref [6]).

1.6.1 Environment assumptions

21 Assumptions for the TOE environment listed in the Security Target are:

a) The TOE is assumed to be appropriately installed, including connections to device resources as well as being disconnected from the management console when operational.

1.6.2 Physical assumptions

22 Assumptions for the TOE physical environment listed in the Security Target are:

a) The TOE and its connections are assumed to be physically protected from unauthorised access or modification.

1.6.3 Personnel assumptions

23 Assumptions for the users listed in the Security Target are:

a) The TOE is assumed to be managed by users who are capable and trustworthy and will follow the applicable guidance correctly.

1.7 Evaluated Configuration

24 The TOE is firmware, AM740_088 and AH730_087, operating on IBM Power7 Systems hardware models 770 and 795, as described in Section 2 of the ST (Ref [6]). The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance (Ref 32b)).

1.8 Delivery Procedures

25 IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088 is delivered to the customer using the procedure described in the Delivery Procedure (Ref 32a)) which ensures that it is securely transferred from development environment into the responsibility of the customer. The delivery procedures are outlined below.

26 To order the evaluated product, a customer must order a Power Server machine (770 or 795 model) along with the system firmware driver (AM740_088 or AH730_087). Information about Power Servers and the Logical Partition Architecture can be found at www.IBM.com.

27 When the Power Server is shipped to a customer, it is pre-loaded with the latest level of system firmware. Customer must check whether the Power Server is installed with the evaluated firmware (AM740_088 or AH730_087).

28 The evaluated firmware (AM740_088 or AH730_087) is available for download by a customer through the "Fix Central" web page at http://www-933.ibm.com/support/fixcentral/?mode=10&page=isoiec.html.

29 From that website, the customer enters the server type and model that they have and then chooses the evaluated firmware images (AM740_088 or AH730_087). The customer downloads the ISO image file and writes to a DVD to be used by the HMC to install the evaluated firmware.

30 In order to check that the firmware downloaded is not tampered, IBM publishes a checksum value in the readme file for the firmware. The customers can use the AIX sum command to validate the checksum of the rpm file against the published checksum value. In addition, IBM also does a digital signature check of the firmware when firmware is installed.

1.9 Documentation

31 To ensure secure usage of the product, it is important that the TOE is used in accordance with guidance documentation.

32 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

a) IBM Logical Partitioning Architecture on Power Server Common Criteria System Delivery Procedures, v2.1, 7 December 2012

b) Common Criteria Installation Instructions for IBM Logical Partitioning Architecture on Power Server, version 4.0, 20 December 2012

c) Power Systems: Installing and configuring the Hardware Management Console, 2011

d) Power Systems: Managing the Hardware Management Console, 2012

e) Power Systems: Logical partitioning, 2012

2 Evaluation

33 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 4 Augmented with ALC_FLR.2 (EAL4+ ALC_FLR.2). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

34 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

35 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items.

36 It is evaluated that the implemented configuration management system can control changes to those items that have been placed under configuration management system. The developer's configuration management system was also observed during the site visit, and it was found security flaws under configuration management ensures that security flaw reports are not lost or forgotten, and allows a developer to track security flaws to their resolution. This is evaluated to be consistent with the provided evidence.

37 During the site visit, the evaluators examined the development security documentation and determined that it detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the TOE design and implementation. The evaluators confirmed that the developer used a documented life-cycle model which provides necessary control over the development and maintenance of the TOE by using procedures, tools and techniques described by the life-cycle model.

38 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

39 The evaluators analysed the TOE functional specification and design documentation; they determined that the design completely and accurately describes the TOE

security functionality (TSF) interfaces, the TSF subsystems and modules. The design described the TOE subsystems to sufficiently determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing modules and enough information about the SFR-supporting and SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented.

40 The evaluators analysed the TOE security architectural description and determined that the delivery and installation process was secure and the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

2.1.3 Guidance documents

41 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

42 Testing at EAL4 consists of assessing developer tests, performing independent function test, and performing penetration tests. The TOE testing was conducted by evaluators from BAE Systems Detica MySEF at the IBM Lab in Rochester, Minnesota, USA where it was subjected to comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

43 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

44 The evaluators analysed the developer's test coverage and depth analysis, and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the implementation representative, functional specification, TOE design, and security architecture description was complete.

2.1.4.2 Independent Functional Testing

45 Independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a sample of the developer's test plan, and creating test cases that augmented the developer tests.

46 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
To test a sample of retired SLIC Hcalls, to verify that they do not return with any meaningful values.	FDP_ACF.1, FDP_IFF.1	SLIC_HCALL	**PASS**. The TOE does not return any meaningful value and only returns the value that is expected to be displayed; in this case, the value is 5.
To test a sample of retired RPA Hcalls, to verify that they do not return with any meaningful values.	FDP_ACF.1, FDP_IFF.1	RPA_HCALL	**PASS**. The TOE only returns value r3 which indicates that RPA Hcall has failed.
To verify that an assigned I/O bus is only accessible by the Partition that owns that bus, and that assigned I/O buses are associated with the Partition ID of the owner.	FIA_USB.1, FDP_ACF.1	SLIC_HCALL	**PASS**. The partition can only access the I/O buss that is associated with the partition ID only.
To verify that the H_SET_TOD RPA HCALL cannot be performed by partitions.	FDP_IFF.1	RPA_HCALL	**PASS**. The partition could not set up the system time.
To verify that a new partition cannot be created with the same partition ID as an existing partition.	FMT_MSA.3	–	**PASS.** The TOE implements proper resource access control policy and partition separation policy.
Simulate an I/O device failure by removing a physical Ethernet card assigned to a running partition.	FPT_FLS.1	LPEVENT	**PASS.** The error is logs by HMC and the TOE still maintains the

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
			secure state.
Attempt to set the minimum memory value to a value higher than the amount of assigned memory.	FDP_IFF.1, FDP_ACF.1	SLIC_HCALL	**PASS.** The TOE only allows the minimum value set and large value are interpreted as an invalid value.

47 The testing of the TOE produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

48 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE and to determine whether these were exploitable in the intended operating environment of the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, security architecture description, and implementation representation.

49 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE, in its operational environment, is resistant to attack performed by an attacker possessing a High attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

50 The penetration tests focused on the network leakage from the management console.

51 The penetration testing did not uncover any exploitable vulnerability in the anticipated operating environment. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.4 Testing Results

52 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

53 Based on the results of penetration testing, the evaluators determined that the TOE is resistant to an attacker possessing an Enhanced Basic attack potential.

3 Results of the Evaluation

54 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088 performed by the BAE Systems Detica MySEF.

55 The BAE Systems Detica MySEF found that IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL4+ ALC_FLR.2.

56 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

57 EAL4 provides assurance by a full Security Target (ST) and an analysis of the security functions in the ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation to understand the security behaviour.

58 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhance-Basic attack potential.

59 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

3.2 Recommendations

60 In addition to ensure secure usage of the product, below are additional recommendations for IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088 consumers:

a) The users of the TOE should make themselves familiar with the developer guidance provided with the TOE; and

b) TOE owners should test the the IBM Power 770 and Power 795 server platforms to ensure that the underlying environment meets their requirements.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] IBM Logical Partition Architecture for Power 7 Security Target, v0.33, 8 March 2013

[7] EAL4+ ALC_FLR.2 Evaluation of IBM Logical Partition Architecture for Power7 operating on IBM Power Systems hardware with AH730_087 or AM740_088, v1.0, 25 March 2013

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
BPA	Bulk Power Assembly
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
FSP	Flexible Service Processor
HMC	Hardware Management Console
I/O	Input/Output
IEC	International Electrotechnical Commission
ISCB	Information Security Certification Body
ISO	International Standards Organisation
LPAR	Logical Partition Architecture

Acronym	Expanded Term
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
RFC	Request for comment
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA.
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65.
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.

Term	Definition and Source
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user that does not affect the operation of the TSF.

--- END OF DOCUMENT ---