Common Criteria for Information Technology Security Evaluation

Public Version

Of the

Security Target for PR/SM for the IBM System z10™ Enterprise Class

and

IBM System z10™ Business Class

Version 8.3

January 29, 2009

This Security Target was developed for the evaluation of the Processor Resource/Systems Manager™ (PR/SM™) for the IBM System z10 EC and IBM System z10 BC platforms 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 the public version 8.3 of the ST Document for the PR/SM Licensed Internal Code (LIC) on the IBM System z10 Enterprise Class (z10 EC™) and the IBM System z10 Business Class (z10 BC™) processors, at LIC Driver 76 Control Level 3. LIC is microcode licensed by IBM. The document date is January 29, 2009.

For the remainder of this document, the IBM System z10 EC and IBM System z10 BC will be referred to as z10™.

1.2 Security Target Overview

This Security Target was developed for the evaluation of PR/SM for the z10 platform 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.

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

Chapter 2 is a detailed description of the TOE, including the version subject for this evaluation and an overview of the LPAR architecture and design.

Chapter 3 discusses the TOE Security environment, including assumptions (A.xx), threats (T.xx), and organizational security policies (P.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 LIC kernel running on the z10. The z10 general-purpose data processing systems can only be initialized in LPAR mode. PR/SM provides the capability that enables the z10 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®, z/VM®, VIF, VM/ESA®, VSE/ESA™, TPF or LINUX.

PR/SM 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 PR/SM related to normal operations and maintenance of the system are not considered as security enforcing functions because the TOE will be configured to provide a configuration consistent with secure isolation such that these operations cannot be in conflict with the security policy of PR/SM.

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

1.3 Assurance Level

The assurance level for this Security Target is EAL5. The business requirements for customers of the z10 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 CC Conformance Claim

This ST is CC Part 2 conformant and Part 3 conformant, with a claimed Evaluation Assurance Level of EAL5.

The evaluation is based on the Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, Parts 1 to 3.

2 TOE Description

2.1 Definition of TOE

The target of the evaluation is the PR/SM LIC kernel running on the IBM z10 hardware platforms which includes the following models.

z10 EC Model Number	Feature Code	Number of CPs
E12	6700	0*
E12	6701	1
E12	6702	2
E12	6703	3
E12	6704	4
E12	6705	5
E12	6706	6
E12	6707	7
E12	6708	8
E12	6709	9
E12	6710	10
E12	6711	11
E12	6712	12
E26	6713	13
E26	6714	14
E26	6715	15
E26	6716	16
E26	6717	17
E26	6718	18
E26	6719	19
E26	6720	20
E26	6721	21
E26	6722	22
E26	6723	23
E26	6724	24
E26	6725	25
E26	6726	26
E40	6727	27
E40	6728	28
E40	6729	29
E40	6730	30
E40	6731	31
E40	6732	32
E40	6733	33
E40	6734	34
E40	6735	35
E40	6736	36
E40	6737	37
E40	6738	38
E40	6739	39

E40	6740	40
E56	6741	41
E56	6742	42
E56	6743	43
E56	6744	44
E56	6745	45
E56	6746	46
E56	6747	47
E56	6748	48
E56	6749	49
E56	6750	50
E56	6751	51
E56	6752	52
E56	6753	53
E56	6754	54
E56	6755	55
E56	6756	56
E64	6757	57
E64	6758	58
E64	6758	59
E64	6760	60
E64	6761	61
E64	6762	62
E64	6763	63
E64	6764	64

Table 2-1 - z10 EC Capacities and number of Central Processors

* Model E12 ordered with 0 CPs has no central processors (CP) but could be all IFLs or all ICFs (see Appendix B.2 under Processor Unit for details)

z10 BC Model Number	Feature Code	Model Capacity ID	# CPs
E10	5013	A00	0*
E10	5014	A01	1
E10	5015	A02	2
E10	5016	A03	3
E10	5017	A04	4
E10	5018	A05	5
E10	5019	B01	1
E10	5020	B02	2
E10	5021	B03	3
E10	5022	B04	4
E10	5023	B05	5
E10	5024	C01	1
E10	5025	C02	2
E10	5026	C03	3
E10	5027	C04	4
E10	5028	C05	5
E10	5029	D01	1
E10	5030	D02	2
E10	5031	D03	3
E10	5032	D04	4
E10	5033	D05	5

E10	5034	E01	1
E10	5035	E02	2
E10	5036	E03	3
E10	5037	E04	4
E10	5038	E05	5
E10	5039	F01	1
E10	5040	F02	2
E10	5041	F03	3
E10	5042	F04	4
E10	5043	F05	5
E10	5044	G01	1
E10	5045	G02	2
E10	5046	G03	3
E10	5047	G04	4
E10	5048	G05	5
E10	5049	H01	1
E10	5050	H02	2
E10	5051	H03	3
E10	5052	H04	4
E10	5053	H05	5
E10	5054	I01	1
E10	5055	I02	2
E10	5056	I03	3
E10	5057	I04	4
E10	5058	I05	5
E10	5059	J01	1
E10	5060	J02	2
E10	5061	J03	3
E10	5062	J04	4
E10	5063	J05	5
E10	5064	K01	1
E10	5065	K02	2
E10	5066	K03	3
E10	5067	K04	4
E10	5068	K05	5
E10	5069	L01	1
E10	5070	L02	2
E10	5071	L03	3
E10	5072	L04	4
E10	5073	L05	5
E10	5074	M01	1
E10	5075	M02	2
E10	5076	M03	3
E10	5077	M04	4
E10	5078	M05	5
E10	5079	N01	1
E10	5080	N02	2
E10	5081	N03	3
E10	5082	N04	4
E10	5083	N05	5
E10	5084	O01	1
E10	5085	O02	2
E10	5086	O03	3
E10	5087	O04	4
E10	5088	O05	5
E10	5089	P01	1

E10	5090	P02	2
E10	5091	P03	3
E10	5092	P04	4
E10	5093	P05	5
E10	5094	Q01	1
E10	5095	Q02	2
E10	5096	Q03	3
E10	5097	Q04	4
E10	5098	Q05	5
E10	5099	R01	1
E10	5100	R02	2
E10	5101	R03	3
E10	5102	R04	4
E10	5103	R05	5
E10	5104	S01	1
E10	5105	S02	2
E10	5106	S03	3
E10	5107	S04	4
E10	5108	S05	5
E10	5109	T01	1
E10	5110	T02	2
E10	5111	T03	3
E10	5112	T04	4
E10	5113	T05	5
E10	5114	U01	1
E10	5115	U02	2
E10	5116	U03	3
E10	5117	U04	4
E10	5118	U05	5
E10	5119	V01	1
E10	5120	V02	2
E10	5121	V03	3
E10	5122	V04	4
E10	5123	V05	5
E10	5124	W01	1
E10	5125	W02	2
E10	5126	W03	3
E10	5127	W04	4
E10	5128	W05	5
E10	5129	X01	1
E10	5130	X02	2
E10	5131	X03	3
E10	5132	X04	4
E10	5133	X05	5
E10	5134	Y01	1
E10	5135	Y02	2
E10	5136	Y03	3
E10	5137	Y04	4
E10	5138	Y05	5
E10	5139	Z01	1
E10	5140	Z02	2
E10	5141	Z03	3
E10	5142	Z04	4
E10	5143	Z05	5

Table 2-2 - z10 BC Capacities and number of Central Processors

* Model E10 ordered with 0 CPs has no central processors (CP) but could be all IFLs or all ICFs (see Appendix B.2 under Processor Unit for details)

The above mentioned hardware is not part of the TOE.

The TOE subject of this Security Target is LIC Driver Level D76 Control Level 3 Date: 18 Sept 2008.

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

2.2 z10 Overview

The IBM System z10 are world class enterprise servers designed to meet your business needs. The System z10 are built on the inherent strengths of the IBM System z platform and are designed to deliver new technologies and virtualization that provide improvements in price/performance for key new workloads. The System z10 future extends System z leadership in key capabilities with the delivery of expanded scalability for growth and large scale consolidation, improved security and availability to reduce risk, and just-in-time capacity deployment, helping to respond to changing business requirements.

z10 General Purpose Models

The System z10 delivers:

- Improved total system capacity in a 64-way server, offering increased levels of performance and scalability to help enable new business growth
- Quad-core 4.4 and 3.5 GHz processor chips that can help improve the execution of CPU intensive workloads
- On z10 EC, up to 1.5 terabytes of available real memory per server for growing application needs (with up to 1 TB real memory per LPAR).
- On z10 EC, increased scalability with 36 available subcapacity settings
- Just-in-time deployment of capacity resources which can improve flexibility when making temporary or permanent changes. Activation can be further simplified and automated using z/OS Capacity Provisioning (available on z/OS V1.9 with PTF for APAR OA20824 and z/OS 1.10, when available).
- Increased flexibility for just-in-time offerings with ability for more temporary offerings installed on the CPC and ways to acquire capacity backup
- Ability to allow production workload to be executed on a CBU Upgrade during a CBU test provided that certain contract terms are in effect with IBM
- On z10 BC, a single model E10 offering increased granularity and scalability with 130 available capacity settings.
- On z10 BC, up to a 5-way general purpose processor and up to 5 additional Specialty Engine processors or up to a 10-way IFL or ICF server for increased levels of performance and scalability to help enable new business growth.

- On z10 BC, up to 120 GB of available real memory per server for growing application needs (with up to 248 GB of real memory planned in June 2009). Also a new 8GB fixed Hardware System Area (HSA) which is managed separately from customer memory. This fixed HSA is designed to improve availability by avoiding outages.
- Plan ahead memory that allows for non disruptive memory increases.
- New temporary capacity offering Capacity for Planned Event (CPE), a variation on CBU. CPE can be used when capacity is unallocated, but available, and is needed for a short term event.
- On z10 EC, a new 16 GB fixed Hardware System Area (HSA) which is managed separately from customer memory. This fixed HSA is designed to improve availability by avoiding outages.
- Memory and books that are interconnected with a point-to-point symmetric multi processor (SMP) network running with an InfiniBand® host bus bandwidth at 6 GBps designed to deliver improved performance.
- The new InfiniBand Coupling Links (planned to be available second quarter 2008) rated at 6GBps which are designed to provide a high speed solution to the 10 meter limitation of ICB4 since they will be available in lengths up to 150 meters.
- The new OSA-Express3 10 GbE LR with double the port density designed to deliver improved connectivity to web applications.
- HiperSockets™ Improvements with Multiple Write Facility for performance and Layer2 Support, allowing IP clients to be included in HiperSockets environments
- Encryption accelerator provided on quad-core chip, which is designed to provide high speed cryptography for protecting data in storage. CP Assist for Cryptographic Function (CPACF) offers more protection and security options with Advanced Encryption Standard (AES) 192 and 256 and stronger hash algorithm with Secure Hash Algorithm (SHA-512 and SHA-384)
- Large page support (1 megabyte pages)
- Up to 336 FICON® Express4 channels
- Improved access to data with High Performance FICON for System z (zHPF) on both FICON Express4 and FICON Express2
- Enhanced problem determination, analysis, and manageability of the storage area network (SAN) by providing registration information to the fabric on the name server for both FICON and FCP
- OSA-Express3 Gigabit Ethernet and 1000BASE-T for the Network Control Program, providing Channel Data Link Control protocol support between the z10 and IBM Communications Controller for Linux on System z (CCL) allowing systems administrators to configure, manage, and operate their CCL Network Control Programs in the same manner as their ESCON-attached 374x NCPs
- Protection from network intrusion with OSA-Express QDIO data connection isolation for z/VM virtualized environments on System z10 and System z9
- Long Reach 1x InfiniBand coupling links - an alternative to ISC-3 facilitating coupling link consolidation
- Coupling Facility Control Code Level 16 - to help deliver faster service time for CF Duplexing, and improvements to the efficiency of workload distribution when using shared queues in the Coupling Facility
- Updates to Server Time Protocol for enhanced time accuracy, availability, and systems management

- Support for Longer Personal Account Numbers for stronger data protection on Crypto Express
- Trusted Key Entry Licensed Internal Code 5.3 enhancement to support Advanced Encryption Standard (AES) encryption algorithm, audit logging, and an infrastructure for payment card industry data security standard (PCIDSS)
- Integrated Encryption designed to provide high-speed cryptography for protecting data in storage. CP Assist for Cryptographic Function (CPACF) offers more protection and security options with Advanced Encryption Standard (AES) 192 and 256 and stronger hash algorithms with Secure Hash Algorithm (SHA-384 and SHA-512).
- Integrated Hardware Decimal Floating Point unit on each core on the Processor Unit (PU), which can aid in decimal floating point calculations and is designed to deliver performance improvements and precision in execution.
- Production workload may now be executed on a CBU Upgrade during a CBU Test provided that certain contract terms are in effect with IBM.
- The new InfiniBand Coupling Links with a link data rate of 6 GBps, designed to provide a high-speed solution and increased distance (150 meters) compared to ICB-4 (10 meters).
- FCP - increased performance for small block sizes
- SCSI Initial Program Load (IPL) - now a base function
- Platform and name server registration in FICON channel.
- Extended-distance FICON - helps avoid degradation of performance at extended distances.
- Increased performance for Local Area Network connectivity with new OSA-Express3 I/O features providing double the port density, increased throughput, and reduced latency. OSA-Express3 10 GbE Long Reach (LR) and Short Reach (SR), OSA Express3 GbE 4-port LX and SX, OSA-Express3-2P GbE SX, OSA-Express3 1000BASE-T 4-port card and OSA-Express3-2P 1000BASE-T.
- Fiber Quick Connect (FQC) for FICON LX channels. FQC is a fiber harness integrated in the System z10 frame for a 'quick' connect. It offers harness cabling, harness brackets and mounting hardware. FQC is offered as a feature on the System z10 for connections to ESCON® channels and new for FICON LX channels. It can be ordered in conjunction with an Enterprise Fibre Cabling Services structured (trunk) solution. These harnesses are installed when your system is built, and your System z10 arrives ready to connect the trunk cables at your site.
- IBM Site and Facilities Services
- Support for IBM Systems Director Active Energy Manager for Linux on System z for a single view of actual energy usage across multiple heterogeneous IBM platforms within the infrastructure. AEM V3.1 is a key component of IBM's Cool Blue TM portfolio within Project Big Green. *

* This satisfies the statement of direction announced in Software Announcement 207-289, dated November 13, 2007, for IBM Systems Director Active Energy Manager for POWER, V3.1, which stated: Future System z servers plan to support the monitoring functions of IBM Systems Director Active Energy Manager.

PR/SM is a hardware facility that enables the resources of a single physical machine to be divided between distinct, predefined logical machines called "logical partitions". Each logical partition is a domain of execution, and is considered to be a subject capable of running a conventional system control program (SCP) such as z/OS, z/VM, VIF, VM/ESA, VSE/ESA, TPF or Linux. These operating systems run in a PR/SM partition.

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 ever allocated to only 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. The use of LIC prevents untrusted code from masquerading as part of the TOE and abusing TOE privileges. The TOE is composed of:

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

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

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

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

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 on the Hardware Management Console or for service mode on the support element. A user profile consists of a user identification, a password, managed resource roles and task roles

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

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

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

The following general definitions can be established:

Security Administrator – any user(s) of the HMC who is defined with a user role(s) containing at least all of the following tasks:

- Archive Security Logs
- Change LPAR Controls
- Change LPAR Group Controls
- Change LPAR I/O Priority Queuing
- Change LPAR Security
- Customize/Delete Activation Profiles
- Customize User Controls

- Input/Output (I/O) Configuration
- Logical Processor Add
- Manage Users Wizard
- Reassign Channel Path
- User Profiles
- View Security Logs

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

The following table lists the console actions and the corresponding default user IDs that can perform these console actions.

Table 2-3 – Default System Administrator User IDs and Console Actions

Console Actions	Default User ID				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Analyze Console Internal Code					X
Archive Security Logs			X	X	X
Authorize Internal Code Changes			X		X
Backup Critical Console Data			X		X
Block Automatic Licensed Internal Code Change Installation				X	
Certificate Management			X	X	X
Change Console Internal Code		X	X		X
Change Password	X	X	X	X	X
Configure 3270 Emulators			X		
Configure Data Replication				X	
Console Default User Settings				X	
Console Messenger	X	X	X	X	X
Copy Console Logs to Media					X
Copy Support Element Data					X

Console Actions	Default User ID				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Create Welcome Text				X	
Customize API Settings				X	
Customize Auto Answer Settings		X	X	X	X
Customize Automatic Logon				X	
Customize Console Data/Time	X	X	X	X	X
Customize Console Services		X	X	X	X
Customize Customer Information			X		X
Customize Modem Settings			X		X
Customize Network Settings				X	X
Customize Outbound Connectivity			X		X
Customize Product Engineering Access				X	
Customize Remote Service	X	X	X	X	X
Customize Scheduled Operations			X		X
Customize Support Element Date/Time	X	X	X	X	X
Customize User Controls				X	
Domain Security				X	X
Enable Electronic Service Agent				X	
Enable FTP Access to Mass Storage Media			X		
Format Media	X	X	X	X	X
Format Security Logs to DVD-RAM			X	X	X
Hardware Management Console Settings		X	X	X	X
Installation Complete Report					X
Logoff or Disconnect	X	X	X	X	X
Manage Enterprise Directory Server Definitions				X	
Manage Print Screen Files	X	X	X	X	X

Console Actions	Default User ID				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Manage Remote Connections	X	X	X	X	X
Manage Remote Support Requests	X	X	X	X	X
Manage Users Wizard				X	
Migrate Channel Configuration Files			X		X
Monitor System Events			X		
Network Diagnostic Information	X	X	X	X	X
Object Locking Settings	X	X	X	X	X
Offload Virtual RETAIN® Data to DVD-RAM	X	X	X	X	X
Password Profiles				X	
Perform a Console Repair Action					X
Reassign Hardware Management Console					X
Rebuild Vital Product Data					X
Remote Hardware Management Console	X	X	X	X	X
Report a Problem	X	X	X		X
Restore Legacy HMC Data					X
Save Upgrade Data					X
Save/Restore Customizable Console Data				X	
Shutdown or Restart	X	X	X	X	X
Single Step Console Internal Code		X	X		X
Tip of the Day	X	X	X	X	X
Transmit Console Service Data	X	X	X	X	X
Transmit Vital Product Data			X		X
User Profiles				X	
User Settings	X	X	X	X	X
Users and Tasks	X	X	X	X	X

Console Actions	Default User ID				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
View Console Events	X	X	X	X	X
View Console Information	X	X	X	X	X
View Console Service History	X	X	X	X	X
View Console Tasks Performed					X
View Licenses	X	X	X	X	X
View Security Logs			X	X	X

The following table lists the tasks that can be performed on the objects and the corresponding default user IDs.

Table 2-4 – Default System Administrator User IDs and Tasks

Tasks	Default User IDs				
	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
Recovery					
Single Object Operations	X	X	X	X	X
Start All		X	X		X
Stop All		X	X		X
Reset Normal	X	X	X		X
PSW Restart		X	X		X

Tasks	Default User IDs				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Reset Clear	X	X	X		X
Load	X	X	X		X
Integrated 3270 Console	X	X	X		X
Integrated ASCII Console	X	X	X		X
Access Removable Media			X		X
Load from CD-ROM, DVD or Server			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
Restore Critical Data					X
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-RAM			X		X
Perform Transfer Rate Test					X
Change Management					
Engineering Changes (ECs)					X
Single Step Internal Code Changes		X	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

Tasks	Default User IDs				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Alternate Support Element Engineering Changes (ECs)			X		X
Concurrent Upgrade Engineering Changes (ECs)			X		X
Save Legacy Upgrade Data					X
Remote Customization					
Remote Service			X		X
Customer Information			X		X
Support Element Operations Guide	X	X	X	X	X
Operational Customization					
Customize/Delete Activation Profiles			X		
Customize Activity Profiles	X	X	X	X	X
View Activation Profiles	X	X			X
Automatic Activation			X		
Customize 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
Change LPAR Group Controls			X		X
Logical Processor Add			X		X
Object Definition					
Change Object Definition				X	X
Add Object Definition				X	X

Tasks	Default User IDs				
	OPERATOR	ADVANCED	SYSPROG	ACSADMIN	SERVICE
Remove Object Definition				X	
Reboot Support Element				X	X
Configuration					
Transmit Vital Product Data			X		X
View Frame Layout			X		
Edit Frame Layout					X
System (Sysplex) Time			X		X
Input/Outpu (I/O) Configuration Save and Restore					X
System Input/Output Configuration Analyzer			X		X
z/VM Virtual Machine Management					
Activate			X		
Choose z/VM Virtual Machines to Manage			X		
Deactivate			X		
Edit the VMRM Active Measurement Data			X		
Grouping			X		
Maintain z/VM Profiles			X		
Maintain z/VM Prototypes			X		
Maintain z/VM Virtual Machines			X		
Maintain z/VM Volume Space			X		
Monitor System Events			X		
Undefine z/VM Virtual Machines for Management			X		
View the VRM Measurement Data			X		
z/VM Virtual Network Information			X		

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

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

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

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

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

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

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

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

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

PR/SM supports and uses the "start interpretive execution" (SIE) instruction to create an interpretative execution environment in which the logical partitions execute. PR/SM begins execution in non-SIE mode. When a logical partition is to be activated PR/SM establishes the parameters for each logical processor allocated to the partition in a control block called a "state description". PR/SM executes a SIE instruction, which dispatches the logical processor in SIE mode. The PR/SM hardware executes instructions in the logical processor in SIE mode until an

exception condition occurs, which causes control to return to PR/SM in non-SIE mode. The exception conditions are events that cannot be handled in interpretative mode. PR/SM receives control in non-SIE mode. PR/SM maintains a state description for each logical processor of each logical partition so that each time a logical processor is dispatched, it is in the same context as when it last had control. Since this state description is updated by the hardware, it is impossible for one logical partition to acquire control with the wrong context (i.e. the context of another logical partition). The non-SIE/SIE distinction is a powerful privilege differentiation between PR/SM and the logical partitions.

In LPAR mode, the System z10 provides support for several features that are very helpful in many customer environments. However, these features are not recommended in a secure environment. As a result, the TOE provides security related controls to disable such features assuring separation of the logical partition(s). The security related controls are outlined below:

- **Logical Partition Isolation**

  This control reserves reconfigurable unshared channel paths for the exclusive use of a logical partition. Channel paths assigned to an isolated logical partition are not available to other logical partitions and remain reserved for that LP when they are configured offline.

- **I/O Configuration Control Authority**

  This control can limit the ability of the logical partition to read or write any IOCDS in the configuration locally or remotely. Logical partitions with control authority for the I/O configuration data can read and write any non-write protected IOCDS in the configuration, and can change the I/O configuration dynamically.

- **Global Performance Data Control Authority**

  This control limits the ability of a logical partition to view central processor activity data for other logical partitions. Logical partitions with control authority for global performance data can view CP utilization data and Input/Output (IOP) busy data for all of the logical partitions in the configuration. A logical partition without control authority for the performance data can view only the CP utilization data for itself.

- **Cross-Partition Authority**

  This control can limit the capability of the logical partition to issue certain control program instructions that affect other logical partitions. Logical partitions with cross-partition authority can issue instructions to perform a system reset of another logical partition, deactivate any other logical partition, and provide support for the automatic reconfiguration facility.

In addition to the security controls mentioned above, the TOE also insures that central and expanded storage for each logical partition is isolated and cannot be shared with other logical partitions. The TOE rigidly enforces this “no sharing” rule during logical partition definition, logical partition activation, logical partition reconfiguration and during logical partition execution.

The TOE also “removes” central processors (CPs) from logical partitions by virtualizing physical CPs. Virtualized physical CPs are referred to as logical processors. Within the TOE, each logical CP is represented as a data structure that is associated with its specific logical partitions preventing the transfer of data between partitions.

Thus, when PR/SM is initialized for secure operation, one partition cannot gain access to the data within another partition nor modify any aspect of another partition.

With z/Architecture® or S/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 S/390 architecture.

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 low-level 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;

- 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.

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

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

  f) 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.

- 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 (Service calls are passed on to the SE by LPAR). 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 (e.g. serialization of access to IOCDS).

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 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. 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, 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 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

The environment of the hardware is physically secured against unauthorized access. Access to I/O devices is restricted to authorized personnel. In particular the hardware management console and the Local Area Network (LAN) connecting it to the SEs must be physically protected from access other than by authorized system administrators.

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.Sep_Strength - Separation Strength

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. The simultaneous existence of any non-isolated, co-operating partitions and the configuration of those partitions will have no effect on the isolation of partitions as defined herein. To be used as a strict separation virtual machine monitor, PR/SM must be configured in the following manner:

1. Devices must be configured so that no device is accessible by any partition other than the partition to be isolated (although they may be accessible by more than one channel path).
2. Each I/O (physical) control unit must be allocated only to an isolated partition in the current configuration.
3. The Security Administrator must not reconfigure a channel path owned by an isolated partition unless all attached devices and control units are attached to that path only.
4. The Security Administrator must ensure that all devices and control units on a reconfigurable path owned by an isolated partition are reset before the path is allocated to another partition.
5. No channel paths may be shared between an isolated partition and any other partition(s).
6. The System Administrator must ensure that the number of processors dedicated to activated partitions is less than the total number available.
7. Dynamic I/O configuration changes must be disabled.
8. If I/O Priority Queuing is enabled for the system an isolated partition's minimum and maximum I/O Priority values must be equal.
9. For isolated partitions, Workload Manager must be disabled so that CPU and I/O resources are not managed across partitions.
10. An isolated partition must not be configured to enable hipersockets (Internal Queued Direct I/O).
11. Partitions must be prevented from receiving performance data from resources that are not allocated to them (global performance data control authority must be disabled).
12. At most one partition can have I/O configuration control authority (i.e. no more than one partition must be able to update any IOCDS) and this partition must be administered by a trustworthy administrator (i.e. the administrator of this partition is considered a System Administrator of the TOE).
13. The Security Administrator must ensure that write access is disabled for each IOCDS, unless that IOCDS is to be updated (the current IOCDS must not be updated).
14. The Security Administrator must verify any changed IOCDS after a power-on reset with that IOCDS, before any partitions have been activated (the Security Administrator may determine whether the IOCDS has been changed by inspecting the date of the IOCDS).
15. No partition may have cross-partition control authority (i.e. no partition should be able to reset or deactivate another partition).
16. No isolated partition may have coupling facility channels that would allow communication to a Coupling Facility partition.[1]

[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.

17. The 'Use dynamically changed address' and 'Use dynamically changed parameter' checkboxes must not be selected in the Image or Load profile.

18. No Isolated partition should have the following Counter Facility Security Options enabled:

- Crypto activity counter set authorization control
- Coprocessor group counter sets authorization control

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

A.Admin_Secure – Administrative Personnel Security

Logical partitions within the System z10 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.

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, or logical processors 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 PR/SM Planning Guide Appendix: Developing, building and delivering a certified system (which will be referred in the remainder of this document as the Trusted Facility Manual (TFM)). Anyone attempting to modify the log would need intimate designer level knowledge of the system, and have access to development tools.

3.4 Organizational Security Policies

The TOE complies with the following organizational security policies:

P.SEP – Separation of hardware into partitions

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

4 Security Objectives

4.1 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.

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.

4.2 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 must 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 must 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, and verification of the profiles.

OE.Phys_Prot – Restricted physical and remote access

Physical access and remote access to the HMC and System z10 must be restricted only to authorized and approved users.

The HMC and System z10 must be installed in restricted areas for the purposes of limiting accessibility by company personnel and avoiding physical destruction or alteration of the hardware. In particular the hardware management console and the Local Area Network (LAN) connecting it to the SEs must be physically protected from access other than by authorized system administrators.
Additionally, this restricted access applies to the remote support facility as this is outside the scope of the evaluations.

OE.SIE – Memory access control

The underlying hardware must provide separation mechanism that can be used by the TOE to protect the TSF and TSF data from unauthorized access and modification.

The underlying processors must support the enforcement of memory access control defined by a caller of a specific processor instruction.

OE.CHANNEL – Channel access control

The underlying physical I/O LIC must provide separation mechanism that can be used by the TOE to restrict access of one partition to authorized logical I/O resources.

The physical I/O resources LIC must support the enforcement to restrict access requests from one partition to the partition's associated logical I/O resources.

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 System z10.

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, and refinements (if any) indicated in **bold** type, and selections indicated in *italic* font.

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, **…**). Access to objects by subjects will be mediated by this policy to insure that subjects are only able to gain access to authorized objects.

Information Flow Control 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, **…**) and the logical processors instantiated on a physical processor on behalf of a logical partition. Flow of information between objects and subjects, and between objects and objects will be mediated by this policy to insure that information flow is only possible when subjects and objects are associated with the same logical partition.

Memory Access Control Policy (SFP for the TOE environment)

The TOE underlying processor implements a memory access control policy enforced for instructions provided by the processor (subjects), limiting access to memory locations of the hardware (objects). Using a particular processor instruction, i.e. the SIE instruction, the processor can be loaded with memory ranges applicable for subsequent instructions. In case privileged (supervisor mode) instructions are invoked, the processor remains bound by the storage limitations imposed by the SIE instruction. The processor implements a second SIE instruction that can be stacked on the first SIE, but this has no effect on the TOE, because the second SIE can only be set within the scope of memory restrictions defined by the first SIE instruction, managed by the TOE.

Channel Access Control Policy (SFP for the TOE environment)

The TOE underlying hardware implements a channel access control policy enforced on channel subsystem instructions (subjects), limiting access to I/O resources (objects).

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
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_SMF.1	Specification of Management Functions
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

Component	Component Name
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;
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**

Application note: The audit subsystem is always active and can be neither shut down nor be activated. Therefore, FAU_GEN.1.1 a) does not apply.

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.

Application Note: Apart from any user impersonating the generic role Security Administrator as defined in section 2.2 also users assigned the role Access Administrator (ACSADMIN) are granted explicit read-access to the audit records.

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* unauthorized 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 record* and **take no other actions** 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: **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: **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 an 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: **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. **resources**
   b. **storage**
   c. **processors**
   d. **CHPIDs**
   e. **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**

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**

Application Note: This SFR was editorially refined without changing the requirement.

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 an isolated partition, other partitions should perceive no effects at all. Neither shall an isolated partition perceive effects from an operation executed on behalf of non-isolated, co-operating partitions.**
3. ***I/O isolation:*** **I/O devices associated with an isolated partition affect the state perceived by only that partition. I/O devices associated with non-isolated, co-operating partitions will not affect the state perceived by any isolated 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 an isolated partition must depend only on the state of that partition and is independent of the state of any non-isolated, co-operating partitions.**

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 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 partition has cross-partition 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**

Application Note: Within the scope of the TOE, an individual user is a logical partition unless explicitly stated otherwise.

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.

Application Note: This identification requirement applies to logical partitions as well as administrative users working on the HMC/SE.

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.**

Application Note: According to A.Sep_Strength.11, 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_SMF.1 Specification of Management Functions
FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **object security attributes management**.

FMT_SMR.1 Security roles
FMT_SMR.1.1 The TSF shall maintain the roles:

- **Operator**
- **Advanced Operator**
- **System Programmer**
- **Service Representative**
- **Access Administrator.**

and also allow customized user roles to be defined.

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

Application Note: Any of the above roles are associated with the generic role System Administrator. The tasks specific to the generic role of Security Administrator are listed in Section 2.2.

FPR_UNO.1 Unobservability
FPR_UNO.1.1 For isolated partitions, the TSF shall ensure that **any users/subjects** are unable to observe **any operation** on **any object/resource** by **any other user/subject**.

Application Note: Users/subjects are defined as the logical partitions and the software running in these partitions which is a consistent view with FIA_ATD.1.

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.

Application Note: The possible value for selection “other conditions” has been refined to reflect the functionality of the TOE.

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**.**

Application Note: 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 and/or information flow control SFPs 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.

Application Note: The TOE uses a hardware timer to maintain its own time stamp. This hardware timer is protected from tampering by untrusted subjects. The start value for this timer may be set by the system administrator, but the system administrator may also start a program that uses an external trusted time source to set this initial value.

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*: **performing a reset or 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 *subjects* can use *over a specified period of time***.**

Application Note: The term “subject” is equivalent to “logical processors” in this context, since no other subjects may use processor time slices.

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

The assumptions stated for the environment 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.

The only IT environment where requirements are stated is the underlying processor that has to provide the mechanism to protect the TSF and TSF data from unauthorized access and tampering. This is expressed with the following security functional requirement for the processor used to execute TOE software:

FDP_ACC.1 Subset access control (1)
FDP_ACC.1.1 The IT Environment shall enforce the **memory access control policy** on **instructions as subjects and memory locations as objects.**

FDP_ACF.1 Security attribute based access control (1)
FDP_ACF.1.1 The IT Environment shall enforce the **memory access control policy** to objects based on **the memory configuration defined.**

FDP_ACF.1.2 The IT Environment shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **access to memory locations is based on the memory configuration defined by the invocation of the SIE instruction. When in SIE mode access to memory is restricted by the environment defined when the SIE instruction was invoked.**

Application Note: The SIE instruction causes the processor to adhere to memory definitions supplied with the invocation of SIE. The processor only allows access to the defined memory. The “SIE mode” sets special purpose registers in the processor, which are not visible to any application running on the processor.

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

FDP_ACF.1.4 The IT Environment shall explicitly deny access of subjects to objects based on the **following rule: [none]**.

FMT_MSA.3 Static attribute initialization (1)
FMT_MSA.3.1 The IT Environment shall enforce the **memory access control policy** to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The IT Environment shall allow the **no role** to specify alternative initial values to override the default values when an object or information is created.

Application Note: The „default” values in this case are seen as the values the processor has after start-up. They have to be „permissive”, since the initialization routine needs to set up the memory and must have the ability to perform privileged instructions.

FDP_ACC.1 Subset access control (2)
FDP_ACC.1.1 The IT Environment shall enforce the **channel access control policy** on **I/O resource instructions as subjects and logical I/O resources as objects.**

FDP_ACF.1 Security attribute based access control (2)
FDP_ACF.1.1 The IT Environment shall enforce the **channel access control policy** to objects based on **the logical I/O resoure association with a partition ID.**

FDP_ACF.1.2 The IT Environment shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **access to logical I/O devices is based on the partition ID of the requesting logical partition.**

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

FDP_ACF.1.4 The IT Environment shall explicitly deny access of subjects to objects based on the **following rule: [none]**.

FMT_MSA.3 Static attribute initialization (2)
FMT_MSA.3.1 The IT Environment shall enforce the **channel access control policy** to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The IT Environment shall allow the **no role** to specify alternative initial values to override the default values when an object or information is created.

Application Note: The „default" values in this case are seen as the values the channel processor has after start-up. They have to be „permissive", since the initialization routine needs to set up the memory and must have the ability to perform privileged instructions.

6 TOE Summary Specification

As defined in chapter 2 the TOE consist of the PR/SM LIC kernel running on the System z10 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 the 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 4 MB is reserved for LPAR's core image. LPAR will allocate the rest of its storage from the range of 4 MB to 1.5 GB. All storage used by LPAR must fit below 1.5 GB in HSA. Since 0 to 1.5 GB is reserved exclusively for LPAR use, "real" HSA is allocated starting at 1.5 GB in 256 MB increments.

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 thru 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 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.

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 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 to 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_SMF.1, FMT_SMR.1]

b) The TOE will help to 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_SMF.1, 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 to 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 to 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: FPR_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 always be 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]. Note: When archiving audit logs to CD, the audit log will be pruned to 20% of its capacity if the audit log exceeds 20% of the audit storage capacity.

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 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

Component	Security Functions
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)
FMT_MSA.3	Reliability of Service
FMT_MTD.1	Authorized Administration (a)
FMT_SMF.1	Authorized Administration(a),(b)
FMT_SMR.1	Authorized Administration(a),(b);

Component	Security Functions
	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_SMF.1, FMT_SMR.1
Authorized Administration (b)	FDP_ACC.2, FDP_ACF.1 (Activation, Allocation), FMT_SMF.1, 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_ATD.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)	FPR_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 System z10 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. PR/SM development is 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. The HMC/SE tests are described in the HMC Testplans – Standard Regression**.**

ACM_SCP.3 – Development tools CM coverage

An internal document discusses the processes by which design documentation, test documentation and development tools are tracked. Change control as well as authorization control is also discussed.

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 – Semiformal 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 TFM 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 insure continued operation in conjunction with the security polity.

ADV_HLD.3 – Semiformal high-level design

The high-level design for PR/SM on the System z10 is documented in proprietary internal documents. These documents also contain a description of the major structural elements of LPAR 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 is discussed in the document Philosophy of Protection for PR/SM on System z. PR/SM's modular design and component interactions are discussed in proprietary internal documents. An architectural description of each component is also provided.

ADV_LLD.1 – Descriptive 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.
Modules noted in the section "LLD" are either in **bold** text or plain text. **Bold** text modules enforce the security aspects of the component. Plain text modules are required to support, but not enforce the component.

ADV_SPM.3 - Formal TOE Security Policy Model

A formal mathematical model for the security policy has been created which shows the required correspondence. A companion document has been provided to show the correspondence between the model and the functional

implementation of the TOE.

AGD_ADM.1 – Administrator guidance
The TFM provides guidance required helping to insure 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 TFM 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 insure 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 the Site Security Manual.

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 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.

ATE_IND.2 – Independent Testing Sample
By independent testing and repeating a subset of developer tests, the evaluator will gain confidence in the developer's testing effort and in the test results.

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.

The results of this work are documented in a document entitled: EAL5 Covert Channel Analysis Report, Version 8.0.

AVA_MSU.2 – Validation of Analysis

The required guidance documentation is provided in the TFM 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 insure 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. BSI has agreed with this interpretation.

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

The functional components were selected from CC components defined in part 2 of the Common Criteria. Functional component FMT_SMF.1 (Specification of Management Functions) has been added in accordance with AIS 32, Final Interpretation 065. The use of component refinement was accomplished in accordance with CC guidelines.

8.1 TOE Description Rationale

The target of evaluation, PR/SM on z10 Servers 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

Table 8-1 – Threats Related to Objectives

POLICIES	OBJECTIVES
P.SEP	OE.SIE OE.CHANNEL

Table 8-2 – Organizational Security Policies mapped to Environment 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. A Security Policy has 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 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.
O.Resource**.** provides functions that enable control of the physical processor running time and cross partition functions.

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.

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.

Environment Objectives mapped to Assumptions	OE.Data Store	OE.Perss	OE.Sec_Setup	OE.Phys_Prot	OE.SIE	OE. CHANNEL
A.Phys_Secure				*		
A.No_Remote				*		
A.Sep_Strength			*			
A.Admin_Secure		*				
A.Data_Secure	*					

Table 8-3 – 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 insure that only trusted personnel have access to the processor hardware, IO and consoles, these assets are to be protected in restricted access areas. In particular

the hardware management console and the Local Area Network (LAN) connecting it to the SEs must be physically protected from access other than by authorized system administrators.

As specified in OE.Phys_Prot, the method for providing physical security of the hardware is assumed to be restricted access. Restricted access will insure 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.Sep_Strength – Separation Strength

For conformance with the scope of the evaluation for isolated partitions, the z10 must be setup and initialized in Strict Separation Mode as defined in the TFM, 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 z10 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.

P.SEP – Separation of hardware into partitions

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

The policy requires the hardware to provide independent partitions, which are separated from each other by the environment with the objective OE.SIE that provides a special execution environment for a software component enforcing that objective. In addition, OE.CHANNEL provides the capability of associating I/O resources to logical partitions to restrict access to arbitrary I/O resources.

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, FMT_SMF.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 8-4 – 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 and FMT_SMF.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 help insure 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 insure 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 insure 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 help insure 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.

8.3.3 Security Requirements Coverage (IT environment)

OE.SIE - Memory access control

The security functional requirements FDP_ACC.1 (1), FDP_ACF.1 (1) and FMT_MSA.3 (1) for the IT environment define an access control policy on memory regions such that memory regions can be defined limiting subsequent instructions performed by the processor to this memory. The models of the z10 processor used in the hardware underlying the TOE provide this support as documented in the processor manuals using the SIE instruction. This all contributes to satisfy the objective OE.SIE for the IT environment.

OE.CHANNEL - Channel access control

The security functional requirements FDP_ACC.1 (2), FDP_ACF.1 (2) and FMT_MSA.3 (2) for the IT environment define an access control policy on channel instructions to access logical I/O resources to limit requesting partitions to the logical I/O resources they are allowed to access. The mapping between partition IDs and logical I/O resources devices is set up by the TOE. This all contributes to satisfy the objective OE.CHANNEL for the IT environment.

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.

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

FDP_IFC.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 to ensure that the information in a physical processor 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 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)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 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_SMF.1
The IT security function Authorized Administration (a,b) fulfills the requirement because:
a) The TOE allows the management of security attributes of objects for the access control SFP.

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. The authority level can be one or more of the default roles provided: Operator, Advanced Operator, System Programmer, Service Representative, Access Administrator or the authority level can be one that is based on a customized user role(s).

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 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 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 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	Yes
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_SMF.1, FMT_SMR.1, FDP_IFC.1	Yes
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Yes
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	Yes

Component	Dependencies	Resolved
FMT_SMF.1	None	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 8-5 – Summary of Security Functional Requirements Dependencies

* Dependency of FMT_MSA.1 to FDP_ACC.1 is resolved by the use of the hierarchical SFR FDP_ACC.2.

Component	Dependencies	Resolved
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Yes
FMT_MSA.3*	FMT_MSA.1, FMT_SMR.1	No

Table 8-6 – Summary of environmental Security Functional Requirements Dependencies

* The security functional requirements FMT_MSA.3 (1) and FMT_MSA.3 (2) for the IT environment do not satisfy the dependency to FMT_MSA.1 and FMT_SMR.1. The following rationale applies: Both dependencies are not resolved, because the access control policy of the underlying processor and the access control policy of the channel instructions are static and can not be managed by any role. Therefore, neither a management of the access control policies is required (which FMT_MSA.1 would define) nor a role model for management is required (which FMT_SMR.1 would define). The dependencies defined in part 2 of the CC for this security functional requirement therefore do not apply here.

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 z10 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

© Copyright IBM Corporation 1994, 2008. All rights reserved.

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Produced in the United States of America,
All Rights Reserved
Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.
More details on IBM UNIX hardware, software and solutions may be found at ibm.com/servers/unix/.

ESCON®
FICON®
HiperSockets
IBM®
OS/390®
Processor Resource/Systems Manager
PR/SM
RETAIN®
S/360
S/370
S/390®
System z10
System z
VM/ESA®
VSE/ESA
Z10
z10 EC
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.

InfiniBand is a registered trademark of the InfiniBand Trade Association.

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 applications 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	Communicating data between separated parts of the TOE.
Object	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 to be 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 30 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.

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.

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.

The reconfigurable part of a configuration identifies the number of logical 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.

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.

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 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.

Processor Unit (PU) – is the generic term for the z/Architecture processor on the Multichip Module (MCM) that can be characterized as a:

- Central Processor (CP) to be used by an operating system
- Internal Coupling Facility (ICF) to be used by the Coupling Facility Control Code (CFCC)
- Integrated Facility for Linux (IFL)
- Additional System Assist Processors (SAPs) to be used by the Channel Subsystem (CSS)
- IBM z10 Integrated Information Processor (zIIP)
- IBM z10 Application Assist Processor (zAAP)

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.

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

END OF THE DOCUMENT