Common Criteria for Information Technology Security Evaluation

Public Version
of the
Security Target for
PR/SM for the IBM eServer
zSeries z900 GA3 and z800
EAL5 Certification
Approved

Version 2.1

February 11, 2003

This Security Target was developed for the evaluation of the Processor Resource/ System Manager™ (PR/SM™) for the IBM eServer™ zSeries™ 900 (z900) and 800 (z800) family of Processors according to the Common Criteria level EAL5. The intention of this Security Target is also to show the compliance of PR/SM with the requirements identified in the Common Criteria for those functions identified in this document

Table of Contents

List of Tables

1 Introduction

1.1 Security Target Identification

This is version 2.1 of the ST Document for LPAR on z800 and z900. The document date is February 11, 2003.

1.2 Security Target Overview

This Security Target was developed for the evaluation of the Processor Resource/ System Manager (PR/SM) for the IBM eServer zSeries z800 and z900 family of Processors according to the Common Criteria level EAL5. The intention of this Security Target is also to show the compliance of PR/SM with the requirements identified in the Common Criteria for those functions identified in this document. For the remainder of this document z800 and z900 together will be refered to as zSeries.

Chapter 1 contains general introductory information, ST identification, target assurance level and reference information.

Chapter 2 is a detailed description of the Target of Evalutaion (TOE) and an overview of the Logical Partition LPAR) architecture and design.

Chapter 3 discusses the TOE Security environment, including assumptions (A.xx), threats (T.xx) and environment threats (TE.xx).

Chapter 4 contains a definition of the Security Objectives (O.xx) and Environment Security Objectives(OE.xx)

Chapter 5 contains details of the Security Function Policies (SFP) and Security Functional Requirements (SFR).

Chapter 6 is the TOE Summary Specification describing how LPAR is initialized as well as where LPAR resides in storage. Additionally, a general overview of the flow of information between LPAR and the HMC is provided. TOE Security Functions (SF) are described and TOE assurance requirements are discussed.

Chapter 7 is the Protection Profile Conformance Claim.

Chapter 8 is the Rationale section, containing rationale for the Security Objectives, Security Requirements, TOE Summary Specification, Internal Consistency and Mutual Support, and Strength of Function.

Appendix A is a glossary of Common Criteria terminology.

Appendix B is a glossary of terminology specific to PR/SM and LPAR.

Description of the TOE

The TOE is the PR/SM Microcode kernel running on the IBM eServer zSeries. The zSeries is a general-purpose data processing system that can be initialized in one of two operating modes: basic mode or LPAR mode. The Processor Resource/Systems Manager (PR/SM) provides the capability that enables the zSeries to be initialized in LPAR mode.

PR/SM is a hardware facility that enables the resources of a single physical machine to be divided between distinct, predefined logical machines, called “logical partitions”. Each logical partition is a domain of

execution and is considered to be an object capable of running a conventional System Control Program (SCP) such as z/OS™, OS/390®, z/VM™, VIF, VM/ESA®, VSE/ESA™, TPF or Linux®.

PR/SM licensed internal code (LIC) provides the Security Administrator 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 this Security Target. Additional functions of zSeries LPAR 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 zSeries LPAR.

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

1.3 Assurance Level

The assurance level for this Security Target is EAL5. The business requirements for customers of the zSeries identify EAL5 as the necessary assurance level for evaluation. This is due to the strong need to have logical partitions provide the same isolation as air-gapped systems. A high assurance level is needed to satisfy this need.

1.4 Related Standards and Documents

[1] PR/SM Planning Guide, IBM, SB10-7033

[2] ISO 15408 – Information Technology – Security Techniques – Evaluation Criteria for IT Security (Hereafter referred to as Common Criteria or CC)

1.5 CC Conformance Claim

This TOE has been developed to conform to the functional components as defined in the Common Criteria version 2.1, part 2, with the assurance level of EAL5. No additional functional components have been defined or used.

2 TOE Description

2.1 Definition of TOE

Microcode Level

The target of the evaluation is the PR/SM Microcode kernel running on the IBM eServer zSeries hardware platform, which includes the following models. The various models of the zSeries servers use identical processor chips, but different numbers on each MCM.

Table 2-1 - zSeries Models and Number of CPs

z900 MODEL NUMBER	Number of Cps
101	1
102	2
103	3
104	4
105	5
106	6
107	7
108	8
109	9
110	10
111	11
112	12
113	13
114	14
115	15
116	16
2C1	1
1C1	1
2C2	2
1C2	2
2C3	3
1C3	3
2C4	4
1C4	4
2C5 `	5
1C5	5
2C6	6
1C6	6
2C7	7
1C7	7
2C8	8
1C8	8

2C9	9
1C9	9
210	10
211	11
212	12
213	13
214	14
215	15
216	16

z800 MODEL NUMBER	Number of Cps
0E1	1
0A1	1
0B1	1
0C1	1
001	1
0A2	2
0X2	2
002	2
003	3
004	4

Microcode Driver Level Driver: D3G Date: 29 Mar. 2002

EC#	DESCRIPTION	MCL
E26989	D3G_1 SSE-PSCNSE LIC	045
E26990	D3G_1 SSE-SOS LIC	066
E26991	D3G_1 SSE-MISR DATA LIC	n/a
E26992	D3G_1 SSE-PSCNCC LIC	039
E26996	D3G_1 SSE-PSCNCC-RAP LIC	045
E26993	D3G_1 SSE-POWERC LIC	003
E26997	D3G_1 SSE-POWERC-RAPLIC	005
E26994	D3G_1 SSE-IQDIO LIC	003
J11201	D3G_1 SSE-FICON BRIDGE LIC	003
J11202	D3G_1 SSE-CHANNEL DIAGS	001
J11203	D3G_1 SSE-PCX	n/a
J11204	D3G_1 SSE-HYDRA	020
J11205	D3G_1 SSE-PCI CRYPTO CHAN	003
J11206	D3G_1 SSE-FCS (Disruptive)	009
J11207	D3G_1 SSE-CFCC (Disruptive)	013
J11208	D3G_1 SSE-LPAR HV LIC	004
J11209	D3G_1 SSE-CHANNEL CODE LIC	002
J11210	D3G_1 SSE-OSA FLASH ROM	002
J11211	D3G_1 SSE-I390/PU ML RAP LIC	050
J11212	D3G_1 SSE-I390/PU ML LIC	044
J11213	D3G_1 SSE-CODE (SSE/SP)	086

J11215	D3G_1 SSE-C-PART (2647 TP)	002
J11219	D3G_1 HHMC-D-PART	n/a
J11221	D3G_1 HHMC/TKEWS-ISA-C-PART	n/a
J11233	D3G_1 SSE-FCP lic	006

For the remainder of this document, the Licensed Internal Code (LIC) described above will be referred to as zSeries LPAR.

2.2 PR/SM Overview

IBM has introduced the zSeries, the first e-business enterprise server designed for the high-performance data and transaction serving requirements for the next generation of e-business. The zSeries is the first enterprise e-business server of the new IBM brand to provide new tools for managing e-business, new application flexibility, and new innovative technology that are designed to meet those demands. The brand of servers offers numerous upgrade options from S/390® 9672 Generations 5 and 6 server models. S/390 operations are fully compatible with the new architecture - z/Architecture™, based upon 64-bit real addressing. S/390 applications are fully compatible with z/Architecture, insuring viability for S/390 information, assets, and S/390 technology.

zSeries General Purpose Models

zSeries general purpose models provide high performance and flexibility due to an improved design and use of technology advances. The design of these models supports:

z/Architecture

ESA/390 architecture (ESA/390 or ESA/390 TPF)

Parallel Sysplex®

Intelligent Resource Director (IRD)

Workload Manager

Dynamic CHPID Management

I/O Priority Queuing.

Hardware Management Console control

Logically partitioned (LPAR) operating mode

Internal Coupling Facility CPs (ICFs)

Linux

IBM Enterprise Systems Connection Architecture (ESCON® Architecture) and technology for the ESCON channels.

FICON™ Architecture and FICON channels

Parallel channels

Coupling links

InterSystem Coupling-3 (ISC-3) links

Integrated Cluster Bus (ICB-3 and ICB-2) links

Internal Coupling-3 (IC-3) links

Increased number of subchannels

IEEE Floating Point operations

Multiple Image Facility (MIF)

Cryptographic coprocessor features

Open Systems Adapter 2 (OSA-2) features

Open Systems Adapter Express features

Internal Queued Direct Communication

Data compression

Dynamic I/O configuration

CHPID assignment

Internal Battery Feature

Power Sequence Control

Sysplex Timer® attachment

Subspace Group facility

Dedicated Move Page Engine

Fast Sync/Data Mover

Immediate and Relative Instruction facility

Perform Locked Operation facility

Logical string assist

Modified Operating Environments

Capacity upgrade on demand (CUoD)

High levels of reliability, availability, and serviceability

Online information

Information in IBM Resource Link™

The zSeries general purpose models provide the z/Architecture and ESA/390 (and ESA/390 TPF) architectures in two modes of operation:

- Basic mode
- LPAR mode

PR/SM is a hardware facility that enables the resources of a single physical machine to be divided between distinct, predefined logical machines called "logical partitions". Each logical partition is a domain of execution, and is considered to be a subject capable of running a conventional system control program (SCP) such as z/OS, z/VM, OS/390, MVS/ESA™ VM/ESA, TPF or Linux. These operating systems run in either a PR/SM partition or on the base hardware. Linux, however, may run in a PR/SM partition only and cannot run on the base hardware.

Access Modes and States

activated - in this state, a logical partition can access system resources via SIE mode.

allocated - a partition may only use a resource that is allocated to it.

attached - IO devices are attached to control units, and control units are attached to channel paths. This connectivity is described in the IOCDS part of the configuration. I/O devices are considered to be attached to the channel paths to which their control units are attached.

authorized - a logical partition may be authorized to perform certain tasks with security implications. The possible authorizations are:

- I/O configuration control authority - the partition can update any IOCDS which is not write protected
- Global performance data control authority - the partition can view CPU and Input/Output Processor busy data for all logical partitions
- Cross-partition control authority - the partition can issue system control instructions that affect other partitions, i.e. to reset or deactivate another partition.

candidate access - a channel path or I/0 device may only be allocated to a logical partition which has candidate access to it. The Security Administrator defines which partitions have access to which paths as part of the IOCDS. The IOCP User's Guide describes how the IOCDS is set up using the IOCP utility. In the IOCDS, the access list for each device defines which partitions have candidate access to the device. The initial access list and candidate access list for each channel path together define which partitions have candidate access to the channel path.

check-stopped - this state indicates that a physical or logical processor has been subject to an unrecoverable failure.

deactivate - in this state, a logical partition is prevented from running, i.e. it is denied access to all objects.

dedicated - a dedicated channel path is only ever allocated to a single partition. A dedicated physical processor is used exclusively by a single partition while the logical processor executing on the dedicated processor is online and not check-stopped. (Note that the exclusivity is only between partitions: a dedicated processor is still shared with the PR/SM controlling code).

isolated - when a partition is isolated, its non-shared channel paths remain allocated to the partition even when the channel path is off-line.

online/off-line - a logical processor or channel path may be configured online or off-line. A resource cannot be used while it is off-line.

reconfigurable - a reconfigurable resource may be moved between partitions, but is allocated to at most one partition at any one time.

shared - the resource may be allocated to more than one partition at once.

write protected - the IOCDS part of a configuration cannot be modified by any partition if it is write protected.

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

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

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

c) Central processor (PU, i390) LIC.

CP Millicode

CP Millicode performs the more complex instructions in the zSeries architecture. The millicode is written and assembled in a manner very similar to the zSeries Assembler Language Code. Through a combination of millicode, and the less complex hardwired instructions, the zSeries processor is able to support the complete zSeries instruction set.

I390 code (Internal 390 code)

The i390 code runs on the SAP (System Assist Processor). Most of its functions are I/O related involving the running of the channel subsystem. In addition, i390 code is involved in FEDC (First Error Data Capture), RMF™ (Resource Management Facility) and SMF (Storage Management Facility). I390 code is frequently invoked during certain SCLP (Service Call Logical Processor) commands, sometimes issued by LPAR, as well as various resets and machine initialization/set-up during IML.

d) The LIC in the channel subsystem (CHNL) responsible for maintaining data separation in the handling of I/O requests and responses;

The Hardware Management Console(HMC) / Support Element(SE) workplace is the window from where you start tasks for monitoring and operating the CPC. Your user mode determines which tasks and controls you can use on the workplace. Not all tasks are available for each user mode. Refer to the table below to determine which user modes are allowed to perform which tasks.

The following user modes are available:

Operator - A person with Operator authority typically performs basic system startup and shutdown operations using predefine procedures.

Advanced Operator - A person with Advanced Operator authority possesses Operator authority plus the ability to perform some additional recovery and maintenance tasks.

System Programmer - A person with System Programmer authority has the ability to customize the system in order to determine its operation.

Access Administrator - A person with Access Administrator authority has the ability to create, modify, or delete user profiles for the user modes on the Hardware Management Console or for service mode on the support element. A user profile consists of a user identification, password, and user mode.

Service Representative - A person with Service Representative authority has access to tasks related to the repair and maintenance of the system.

The following general definitions apply to the above user modes:

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

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

The table below identifies the specific tasks allowed for each of the 5 user modes.

Table 2-2 System Administrator Modes and Tasks

Console Action	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
View Console Events	x	x	X	x	x
View Console Service History	x	x	X	x	x
Save/Restore Customizable Console Data				x	
Customize Console Date/Time	x	x	X	x	x
Change Console Internal Code		x	x		x
Analyze Console Internal Code					x
Backup Critical Console Data			x		x
Perform a Console Repair Action					x
View Console Information	x	x	x	x	x
Customize Automatic Logon				x	
User Profiles				x	
Customize User Controls				x	
Customize Product Engineering Access				x	
Hardware Management Console Settings	x	x	x	x	x
Enable Hardware Management Console Services		x	x	x	x

Console Action	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Customize Scheduled Operations			x		x
Remote Support Telephone Queue	x	x	x	x	x
Transmit Console Service Data	x	x	x	x	x
Authorize Internal Code Changes			x		x
Delete Staging Area Files					x
Customize Account Information			x		x
Customize Dial Information			x		x
Customize Problem Management			x		x
Domain Security				x	x
Enable Pager Notification			x		
Installation Completion Report					x
Report a Problem	x	x	x		x
IBM Service Support System					x
SNMP Configuration				x	
View Console Tasks Performed					x
Configure 3270 Emulators			x		
Network Diagnostic Information	x	x	x	x	x
Rebuild Vital Product Data					x
Archive Security Logs			x		x
View Security Logs			x		x
Save Upgrade Data					x
Reassign Hardware Management Console					x
Enable Electronic Service Agent for zSeries				x	
Format DVD Cartridge			x		x

Console Action	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Log Off	x	x	x	x	x
Single Step Console Internal Code Changes		x	x		X

Task	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Daily					
Activate	x	x	x		x
Reset Normal	x	x	x		x
Deactivate	x	x	x		x
Grouping			x	x	
Activity	x	x	x	x	x
CPC Recovery					
Single Object Operations	x	x	x	x	x
Start		x	x		x
Stop		x	x		x
Reset Normal	x	x	x		x
PSW Restart		x	x		x
Reset Clear	x	x	x		x
Load	x	x	x		x
Service					
Service Status	x	x	x	x	x
Perform Problem Analysis	x	x	x		x
View Service History	x	x	x		x
Backup Critical Data			x		x
Hard Disk Restore					x
Checkout Tests					x

Task	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Report a Problem	x	x	x		x
Transmit Service Data	x	x	x	x	x
Archive Security Logs			x		x
Format Security Logs to DVD			x		x
Change Management					
Engineering Changes (ECs)			x		x
Retrieve Internal Code		x	x		x
Change Internal Code		x	x		x
Product Engineering Directed Changes					x
System Information	x	x	x	x	x
Alternate Support Element			x		x
Special Code Load					x
Single Step Internal Code Changes		x	x		x
CPC Remote Customization					
Remote Service			x		x
Problem Management			x		x
Operations Management			x		x
Account Information			x		x
Support Element Operations Guide	x	x	x	x	x
CPC Operational Customization					
Customize/Delete Activation Profiles			x		
Customize Activity Profiles	x	x	x	x	x
View Activation Profiles	x	x			x
Automatic Activation			x		

Task	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Scheduled Operations			x		x
Customize Support Element Date/Time	x	x	x	x	x
Change LPAR Controls			x		x
Configure Channel Path On/Off		x	x		
Reassign Channel Path		x	x		x
OSA Advanced Facilities			x		x
Enable I/O Priority Queuing			x		x
Change LPAR I/O Priority Queuing			x		x
Object Definition					
Change Object Definition				x	x
Add Object Definition				x	x
Remove Object Definition				x	
Reboot Support Element				x	x
CPC Configuration					
Perform Model Conversion					x
Transmit Vital Product Data			x		x
View Frame Layout			x		
Edit Frame Layout					x

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

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

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

Standard hardware resources such as a central processor, including computation and control registers, timers, clocks and optional co-processors, storage; and I/O resources are objects allocated to logical partitions. These objects are subject to a non-discretionary access control policy under which each logical partition is only permitted access to resources allocated to it. Logical partitions are logical objects that are built from existing physical objects. These logical objects fall into one of three classes:

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

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

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

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

A system control program (SCP) running in a logical partition can support zSeries and ESA/390 architectural mode. This is set when a partition is defined, and cannot be altered while the partition is activated.

PR/SM supports and uses the "start interpretive execution" (SIE) instruction to create an interpretative execution environment in which the logical partitions execute. PR/SM begins execution in non-SIE mode. When a logical partition is to be activated, PR/SM establishes the parameters for each logical processor allocated to the partition in a control block called a "state description". PR/SM executes a SIE instruction, which dispatches the logical processor in SIE mode. The PR/SM hardware executes instructions in the logical processor in SIE mode until an exception condition occurs which causes control to retum to PR/SM in non-SIE mode. The exception conditions are events that cannot be handled in interpretative mode. PR/SM receives control in non-SIE mode. PR/SM maintains a state description for each logical processor of each logical partition so that each time a logical processor is dispatched, it is in the same context as when it

last had control. Since this state description is updated by the hardware, it is impossible for one logical partition to acquire control with the wrong context (i.e. the context of another logical partition). The non-SIE/SIE distinction is a powerful privilege differentiation between PR/SM and the logical partitions.

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

- **Logical Partition Isolation**

  This control reserves reconfigurable unshared channel paths for the exclusive use of a logical partition. Channel paths assigned to an isolated LP 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 LP 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 CP 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 LP, deactivate any other LP, and provide support for the automatic reconfiguration facility.

In addition to the security controls mentioned above, the TOE is designed to ensure that central and expanded storage for each logical partition are 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 the 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/360™, S/370™ 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 architectures.

2.3 Design Considerations

2.3.1 Introduction

This section identifies which architectural components within the PR/SM product are responsible for implementing each security function, and describes why the functions performed by these components cannot be disabled, interfered with or bypassed by interactions with other components.

The architectural components of PR/SM, the external entities and the possible interactions between them are identified in Section 2.3.1, based on the architectural design. The detailed design and code are correct refinements of this architectural design, and therefore no new interactions between components are introduced at lower levels in the design (because there are no untrusted sub-components within the PR/SM architectural components). These design representations therefore only need to be considered where the architectural design contains insufficient detail to determine whether a binding error exists or not.

Particular design binding issues are discussed as follows:

a) the duplication of the configuration in different components in Section 2.3.3;

b) the multiple instantiation of the LPAR component in Section 2.3.4;

2.3.2 Possible Interactions

- Architectural Components

  The architectural components in PR/SM are:

  a) Support Element Code (SE) on the SE hardware, including DASD (holding IOCDSs) and an associated Hardware Management Console (HMC);

  b) LPAR LIC, running as part of each logical processor (when in LPAR mode) on the central processor hardware;

  c) Central Processor (CP, i390, millicode), including execution elements and the caches for instructions and data being processed;

  d) Channel Subsystem (CSS), including channel and I/O processor (IOP) LIC, expanded storage;

  e) System Control Element (SCE), including main storage and caches for access to this storage.

The latter three components are referred to collectively in this document as the resource access components, as they are the means by which the system accesses the physical processor, storage and channel resources.

- External Entities

  The external entities in PR/SM are:

  a) the SCP code running on each logical processor, which executes instructions and causes interrupts;

  b) resources (processor elements, storage, channel units, devices);

  c) the System Administrator at the HMC console.

- Interactions

The System Administrator interacts with PR/SM through the HMC/SE component only.

The resources interact with the PR/SM through the resource access components only.

Although some of the SCP code effectively runs directly on the physical processor, all security-relevant interactions are intercepted by the logical processor management function of the LPAR component. Communications from a partition are relayed to the SE via LPAR.

LPAR mediates all communications with the SE. The security-relevant interactions between the SE and LPAR components are those relating to changes in the configuration of the product (e.g., activation of partitions, allocation of storage).

The security-relevant interactions between the LPAR and the resource access components are:

a) the establishment of resource ownership by LPAR to be enforced by the resource access components (e.g. storage protection, channel ownership).

b) resource events (e.g. I/O interrupts) to be directed to the appropriate partition by LPAR.

2.3.3 Binding of Configuration in SE and LPAR

The binding of many of the security functions depends on the binding between the current configuration held in the Support Element (SE), and the current configuration being enforced by LPAR. This is discussed in this section.

Modifications to the configuration are serialized through the SE, regardless of whether they are made by the Security Administrator (where changes are input from the console) or authorized partitions. The serialization is via the request/response nature of the interface between the SE and LPAR, via the use of the System Logical Processor to serialize LPAR actions, and via the use of locks to serialize access to the configuration.

On receipt of a request to change the configuration, the SE validates the request and then sends a request to LPAR to implement the change. LPAR attempts to do so, and returns a response on completion. The SE will only change the stored configuration if LPAR succeeds in implementing the change.

The only security-relevant attributes of the configuration (i.e. attributes that are referenced in security functions) that may change independently of the SE are:

a) whether or not processors are check-stopped;

b) the online/offline status of processors;

c) the online/offline status of channels and devices.

Changes to these statuses are communicated to the SE by LPAR.

The configuration is stored in the SE and in the system area of main storage, which is allocated on system initialization. Storage protection mechanisms are designed to ensure that partitions cannot modify this configuration directly. Because of this, only modifications permitted by the security functions can be made to the configuration i.e. the configuration cannot be interfered with. No functions are provided in the interface to the SE or LPAR to disable the enforcement of this configuration (except if the product is used in basic mode, i.e. not within the environment of use). The enforcement of the configuration by LPAR cannot be bypassed, because there is no means for the partitions to bypass the entry of LPAR mode and the interception of security-relevant instructions and interrupts.

From the above, all security functions that are concerned with the enforcement of the configuration cannot be disabled, bypassed or interfered with.

2.3.4 Binding of LPAR Instances

Of significance to the binding analysis is the fact that the LPAR LIC is distributed between processors, and is also reentrant. There is therefore the potential for interference between different instances of the LPAR LIC. This is overcome by the use of semaphores, locks, and a single system logical processor, which serializes LPAR actions where global processing is required (as in Section Binding of Configuration in SE and LPAR). The correct implementation of these serialization mechanisms is a correctness and not an effectiveness issue, except for possible covert timing channels caused by the serialization, which are identified in the construction vulnerability analysis.

3 TOE Security Environment

3.1 TOE Environment and Usage Description

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

The acquisition and management of computer systems is subject to economies of scale in many areas. Leasing or purchase costs may be lower for a single large machine than for a number of smaller machines of equivalent total processing capacity. There may also be savings in operational costs resulting from lower machine room capacity and fewer operations staff.

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

PR/SM provides the facility to partition a single platform to run any combination of z/OS, OS/390, z/VM, VIF, VM/ESA, VSE/ESA, TPF or Linux allowing requirements for different operating system environments to be met.

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

3.2 Assumptions

The specific conditions listed below are assumed to exist in a secure LPAR environment and are outside the security functionality of the TOE.

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

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

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

PR/SM provides a powerful tool for enforcing separation between multiple workloads on a single platform. If this separation is to be used in support of confidentiality requirements, then it will be necessary to create an environment in which the hardware is physically secure, and to restrict access to I/O devices to authorized personnel. In particular, the hardware management console must be physically protected from access by other than authorized system administrators.

Control of physical access to the HMC is the responsibility of the customer. However, the following options or settings are provided to help control physical access.

- Locking PC case
- Power-on password on PC
- Disablement of PC if case is opened

- PC will not boot from floppy or DVD-RAM

The SE provides the following mechanisms to help restrict unauthorized access:

- Physical access security is a customer responsibility. However, the SE resides behind the processor covers that should remain closed and locked at all times.

A.No_Remote - The remote support facility must be disabled.

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

A.LPAR_Only – LPAR mode is the only valid mode of operation for the evaluated product.

The administrator may power-on reset the machine in either basic or logical partition (LPAR) mode. This security target applies only to the use of the machine in LPAR mode.

A.Sep_Mode - Strict Separation Mode

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

1. The devices should be configured so that no device is accessible by more than one partition (although they may be accessible by more than one channel path);
2. Each I/O (physical) control unit should be allocated to a single partition in the current configuration;
3. The Security Administrator should not reconfigure a channel path unless all attached devices and control units are attached to that path only;
4. The Security Administrator should ensure that all devices and control units on a reconfigurable path are reset before the path is allocated to another partition;
5. No channel paths should be shared between partitions;
6. The amount of reserved storage for a partition should be zero;
7. Dynamic I/O configuration changes should be disabled (i.e. changes require a power-on reset);
8. Partitions should be prevented from receiving performance data from resources that are not allocated to them (no partition should have global performance data control authority);
9. At most one partition should have I/O configuration control authority (i.e. no more than one partition should be able to update any IOCDS);
10. The Security Administrator should ensure that write access is disabled for each IOCDS, unless that IOCDS is to be updated (the current IOCDS should not be updated);
11. The Security Administrator should verify any changed IOCDS after a power-on reset with that IOCDS, before any partitions have been activated (the Security Administrator may determine whether the IOCDS has been changed by inspecting the date of the IOCDS);

12. No partition should have cross-partition control authority (i.e. no partition should be able to reset or deactivate another partition).
13. No partition should have coupling facility channels that would allow communication to a Coupling Facility partition.[1]
14. No partition should be configured to allow Internal Queued Direct Communication.
15. No partition should have Workload Manager, Dynamic CHPID Management or I/O Priority Queuing enabled.

A.Admin_Secure – Administrative Personnel Security

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

A.Logical_Secure – Logical Access Security

These HMC configuration options can help control logical access:

1. HMC Operator Logon controls an individual's access to the HMC. The HMC Operator Logon can also be used to limit the objects to be controlled and the tasks available to an individual.
2. Secure desktop can prohibit any application from being started.

The SE provides the following mechanisms to help restrict unauthorized access:

1. Logical access security - logical access is controlled by the SE code in conjunction with the HMC:
    a. Secure desktop is standard and unchangeable.
    b. Disruptive actions are recorded.
    c. Direct logon to the SE is for service only.
    d. HMC Operator Logon controls individuals who have access to the SE control facilities and can limit the objects controlled and available controls to the individual.

2. SE Connections - the SE can make connections only through its LANs.
    a. Incoming LAN connections use a proprietary method.
    b. HMC to SE request formats are IBM proprietary.
    c. Automation APIs can be enabled or disabled and require a password.
    d. Telnet daemon cannot be started.
    e. FTP daemon requires a password; only known to the HMC.
    f. Domain name and password customizable to limit HMC access.
    g. No browser access available.
    h. No NetOp access is available.
    i. No DTOC/DCAF access without HMC.

[1] The coupling facility provides shared storage and shared storage management functions for the sysplex (for example, high speed caching, list processing, and locking functions). Applications running on z/OS and OS/390 images in the sysplex define the shared structures used in the coupling facility. These images efficiently share data so that a transaction processing workload can be processed in parallel across the sysplex.

3.3 Threats

3.3.1 Threats countered by the TOE

PR/SM may be used in a variety of threat environments, and for each intended use of the product an analysis should be performed which compares the specific threats within that environment against the claimed functionality.

The possible threats can be classified into the following two cases:

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

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

T.Access_Data – Illegal access to data

access by a partition to data that is not owned by that partition (i.e. data in the storage and I/O resources allocated to another partition and not including system data);

T.Access_CPU – Illegal access or control of processors and storage

access by a partition to allocate or deallocate storage, logical processors or coprocessors outside the limits of the configuration;

T.Access_IOCA – Illegal access of the I/O Configuration

access by a partition without I/O configuration control authority to any IOCDS;

T.Access_Perf – Illegal access to performance data

access by a partition without global performance data control authority to CPU and Input/Output processor data for all partitions;

T.Lpar_XCTL – Illegal control of another logical partition

access by a partition without cross-partition control authority to current configuration data (to reset or deactivate a partition only).

T.Obj_Reuse – Illegal transfer of data during context switch

data transferred with resources (object reuse) when those objects are reallocated from one partition to another;

T.Audit_Data – Illegal modification of the content of the security log.

By design, the contents of the security log cannot be modified while it is contained in the TOE. An attacker might want to attempt to modify the audit log to remove any evidence that he setup the system in a manner inconsistent with the directions in the Trusted Facility Manual. Anyone attempting to modify the log would need intimate designer level knowledge of the system, and have access to development tools.

3.3.2 Threats countered by the Environment

TE.Unauth_Access - Unauthorized access to physical resources of the TOE

Personnel without a need to know, or responsibility for operations should not be allowed access to the zSeries server, the HMC or SE, or the archival copies of the audit log. Such access could allow these unauthorized personnel access to information outside of their scope of responsibility.

TE.False Setup - Initial Setup of the Operational Configuration of the TOE inconsistent with TFM Guidance.

Authorized personnel, attempting to establish an insecure configuration for the purpose of circumventing the security policy, could bypass the specified setup requirements in the Trusted Facility Manual.

4 Security Objectives

TOE Security Objectives

This section defines the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. Each objective is stated in bold type font. An application note, in normal font, which supplies additional information and interpretation, follows it.

O.Identity - Identity

The TOE must ensure that each logical partition has a unique identity.

A zone number uniquely identifies each logical partition.

O.Auth_Admin - Authorized Administration

The TOE provides facilities to enable an authorized administrator to effectively manage the TOE and its security functions.

The security functions provided by the TOE are designed to enable secure administration of:

IOCDSs

- Logical Processors and Storage.
- I/O Channel Paths, Control Units and Devices.
- Cross Partition Functions
- Performance Data Access

O.Auth_Ops - Authorized Operations

The TOE provides facilities to enable authorized users to effectively operate the TOE in a secure manner.

The security functions provided by the TOE are designed to enable secure operation in the following areas:

- Partition Activation
- Processor and Storage Allocation
- Processor Execution
- Message Transfers

O.Audit - Audit and Accountability

The TOE will provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also to hold users accountable for any actions that they perform that are relevant to security.

The TOE will record the security-relevant actions of the System Administrator in an audit log. Deletions, modifications and reading of the audit log are controlled in a secure manner.

O.REUSE - Object Reuse

The TOE will provide the means of allowing a subject to use a resource or service without the user identity or contents of the resource being disclosed to other entities.

The TOE will ensure no information is disclosed via storage, channels, physical processors or coprocessors.

O.RESOURCE - Reliability of Service

The TOE will provide the means of controlling the use of resources by its users and subjects so as to prevent unauthorized denial of service.

The TOE will provide functions that enable control of the physical processor running time and cross partition functions.

Environment Security Objectives

The following are the security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they do not require the implementation of functions in the TOE hardware and/or software. These security objectives are assumed to be in place in the TOE environment. They are included as necessary to support the TOE security objectives in addressing the security problem defined in the TOE security environment.

OE.Data_Store – Off-TOE Data Storage

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

The audit log information from the TOE may be stored separately from the TOE for archival purposes. The personnel and systems, if any, in charge of this information are responsible for the maintenance of its required security.

OE.Perss – Personnel

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

Since the System Administrator has full access to system data, careful selection and training of administrators and others in privileged positions works to detect, prevent, or counter other attacks, and deters compromise of system data.

OE.Sec_Setup – Secure Setup

The TOE shall be protected during the setup phase.

The TOE shall be protected during the setup phase to ensure that the operations that have to be performed in this phase to set up the TOE for normal operation within the intended environment and for the intended operation is done in accordance with the guidelines within this Security Target.

Verification shall include inspection of the IOCDS definition, verification of the partition security controls, verification of the profiles.

OE.Phys_Prot – Restricted physical and remote access

Physical access and remote access to the HMC and zSeries should be restricted only to authorized and approved users.

The HMC and zSeries should be installed in restricted areas for the purposes of limiting accessibilty by company personnel and avoiding physical destruction or alteration of the hardware. Additionally, this restricted access applies to the remote support facility as this is outside the scope of the evaluations.

5 IT Security Requirements

5.1 TOE IT Security Requirements

This section contains the functional requirements that are satisfied by PR/SM on the IBM zSeries.

5.1.1 TOE IT Security Functional Requirements

Table 5.1 lists the IT security functional components. Following the table, each requirement is listed with assignments, selections and refinements (if any) indicated in **bold** type.

5.1.1.1 TOE Security Function Policies

The TOE implements several policies that are mentioned in the security functional requirements. Those policies are:

Access Control Security Function Policy (SFP)

The TOE implements an access control policy between subjects (users) and objects. The subjects or users are the logical partitions (LPARS) defined in the IOCDS and the System Administrator. The objects are the physical resources of the processor (CPs, storage, CHPIDS, audit data, performance data, IOCDSs, profiles, etc). Access to objects by subjects will be mediated by this policy to help ensure that subjects are only able to gain access to authorized objects.

Information Flow Control Security Function Policy (SFP)

The TOE implements an information flow control policy between subjects (users) and objects, and between objects and objects. The subjects or users are the logical partitions (LPARS) defined in the IOCDS and the System Administrator. The objects are the physical resources of the processor (CPs, storage, CHPIDS, audit data, performance data, IOCDSs, profiles, etc) and the logical processors instantiated on a physical processor on behalf of a logical partition. . Flow of information between objects and subjects, and between objects and objects will be mediated by this policy to ensure that information flow is only possible when subjects and objects are associated with the same logical partition.

5.1.1.2 TOE Setup and Initialization

The TOE has to be setup and initialized such that a specific environment is defined.

5.1.1.3 Security Functional Components from the Common Criteria

The following table shows the security functional components selected from Part 2 of the Common Criteria.

Component	Component Name
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity association
FAU_SAR.1	Audit Review

Component	Component Name
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_STG.1	Protected Audit Trail Storage
FAU_STG.4	Prevention of Audit Data Low
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset Information Flow Control
FDP_IFF.1	Information Flow Control
FDP_RIP.2	Full residual information protection.
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action.
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security Roles
FPR_UNO.1	Unobservability
FPT_AMT.1	Abstract machine test
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_SEP.3	Complete reference monitor
FPT_STM.1	Reliable time stamps
FPT_TRC.1	Internal TSF consistency
FPT_TST.1	TSF testing
FRU_RSA.1	Maximum quotas
FTA_TSE.1	TOE session establishment

Table 5-1 – Security Functional Components

FAU_GEN.1 Audit data generation
FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions (does not apply as audit is always active);

b) All auditable events for the *basic* level of audit; and
c) Auditable events include:

1. **creating or modifying the IOCDS part of a configuration;**
2. **modifying the reconfigurable part of a configuration;**
3. **selecting a configuration;**
4. **performing a power-on reset;**
5. **activating or deactivating logical partitions.**
6. **logging on or off the console.**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the ST:

- **profile contents**
- **power-on reset options**

FAU_GEN.2 User identity association
FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **the Security Administrator** with the capability to read **all audit information** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review
FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable Audit Review
FAU_SAR.3.1 The TSF shall provide the ability to perform *searches, sorting,*
of audit data based on **date or event** criteria.

FAU_STG.1 Protected audit trail storage
FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.
FAU_STG.1.2 The TSF shall be able to *prevent* modifications to the audit records.

FAU_STG.4 Prevention of audit data loss
FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* if the audit trail is full.

FDP_ACC.2 Complete access control
FDP_ACC.2.1 The TSF shall enforce the **access control SFP** on the **subjects [defined logical partitions and the System Administrator] and objects [physical CPs, physical storage, CHIPDs/Control Units/Devices, global performance data,]** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control (activation)

FDP_ACF.1.1 The TSF shall enforce the **access control SFP** to objects based on:

1. **Cross Partition Authority**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

A logical partition with cross-partition authority or a System Administrator can deactivate or reset a logical partition;

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[none]**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rules [**none**].

FDP_ACF.1 Security attribute based access control (allocation)

FDP_ACF.1.1 The TSF shall enforce the **access control SFP** to objects based on:

1. **Resource limits (number of logical processors, physical processor time slices, amount of storage)**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

A logical partition can allocate the resources

1. **logical processor**
2. **storage**

only within the resource limits as defined in the image profile.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[none]**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rules [**none**].

FDP_ACF.1 Security attribute based access control (Channel path)

FDP_ACF.1.1 The TSF shall enforce the **access control SFP** to objects based on:

1. **Candidate Access**
2. **Logical Partition Isolation Authority**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

A channel path may only be allocated to a logical partition with candidate access to it.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[none]**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rules:

1. **If a channel path is dedicated to a logical partition, it cannot be de-allocated from that partition.**
2. **If a channel path is reconfigurable and allocated to a logical partition with Logical Partition Isolation Authority, it cannot be de-allocated from that partition.**
3. **A logical partition with Logical Partition Isolation Authority can deconfigure a CHPID and make it available for use by another logical partition.**

FDP_ACF.1 Security attribute based access control (Control Unit/ Devices)

FDP_ACF.1.1 The TSF shall enforce the **access control SFP** to objects based on:

1. **Candidate Access**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. **A logical partition has Access to a control unit if the control unit is on a channel path allocated to the logical partition.**
2. **A logical partition has Access to a device if the device is attached to a control unit on a channel path allocated to the logical partition, and the logical partition has candidate access to the device.**

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[none]**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the rules [**none**].

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce **the information flow control SFP** on:

1. **Subjects:**
   a. **Activated logical partitions**
2. **Objects:**
   a. **System Administrators,**
   b. **resources**
   c. **storage**
   d. **processors**
   e. **co-processors**
   f. **CHPIDs**
   g. **I/O Control Units and Devices**

which prevents the transfer of information between subjects and objects if they are not associated with the same logical partition. The following operations are mediated:

- Read central storage
- Write central storage
- Read expanded storage
- Write expanded storage
- Read I/O
- Write I/O

- Read central processor
- Write central processor
- Read co-processor
- Write co-processor

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce **the information flow control SFP** based on the following types of subjects:

1. Activated Logical Partitions

and information security attributes:

1. partition identifier
2. Cross Partition Authority
3. Global Performance Data Authority

The following information flow rules are enforced:

1. ***Describable effect:*** **When an operation is executed on behalf of a logical partition, the effects that partition perceives must be capable of complete description only in terms of objects known to that partition.**

2. ***Isolation of effect:*** **When an operation is executed on behalf of a partition, other partitions should perceive no effects at all.**

3. ***I/O isolation:*** **I/O devices associated with a partition affect the state perceived by only that partition.**

4. **I*/O-State effect:* I/O devices must not be able to cause dissimilar behavior to be exhibited by states that a partition perceives as identical.**

5. ***State-I/O effect:*** **A partition's I/O devices must not be able to perceive differences between states that the partition perceives as identical.**

6. ***Isolation determinacy:*** **The selection of the next operation to be executed on behalf of a partition must depend only on the state of that partition.**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. ***Describable effect:*** **When an operation is executed on behalf of a logical partition, the effects that partition perceives must be capable of complete description only in terms of objects known to that partition.**

2. ***Isolation of effect:*** **When an operation is executed on behalf of a partition, other partitions should perceive no effects at all.**

3. ***I/O isolation:*** **I/O devices associated with a partition affect the state perceived by only that partition.**

4. **I/O-State effect: I/O devices must not be able to cause dissimilar behavior to be exhibited by states that a partition perceives as identical.**

5. ***State-I/O effect:*** **A partition's I/O devices must not be able to perceive differences between states that the partition perceives as identical.**

6. ***Isolation determinacy:*** **The selection of the next operation to be executed on behalf of a partition must depend only on the state of that partition.**

FDP_IFF.1.3 The TSF shall enforce the additional information flow control SFP rules.
[NONE]

FDP_IFF.1.4 The TSF shall provide the following list of additional SFP capabilities.
[NONE]

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules:

1. **the logical partition has cross-partition control authority and the access is to reset or deactivate a logical partition;**
2. **Transfer of a message between a logical partition and a resource can occur if the the partition has cross-partition control authority and one of the following is true:**
   i) the message is a request to reset a partition,
   ii) the message is a response to a request to reset a partition,
   iii) the message is a request to deactivate a partition,
   iv) the message is a response to a request to deactivate a partition.
3. **A logical partition with Global Performance Data control authority can view the performance data of all other logical partitions.**

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules:
[NONE]

FDP_RIP.2 Full residual information protection
FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all objects.

FIA_ATD.1 User attribute definition
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

1. **Partition Identifier**
2. **Resource limits**
3. **Partition scheduling parameters**

Refinement:

Within the scope of the TOE, an individual user is a logical partition.

FIA_UID.2 User identification before any action
FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FMT_MSA.1 Management of security attributes (authorities)

FMT_MSA.1.1 The TSF shall enforce the **access control SFP,** to restrict the ability to ***assign*** the security attributes

1. **I/O Configuration Control Authority,**
2. **Cross Partition Authority,**
3. **Logical Partition Isolation Authority,**
4. **Global Performance Data Control Authority**

to **the Security Administrator**

Refinement:

According to A.Sep_Mode, 8., no logical partition should have Global Performance Data Control Authority.

FMT_MSA.1 Management of security attributes (resource limits)

FMT_MSA.1.1 The TSF shall enforce the **access control SFP,** to restrict the ability to ***modify*** the security attribute

1. **Resource limits (number of logical processors, amount of storage)**
2. **Partition Scheduling Parameters**

to the **Security Administrator**.

FMT_MSA.1 Management of security attributes (candidate access)

FMT_MSA.1.1 The TSF shall enforce the **access control SFP,** to restrict the ability to ***assign*** the security attribute

1. **candidate access**

to the **Security Administrator**.

FMT_MSA.3 Static attribute initialization
FMT_MSA.3.1 The TSF shall enforce the **access control SFP,** to provide *restrictive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow the **Security Administrator** to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data (configuration)

FMT_MTD.1.1 The TSF shall restrict the ability to ***modify*** the

- **IOCDS part of the configuration**

- **reconfigurable part of the configuration**
- **image profile**
- **reset profile**

to the **Security Administrator or logical partition with I/O Configuration Control Authority.**

FMT_SMR.1 Security roles
FMT_SMR.1.1 The TSF shall maintain the roles:
- **Operator**
- **Advanced Operator**
- **System Programmer**
- **CE**
- **Access Administrator.**

Any of the above roles are associated with the generic role System Administrator. The roles of System Programmer and CE are associated with the generic role Security Administrator.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that **any users/subjects** are unable to observe **any operation** on any **object/resource** by **any other user/subject**.

FPT_AMT.1 Abstract machine testing
FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up, periodically during normal operation, at the request of an Authorized user, and as part of recovery actions* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_ITT.1 Basic internal TSF data transfer protection
FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure and modification* when it is transmitted between separate parts of the TOE**.**

Refinement:

Internal TSF data, specifically the audit log, is protected when synchronized between dual SEs.

FPT_SEP.3 Complete reference monitor
FPT_SEP.3.1 The un-isolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.3.2 The TSF shall enforce separation between the security domains of subjects in the TSC.
FPT_SEP.3.3 The TSF shall maintain the part of the TSF that enforces the access control SFP in a security domain for its own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to the TSP.

FPT_STM.1 Reliable time stamps
FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_TRC.1 Internal TSF consistency

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.
FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for **recording of auditable events.**

FPT_TST.1 TSF testing
FPT_TST.1.1 The TSF shall run a suite of self tests during *initial start-up, periodically during normal operation, at the request of the authorized user,* at the conditions: **reset, recovery,** to demonstrate the correct operation of the TSF.
FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.
FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

FRU_RSA.1 Maximum quotas
FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources:

1. **physical processor time slices**

that *logical processors* can use *over a specified period of time.*

FTA_TSE.1 TOE session establishment
FTA_TSE.1.1 The TSF shall be able to deny session establishment based on

1. **the unavailability of necessary physical resources (CPs, storage, channels)**
2. **exceeding the scheduling parameters for the logical partitions**

5.1.2 TOE IT Security Assurance Requirements

The TOE will be conformant to the assurance requirements required for level EAL5.

5.2 Security Requirements for the IT Environment

There are no requirements stated in the form of Common Criteria components for the IT environment. But the assumptions stated for the environment as well as the organizational security policies need to be satisfied by the IT environment. It is expected that any system integrating the TOE will provide documentation and procedures as well as technical measures (e. g. within the host system) to demonstrate that the assumptions are fulfilled and the policies are implemented. A separate system audit or system accreditation process has to check this.

6 TOE Summary Specification

As defined in chapter 2 the TOE consist of the PR/SM Microcode kernel running on the zSeries Hardware. This LIC implements the security functions specified in chapter 5. This chapter provides a more detailed description of the TOE interfaces and internals and how the TOE implements the security functional requirements.

The first section describes how LPAR is initialized as well as where LPAR resides in storage. This information is provided to provide a better understanding of the secure nature of LPAR code.

The second section provides a general overview of the flow of information between LPAR and the HMC. The last section describes the security functions of the TOE and relates them to the security functional requirements listed in chapter 5.1.

6.1 LPAR Kernel

The LPAR core image is loaded into X'2000' in Hardware System Area (HSA) by the Support Element. The Support Element then sets the prefix register of one processor to the beginning of the image and restarts this processor thereby turning control to LPAR initialization LIC. After LPAR initialization completes, a Security Administrator may allocate system resources via partition definition panels.

The amount of storage used by LPAR in HSA depends on the number of physical processors installed, the number of partitions defined, and the number of I/O devices defined in the IOCDS. All storage between X'0' and 2 MB is reserved for LPAR's core image. Since this area of HSA is reserved exclusively for LPAR's core image, "real" HSA is allocated starting at 2 MB in 1 MB increments. LPAR will allocate the rest of its storage in "real" HSA. All other storage LPAR uses must fit below 2 GB in HSA.

HSA is an area of central storage that is inaccessible to programs resident in logical partitions and is therefore secure.

6.2 Information Flow to/from HMC

Information flow between LPAR and the HMC is accomplished through a proprietary mechanism.

When a System Administrator wishes to activate a partition, the activation request is initiated from the HMC. LPAR will receive an external interrupt and issue an instruction to obtain a description of the partition the System Administrator wishes to activate. LPAR will attempt to construct the partition and will inform the HMC of the success or failure of the command.

6.3 TOE Security Functions

The following section describes the security functions of the TOE and how they relate to the security functional requirements listed in chapter 5.1. This provides a better understanding of the TOE security functions and the mapping to the Common Criteria.

6.3.1 TOE Security Functions Description

The following section provides a list of Security Functions of the TOE and describes how they map to the Security Functional Requirements of Chapter 5.

6.3.1.1 Logical Partition Identity

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

This security function contributes to help satisfy the security functional requirement FIA_UID.2.

6.3.1.2 Authorized Administration

The authority level specified when defining a new user determines the tasks made available to that user. This capability allows an authorized administrator to effectively manage the TOE and its security functions in the following way:

a) The TOE will help prevent access to the IOCDS part of a configuration by a user, unless

> I/O Configuration Control is enabled AND IOCDS Write Protection is disabled AND the user must be a Security Administrator (in the case of Standalone IOCP).

[Satisfies SFRs: FDP_ACC.2 , FMT_MTD.1, FMT_SMR.1]

b) The TOE will help prevent access to the reconfigurable part of a configuration by a user unless
   i. the user is the Security Administrator, or
   ii the user is a logical partition and:
      a) The logical partition has cross-partition control authority and the access is to deactivate or reset a logical partition; or
      b) The access is to deallocate storage or logical processor resources allocated to the partition itself; or
      c) The access is to allocate storage or logical processor resources to the partition itself.

[Satisfies SFRs: FDP_ACF.1 (Activation, Allocation), FDP_ACC.2, FMT_SMR.1]

c) The TOE can be configured so that no logical partition has I/O configuration control authority. When it is necessary to change an IOCDS, PR/SM can be configured so that only one logical partition has I/O configuration control authority.

[Satisfies SFRs: FMT_MSA.1 (Authorities)]

d) The TOE can be configured so that no logical partition has cross-partition control authority. [Satisfies SFRs: FMT_MSA.1 (Authorities)]

e) The TOE will permit the set of logical partitions with candidate access to a channel path to be restricted. A channel path can only be allocated to a logical partition if that partition has candidate access to the path. [Satisfies SFRs: FTA_TSE.1, FDP_ACC.2, FDP_ACF.1 (Channel Path), FMT_MSA.1(candidate access)]

f) The TOE will permit the set of logical partitions with candidate access to an I/O device on a shared channel path to be restricted. An I/O device will not be allocated to a partition without candidate

access to it, even if the shared channel path to which the device is attached is allocated to the partition. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (Control Unit/Devices)]

g) The TOE can be configured to help prevent the shared use of any channel path, control unit or I/O device between logical partitions. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (Channel Path, Control Unit/Devices)]

h) The TOE will permit a channel path to be allocated exclusively to one logical partition either by identifying the channel path as dedicated, or by designating the owning partition as isolated (isolation only applies to the partition's reconfigurable channel paths). The TOE will prevent the de-allocation of such a channel path from the partition, even when the channel path is off-line. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (Channel Path), FDP_IFC.1]

i) The TOE will help ensure that a reconfigurable or dedicated channel path is never shared. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (Channel Path), FDP_IFC.1]

j) The TOE will help ensure that control units and I/O devices cannot be allocated independently of the channel path to which they are attached. A control unit is allocated to a partition if a channel path to which it is attached is allocated to the partition. An I/O device is allocated to a partition if a control unit to which it is attached is allocated to the partition, and the partition has candidate access to the device. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (Channel Path, Control Unit/Devices)]

k) The TOE can be configured so that a logical partition has dedicated use of the physical processors allocated to it. The TOE will ensure that a dedicated physical processor is allocated to only one logical partition, and will prevent the de-allocation of the physical processor while the logical processor using it is online and not check-stopped. [Satisfies SFRs: FDP_ACC.2, FPR_UNO.1, FDP_IFC.1]

l) The TOE can be configured so that no logical partitions have global performance data control authority. In this case, a logical partition will only be able to gather performance data about the resources allocated to it. [Satisfies SFRs: FMT_MSA.1 (Authorities), FPR_UNO.1, FDP_ACC.2]

6.3.1.3 Authorized Operations

The authority level specified when defining a new user determines the tasks made available to that user. This capability allows an authorized administrator to effectively operate the TOE and its security functions in the following way:

a) The TOE will help ensure that only logical partitions in the current configuration are activated. Only activated partitions and the System Administrator will be permitted access to objects. [Satisfies SFRs: FDP_ACC.2, FIA_UID.2, FMT_MSA.1 (resource limits), FMT_SMR.1]

b) The TOE will help ensure that logical processor is allocated exclusively to a single partition, and that the number of logical processors allocated to a partition does not exceed the limit specified in the current configuration. Once deallocated, a logical processor cannot be reallocated to another partition. [Satisfies SFRs: FDP_ACF.1 (allocation), FIA_ATD.1, FTA_TSE.1, FMT_MSA.1 (resource limits)]

c) The TOE will help ensure that a storage resource is never shared, and that the amount of storage allocated to a logical partition does not exceed the limit specified in the current configuration. [Satisfies SFRs: FDP_ACC.2, FDP_ACF.1 (allocation), FDP_IFC.1, FIA_ATD.1, FPR_UNO.1, FTA_TSE.1, FMT_MSA.1 (resource limits)]

d) The TOE will help ensure that at most one logical processor can execute on a physical processor at any given time. Processors from different partitions may be dispatched on the same processor at

different times. [Satisfies SFR: FDP_UNO.1]

e) The TOE will help prevent the transfer of a message between a logical partition and resources that are not allocated to it, except where the logical partition is explicitly authorized to do so. For example, PR/SM will intercept I/O interrupts that are not for the currently executing logical processor and will present them to the appropriate logical processor. [Satisfies SFRs: FDP_IFC.1, FPR_UNO.1, FDP_IFF.1]

6.3.1.4 Audit and Accountability

The TOE implemented a Security Log that is designed to be always enabled and contains a record of security relevant events. The View Security Log task allows an administrator to view the log recorded while the Archive Security Log task allows an administrator to create an archival copy of the security log. [satisfies SFRs: FAU_SAR.1]. The View Security Log task also allows an administrator to search or sort the security relevant events based on date or event criteria. [satisfies SFRs: FAU_SAR.3]. The log data assists an administrator in detection of potential attack or misconfiguration of the TOE security features.

a) The TOE will record in an audit log the security-relevant actions of the System Administrator. [satisfies SFRs: FAU_GEN.1] These actions are:

   i. Creating or modifying the IOCDS part of a configuration;

   ii. Modifying the reconfigurable part of a configuration;

   iii. Selecting a configuration to become the next current configuration;

   iv. Installing a selected configuration by a power-on reset, or activation;

   v. Activating or deactivating logical partitions.

   vi. Logging on or off the console.

b) Each audit log entry will be able to be associated with the identity of the System Administrator that caused the event. [satisfies SFRs: FAU_GEN.2].

c) Each audit log entry contains a reliable timestamp. [satisfies SFRs: FPT_STM.1].

d) The TOE will prevent the deletion or modification of these audit records by any user, except when the allocated audit space has been filled. In this case, the system will prune the log to two-thirds (2/3) of its capacity. [satisfies SFRs: FAU_STG.1 and FAU_STG.4]

e) The TOE will prevent the reading of the audit log by logical partitions. [satisfies SFRs: FAU_SAR.2]

6.3.1.5 Object Reuse

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

a) The TOE will ensure the clearing of information from a storage resource before that resource is

allocated to a logical partition. [Satisfies SFR: FDP_RIP.2]

b) The TOE will ensure that the information in a physical processor or coprocessor that is available to the currently executing logical processor is unaffected by any previously executing logical processor from another logical partition. For example, on a context switch, the control registers, general registers and program status word in the physical processor will be restored to their previously saved values. [Satisfies SFR: FPR_UNO.1, FDP_IFF.1]

c) The TOE will send a reset signal to a non-shared channel path and its attached I/O devices before that channel is allocated to a logical partition. [Satisfies SFR: FDP_RIP.2]

6.3.1.6 Reliability of Service

The TOE implemented a Reset profile to define the initial operational characteristics of the physical processors. [Satisfies SFR: FMT_MSA.3] Two of the parameters in the Reset profile are the processor running time and wait completion. These parameters provide the ability to share physical processor resources on either an event-driven basis or a time-driven basis. Disabling event driven dispatching causes shared physical processor resources to be distributed on the basis of time intervals according to the weights specified to effectively prevent unauthorized denial of service.

a) The TOE will enable the utilization of a physical processor resource by a logical partition to be restricted. [Satisfies SFR: FRU_RSA.1]

b) The logical partition can be prevented from releasing allocated processor time, or from receiving more than a configurable proportion of processor time. [Satisfies SFR: FTA_TSE.1]

6.3.1.7 Self Test

The TOE implemented a set of self-test functions that are executed when the TOE is started or reset [Satisfies SFR: FPT_TST.1], and periodically during normal execution [Satisfies SFR: FPT_SEP.3]. These functions help ensure that critical hardware functions work properly [Satisfies SFR: FPT_AMT.1, FPT_STM.1] and that the TOE has not been tampered with when it was powered off. [Satisfies SFR: FPT_TST.1]

6.3.1.8 Alternate Support Element

The TOE implemented functions that permit a quick switch to another Support Element when the primary Support Element has a hardware problem. Mirroring functions are performed on a regular basis to communicate any hard disk changes from the primary SE to the alternate SE [Satisfies SFR: FPT_TRC.1]. The Support Elements communicate using TCP/IP over a private Ethernet network that connects cage controllers and support elements. [Satisfies SFR: FPT_ITT.1]

6.3.2 Mapping of Security Functions and SFRs.

The following table shows the correspondence of the SFRs to the security functions of the TOE.

Component	Security Functions
FAU_GEN.1	Audit and Accountability (a)
FAU_GEN.2	Audit and Accountability (b)
FAU_SAR.1	Audit and Accountability
FAU_SAR.2	Audit and Accountability (e)
FAU_SAR.3	Audit and Accountability
FAU_STG.1	Audit and Accountability (d)
FAU_STG.4	Audit and Accountability (d)
FDP_ACC.2	Authorized Operations (a),(c); Authorized Administration (a,b,e,f,g,h,i,j,k,l)
FDP_ACF.1 (Activation)	Authorized Administration(b)
FDP_ACF.1 (Allocation)	Authorized Administration (b); Authorized Operations (b),(c)
FDP_ACF.1 (Channel Path)	Authorized Administration (e),(g),(h),(i),(j)
FDP_ACF.1 (CU/Devices)	Authorized Administration (f),(g),(j)
FDP_IFC.1	Authorized Administration (h),(i),(k); Authorized Operations (c),(e)
FDP_IFF.1	Authorized Operations (e); Object Reuse (b)
FDP_RIP.2	Object Reuse (a),(c)
FIA_ATD.1	Authorized Operations (b,c)
FIA_UID.2	Logical Partition Identity, Authorized Operations (a)
FMT_MSA.1 (Authorities)	Authorized Administration (c),(d),(l)
FMT_MSA.1 (Rsrc. Limits)	Authorized Operations (a),(b),(c)
FMT_MSA.1 (Cand. Access)	Authorized Administration (e)

Component	Security Functions
FMT_MSA.3	Reliability of Service
FMT_MTD.1	Authorized Administration (a)
FMT_SMR.1	Authorized Administration(a),(b); Authorized Operations (a)
FPR_UNO.1	Authorized Administration (k),(l); Authorized Operations (c),(d),(e); Object Reuse (b)
FPT_AMT.1	Self Test
FPT_ITT.1	Alternate Support Element
FPT_SEP.3	Self Test
FPT_STM.1	Audit and Accountability (c); Self Test
FPT_TRC.1	Alternate Support Element
FPT_TST.1	Self Test
FRU_RSA.1	Reliability of Service (a)
FTA_TSE.1	Authorized Administration (e), Authorized Operations (b),(c); Reliability of Service (b)

Table 6-1 - SFR and Security Function Correspondence

Security Functions	SFR
Audit and Accountability	FAU_SAR.1, FAU_SAR.3
Audit and Accountability (a)	FAU_GEN.1
Audit and Accountability (b)	FAU_GEN.2
Audit and Accountability (c)	FPT_STM.1
Audit and Accountability (d)	FAU_STG.1, FAU_STG.4
Audit and Accountability (e)	FAU_SAR.2
Authorized Administration (a)	FDP_ACC.2 , FMT_MTD.1, FMT_SMR.1
Authorized Administration (b)	FDP_ACC.2, FDP_ACF.1 (Activation, Allocation), FMT_SMR.1
Authorized Administration (c)	FMT_MSA.1 (Authorities)
Authorized Administration (d)	FMT_MSA.1 (Authorities)
Authorized Administration (e)	FDP_ACC.2, FDP_ACF.1 (Channel Path), FMT_MSA.1(Candidate Access), FTA_TSE.1
Authorized Administration (f)	FDP_ACC.2, FDP_ACF.1 (Control Unit/Devices)

Authorized Administration (g)	FDP_ACC.2, FDP_ACF.1 (Channel Path, Control Unit/Devices)
Authorized Administration (h)	FDP_ACC.2, FDP_ACF.1 (Channel Path), FDP_IFC.1
Authorized Administration (i)	FDP_ACC.2, FDP_ACF.1 (Channel Path), FDP_IFC.1
Authorized Administration (j)	FDP_ACC.2, FDP_ACF.1 (Channel Path, Control Unit/Devices)
Authorized Administration (k)	FDP_ACC.2, FPR_UNO.1, FDP_IFC.1
Authorized Administration (l)	FMT_MSA.1 (Authorities), FPR_UNO.1, FDP_ACC.2
Authorized Operations (a)	FDP_ACC.2, FIA_UID.2, FMT_MSA.1 (Resource Limits), FMT_SMR.1
Authorized Operations (b)	FDP_ACF.1 (Allocation), FIA_ADT.1, FTA_TSE.1, FMT_MSA.1 (Resource Limits)
Authorized Operations (c)	FDP_ACC.2, FDP_ACF.1 (Allocation), FDP_IFC.1, FIA_ATD.1, FPR_UNO.1, FTA_TSE.1, FMT_MSA.1 (Resource Limits)
Authorized Operations (d)	FDP_UNO.1
Authorized Operations (e)	FDP_IFC.1, FPR_UNO.1, FDP_IFF.1
Object Reuse (a)	FDP_RIP.2
Object Reuse (b)	FPR_UNO.1, FDP_IFF.1
Object Reuse (c)	FDP_RIP.2
Logical Partition Identity	FIA_UID.2
Reliability of Service	FMT_MSA.3
Reliability of Service (a)	FRU_RSA.1
Reliability of Service (b)	FTA_TSE.1
Self Test	FPT_AMT.1, FPT_TST.1, FPT_SEP.3, FPT_STM.1
Alternate Support Element	FPT_ITT.1, FPT_TRC.1.

Table 6-2 Security Function and SFR Correspondence

6.4 Assurance Requirements

ACM_AUT.1 – Partial CM Automation

Development of the zSeries is complex and performed by multiple developers. In this environment changes are controlled with the support of automated tools that handle numerous changes and only allow them to be performed by authorized developers.

LPAR and HMC/SE development are performed according to an ISO certified process.

ACM_CAP.4 – Generation Support and Acceptance Procedures

The required documentation is essentially the same as specified for ACM_AUT.1. In addition each time the TOE is built any modified or newly created configuration items are subject to tests to ensure the integrity of the build.

ACM_SCP.3 – Development tools CM coverage

Standard development processes are used to track design documentation, test documentation and development tools. Change control as well as authorization control is also discussed in the associated sections.

ADO_DEL.2 – Detection of Modification

The required documentation for initial TOE delivery is provided in the Installation Manual – Physical Planning and the Install Guide documents. Updates to the TOE once installed are provided through the release of new Engineering Change (EC) levels or via the Microcode Fix (MCF) process.

ADV_FSP.3 - Functional Specification

The specifications for the security functions of the TOE are documented in the PR/SM Planning Guide; Chapter 3 - Security Related Controls section. A detailed outline for complete exploitation of the TOE's security functions is found in the PR/SM: Planning for Security document.

ADO_IGS.1 – Installation, generation and start-up procedures

The required guidance for the installation, generation and start-up procedures is provided in the Trusted Facility Manual which provides the necessary information regarding establishing the correct physical environment, how to prepare the system for secure operation, procedures on how to correctly initialize the TOE, and operational considerations to help to ensure continued operation in conjunction with the security policy.

ADV_HLD.3 – Semiformal high-level design

The high-level designs for PR/SM and HMC/SE on the zSeries are documented in a proprietary internal document. These documents contain a description of the major structural elements and the function they provide. The documents further refine the structural elements into subsystems. The interrelationships of the subsystems are represented by flow diagrams.

ADV_IMP.2 - Implementation of the TSF

Implementation at the source code level is provided to the evaluators on a need-to-know basis under a nondisclosure agreement. A companion document, the Correspondence document provides the path from the SFRs to the actual implementation for all components of the TOE.

ADV_INT.1 – Modularity

PR/SM's modular design and component interaction are discussed in proprietary internal documents. An architectural description of each component is also provided.

ADV_LLD.2 – Semiformal low-level design

Internal proprietary documents provide a semiformal representation of the low-level design for PR/SM and the HMC/SE.

ADV_RCR.2 – Semiformal correspondence demonstration
An internal proprietary document associates each component of the Security Target with the corresponding functional specification, high-level design, and low-level design documentation.

ADV_SPM.3 - Formal TOE Security Policy Model
A formal mathematical model for the security policy has been created which shows the required correspondence.

AGD_ADM.1 – Administrator guidance
The Trusted Facility Manual provides guidance required helping to ensure a secure environment. All security parameters are described along with warnings about security settings that should be controlled in a secure processing environment.

AGD_USR.1 – User Guidance
The required guidance documentation is provided in the Trusted Facility Manual which provides the necessary information regarding establishing the correct physical environment, how to prepare the system for secure operation, procedures on how to correctly initialize the TOE, and operational considerations help to ensure continued operation in conjunction with the security polity.

ALC_DVS.1 – Identification of Security Measures
The security measures that are necessary to help protect the confidentiality and integrity of the TOE design and implementation are described in Site Security Manuals.

ALC_LCD.2 – Standardized Life Cycle Model
An internal proprietary document describes the process used to develop the TOE. This process represents the Incremental Model life cycle which in which the product is designed, implemented, integrated and tested as a series of incremental builds.

ALC_TAT.2 – Compliance with implementation standards
Well-defined development tools are in place for the implementation of the TOE.

ATE_COV.2 - Analysis of Coverage
The test suite used to verify the correct implementation of the TOE has been constructed to provide a one-to-one correspondence between individual tests and the specific security relevant functions of the TOE. In some cases, a test will cover more than one security function. This is due to the nature of some of these functions. (For example, many functions will also leave an audit trail and the test therefore includes the audit capability as well).

Additionally, the execution and verification of the test suite will include validation of the correctness of the external interfaces of the TOE as they are necessary for the invocation, execution and completion of the individual tests.

ATE_DPT.2 Testing: low-level design
Developers perform low-level testing whenever a new requirement is added into LPAR code.

ATE_FUN.1 – Functional testing
An internal proprietary document contains test plans, procedural descriptions and the goal of the test. Test results from the execution of the tests demonstrate that each tested security functions behaved as specified.

AVA_CCA.1 - Covert Channel Analysis

A thorough and systematic analysis of the implementation of the TOE was conducted to identify potential vulnerabilities in each subsystem of the TOE. Each vulnerability was subsequently examined by the appropriate designers to determine:

- Existence of the theoretical vulnerability
- Method and feasibility of exploitation
- Estimate of the bandwidth.

AVA_MSU.2 – Validation of Analysis

The required guidance documentation is provided in the Trusted Facility Manual which provides the necessary information regarding establishing the correct physical environment, how to prepare the system for secure operation, procedures on how to correctly initialize the TOE, and operational considerations to help to ensure continued operation in conjunction with the security polity.

AVA_SOF.1 - Strength of TOE Security Function Evaluation

While the assurance requirements for EAL5 call for this item, this only applies for functions that return measurable values and therefore is not applicable for LPAR.

AVA_VLA.3 - Moderately Resistant

The attack potential was calculated and shown to be within the guidelines specified in the CEM.

7 Protection Profile Conformance Claim

This Security Target does not claim conformance to any Protection Profile.

8 Rationale

8.1 TOE Description Rationale

The target of evaluation, PR/SM on zSeries CMOS Server has been defined. In addition the setup phase has been described showing how the TOE is to be set up for the intended operational environment. The security objectives, threats, and security functional requirements have been described and mapped to the security functions implemented within the TOE.

8.2 Security Objectives Rationale

This section demonstrates that the stated security objectives counter all identified threats.

8.2.1 Security Objectives Coverage

The following tables provide a mapping between the threats and the security objectives, and assumptions, illustrating that each security objective covers at least one threat, policy or assumption and that each threat, policy, or assumption is covered by at least one security objective.

THREATS	OBJECTIVES
T.Access_Data	O.Identity, O.Auth_Ops
T.Access_CPU	O.Identity, O.Auth_Ops
T.Access_IOCA	O.Identity, O.Auth_Admin
T.Access_Perf	O.Identity, O.Auth_Admin
T.Lpar_XCTL	O.Identity, O.Auth_Admin, O.Resource
T.Obj_Reuse	O.Reuse
T.Audit_Data	O.Audit
TE.Unauth_Access	OE.Data_Store, OE.Perss, OE.Phys_Prot
TE.False_Setup	OE.Sec_Setup

Table 8-1 - Threats Related to Objectives

8.2.2 Security Objectives Sufficiency

Separation of the physical resources of the processor into separate independent and isolated logical domains is the purpose of the TOE. The TOE is intended to prove a very high level of isolation of these logical partitions. In addition to the objectives for the TOE also objectives for the TOE environment have been defined. Those objectives for the TOE environment are addressed by assumptions on the TOE environment. Operational Security Policies have been defined that assist in establishing the correct environment that will be used by the TOE to enforce the security policy. The table above provides the mapping between the objectives, threats, and policies. The tables show that each objective addresses at least one threat and that each threat is covered by at least one objective, or policy. It is the intention to provide a comprehensive list

of threats that may compromise the isolation of partitions. Below follows a justification for each identified threat that the security objectives are suitable to counter it.

T.Access_Data – Illegal Access to Data
O.Identity helps to remove the threat of illegal access to data by a partition by assigning a zone number to each logical partition which provides it with a unique identity. O.Identity is additionally supported by O.Auth_Ops which then uses the unique zone number to establish ownership of processor and storage resources during partition activation and then prevents any illegal access to data or storage or message transfers during normal processor execution.

T.Access_CPU – Illegal Access or Control of Processors and Storage
O.Identity helps to remove the threat of illegal access or control of processors and storage a partition by assigning a zone number to each logical partition which provides it with a unique identity. O.Identity is additionally supported by O.Auth_Ops which then uses the unique zone number to ensure that the limits established at partition activation for storage, logical processors and coprocessors are not exceeded during normal processor execution.

T.Access_IOCA – Illegal Access of the IO Configuration
O.Identity helps to remove the threat of illegal access to the I/O configuration by a partition by assigning a zone number to each logical partition which provides it with a unique identity. O.Identity is additionally supported by O.Auth_Admin which then uses the unique zone number to restrict access to the IOCDS to only those logical partitions which have I/O configuration control authority.

T.Access_Perf – Illegal Access to Performance Data
O.Identity helps to remove the threat of illegal access to performance data by a partition by assigning a zone number to each logical partition which provides it with a unique identity. O.Identity is additionally supported by O.Auth_Admin which then uses the unique zone number to restrict access to the CPU and I/O processor performance data to only those logical partitions which have global performance data control authority.

T.Lpar_XCTL – Illegal control of another logical partition

O.Identity helps to remove the threat of illegal access to partition controls by a partition by assigning a zone number to each logical partition that provides it with a unique identity. O.Identity is additionally supported by O.Auth_Admin. Only when the Cross Partition functions are enabled due to O.Auth_Admin can one authorized partition take over control of an authorized target partition.

T.Obj_Reuse – Illegal transfer of data during context switch.
O_Reuse: The TOE provides the means to allow the subject to use a resource or service without the user‘s identity or contents of the resource being disclosed to other entities. When objects are reallocated from one subject to another, the objects are either reset (cleared) or are dedicated to one subject and therefore cannot be reallocated. A_LPAR_Only: O_Reuse assumes the TOE is in LPAR mode. A_SEP_Mode: The TOE provides the means to ensure complete separation of objects as well as preventing any subject from obtaining information about any other subject.

T.Audit_Data – Illegal modification of the content of the security log.
O.Audit helps to eliminate this threat by insuring that all security relevant events occurring on the system are recorded in a non-volatile audit log. All events are guaranteed to be recorded and no modifications can be made to the audit log except those consistent with the policy enforced by the TOE.

TE.False_Setup – Initial Setup of the Operational Configuration of the TOE inconsistent with TFM Guidance.
O.Sec_Setup helps to counter this threat by ensuring that the required setup for the TOE is established in accordance with the guidance in the Trusted Facility Manual. Evidence of the necessary actions can be discerned by inspection of the audit log.

TE.Unauth_Access - Unauthorized Access to physical resources of the TOE
OE.Phys_Prot helps to eliminate this threat by requiring that the HMC and zSeries be installed in a restricted area in order to limit accessibility, avoid physical destruction or alteration of the hardware, and avoid access via the remote support facility. OE.Phys_Prot is additionally supported by OE.Perss which requires that personnel working as System Administrators or other privileged positions be carefully selected and trained. Finally OE.Data_Store requires that Audit Log data stored off of the TOE must be controlled for confidentiality and integrity according to the owner's needs.

Environment Objectives mapped to Assumptions	OE.Data Store	OE.Perss	OE.Sec_Setup	OE.Phys_Prot
A.Phys_Secure				*
A.No_Remote				*
A.LPAR_Only			*	
A.Sep_Mode			*	
A.Admin_Secure		*		
A.Logical _Secure				*
A.Data_Secure	*			

Table 8-2 Environment Objectives Mapped to Assumptions

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

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

OE.Data_store defines that the security and integrity of the audit log is predicated on the assumption that the System Administrator will prune the Audit Log prior to reaching its capacity and physically protect archived data off-TOE. Because there is no functionality within the TOE to prevent the Audit Log from over-writing itself, such an environment is key to the security of the Audit Log.

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

The TOE does not provide any mechanism for physical protection of the actual processor, IO control units and devices, and Hardware Management Console. Therefore to help ensure that only trusted personnel have access to the processor hardware, IO and consoles, these assets are to be protected in restricted access areas.

As specified in OE.Phys_Prot, the method for providing physical security of the hardware is assumed to be restricted access. Restricted access will help ensure that assets used by the TOE, which are outside the domain of the TOE, remain secure.

A.No_Remote – The remote support facility must be disabled

The scope of the evaluation of the TOE was limited to exclude interaction between the remote support facility and the TOE. Therefore, to be compliant with the evaluation, the remote support facility must be disabled by removing the phone connection from the HMC modem.

In addition to restricting physical access to the HMC, OE.Phys_Prot requires that access via the remote support facility must also be prevented since this facility is not necessarily secure and outside of the TOE.

A.LPAR_Only – LPAR mode is the only valid mode of operation for the evaluated product.

Unless the zSeries is setup and initialized in LPAR mode, no partitions can be created, therefore the remaining discussion is not relevant.

By definition, the TOE requires the zSeries in LPAR mode which is required to securely setup partitions. OE.Sec_Setup requires that the TOE must be protected during the set-up phase to ensure that a secure environment is created. To guarantee that LPAR mode is a valid mode of operation, the objective of a secure environment during setup must be achieved.

A. Sep_Mode – Strict Separation Mode

For conformance with the scope of the evaluation, the zSeries must be setup and initialized in Strict Separation Mode as defined in the Trusted Facility Manual, and in Section 3.2 of this document.

Protection of the TOE for establishment of the required strict separation mode, as specified by OE.Sec_Setup helps to guarantee that all of the defined requirements to establish secure separation will be completed to provide the operational environment consistent with the scope of the evaluation.

A.Admin_Secure – Administrative Personnel Security

As any administrative personnel, who have access to the zSeries, will also have access to any and all information on that processor, these personnel must be cleared to the level required by the level of information and need-to-know that applies to the system.

OE.Perss requires that System and Security Administrators are authorized with the required need to know for all levels of the TOE. This is required to satisfy the assumption of secure administration.

A. Logical_Secure – Logical Access Security

Complementary to the physical security objectives, logical security as managed by the HMC and SE provides access control based on roles and responsibilities defined for the various System Administrator personnal at the installation.

Physical protection and security of the HMC and SE as specified in OE.Phys_Prot, provides the basis for implementation of access control based logical security.

8.3 Security Requirements Rationale

This section provides the rationale for necessity and sufficiency of security requirements, demonstrating that each of the security objectives is addressed by at least one security requirement, and that every security requirement is directed toward solving at least one objective.

8.3.1 Security Requirements Coverage

The following tables provide a mapping of the relationships of security requirements to objectives, illustrating that each security requirement covers at least one objective and that each objective is covered by at least one security requirement.

OBJECTIVES	REQUIREMENTS
O.Identity	FDP_ACF.1, FIA_ATD.1, FIA_UID.2
O.Auth_Admin	FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMR.1
O.Auth_Ops	FDP_ACC.2, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FPT_AMT.1. FPT_SEP.3, FPT_TST.1,
O.Audit	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.4, FMT_MTD.1, FPT_ITT.1, FPT_STM.1, FPT_TRC.1,
O.Reuse	FDP_RIP.2, FPR_UNO.1
O.Resource	FDP_ACC.2, FMT_MSA.1, FMT_MSA.3, FRU_RSA.1, FTA_TSE.1

Table 8-3- Objectives Related to Requirements

8.3.2 Security Requirements Sufficiency

The table above shows that each objective is addressed by at least one security functional requirement.

O.Identity – Identity

The objective demands that each logical partition have a unique identity. The objective is covered by FIA_ATD.1 that defines the security attributes belonging to an individual logical partition. FIA_UID.2 requires that each logical partition is identified before any TSF-mediated action is performed on behalf of that logical partition. Finally FDP_ACF.1 enforces access control SFP to objects based on the list of security attributes.

O.Auth_Admin – Authorized Administration

O.Auth_admin requires security functions provided by the TOE to help enable secure administration of the following: IOCDS, logical processors and storage, I/O channel paths and control units, cross partition functions and performance data access. The TOE provides restrictive default values for security attributes governing these security functions as specified in FMT_MSA.3. The TSF ensures that only the Security Administrator can alter these security attributes as per FMT_SMR.1. FDP_ACF.1 specifies the TSF shall enforce the access control SFP to objects based on security attributes including partition scheduling parameters (logical processors and storage), and global performance data (performance data access). I/O channel paths and control units are covered by the security functions enforced in FMT_MSA.1 (I/O Configuration Control Authority and Logical Partition Isolation). The TSF restricts the ability to change the IOCDS to the Security Administrator as covered in FMT_MTD.1.

O.Auth_Ops – Authorized Operations

O.Auth_Ops requires that the TOE provide an authorized administrator an effective means to manage the TOE and its security functions. FDP_ACC.2 provides authorized allocation of subjects to objects. FDP_ACF.1 provides for the establishment of security attributes and rules governing operations and access by subjects to objects based on these attributes. FMT_MSA.1 and FMT_MSA.3 to help ensure that once the authorization (or lack of authorization) is set, these attributes cannot be changed. FMT_MTD.1 allows only the Security Administrator the ability modify these settings. FPT_AMT.1 , FPT_SEP.3 and FPT_TST.1 provide for periodic validation of the correct operation of the TOE to help ensure that there can be no compromise in the execution of authorized operations. FDP_IFF.1 and FDP_IFC.1 specify that the TSF shall enforce the information flow control SFP on logical partitions based on security attributes including: global performance data access, I/O configuration control, cross partition reset/deactivate capability, and logical partition isolation.

O.Audit – Audit and Accountability

The objective demands that the TOE provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also to hold users accountable for any actions that they perform that are relevant to security. The objective is covered by FAU_GEN.1, FAU_GEN.2 and FPT_STM.1 that define which events are recorded in the audit log and associates an identity and timestamp with each event. FAU_SAR.1, FAU_SAR.2 and FAU_SAR.3 cover the ability of an authorized Security Administrator to read, search and sort the audit log data. FAU_STG.1, FMT_MTD.1 and FAU_STG.4 cover the prevention of any unauthorized deletions or modification to the audit records as well as specify the actions that occur when the audit log is full. Finally FPT_ITT.1 and FPT_TRC.1 cover the integrity and consistency of the audit log when transmitted between dual Support Elements.

O.Reuse - Reuse

O.Obj_Reuse requires that data is not transferred with resources when those resources are reallocated from one partition to another. FDP_RIP2. And FPR_UNO.1 sufficiently satisfies this requirement. FDP_RIP.2 ensures than any previous content of a resource is made unavailable when that resource is de-

allocated from any and all objects. FPR_UNO.1 ensures that users/subjects are unable to observe any operation on any object/resource by any other object/subject.

O.Resource – Reliability of Service
The objectives states that the TOE will prevent unauthorized access to physical processor running time and cross partition functions. FDP_ACC.2 helps ensure that the access control SFP is enforced to control all operations between subjects and objects. Therefore no subject (partition) can gain unauthorized access to the running time and partition control functions. FMT_MSA.1 and FMT_MSA.3 ensure that once the authorization (or lack of authorization) is set, these attributes cannot be changed. FRU_RSA.1 enforces the running time slices that have been previously defined. Finally, FTA_TSE.1 guarantees adherence to physical resource definitions and scheduling parameters.

8.4 TOE Summary Specification Rationale

The purpose of this section is to describe how the requirements of each of the Security Functional Requirements are satisfied by the IT Security functions.

FAU_GEN.1
The IT security function Audit and Accountability (a) fulfills the requirement because:
a) a security log has been implemented which records all configuration related actions
b) each security log entry contains the date and time of the event, the subject which preformed the action, and the outcome of the action
c) any activation profile updates or power-on reset actions will contain detailed definitions of the parameters

FAU_GEN.2
The IT security function Audit and Accountability (b) fulfills the requirement because:
a) security log entries record the identity of each user when they log on or off the HMC/SE
b) security log entries for requests which originate remotely contain the identity of the requesting user.

FAU_SAR.1
The IT security function Audit and Accountability (View Security Log Task) fulfills the requirement because:
a) a View Security Log task is available which allows the Security Administrator to read the security log entries in a clear and concise format

FAU_SAR.2
The IT security function Audit and Accountability (e) fulfills the requirement because:
a) the View Security Log task is only available to those users which are created with Security Administrator authority (i.e. user mode of System Programmer or Service Representative).

FAU_SAR.3
The IT security function Audit and Accountability (View Security Log Task) fulfills the requirement because:
a) the View Security Log task is provides the capability to search or sort the audit records based on date or event

FAU_STG.1
The IT security function Audit and Accountability (d) fulfills the requirement because:
a) no user or programmatic interfaces exist which allow for the deletion of entries from the Security Log
b) no user or programmatic interfaces exist which allow for the modification of entries in the Security Log

FAU_STG.4
The IT security function Audit and Accountability (d) fulfills the requirement because:
a) the Security Log is managed in such a way that when the allocated audit space has been filled the system will prune the log to two-thirds (2/3) of its capacity by removing the oldest log entries.

FDP_ACC.2
The IT security functions Authorized Administration (a,b,e,f,g,h,i,j,k,l), and Authorized Operations (a),(c) together fulfill the requirement because:
a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user
b) tasks which allow modification of profile and IOCDS definitions are restricted to Security Administrators. Profile definitions specify the resources (physical CPs, physical storage) available to a logical partitions as well as its authority to access Global Performance Data. IOCDS definitions specify the CHPIDS, Control Units and Devices that a logical partition can access.

FDP_ACF.1 (Activation)
The IT security functions Authorized Administration (b) fulfills the requirement because:
a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user
b) only users authorized as Security Administrators are allowed to modify the system configuration in the area concerning cross-partition control authority. This authority provides the capability for a logical partition to reset or deactivate another logical partition.

FDP_ACF.1 (Allocation)
The IT security functions Authorized Administration (b), and Authorized Operations (b,c) together fulfill the requirement because:
a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user
b) only users authorized as Security Administrators are allowed to modify the system configuration in the area concerning allocation of storage and logical processors.
c) the TOE helps ensure that the number of logical processors, amount of storage allocated to a partition cannot exceed the limit specified in the current configuration.
d) the TOE helps ensure that the physical processor time slice allocated to logical processors cannot exceed the limit specified in the current configuration.

FDP_ACF.1 (Channel Path)
The IT security functions Authorized Administration (e,g,h,i,j) together fulfill the requirement because the TOE implemented functions which enforce that:
a) a channel path can only be allocated to a logical partition if that partition has candidate access to the path
b) a logical partition can be prevented from using a shared channel path.
c) a channel path can be allocated exclusively to one logical partition either by identifying the channel path as dedicated, or by designating the owning partition as isolated.
d) a reconfigurable or dedicated channel path is never shared.

e) control units and I/O devices cannot be allocated independently of the channel path to which they are attached.

FDP_ACF.1 (Control Unit/Devices)
The IT security functions Authorized Administration (f,g,j), together fulfill the requirement because the TOE implemented functions which:
a) allow access to an I/O device on a shared channel path to be restricted among the set of logical partitions with candidate access.
b) allow the TOE to be configured to prevent the shared use of any channel path, control unit or I/O device between logical partitions
c) help ensure that control units and I/O devices cannot be allocated independently of the channel path to which they are attached
a)

FDP_ICF.1
The IT security functions Authorized Administration (h,i,k) and Authorized Operations (c,e) together fulfill the requirement because:
a) the TOE can be configured so that no information can flow among subjects and objects if they are not allocated to the same logical partition.

FDP_IFF.1
The IT security functions Authorized Operations (e) and Object Reuse (b) together fulfill the requirement because:
a) the TOE helps prevent the transfer of a message between a logical partition and resources that are not allocated to it, except where the logical partition is explicitly authorized to do so.
b) the TOE helps ensure that the information in a physical processor or coprocessor that is available to the currently executing logical processor is unaffected by any previously executing logical processor from another logical partition

FDP_RIP.2
The IT security function Object Reuse (a,c) fulfills the requirement because:
a) the TOE helps ensure that the contents of physical processors, storage or I/O utilized by different logical partitions will be cleared of any residual information before being utilized by the receiving logical partition.

FIA_ATD.1
The IT security functions Authorized Operations (b,c) together fulfill the requirement because:
a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user.
b) the TOE implemented Reset and Image profiles which allow the specification of partition identifiers, resource limits and partition scheduling parameters

FIA_UID.2
The IT security functions Logical Partition Identity and Authorized Operation (a) together fulfill the requirement because:
a) LPAR identify assigns a unique ID to Logical Partitions
b) Authorized Operations helps to ensure that each user has to identify before any other interaction with the TOE

FMT_MSA.1 (Authorities)
The IT security functions Authorized Administration (c,d,l) together fulfill the requirement because:
a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user.
b) only Security Administrators are allow to change, query or delete : I/O Configuration Control Authority, Cross Partition Authority, Logical Partition Isolation Authority, or Global Performance Data Control Authority.

FMT_MSA.1 (Resource Limits)
The IT security functions Authorized Operations (a,b,c) together fulfill the requirement because:
a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user.
b) only Security Administrators are allow to change, query or delete: resource limits (number of logical processors, amount of storage) or partition scheduling parameters.

FMT_MSA.1 (Candidate Access)
The IT security function Authorized Administration (e) fulfills the requirement because:
a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user.

b) only Security Administrators are allow to change, query or delete candidate access.

FMT_MSA.3
The IT security function Reliability of Service (Reset Profile) fulfills the requirement because:
a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user
b) the TOE has implemented a Default Reset and Image profile which contains restrictive initial values which are used as the basis for the creation of additional profiles
c) the TOE allows Security Administrators to override the restrictive initial values when creating new profiles

FMT_MTD.1
The IT security function Authorized Administration (a) fulfills the requirement because:
a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user
b) the authority to modify the IOCDS, reconfigurable part of the configuration, image profile or reset profile is limited to Security Administrators or logical partitions with I/O Configuration Control authority

FMT_SMR.1

The IT security functions Authorized Administration (a,b) and Authorized Operations (a) together fulfill the requirement because:

a) the TOE implemented a User Profile task used to define user identities, passwords and their corresponding authority level which determines the tasks made available to that user

b) all users which either operate or administer the TOE must first be assigned an identity, password and an authority level of either: Operator, Advanced Operator, System Programmer, CE or Access Administrator

FPR_UNO.1
The IT security functions Authorized Administration (k,l), Authorized Operations (c,d,e), and Object Reuse (b) together fulfill the requirement because:
a) the TOE can be configured so that no logical partitions have global performance data control authority. In this case, a logical partition will only be able to gather performance data about the resources allocated to it
b) the TOE will help to ensure that a storage resource is never shared
c) the TOE helps to ensure that the contents of physical processors, storage or I/O utilized by different logical partitions will be cleared of any residual information before being utilized by the receiving logical partition

FPT_AMT.1
The IT security function Self Test fulfills the requirement because:
a) the TOE implemented a set of self test functions which are executed whenever the TOE is started or reset as well as periodically during normal execution
b) the self tests demonstrate the correct operation of the hardware platform on which the TOE is executing

FPT_ITT.1
The IT security function Alternate Support Element fulfills the requirement because:
a) the TOE helps to protect the Security Log data from disclosure and modification during replication between Support Elements by transmitting the data over a private network

FPT_SEP.3
The IT security function Self Test fulfills the requirement because:
a) it validates that the mechanisms use to protect the TOE are not compromised by insuring that the underlying hardware is fully operational, and by verifying the storage isolation parameters established during TOE setup and initialization have not been modified.

FPT_STM.1
The IT security function Audit and Accountability (c) and Self Test fulfills the requirement because:
a) all Security Log entries are recorded with a timestamp
b) HMC/SE timestamps are retrieved from the HMC/SE hardware clock which is periodically synchronized with the other hardware clocks in the system

FPT_TRC.1
The IT security function Alternate Support Element fulfills the requirement because:
a) any hard disk changes that are mirrored from the primary SE to the alternate SE are checked for consistency through the use of a checksum on the transmitted data
b) all consistency checking of mirrored data is performed before any Security Log updates are allowed

FPT_TST.1
The IT security function Self Test fulfills the requirement because:
a) the TOE implemented a set of self test functions which are executed whenever the TOE is started or reset as well as periodically during normal execution
b) the self tests demonstrate the correct operation of the hardware platform on which the TOE is executing

FRU_RSA.1
The IT security function Reliability of Service (a) fulfills the requirement because:

a) the TOE implemented a Reset profile which allows the utilization of a physical processor resource by a logical partition to be restricted.

FTA_TSE.1
The IT security function Authorized Operations (b,c), Authorized Administration(e), and Reliability of Service (b) together fulfill the requirement because:

a) the TOE helps to ensure that the amount of storage allocated to a logical partition does not exceed the limit specified in the current configuration
b) the TOE helps to ensure that the number of logical processors allocated to a logical partition does not exceed the limit specified in the current configuration
c) a channel path can only be allocated to a logical partition if that partition has candidate access to the path
d) the TOE implemented Reset profile parameters which prevents a logical partition from releasing allocated processor time, or from receiving more than a configurable proportion of processor time

8.5 Internal Consistency and Mutual Support

This section demonstrates that the stated security requirements together form a mutually supportive and internally consistent whole. Internal consistency is demonstrated in an analysis of dependencies. Mutual support is shown through consideration of the interactions between and among the SFRs.

8.5.1 Rationale that Dependencies are Satisfied

The selected security requirements include related dependencies, both direct and indirect. The indirect dependencies are those required by the direct dependencies. All of these dependencies must be met or their exclusion justified.

8.5.1.1 Security Functional Requirements Dependencies

The following table provides a summary of the security functional requirements dependency analysis. No dependencies are excluded. For dependencies on a selective list of components are stated in the CC, the component that has been included in this Security Target is displayed in bold.

A dependency is also resolved, if a hierarchical higher component from the CC has been included in the Security Target. Therefore it might be that not exactly the component as stated in the CC is selected within this Security Target, but a hierarchical higher one.

Component	Dependencies	Resolved
FAU_GEN.1	FPT_STM.1	Yes
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_SAR.3	FAU_SAR.1, FAU_GEN.1	Yes

Component	Dependencies	Resolved
FAU_STG.1	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	Yes
FDP_ACC.2	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Yes
FDP_IFC.1	FDP_IFF.1	Yes
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	Yes
FDP_RIP.2	None	Yes
FIA_ATD.1	None	Yes
FIA_UID.2	None	Yes
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1	Yes
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMR.1	Yes
FMT_SMR.1	FIA_UID.1	Yes
FPR_UNO.1	None	Yes
FPT_AMT.1	None	Yes
FPT_ITT.1	None	Yes
FPT_SEP.3	None	Yes
FPT_STM.1	None	Yes
FPT_TRC.1	FPT_ITT.1	Yes
FPT_TST.1	FPT_AMT.1	Yes
FRU_RSA.1	None	Yes
FTA_TSE.1	None	Yes

Table 8-4 - Summary of Security Functional Requirements Dependencies

Security Assurance Dependencies Analysis

The assurance level selected within this TOE is EAL5 with no modifications. The dependencies are defined by the criteria and since they are unmodified in this TOE, all dependencies of the assurance components within this Security Target are resolved.

8.6 Rationale for Strength of Function

The security enforcing function argument only applies to cases where measurable values are obtainable. In the case of zSeries LPAR, this is not possible therefore the Strength of Function claim is not applicable for this Security Target because no mechanism in the TOE is based upon permutational or probabilistic functions.

Appendix - Notices

IBM Corporation
New Orchard Rd,
Armonk, NY 10504

More details on IBM UNIX hardware, software and solutions may be found at ibm.com/servers/unix/.

IBM
IBM logo
IBM eServer
e-business
ESCON
FICON
Lotus
MVS/ESA
OS/390
Parallel Sysplex
PR/SM
Processor Resource/Systems Manager
Resource Link
RMF
S/370
S/390
Sysplex Timer
VM/ESA
VSE/ESA
z/Architecture
z/OS
z/VM
zSeries

are trademarks or registered trademarks of the International Business Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds.

UNIX is a registered trademark of The Open Group in the United States and other countries.

IBM, the IBM logo, the e-business logo, AIX, DB2, DB2 Universal Database, pSeries, RS/6000, SP and WebSphere are registered trademarks or trademarks of the International Business Machines Corporation in the United States and/or other countries.

Other company, product and service names may be trademarks or service marks of others.

IBM may not offer the products, programs, services or features discussed herein in other countries, and the information may be subject to change without notice.

General availability may vary by geography.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Any reliance on these statements is at the relying party's sole risk and will not create any liability or obligation for IBM.

IBM may have patents or pending patent aplications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Appendix A - Glossary

A.1 Common Criteria Terminology

This section contains only those terms that are used in a specialized way in the CC. The majority of terms in the CC are used either according to their accepted dictionary definitions or commonly accepted definitions found in ISO security glossaries or other well-known collections of security terms.

Assets	Information or resources to be protected by the countermeasures of a TOE.
Assignment	The specification of an identified parameter in a component.
Assurance	Ground for confidence that an entity meets its security objectives.
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) from ISO 15408 Part 3 to an EAL or assurance package.
Authentication data	Information used to verify the claimed identity of a user.
Authorized user	A user who may, in accordance with the TSP, perform an operation.
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package.
Dependency	A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.
Evaluation Assurance Level (EAL)	A package consisting of assurance components from ISO 15408 Part 3 that represents a point on the CC predefined assurance scale.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in ISO 15408 Part 3 of the CC.
Human user	Any person who interacts with the TOE.
Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Internal communication channel	A communication channel between separated parts of TOE.
Internal TOE transfer Object	Communicating data between separated parts of the TOE. An entity within the TSC that contains or receives information and upon which subjects perform operations.
Organizational security policies	One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Package	A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secret	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.
Security attribute	Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.
Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
Security Function Policy (SFP)	The security policy enforced by an SF.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Selection	The specification of one or more items from a list in a component.
Strength of Function (SOF)	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.
SOF-basic	A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.
SOF-medium	A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.
SOF-high	A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential.
Subject	An entity within the TSC that causes operations to be performed.
Target of Evaluation (TOE)	An IT product or system, including its associated administrator and user guidance documentation that is the subject of an evaluation.
TOE resource	Anything useable or consumable in the TOE.

TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy (TSP)	A set of rules that regulates how assets are managed, protected and distributed within a TOE.
TOE security policy model	A structured representation of the security policy to be enforced by the TOE.
Transfers outside TSF control	Communicating data to entities not under control of the TSF.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with the necessary confidence to support the TSP.
Trusted path	A means by which a TSF and device physically separated from the TOE can communicate with the necessary confidence to support the TSP.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE.
TSF Scope of Control (TSC)	The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
User	Any entity (human user, resident added application, 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.

Appendix B – PR/SM Glossary

B.1 Subjects

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

Logical Partition – the possible logical partitions are defined in the current configuration object. Only activated logical partitions may use the system.

B.2 Definitions

audit log - security-relevant actions are recorded in an audit log. The audit log file is 10 megabytes in size and can hold records of varying sizes (100 bytes - 1 kilobytes). In a typical installation this would represent many weeks worth of activity. This is also referred to as the security log.

audit record - an entry in the audit log.

configuration - a set of objects (logical partitions and resources) and the relationships between them. This consists of two exclusive parts: the static configuration held in the IOCDS, and the reconfigurable data.

The IOCDS part of a configuration identifies the logical partitions, channel paths, control units, and IO devices in the system; their connectivity and characteristics; the candidate access restrictions and initial allocations for channel paths and IO devices; and whether channel paths are shared, reconfigurable or dedicated. Details of how the IOCDS is set up by the System Administrator are given in [1].

The reconfigurable part of a configuration identifies the number of logical processors, co-processors and storage resources that may be allocated to a logical partition; the actual allocation of resources; scheduling parameters; status information such as whether logical processors and channel paths are online or off-line; and whether logical partitions are authorized, isolated, activated or deactivated.

Note that a single object in a configuration may contain both static data from the IOCDS and reconfigurable data.

channel path - a channel resource which can be allocated to a logical partition. The static attributes of a channel include its type, which partitions have candidate access to it, and whether it is shared, reconfigurable or dedicated. The dynamic attributes of a channel include its current allocation to a partition, and whether it is online.

control unit - a physical unit which may be attached to one or more channel paths (in one or more partitions) and manages a number of I/O devices. A control unit is allocated to a partition if a channel path to which it is attached is allocated to the partition.

coprocessor - a cryptographic facility attached to 1 or 2 of the physical processors.

current configuration - the configuration that is currently being enforced by PR/SM.

Global Performance Partition - the logical partition that is given the authority to view the activity data for other logical partitions.

IOCDS – IO 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.

I/O device - a physical device that may be attached to one or more control units (on one or more channel paths). An I/O device is allocated to a partition if a control unit to which it is attached is allocated to the partition, and the partition has candidate access to the IO device.

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.

logical processor - a logical interface to a physical processor, which allows the physical resource to be shared. Each activated partition has at least one logical processor (and optionally other coprocessor resources). Logical processors are never shared. Allocation of logical processors occurs only at logical configuration activation. The number of logical processors can be altered. When the number of logical processors is decreased, an increment of dispatchability/parallelism is deleted from the partition in a manner that corresponds to varying a physical processor off-line in basic mode.

message - a flow of information, including requests, responses and indications. If a partition has Cross-Partition Control Authority, it can send out a message to reset/deactivate another partition. If a partition as Global Performance Data enabled, it can request performance data (CP utilization data and IOP busy data) for all logical partitions in the configuration.

Partition scheduling parameters - Partition Scheduling Parameters - theses parameters consist of two values: Processor Running Time and Wait Completion. The processor running time is the length of continuous time allowed for the dispatch of a logical CP. The wait completion setting determines if shared CP resources are divided on either an event-driven basis or a time-driven basis.

physical processor - a processor resource which may be dedicated to a single partition or shared between partitions.

profiles – image profiles and reset profiles are utilized. Reset profiles are used to: Select LPAR mode of operation; Select an LPAR mode IOCDS; Optionally specify an LP activation sequence; Enable I/O Priority Queuing. Image Profiles are used to Define LP characteristics and optionally specify automatic load settings

resource - an object that can be allocated to a logical partition, i.e. channel path, control unit, I/O device, storage, physical processor, logical processor.

security log - see audit log.

storage - each activated partition has an initial allocation of central storage. It may also have an initial allocation of expanded storage. Both types of storage are individually contiguous. In some circumstances, further areas of storage, known as reserved central storage and reserved expanded storage, may also be identified. This storage is reserved for future allocation to, and use by, the partition.

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

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

users - The only direct users are the System Administrator and logical partitions.

END OF THE DOCUMENT