National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

International Business Machines Corporation, Rochester, MN 55901

IBM Logical Partition Architecture for Power Systems

Report Number:	**CCEVS-VR-VID10299-2008**
Dated:	**26 November 2008**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Kenneth Elliott
Aerospace Corporation
Columbia, MD

Kenneth Eggers
Orion Security Solutions
McLean, VA

Common Criteria Testing Laboratory

Tammy Compton
Gary Grainger
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 3
3.1 Architecture Overview 3
3.2 Physical Boundaries 4
4 Security Policy 5
4.1 User Data Protection 5
4.2 Identification and Authentication 5
4.3 Security Management 6
4.4 Protection of the TOE Security Functions 6
5 Assumptions 6
6 Documentation 6
6.1 Configuration Management 6
6.2 Delivery and Operation 7
6.3 Design Documentation 7
6.4 Guidance Documentation 7
6.5 Life Cycle 7
6.6 Testing 7
6.7 Vulnerability Assessment 8
7 IT Product Testing 8
7.1 Developer Testing 8
7.2 Evaluation Team Independent Testing 8
8 Evaluated Configuration 8
9 Results of the Evaluation 8
9.1 Evaluation of the Security Target (ASE) 9
9.2 Evaluation of the Configuration Management Capabilities (ACM) 9
9.3 Evaluation of the Delivery and Operation Documents (ADO) 9
9.4 Evaluation of the Development (ADV) 9
9.5 Evaluation of the Guidance Documents (AGD) 10
9.6 Evaluation of the Life Cycle Support Activities (ALC) 10
9.7 Evaluation of the Test Documentation and the Test Activity (ATE) 10
9.8 Vulnerability Assessment Activity (AVA) 10
9.9 Summary of Evaluation Results 10
10 Validator Comments/Recommendations 11
11 Annexes 11
12 Security Target 11
13 Glossary 11
14 Bibliography 12

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of IBM Logical Partition Architecture for Power Systems (henceforth referred to as LPAR). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in November 2008. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2.

LPAR is a product that facilitates the sharing of hardware resources by disparate applications (e.g., AIX, Linux). The product is based on the concept of a 'hypervisor' that is designed to instantiate 'partitions', each with its own distinct resources, that each appear to their hosted applications as a completely functional underlying platform. These partitions are implemented to prevent interference among partitions and to prevent simultaneous sharing of storage and other device resources (adapters).

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validators therefore conclude that the evaluation team’s results are correct and complete.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the IBM Logical Partition Architecture for Power6 Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	IBM Logical Partition Architecture for Power6 operating on IBM Power Systems hardware (models E8A, MMA, and FHA)
Protection Profile	None
ST:	IBM Logical Partition Architecture for Power System Security Target, Version 1.0, November 21, 2008
Evaluation Technical Report	*Evaluation Technical Report for IBM Logical Partition Architecture* *for Power Systems, (Proprietary), Version 4.0, October 27, 2008*
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3 Part 2: Evaluation Methodology, Supplement: ALC_FLR- Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R
Conformance Result	CC Part 2 conformant, CC Part 3 conformant
Sponsor	IBM
Developer	IBM
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD

Item	Identifier
CCEVS Validators	Kenneth Elliott, Aerospace Corporation, Columbia, MD Kenneth Eggers, Orion Security Solutions, McLean, VA

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is a set of hardware and firmware designed to abstract and virtualize physical hardware resources to provide 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.

The TOE is configured using a connected Hardware Management Console (HMC) that, while not included as part of the TOE, provides access to the functions necessary to enable administrative personnel to effectively manage the allocation of resources (i.e., processors, memory, and I/O device adapters) 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.

3.1 Architecture Overview

The TOE consists of a number of layered components as follows:

1. Processor Subsystem consisting of
    a. **PowerPC Hypervisor (PHYP):** provides virtualization and other advanced server functions, and
2. Flexible Service Processor (FSP) Component consisting of
    a. **Hardware:** an IBM pSeries or iSeries (utilizing IBM Power6 CPUs), and
    b. **Firmware:** provides APIs to the hosted processor subsystem and the means to communicate with the HMC to facilitate the dynamic management of partitions
3. Bulk Power Assembly (BPA) consisting of
    a. **Bulk Power Controller (BPC):** controls power available to the rest of the components.

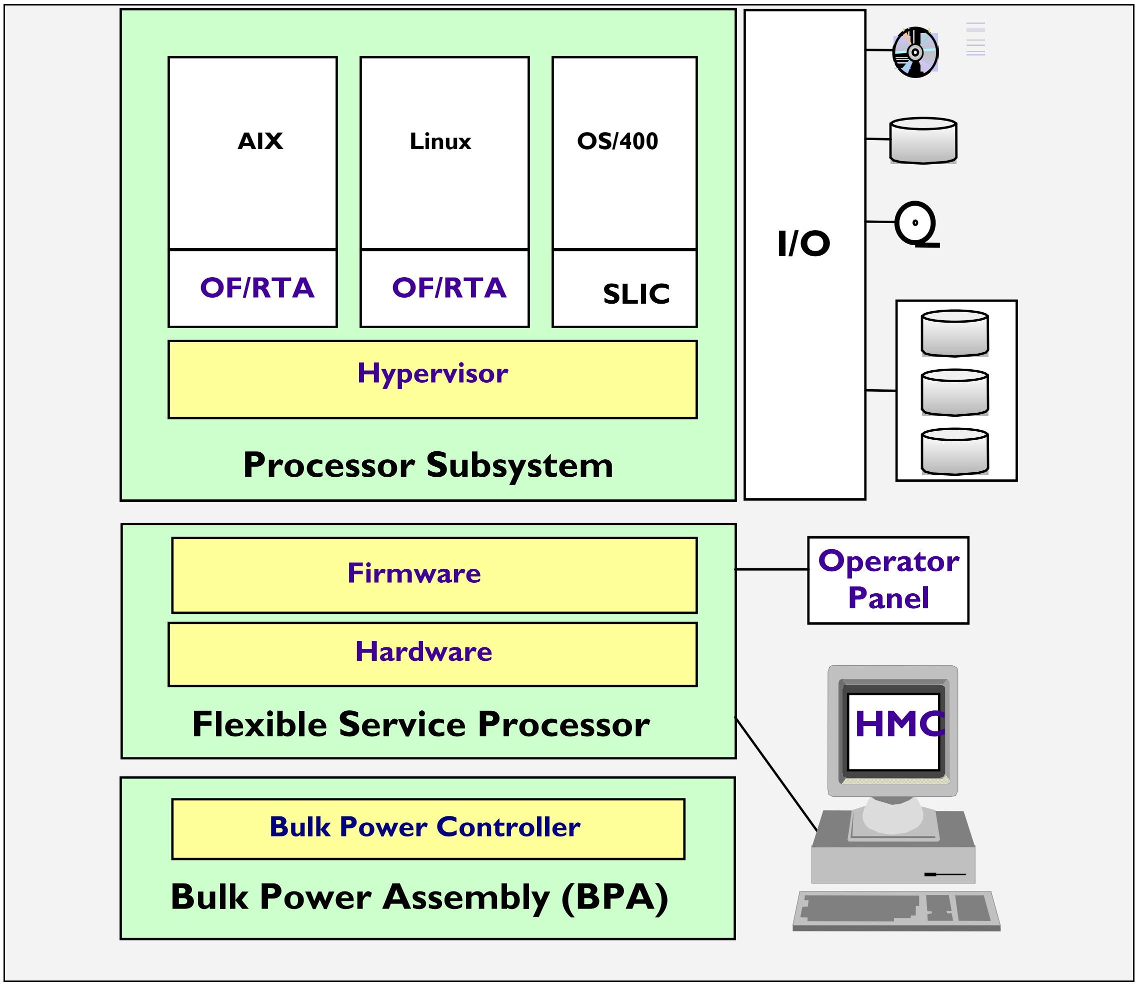

Figure 1: LPAR Architecture

Note that Figure 1 identifies the TOE components in the yellow-filled boxes inside the green-filled boxes. Note that the operating systems within the partitions are subjects instantiated by the TOE and devices are outside scope of the TOE, though the TOE manages connections between partitions and devices.

3.2 Physical Boundaries

As indicated above, the TOE consists of a number of architectural components. The components expose a number of interfaces both externally and internally.

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 Hardware Management Console (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.

The internal interfaces, specifically those not also available externally, include the FSP interface to the Hypervisor.

Note that connections to a broad or public network are supported, but they are treated as resources that can be granted to partitions for operating system use and are not used by

TOE for its own purposes. Similarly, while the TOE controls which device adapters a given partition can access, it does not control or otherwise constrain the nature of those device adapters (and associated devices). Any functions or connections of those device adapters (and devices) are outside the scope of control of the TOE.

4 Security Policy

The Security Functional Policies (SFPs) implemented by LPAR are based upon the basic set of security policies to support data separation: user data protection, identification and authentication, security management, and protection of the TSF.

Note: Much of the description of the LPAR security policy has been extracted and reworked from the LPAR Security Target.

4.1 User Data Protection

The Hypervisor manages the association of CPUs, memory, and I/O device adapters, in a relatively static environment, with partitions containing operating system instances. Memory and I/O device adapters can be assigned to single partitions and when assigned are accessible only by the partition (including OF/RTAS and the OS running in the partition). CPUs can also be assigned a single partition, and only that partition (and occasionally the TOE) can use that CPU. CPUs can also be configured to be shared among a collection of partitions (shared processor partitions or also called micro-partitions) and the Hypervisor will save and restore the hardware register states when switching between partitions.

The Hypervisor also provides a mechanism where users can create LPAR groups (also referred to as eWLM groups) in which partitions belonging to a preconfigured group of partitions are allowed to share the quantity of resources (memory and processors but not I/O) between the partitions. At any point in time, each resource is owned by one and only one partition, but the operating system in the owning partition is given the ability to relinquish the resource allowing another partition in the same group to add the resource. The Hypervisor clears out the state of the resource before it is moved between partitions.

The Hypervisor allows the configuration of I/O device adapters such as Ethernet and virtual logical area network (LAN) which can be used to provide connections between partitions. I/O device adapters are the only mechanisms offered by Hypervisor that facilitate communication between partitions. Such communication is possible only when partitions are explicitly configured to have access to specific I/O device adapters (i.e., those that provide communication services, such as virtual SCSI, virtual LAN, and Ethernet).

With the exception of resource sharing among partitions in a partition group (see above), partitions have no control over the assignment of their resources. The Hypervisor 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.

4.2 Identification and Authentication

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. Since the identification of a partition is guaranteed by the TOE, each partition is continuously authenticated.

4.3 Security Management

All TOE configuration occurs via the interface to the HMC. Since the HMC is disconnected while the TOE is operating in the evaluated configuration the TOE provides no interface to security management functions. Thus, the TOE effectively restricts the ability to change its own configuration when operating in the evaluated configuration.

4.4 Protection of the TOE Security Functions

The components of the TOE protect themselves using the domains provided by the Power6 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 designed such that when the hardware that supports a partition fails, the other partitions will continue uninterrupted.

5 Assumptions

The following assumptions were made during the evaluation of LPAR:

- The TOE is appropriately installed, including connections to device resources, and is disconnected from the management console when operational.

- The TOE and its connections are physically protected from unauthorized access or modification.

- The TOE is managed by users who are capable and trustworthy and follow the applicable guidance correctly.

6 Documentation

The following documentation was used as evidence for the evaluation of the LPAR:

6.1 Security Target

1. IBM Logical Partition Architecture for Power System Security Target, Version 1.0, November 21, 2008

6.2 Evaluation Technical Report

1. Evaluation Technical Report for the IBM Logical Partition Architecture for Power Systems (Proprietary) Version 4.0, October 27, 2008

6.3 Configuration Management

1. IBM Logical Partitioning Architecture on System i and System p Configuration Management Plan, Version 1.5, January 3, 2008
2. Sample DCR Record

6.4 Delivery and Operation

1. IBM Logical Partitioning Architecture on Power Systems Common Criteria System Delivery Procedures, Revision 1.6, August 30, 2008
2. Common Criteria Installation Instructions for IBM Logical Partitioning Architecture on Power Systems

6.5 Design Documentation

1. IBM Logical Partitioning Architecture Design Specification, Revision 0.5, September 1, 2008
2. Power6 CEC Book IV – Implementation Features
3. SLIC HCalls (version 1.0.2 08/25/2008)
4. PHYP and SLIC LP Events (version 1.1.2, 08/08/2008)
5. Power Architecture Platform Requirements+ – PAPR+ Version 2.1
6. System p Partition Firmware to PHYP Interfaces, Part 2: Hidden Hypervisor Calls System p Partition Firmware to PHYP Interfaces, Part 3: LP Events, RTAS Design Notes
7. IBM Logical Partition Architecture for Power6, Security Policy Model, Version 0.2, 09/02/08
8. Implementation subset

6.6 Guidance Documentation

1. Common Criteria Installation Instructions for IBM Logical Partitioning Architecture on Power Systems
2. SA76-0098-00 Logical partitioning guide
3. SA76-0084-00 Installation and Configuration Guide for the Hardware Management Console Version 7 Release 3.1.0 Maintenance Level 0
4. SA76-0085-00 Operations Guide for the Hardware Management Console and Managed Systems Version 7 Release 3.1.0

6.7 Life Cycle

1. IBM Logical Partitioning Architecture on Power Systems Common Criteria System Life Cycle Document, Revision 1, February 9, 2008

6.8 Testing

1. IBM Logical Partitioning Architecture on Power Systems Common Criteria Test Plan, Revision 2.1, February 9, 2008
2. Test code
3. Test Results

6.9 Vulnerability Assessment

1. IBM Logical Partition Architecture for Power6 Vulnerability Analysis, Version 0.3, 08/28/08
2. IBM Logical Partition Architecture for Power6 Misuse Analysis, Version 0. 3, 08/29/08

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the IBM LPAR, Version 2.0, October 27, 2008.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification and high level design. The vendor testing was extensive and covered all of the security functions identified in the ST and interfaces in the design. These security functions include:

- Identification and Authentication
- User Data Protection
- Security Management
- Protection of the TSF

7.2 Evaluation Team Independent Testing

The evaluation team installed the product according the Evaluated Configuration Guide, reran all developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is IBM Logical Partition Architecture for Power6 operating on IBM iSeries or pSeries hardware. To use the product in the evaluated configuration, the product must be configured as specified in the **Common Criteria Installation Instructions for IBM Logical Partitioning Architecture on Power Systems** document.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.2 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3 and CEM version 2.3. The evaluation determined the IBM LPAR TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the LPAR product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from IBM and performed a CM audit.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team’s misuse analysis and vulnerability analysis, and the evaluation team’s performance of penetration tests.

9.9 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements and procedures defined in the CEM. On this basis, the validators determined that conclusions reached by the evaluation team were justified and that the product meets the claims in the ST.

10 Validator Comments/Recommendations

- None.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *IBM Logical Partition Architecture for Power System Security Target,* Version 1.0, 21 November 2008.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.3, August 2005.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.3, August 2005.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.3, August 2005.

[4] Common Criteria Project Sponsoring Organisations. *Common Methodology for Information Technology Security Evaluation*: Evaluation Methodology, Version 2.3, August 2005.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for the IBM Logical Partition Architecture for Power Systems Part 2 (Proprietary)*, Version 4.0, October 27, 2008.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the IBM LPAR, ETR Part 2 Supplement (SAIC and IBM Proprietary),* Version 2.0, October 27, 2008.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] *IBM Logical Partition Architecture for Power Systems Security Target, Version 1.0, November 21, 2008*