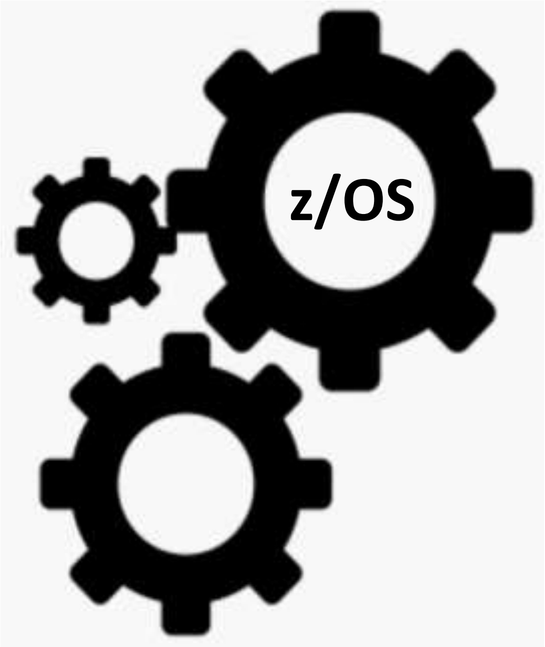


z/OS Is the Rock, but Why? Let Us Count the Ways

Session 26689
Thursday, February 27 at 1:45PM
Room 204A

Presented by Paul R. Robichaux
NewEra Software, Inc.
prr@newera.com

Abstract – z/OS Is the Rock, but Why? Let Us Count the Ways!

Let's face up to it, we're in a war. A war by design that is intended to undermine confidence in our network based information systems and their ability to assure the integrity of revenue generating processes and/or the security they provide over proprietary data and applications. This war is waged against us by hackers on the outside (sometimes nation states) and spies on the inside (our fellow employees or consultants). Each computing platform has its own unique set of hardware and software counter measures that prevent, detect and eradicate such nefarious system intrusions. And, it's here where the z Environment stands alone with the potential of being the most securable general purpose business computing platform available. But, this potential begs for a deeper understanding of this term "securable" and the needs of the individuals changed with maintaining z/OS System Integrity, the undisputed Rock of computing.

This presentation will widen your understanding of why z/OS is the Rock. In it, we will "Count", among others, such topics as – A desired Management Structure, z/OS Initialization, Authorized Program Facility (APF), System Access Facility (SAF), Accessor Environment Element (ACEE), External Security Manager (ESM), Communication Server (CS), Policy Management Agent (PAGENT), zEncryption Ready Technology (zERT) and the Network Management Interface (NMI).

These legacy controls, often disbursed throughout the z/OS organization in order to meet compliance standards that mandate "Separation of Duties", result in "Silos of control and interest" built by trusted professionals, who often lack a needed global perspective. Shedding new light on these Silos will help to eliminate confusion between these complementary, sometimes competing groups, and those who stand to benefit most: Management.

Paul R. Robichaux is CEO and co-founder of NewEra Software, Inc. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his co-founding of NewEra in 1990. He holds a BS in Accounting and a Masters in Business Administration from a Louisiana State University, is a Certified Public Accountant and a frequent speaker at industry events.

The corporate mission of NewEra Software is to provide software solutions that help users avoid z/OS non-compliance, make corrections when needed and in doing so, continuously improve z/OS integrity and Security. https://www.newera.com

z/OS Is the Rock, but Why? Let Us Count the Ways!

A. Requirements
- Discipline
- Commitment
- Mutual Trust

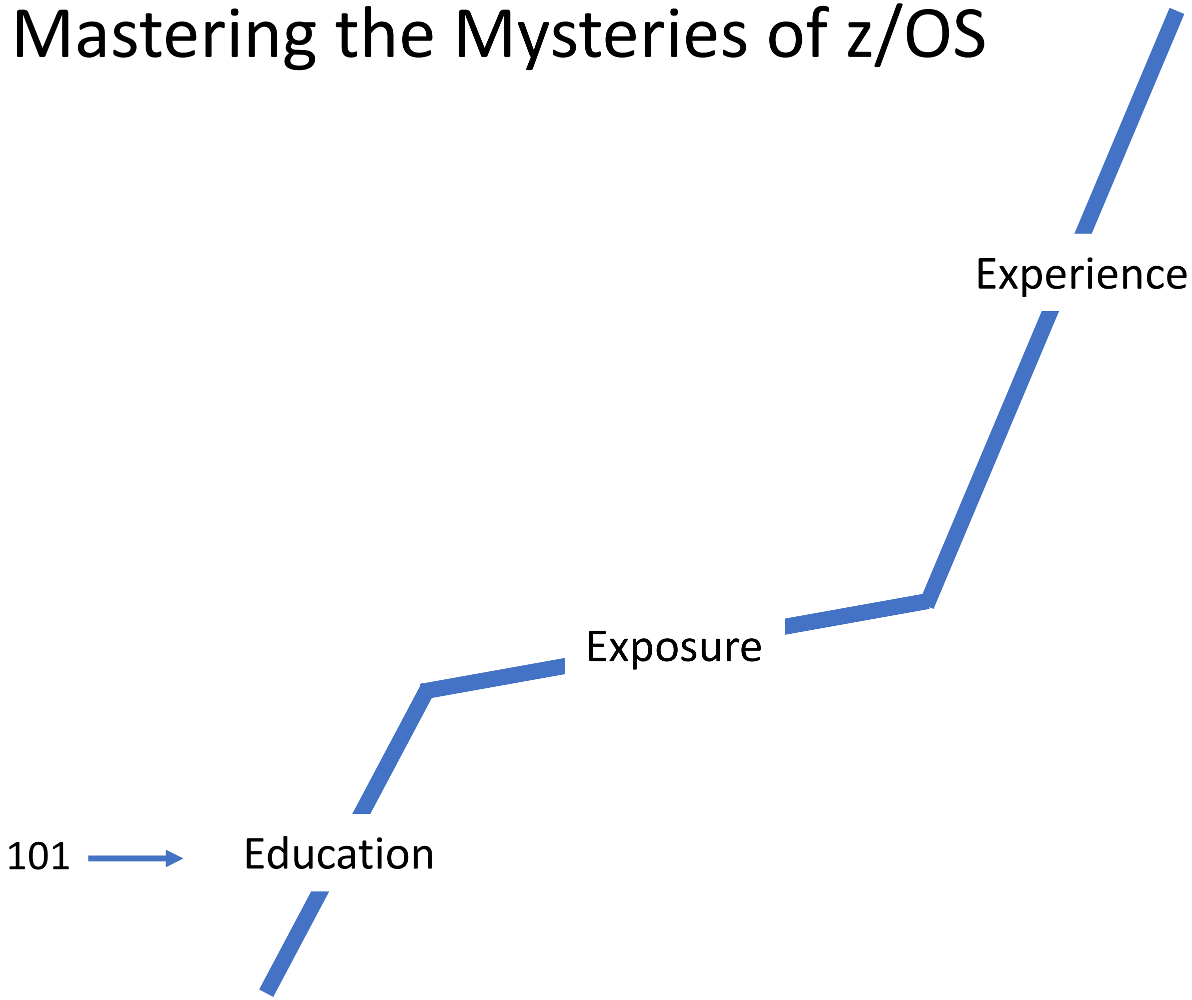
B. Management
- Process
- Service Level Agreements
- Policy Decision Points(PDP/PFP)
- Separation of Duties

C. Assignments - Silos
- Hardware
- A z/OS IPL
- TCP/IP
- IPSec
- ESM

D. All the Detail
- IODF, SAF, APF, DUCT, PAGENT
- zERT, AT-TLS, LCSS, zCX, ACEE

E. What we Fear

Mastering the Mysteries of z/OS



101 → Education

Exposure

Experience

z/OS Is the Rock, but Why? Let Us Count the Ways!

z/OS Is the Rock, but Why? Let Us Count the Ways!

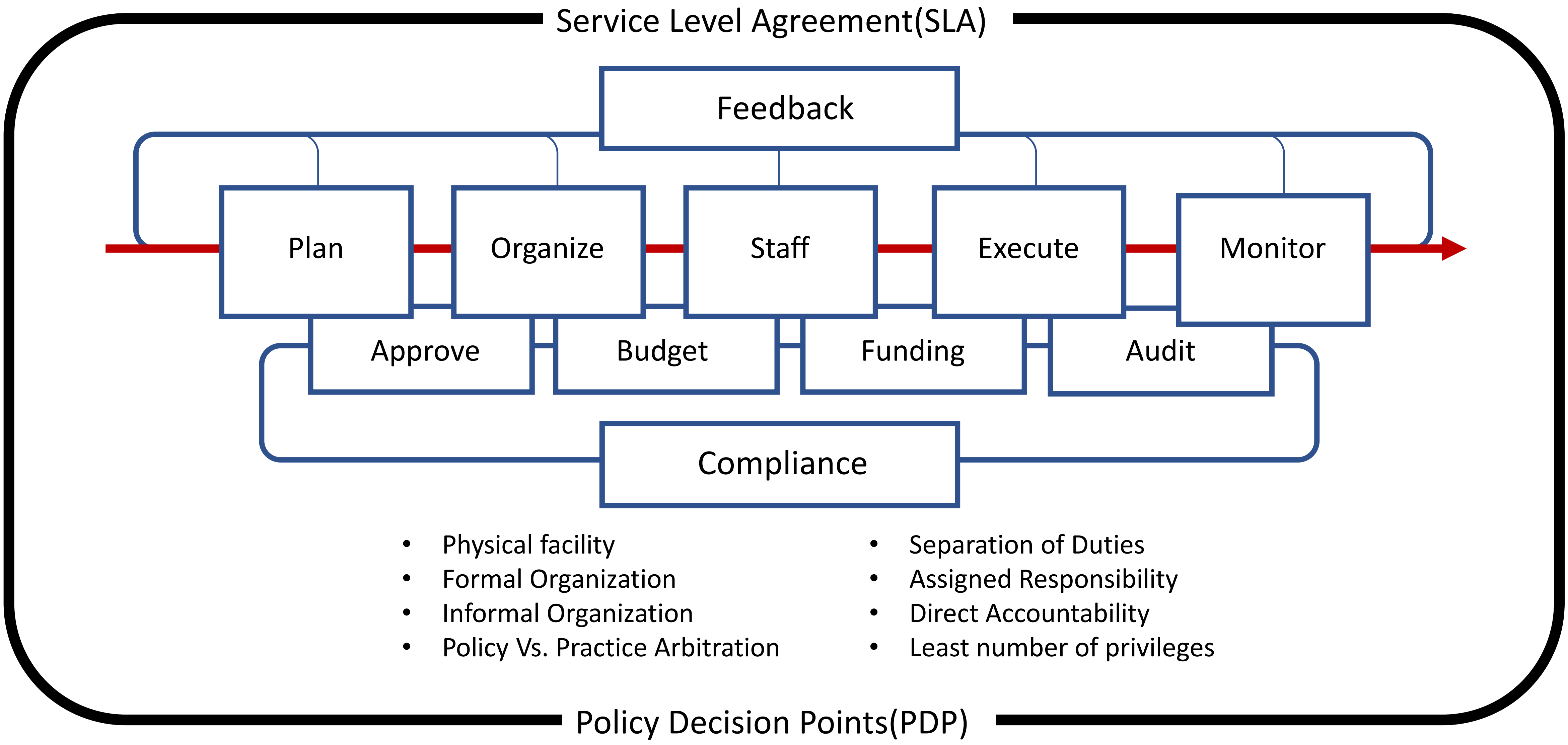
SLA*

Service Level Agreement

* A statement of shared IS objectives:
Reliability, Availability, Serviceability (RAS)
including Integrity and Security(ISEC).

IBM z/OS® System Integrity Statement

z/OS Is the Rock, but Why? Let Us Count the Ways!



- Physical facility
- Formal Organization
- Informal Organization
- Policy Vs. Practice Arbitration

- Separation of Duties
- Assigned Responsibility
- Direct Accountability
- Least number of privileges

z/OS Is the Rock, but Why? Let Us Count the Ways!

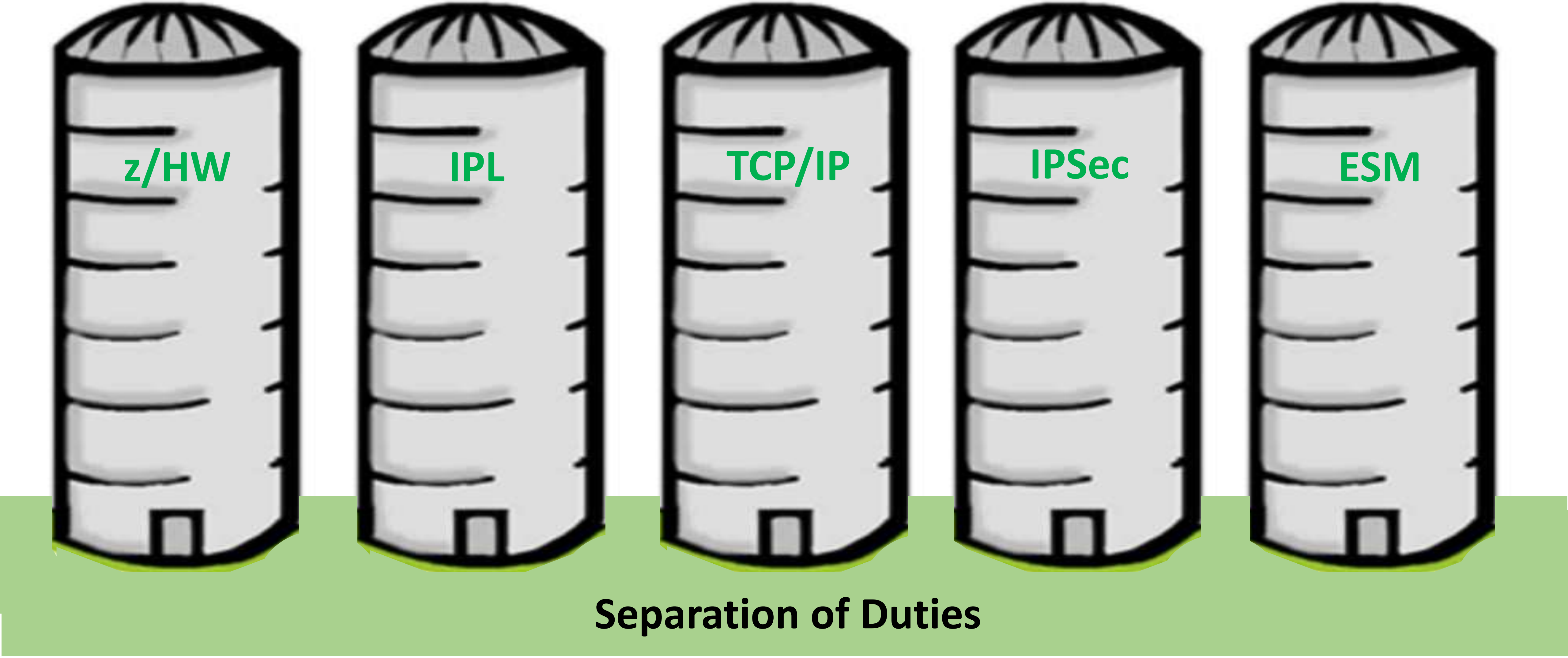
PEP

Policy Enforcement Point

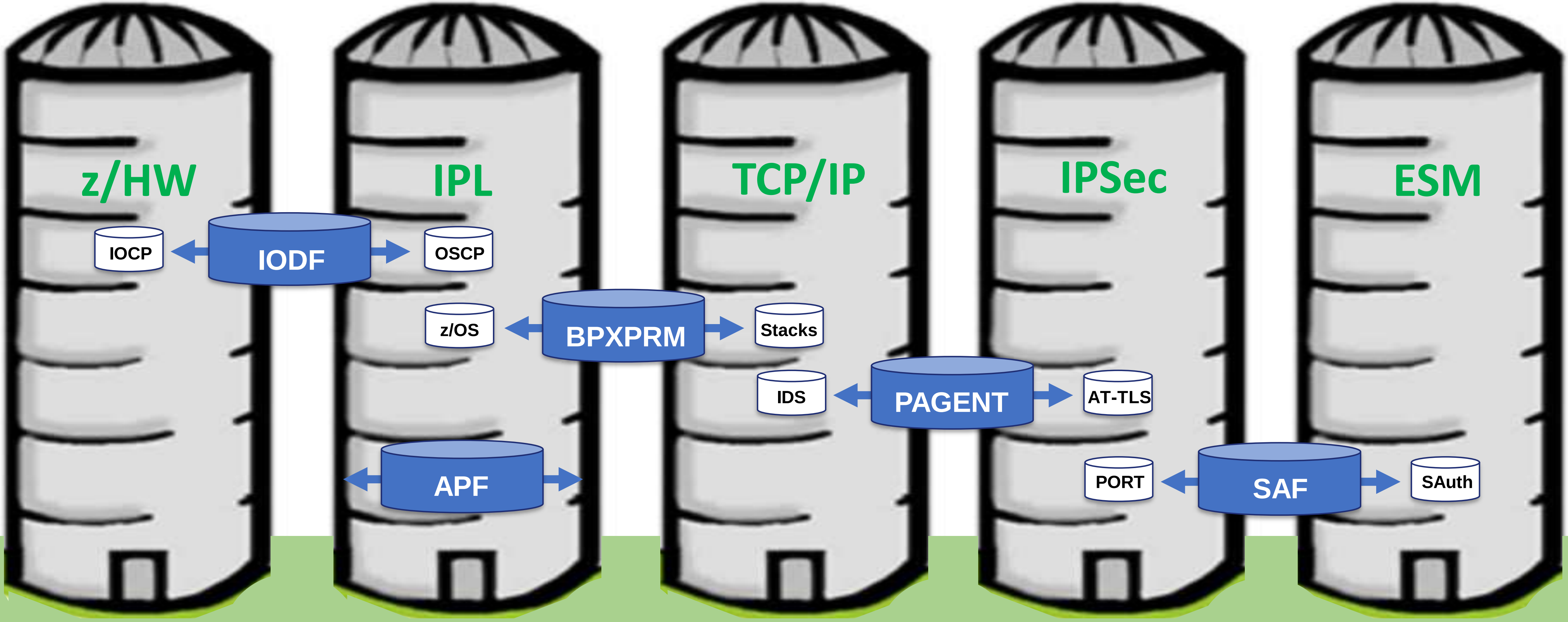
*A system entity that makes authorization decisions for itself or other system entities that request its services.

Best known PDPs – RACF, ACF2, Top Secret

z/OS Is the Rock, but Why? Let Us Count the Ways!



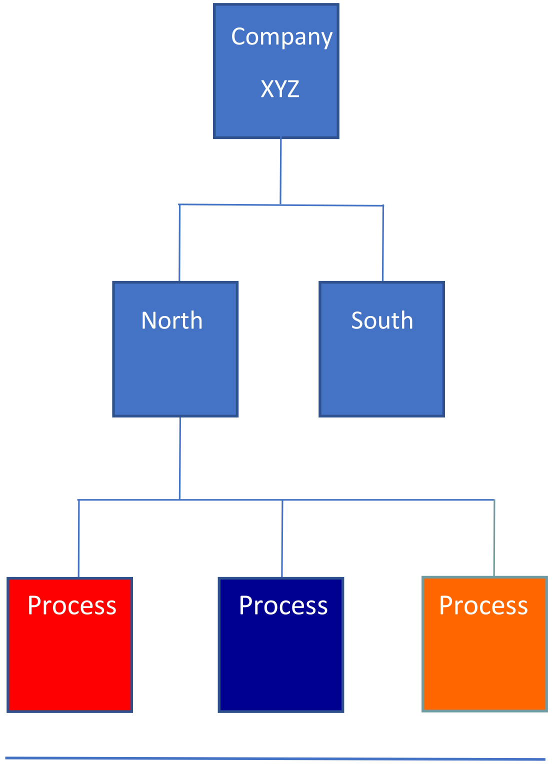
z/OS Is the Rock, but Why? Let Us Count the Ways!



Separation of Duties

z/OS Is the Rock, but Why? Let Us Count the Ways!

z Systems - A General Purpose Business Computer Paradigm



Company XYZ

North

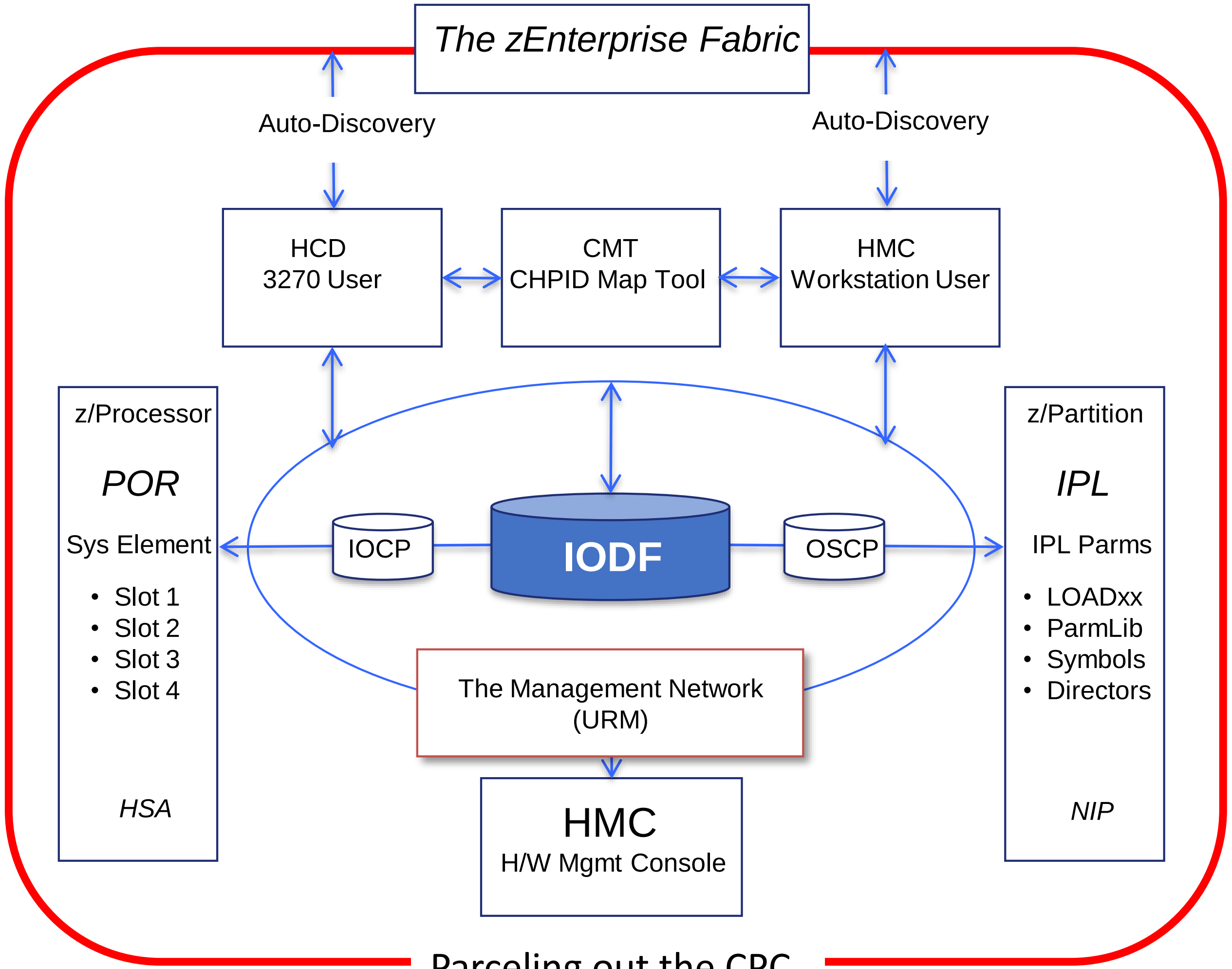
South

Process

Process

Process

Process and Policy Objects



The zEnterprise Fabric

Auto-Discovery

Auto-Discovery

HCD
3270 User

CMT
CHPID Map Tool

HMC
Workstation User

z/Processor

POR

Sys Element

- Slot 1
- Slot 2
- Slot 3
- Slot 4

HSA

IOCP

IODF

OSCP

z/Partition

IPL

IPL Parms

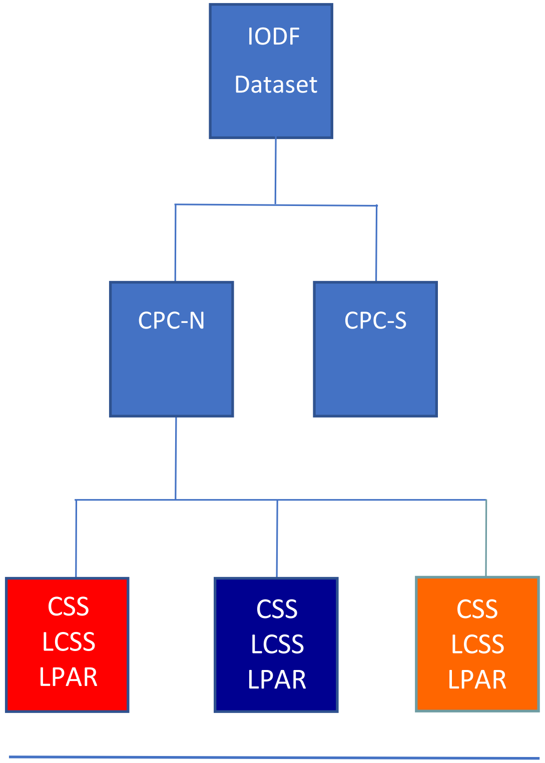
- LOADxx
- ParmLib
- Symbols
- Directors

NIP

The Management Network
(URM)

HMC
H/W Mgmt Console

Parceling out the CPC



IODF

Dataset

CPC-N

CPC-S

CSS
LCSS
LPAR

CSS
LCSS
LPAR

CSS
LCSS
LPAR

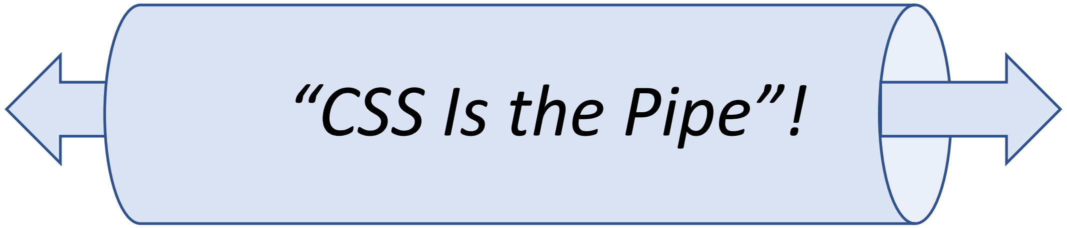
z/Platform, zPDP Objects

z/OS Is the Rock, but Why? Let Us Count the Ways!

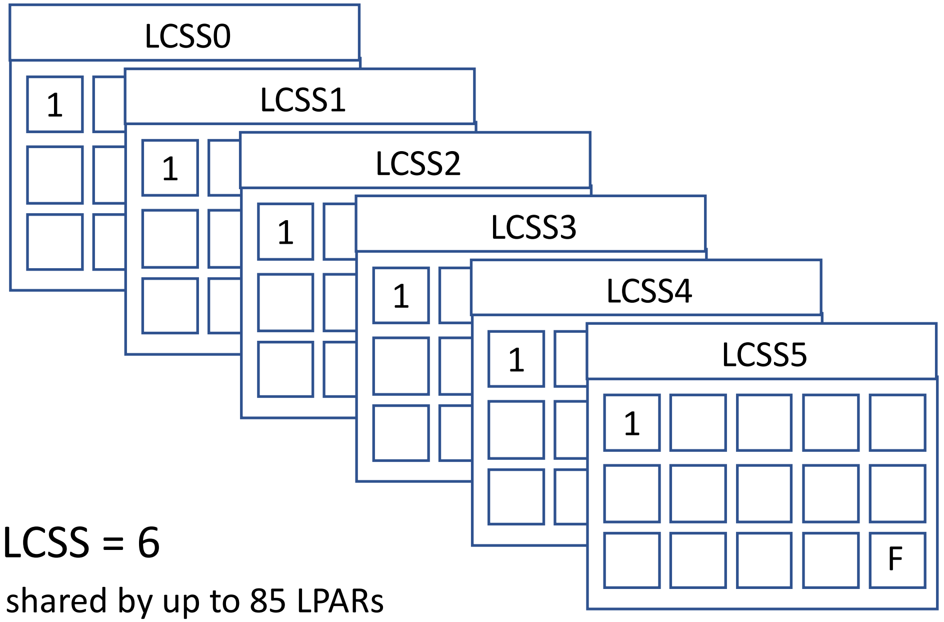
The "Device-Chain" links physical resources to logical z/OS partitions

IOCP **OSCP**

256 Channel Subsystem (CSS)



85 Logical Partitions(LPARS)*



CHPID = 256 x LCSS = 6

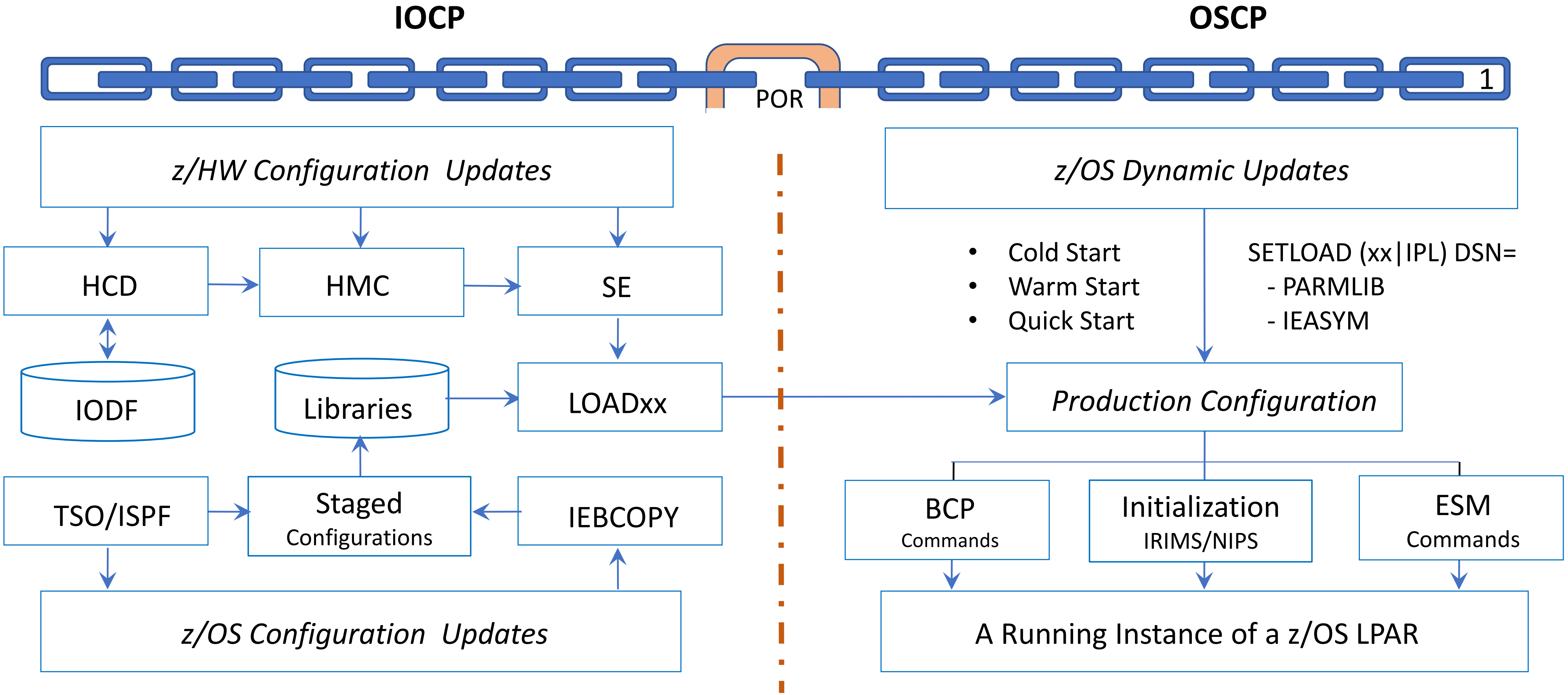
1536 Virtual Interface Paths/zPDP shared by up to 85 LPARs

*An LPAR is considered a Secure Service Container(SSC)

[What is Evaluation Assurance Level (EAL)?]

z/OS Is the Rock, but Why? Let Us Count the Ways!

The "Device-Chain" links physical resources to logical z/OS partitions



IOCP

OSCP

POR

1

z/HW Configuration Updates

HCD

HMC

SE

IODF

Libraries

LOADxx

TSO/ISPF

Staged Configurations

IEBCOPY

z/OS Configuration Updates

z/OS Dynamic Updates

- Cold Start
- Warm Start
- Quick Start

SETLOAD (xx|IPL) DSN=
- PARMLIB
- IEASYM

Production Configuration

BCP Commands

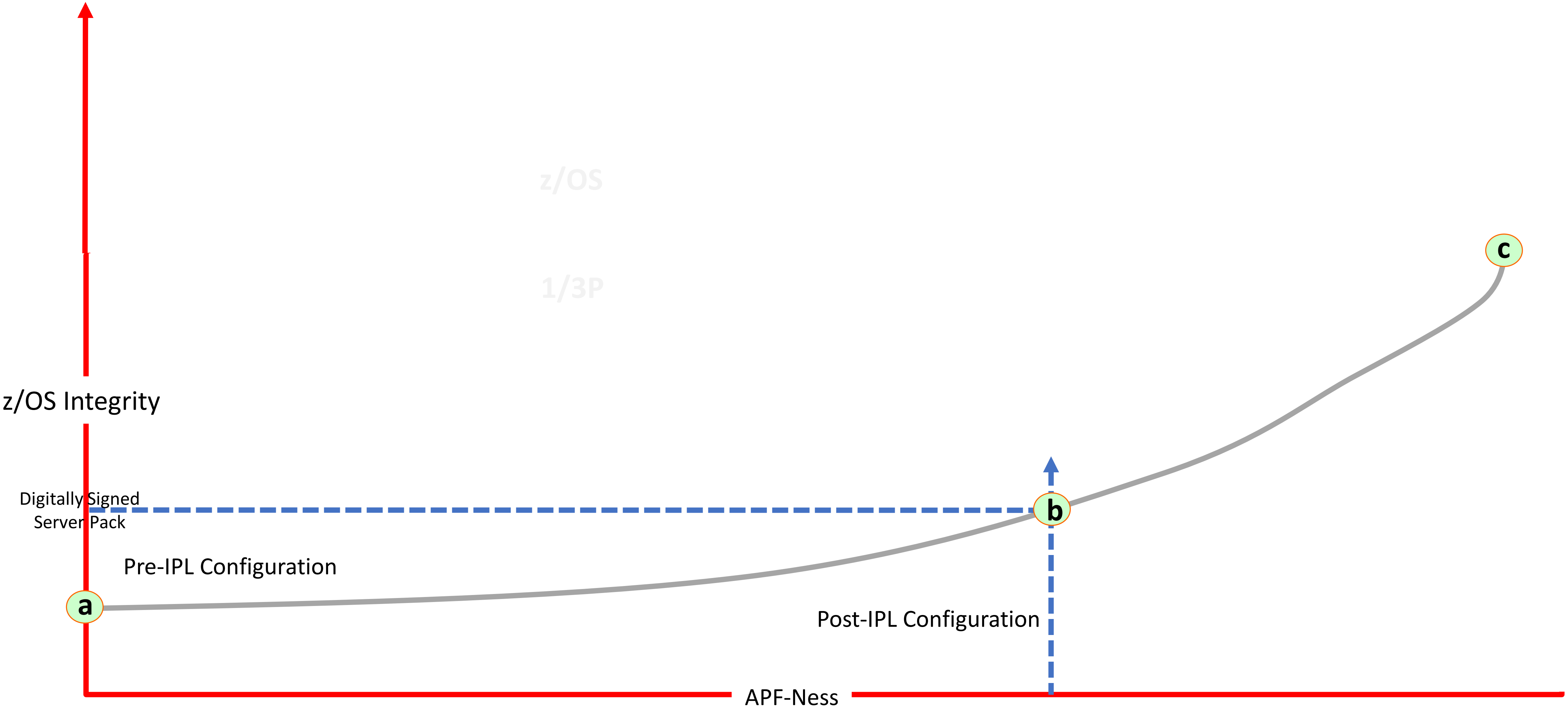
Initialization IRIMS/NIPS

ESM Commands

A Running Instance of a z/OS LPAR

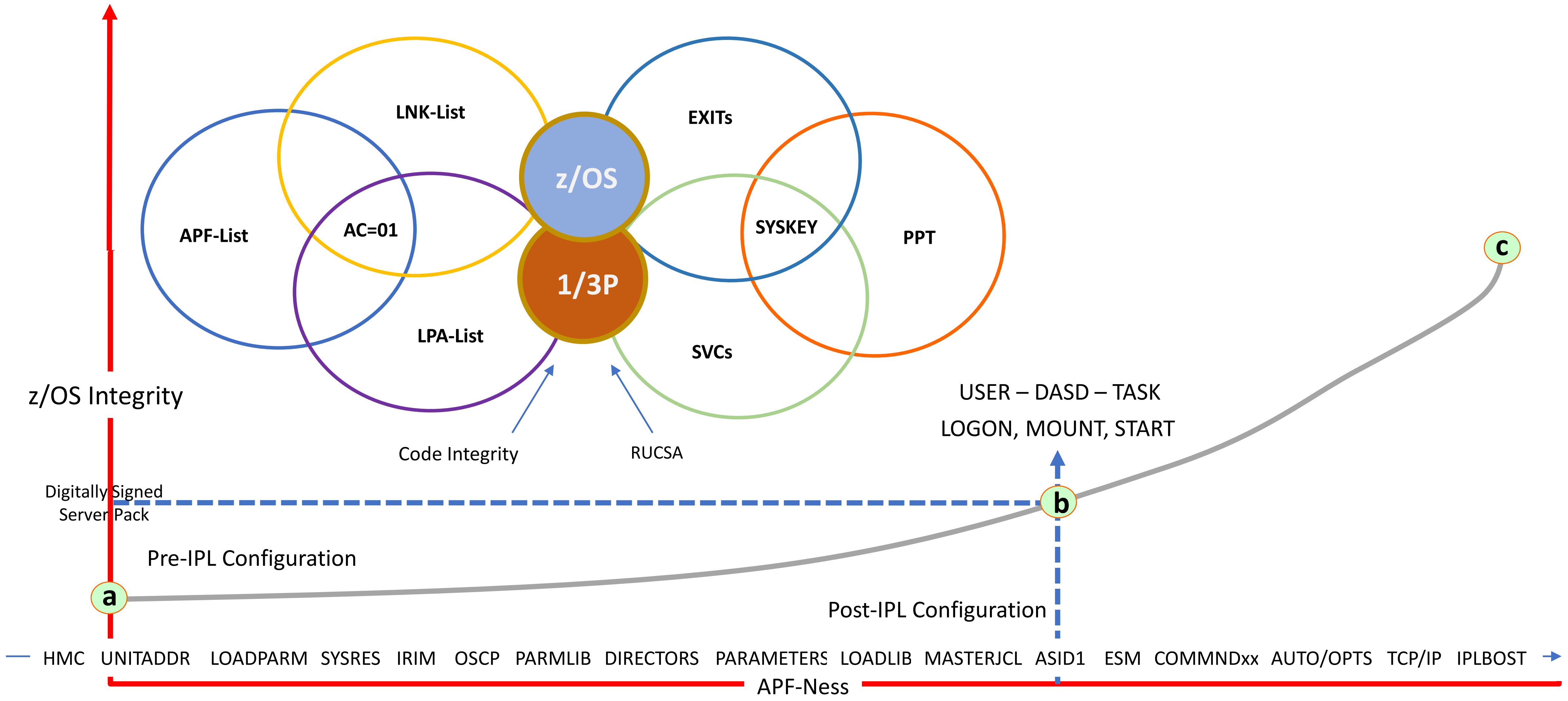
z/OS Is the Rock, but Why? Let Us Count the Ways!

The Initial Program Load(IPL) is the Process that reveals z/OS Integrity



z/OS Is the Rock, but Why? Let Us Count the Ways!

The Initial Program Load(IPL) is the Process that reveals z/OS Integrity



LNK-List

APF-List

AC=01

LPA-List

z/OS

1/3P

EXITs

SYSKEY

PPT

SVCs

Code Integrity

RUCSA

z/OS Integrity

USER – DASD – TASK

LOGON, MOUNT, START

c

b

a

Digitally Signed Server Pack

Pre-IPL Configuration

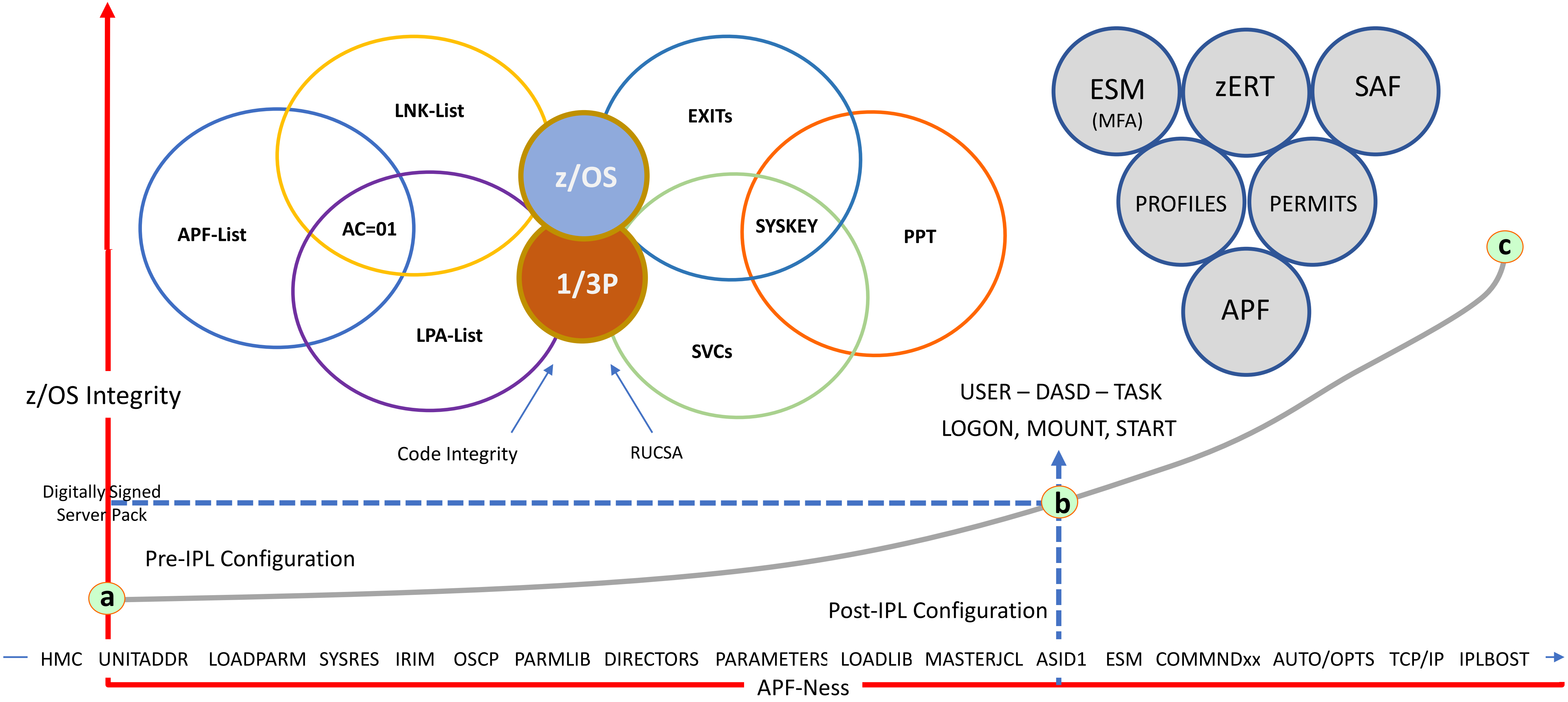
Post-IPL Configuration

HMC UNITADDR LOADPARM SYSRES IRIM OSCP PARMLIB DIRECTORS PARAMETERS LOADLIB MASTERJCL ASID1 ESM COMMNDxx AUTO/OPTS TCP/IP IPLBOST

APF-Ness

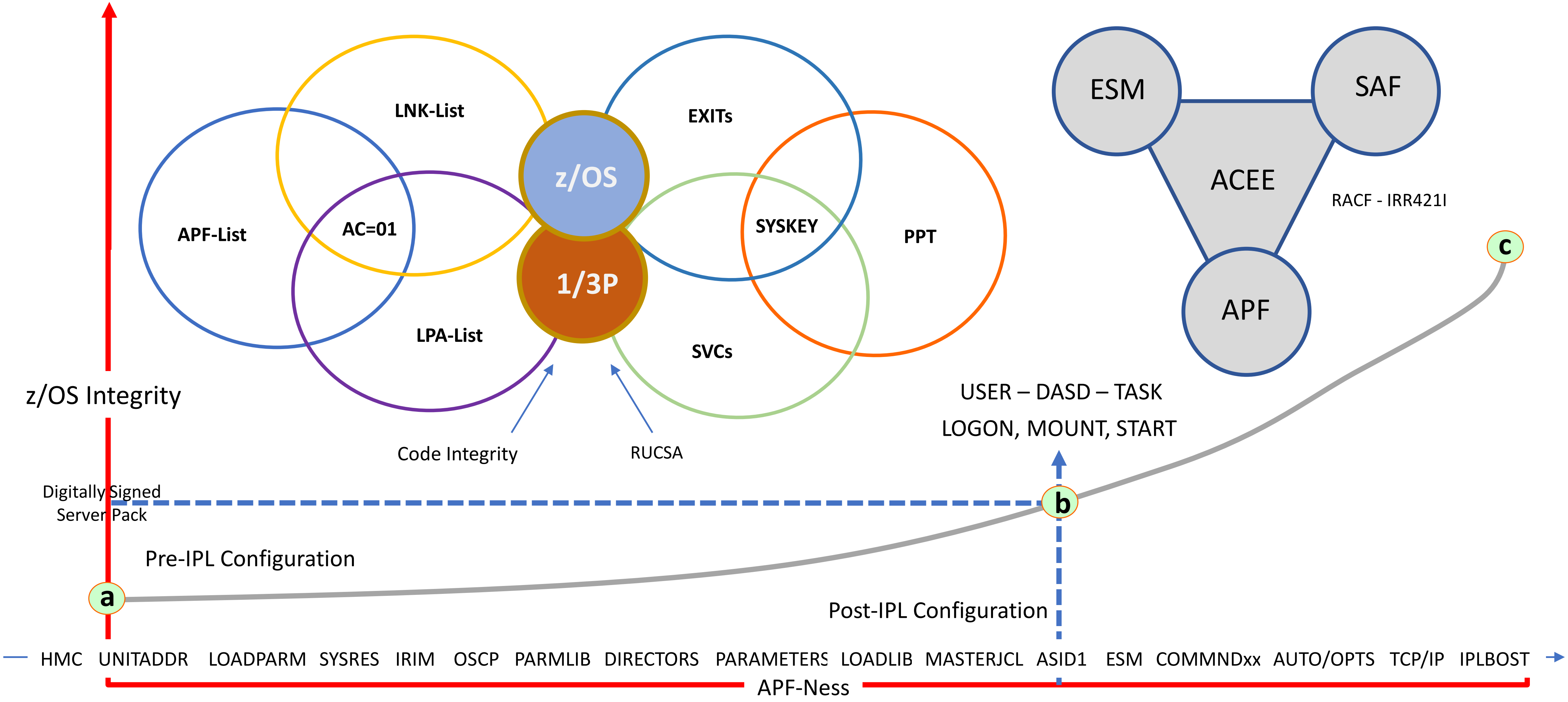
z/OS Is the Rock, but Why? Let Us Count the Ways!

The Initial Program Load(IPL) is the Process that reveals z/OS Integrity



z/OS Is the Rock, but Why? Let Us Count the Ways!

The Initial Program Load(IPL) is the Process that reveals z/OS Integrity



LNK-List

EXITs

z/OS

APF-List

AC=01

SYSKEY

PPT

1/3P

LPA-List

SVCs

Code Integrity

RUCSA

ESM

SAF

ACEE

RACF - IRR421I

APF

c

z/OS Integrity

USER – DASD – TASK

LOGON, MOUNT, START

Digitally Signed

Server Pack

b

Pre-IPL Configuration

a

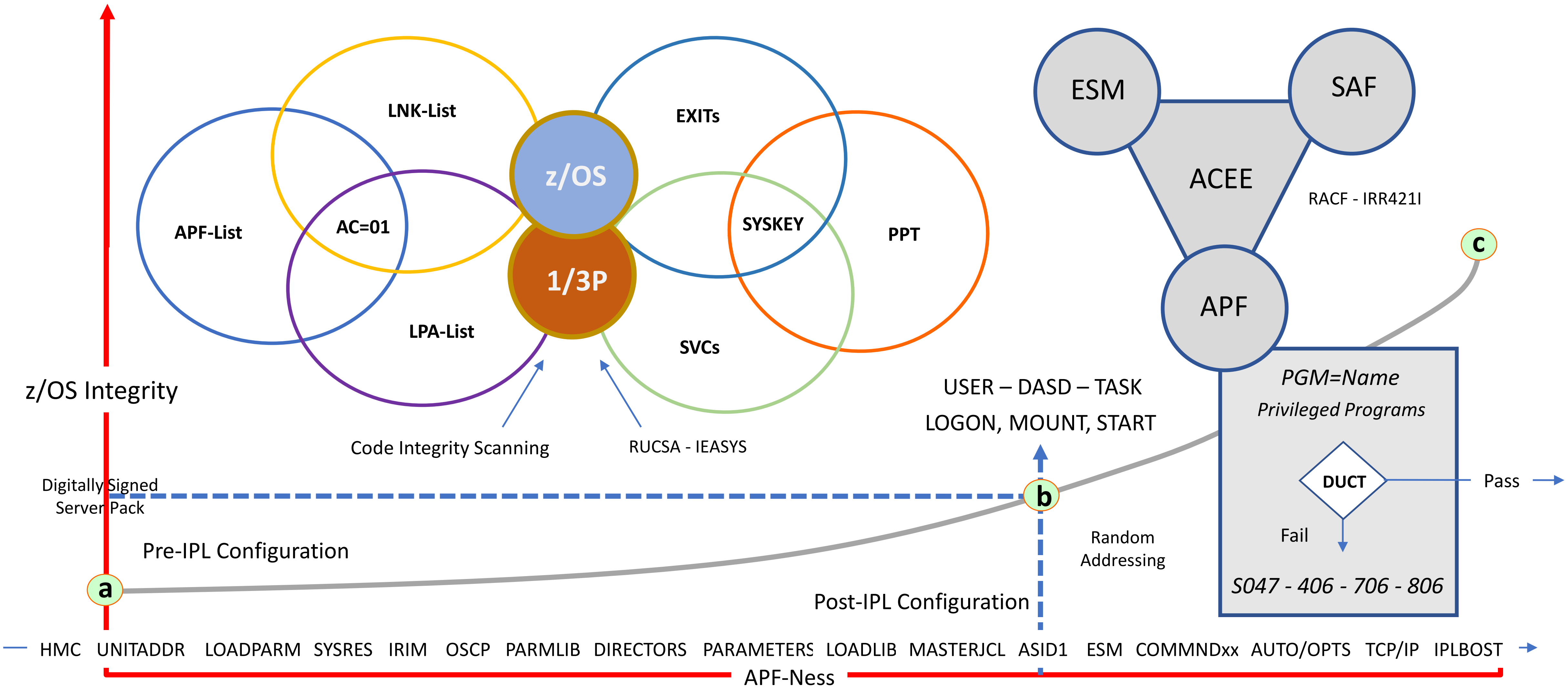
Post-IPL Configuration

HMC UNITADDR LOADPARM SYSRES IRIM OSCP PARMLIB DIRECTORS PARAMETERS LOADLIB MASTERJCL ASID1 ESM COMMNDxx AUTO/OPTS TCP/IP IPLBOST

APF-Ness

z/OS Is the Rock, but Why? Let Us Count the Ways!

The Initial Program Load(IPL) is the Process that reveals z/OS Integrity



LNK-List

EXITs

APF-List

AC=01

z/OS

1/3P

SYSKEY

PPT

LPA-List

SVCs

ESM

SAF

ACEE

RACF - IRR421I

APF

c

z/OS Integrity

Code Integrity Scanning

RUCSA - IEASYS

USER – DASD – TASK

LOGON, MOUNT, START

PGM=Name

Privileged Programs

DUCT

Pass

Fail

S047 - 406 - 706 - 806

Digitally Signed Server Pack

b

Random Addressing

Pre-IPL Configuration

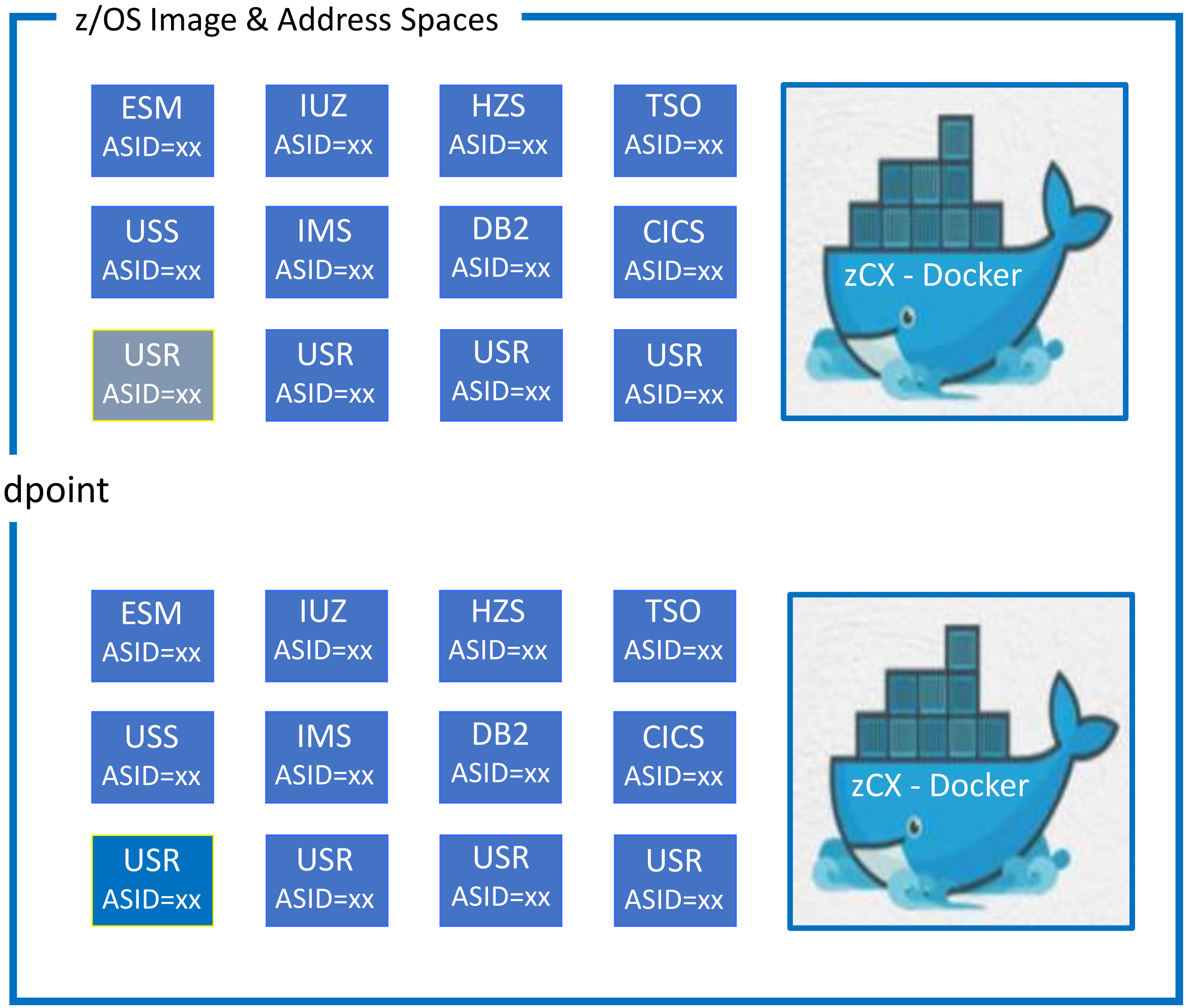
a

Post-IPL Configuration

HMC UNITADDR LOADPARM SYSRES IRIM OSCP PARMLIB DIRECTORS PARAMETERS LOADLIB MASTERJCL ASID1 ESM COMMNDxx AUTO/OPTS TCP/IP IPLBOST

APF-Ness

z/OS Is the Rock, but Why? Let Us Count the Ways!



z/OS Image & Address Spaces

ESM ASID=xx | IUZ ASID=xx | HZS ASID=xx | TSO ASID=xx

USS ASID=xx | IMS ASID=xx | DB2 ASID=xx | CICS ASID=xx

USR ASID=xx | USR ASID=xx | USR ASID=xx | USR ASID=xx

zCX - Docker

Endpoint

ESM ASID=xx | IUZ ASID=xx | HZS ASID=xx | TSO ASID=xx

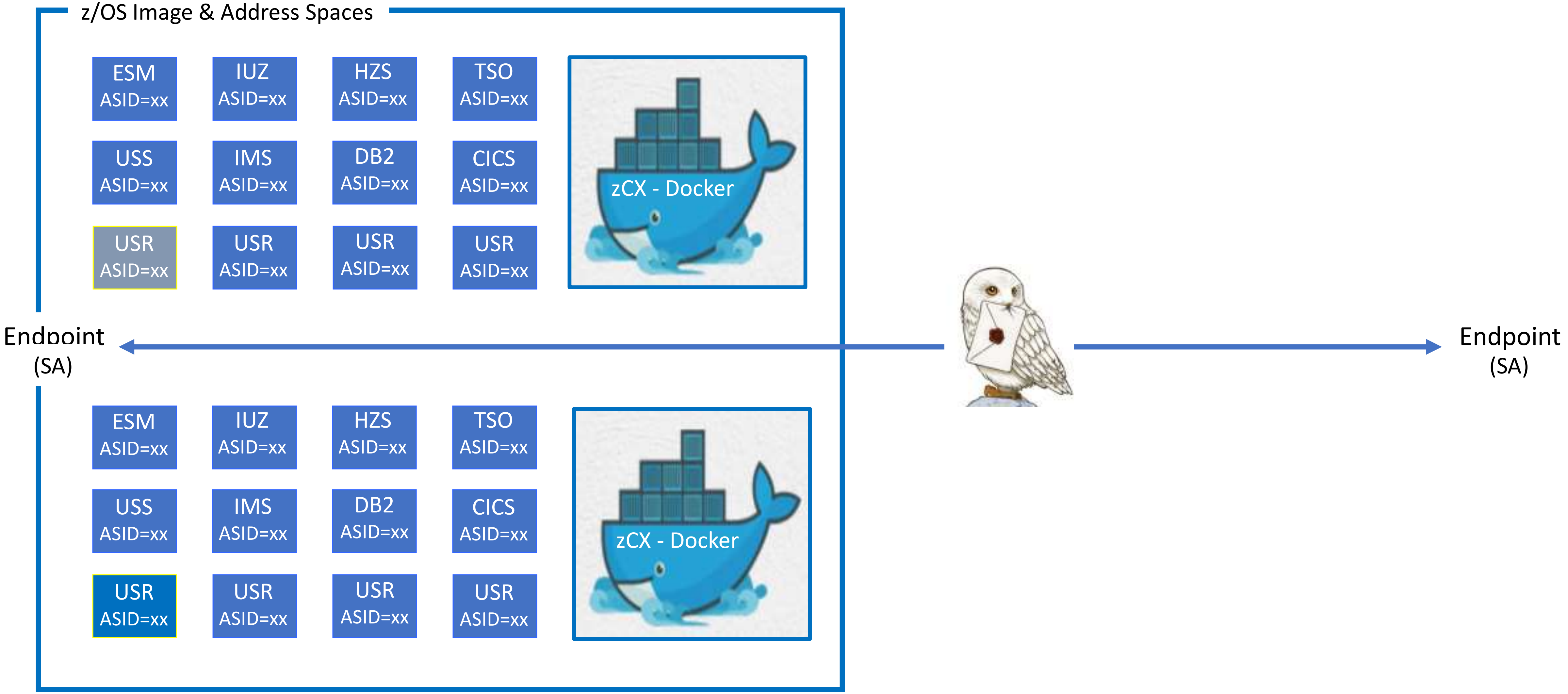
USS ASID=xx | IMS ASID=xx | DB2 ASID=xx | CICS ASID=xx

USR ASID=xx | USR ASID=xx | USR ASID=xx | USR ASID=xx

zCX - Docker

SA - Security Association

z/OS Is the Rock, but Why? Let Us Count the Ways!



z/OS Image & Address Spaces

ESM ASID=xx | IUZ ASID=xx | HZS ASID=xx | TSO ASID=xx

USS ASID=xx | IMS ASID=xx | DB2 ASID=xx | CICS ASID=xx

USR ASID=xx | USR ASID=xx | USR ASID=xx | USR ASID=xx

zCX - Docker

Endpoint (SA)

Endpoint (SA)

ESM ASID=xx | IUZ ASID=xx | HZS ASID=xx | TSO ASID=xx

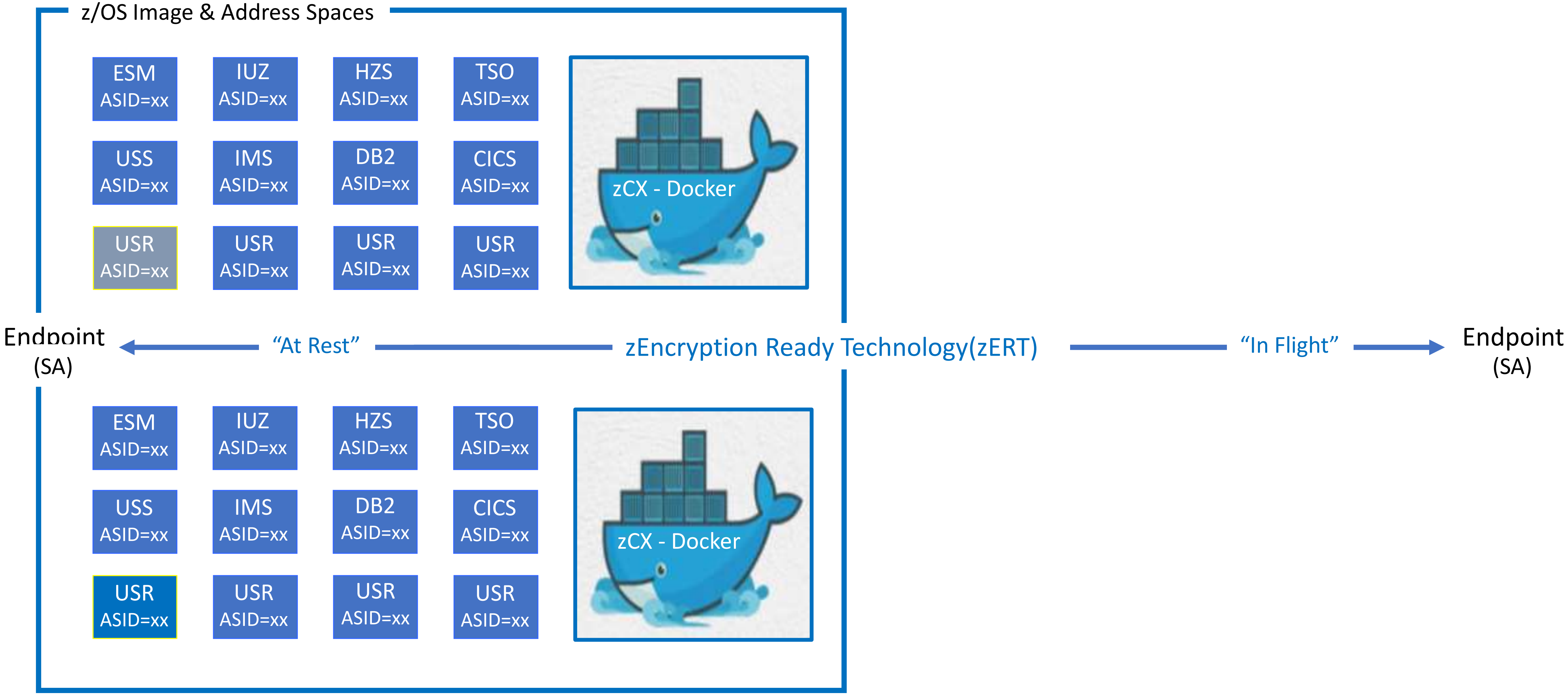
USS ASID=xx | IMS ASID=xx | DB2 ASID=xx | CICS ASID=xx

USR ASID=xx | USR ASID=xx | USR ASID=xx | USR ASID=xx

zCX - Docker

SA - Security Association

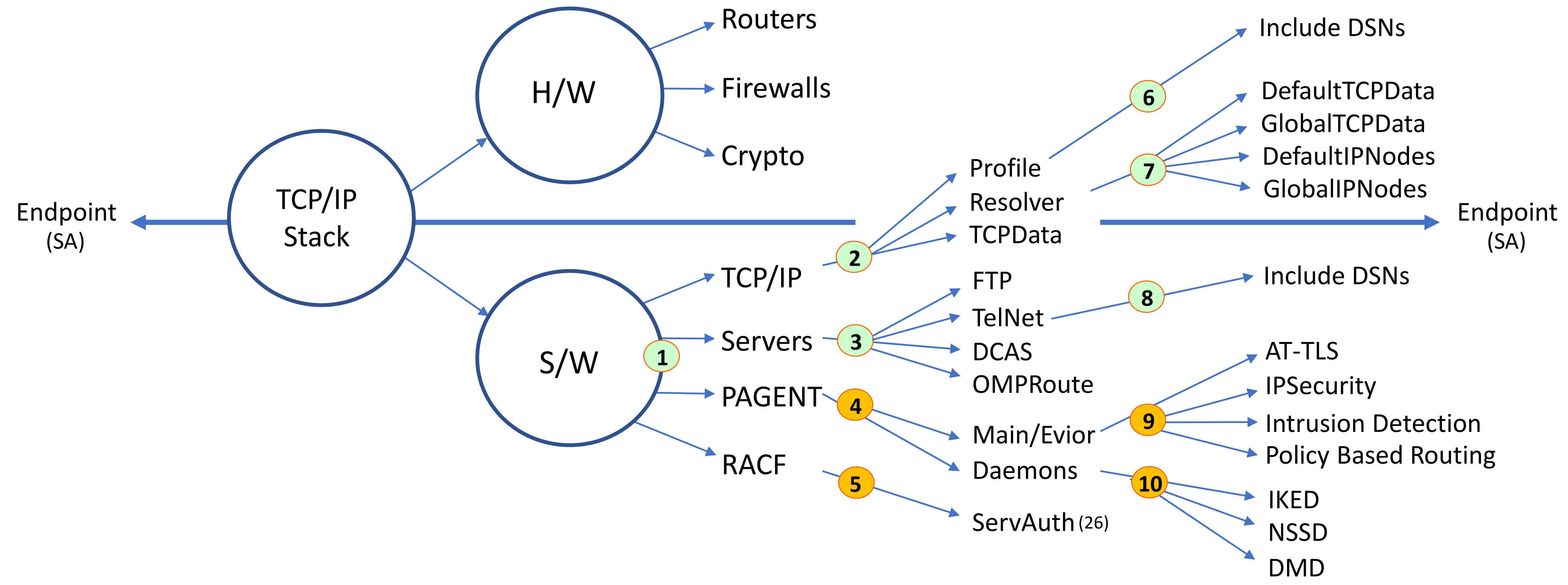
z/OS Is the Rock, but Why? Let Us Count the Ways!



SA - Security Association

z/OS Is the Rock, but Why? Let Us Count the Ways!

IPSec



Endpoint
(SA)

TCP/IP
Stack

H/W

Routers

Firewalls

Crypto

S/W

1

TCP/IP

Servers

PAGENT

RACF

2

Profile

Resolver

TCPData

3

FTP

TelNet

DCAS

OMPRoute

4

Main/Evior

Daemons

5

ServAuth (26)

6

Include DSNs

7

DefaultTCPData

GlobalTCPData

DefaultIPNodes

GlobalIPNodes

8

Include DSNs

9

AT-TLS

IPSecurity

Intrusion Detection

Policy Based Routing

10

IKED

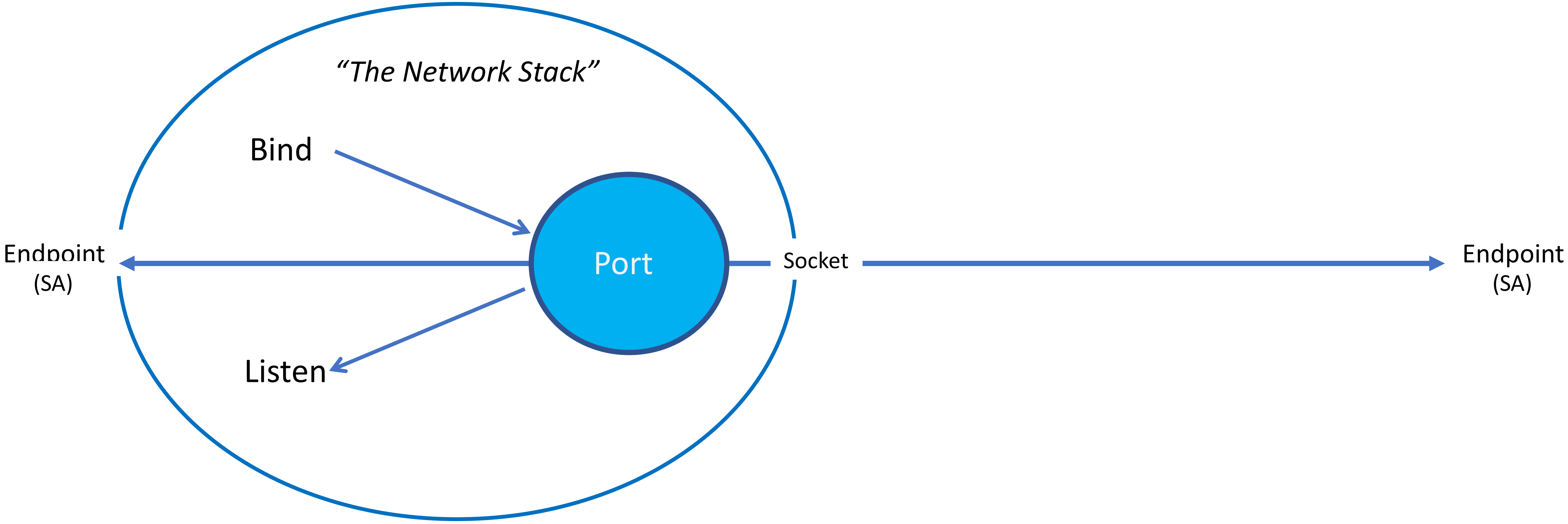
NSSD

DMD

Endpoint
(SA)

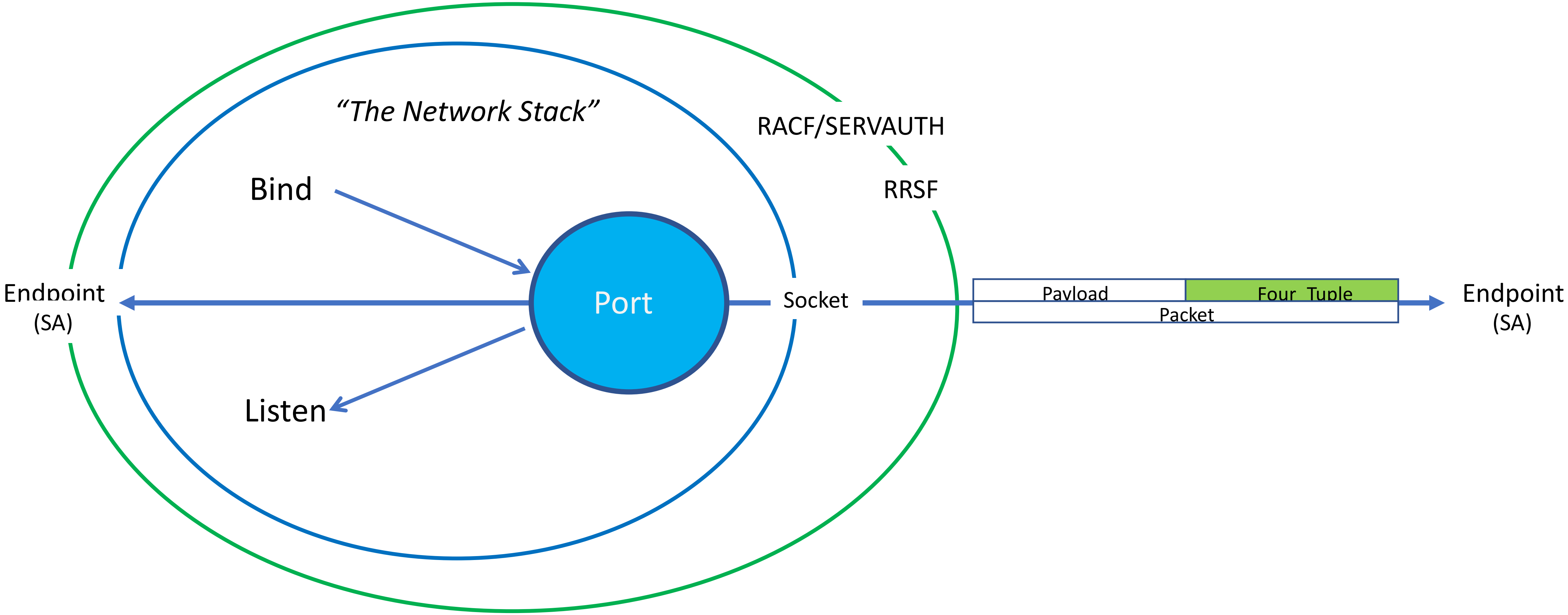
SA - Security Association

z/OS Is the Rock, but Why? Let Us Count the Ways!



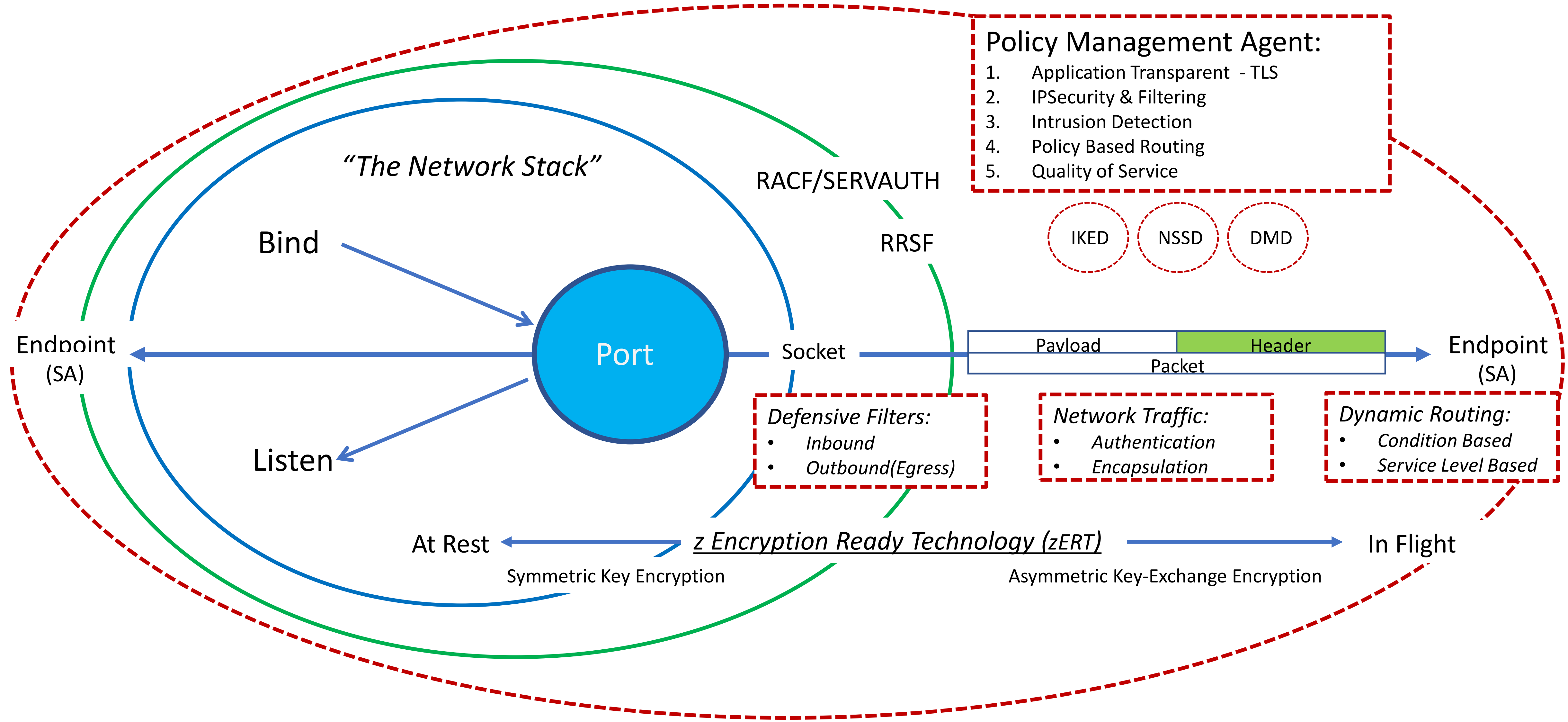
SA - Security Association

z/OS Is the Rock, but Why? Let Us Count the Ways!



SA - Security Association

z/OS Is the Rock, but Why? Let Us Count the Ways!



Policy Management Agent:

1. Application Transparent - TLS
2. IPSecurity & Filtering
3. Intrusion Detection
4. Policy Based Routing
5. Quality of Service

Defensive Filters:

- *Inbound*
- *Outbound(Egress)*

Network Traffic:

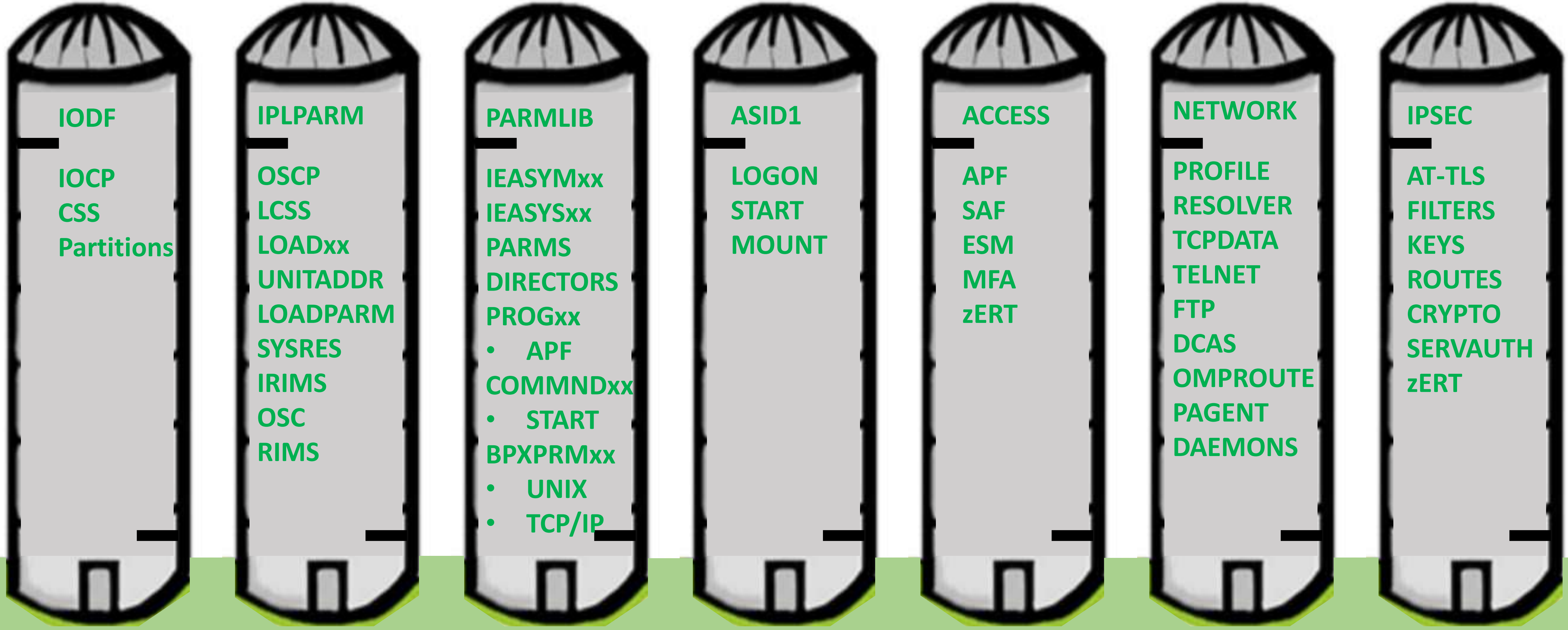
- *Authentication*
- *Encapsulation*

Dynamic Routing:

- *Condition Based*
- *Service Level Based*

SA - Security Association

z/OS Is the Rock, but Why? Let Us Count the Ways!



IODF

IOCP
CSS
Partitions

IPLPARM

OSCP
LCSS
LOADxx
UNITADDR
LOADPARM
SYSRES
IRIMS
OSC
RIMS

PARMLIB

IEASYMxx
IEASYSxx
PARMS
DIRECTORS
PROGxx
- APF

COMMNDxx
- START

BPXPRMxx
- UNIX
- TCP/IP

ASID1

LOGON
START
MOUNT

ACCESS

APF
SAF
ESM
MFA
zERT

NETWORK

PROFILE
RESOLVER
TCPDATA
TELNET
FTP
DCAS
OMPROUTE
PAGENT
DAEMONS

IPSEC

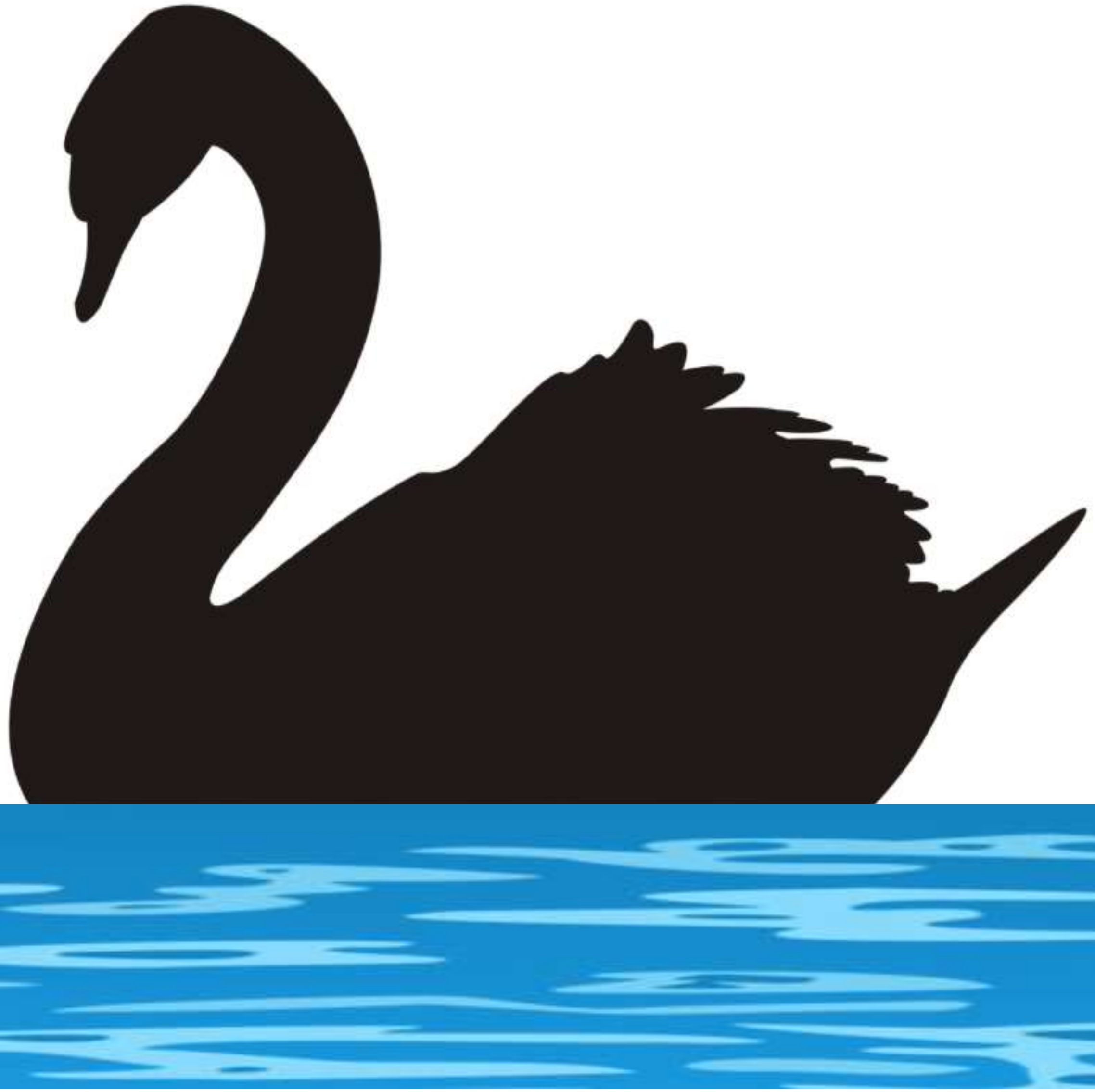
AT-TLS
FILTERS
KEYS
ROUTES
CRYPTO
SERVAUTH
zERT

zSystems Policy Decision Points

z/OS Is the Rock, but Why? Let Us Count the Ways!

What we all fear!

- ***The Improbable***
- ***The Unimagined***
- ***The Unexpected***
- ***The Unforeseen***



z/OS Is the Rock, but Why? Let Us Count the Ways!

Glossary of Terms:

1. ACF2 - Access Control Facility 2 – A CA Technology Security Product (ESM)
2. APAR - Authorized Program Analysis Report describes problem, formally tracked until resolved
3. APF - Authorized Program Facility
4. ASID - The Numeric Address Space Identifier
5. BCP - The Base Control Program - Backbone of z/OS Reliability and Integrity
6. CBPDO - Custom-Built Product Delivery Option
7. CF - Channel Facility
8. CPC - The Central Processing Complex
9. CPACF - CP Assist for Cryptographic Functions
10. CLI - Compare Logical Intermediate - In snippet - test for change in State
11. CSS - Channel Sub-System – Controls data flow input/output.
12. CHPID - Channel Path Identifier – a logical designation
13. CMT - CHPID Mapping Tool – Maps Logical to Physical Channels
14. CVSS - Common Venerability Scoring System
15. DASD - Direct Access Storage Device
16. DEB - Data Extent Block build on OPEN of DCB (Data Control Block). Can examine but not change
17. DPM - Dynamic Partition Manager – Linux specific Partition Management
18. DUCT - Dispatchable Unit Control Table - Control over the Authority State
19. DSFMF - Assign attributes to data sets and objects so system can auto manage storage
20. EAL - Evaluation Assurance Level – A System Integrity Standard – z Systems are EAL 5

z/OS Is the Rock, but Why? Let Us Count the Ways!

Glossary of Terms:

21. EBCDIC - Extended Binary Coded Decimal Interchange Code
22. EDT - Eligible Device Table – I/O devices that are eligible for allocation
23. EOS - End of Service – a date
24. ESM - External Security Manager
25. ESP - Early Support Program
26. FI - Function ID – Generally Applies to PCIe compliant Devices
27. FICON - Fiber Connection - FICON has replaced ESCON
28. FIRST - Forum of Incident Response and Security Teams
29. FMID - Function Module ID - Identifies IBM/Vendor software and its release number
30. GDPS - Geographically Disbursed Sysplex
31. GDPR - General Data Protection Regulations – European Union(EU)
32. HCD - Hardware Configuration Definition
33. HMC - Hardware Management Console
34. HSA - Hardware Storage Area
35. HIPER - High Impact Pervasive – as used in HIPER Fix
36. ICSF - Integrated Cryptographic Services Facility
37. IFL - Integrated Facility for Linux – A System Assist Processor(SAP)
38. IMSI - Initialization Message Suppression Indicator
39. IOCP - I/O Configuration Program – Hardware Portion of IODF
40. IODF - Input/Output Definition File - HCD - IOCP, OSCP and SWCP

z/OS Is the Rock, but Why? Let Us Count the Ways!

Glossary of Terms:

41. IOCDS - Input/Output Configuration Dataset, same as IOCP
42. IOS - Input/Output Subsystem – Sometimes referred as simply I/O
43. IPK - Insert PSW Key - A privileged Instruction - See snippet
44. IRIM - IPL Resource Initialization Modules
45. JCL - JOB Control Language - used to submit job to z/OS
46. LCSS - Logical Channel Sub-System - Up to 6 in a z14 each supports up to 15 LPARs
47. LPAR - Logical Partition – Up to 85 in a z14
48. LTSR - Long-Term Support Release - 2yrs Minimum, 1yr extension is optional at EOS
49. MODESET - Change system status - alter PSW/PKM or State Indicator
50. MFA - Multi-Factor Authentication – MFL Multi-Factor Logon – MFR Multi-Factor Reset
51. NIPCON - A named Console Device used only during a system IPL
52. NIPS - Nucleus Initialization Processing
53. OLTP - Online Transaction Processing – as apposed to Batch Processing
54. OSCP - Operating System Control Program – Software portion of IODF
55. OTP - One-Time Password - TOTP Time-Sensitive One-Time Password
56. PE - Program Error – As would be referenced in a PTF
57. POR - Power on Reset - A base level initialization of hardware and possible IPL
58. PPT - Program Properties Table
59. PR/SM - Processor Resource/System Manager
60. PKM - Program Status Word MASK - Control PSW Key Changes

z/OS Is the Rock, but Why? Let Us Count the Ways!

Glossary of Terms:

61. PCIe - Peripheral Component Interconnect Express
62. PCHID - Physical Channel Identifier - Up to 256 in a z15, shared by all CHPIDs
63. PDE - Pervasive Dataset Encryption – Part of the zERT Strategy
64. PMR - Problem Management Report – How Customers/Users Report Problems
65. PSW - Program Status Word - 0/7 protected & 8/15 not protected
66. PTF - Program Temporary Fix - When applied resolves a related APAR – FIX Package FIXPCK
67. PU - Processor Unit - Up to 107 in a single z14 CPC + SAP – System Assist Processors
68. RCT - Region Control Task - Highest priority Task in Address Space - Controls Swap in/out
69. RIM - Resource Initialization Modules
70. RACF - Resource Access Control Facility - An IBM Security Product (ESM)
71. RRSF - RACF Resource Sharing Facility - One RACF Db to service many systems
72. RSU - Recommended Service Update
73. SAF - System Access Facility - Provided by the Operating System in support of ESM
74. SAP - System Assist Processor - I/O Channel Management, zIIPs, zAAPs, IFL's
75. SIA - System Integrity APAR - Authorized Program Analysis Report
76. SLA - Service Level Agreement - A shared commitment to service i.e. Response Time
77. SPE - Describes a New Function APAR
78. SPKA - Set Storage Protect Key from Address - A Privileged Instruction
79. SMP/E - System Modification Program/Extended
80. SQA - System Query Area - A storage area in main memory

z/OS Is the Rock, but Why? Let Us Count the Ways!

Glossary of Terms:

81.SRB - Service Request Block - Supervisor State - SRB Routine, SRB Mode, Scheduling an SRB
82.SSC - Secure Service Container - A Highly secure LPAR Specific Hyperledger environment
83.SVC - Supervisor Call - Named System Modules - System Service Routines - IBM/USER
84.SWCP - Switch Configuration Program
85.TCB - Task Control Block - Problem State - Application Programs
86.TSS - Top Secret – A CA Technology Security Product (ESM)
87.UCB - Unit Control Block – Software portion of the Device Chain
88.UCW - Unit Control Work – Hardware portion of the Device Chain
89.USS - Unix System Services
90.SAN - Storage Area Network
91.SE - System Element - 1 of 2 CPC specific Workstations
92.SECINT - System Security and Integrity APARs/PTFs
93.SMF - System Management Facility – used to control system event logging
94.SR - Service Request (Tool) - Used to submit program problem/defect/error
95.TKE - Trusted Key Entry Workstation
96.2SV - Two Step Verification of a User Logon and/or Password Reset Credential
97.US-CERT - United States Computer Emergency Readiness Team
98.zEDC - z Enterprise Data Compression – an IBM Product
99.z/OS - A z Mainframe Operating System
100.z/OSMF - The z/OS System Management Facility – a web-based workstation interface

z/OS Is the Rock, but Why? Let Us Count the Ways!

Glossary of Terms:

101 - ACEE	Accessor Environment Element
102 - AH	Authentication Header
103 - API	Application Programming Interface
104 - AT-TLS	Application Transparent-Transport Layer Security (Preferred/Policy Agent)
105 - CA	Certificate Authority - validates a digital certificate’s integrity
106 - DMD	Defense Manager Daemon - used to implement short-term filters
107 - DFS	Defense Filter Store - stores versions of DMD Filters
108 – DOD	Department of Defense
109 - DOI	Domain of Interpretation
110 - EPS	Encapsulated Security Payload
111 – FTP	File Transfer Protocol – For downloading/Uploading Files
112 - GPL	GNU Public License
113 - ICMP	Internet Control Message Protocol
114 - IDC	Intrusion Detection – A type of filtering beyond that provided by firewalls
115 - FIPS	Federal Information Processing Standard - Approve cryptographic modules
116 – ICSF	Integrated Cryptographic Services Facility
117 – IDS	Intrusion Detection System
118 - IKED	Internet Key Exchange Daemon - supports endpoint to endpoint security associations
119 - IP	Internet Protocol
120 - IPSec	Internet Security Protocol

z/OS Is the Rock, but Why? Let Us Count the Ways!

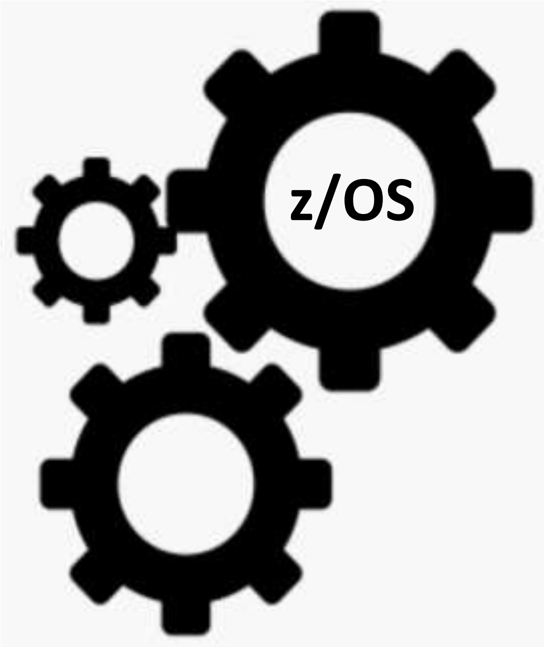
Glossary of Terms:

121 - MAC	Machine Address – unique to every hardware device worldwide
122 - NAT	Network Address Translation – limits IP addresses, saves money, improves security
123 - MODP	Modular exponentiation group
124 - NSSD	Network Security Service Daemon - provides advanced services to IKED Servers/Clients
125 - PEP	Policy Enforcement Point - Routers, Firewalls, Hosts – Policy based logic
126 - PFS	Perfect Forward Secrecy - used to protect symmetric keys that protect the data
127 - PKI	Public Key Infrastructure – defines a method for sharing public/private keys
128 – PKDS	Public Key Dataset
129 - QoS	Quality of Service – Policy Management Agent Defined Rules enforced by TCP/IP Stack
130 - SA	Security Association - shared session and transfer secrets/certificates
131 - SAD	Security Association Database
132 – SAF	System Access Facility – Works with the External Security Manager (ESM)
133 - SPD	Security Policy Database - a store of Policy Agent configuration statements
134 - SSL/TLS	Secure Socket Layer/Transport Layer Security (Basic/Provided Natively)
135 - SWSA	Sysplex Wide Security Association – Stack to Stack traffic across Couple Facility
136 - TCP	Transmission Control Protocol - sends message segments, guarantees delivery in order
137 - TLS	Transport Layer Security
138 - UDP	User Datagram Protocol - send messages, best efforts - “fire and forget”
139 - VIPA	Virtual Internet Protocol Address – DVIPA is a dynamic VIPA
140 – VPN	Virtual Private Network

Your feedback is important!

Submit a session evaluation for each session you attend:

SHARE mobile app -or- www.share.org/evaluation



z/OS Is the Rock, but Why? Let Us Count the Ways

Session 26689

Thursday, February 27 at 1:45PM

Room 204A

Presented by Paul R. Robichaux

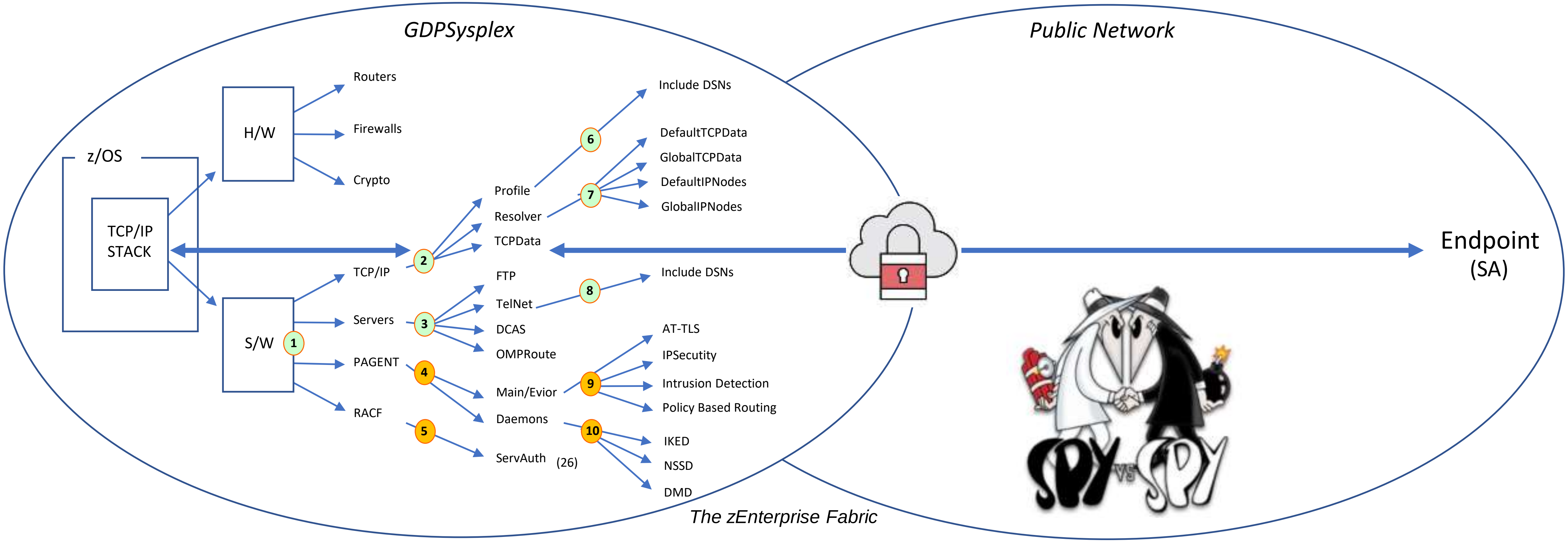
NewEra Software, Inc.

prr@newera.com

Questions?

Cybersecurity – *A new look at Network Defenses in Depth Vs. à La Carte!*

Tuesday 17, March – 11:00PDT – An Introduction to IPComplete and *MYIP



GDPSysplex

Public Network

z/OS

TCP/IP STACK

H/W

Routers

Firewalls

Crypto

S/W

1

TCP/IP

Servers

PAGENT

RACF

2

Profile

Resolver

TCPData

6

Include DSNs

7

DefaultTCPData

GlobalTCPData

DefaultIPNodes

GlobalIPNodes

3

FTP

TelNet

DCAS

OMPRoute

8

Include DSNs

4

Main/Evior

Daemons

9

AT-TLS

IPSecutity

Intrusion Detection

Policy Based Routing

5

ServAuth (26)

10

IKED

NSSD

DMD

Endpoint
(SA)

The zEnterprise Fabric

Defensive Filters:

- *Inbound*
- *Outbound(Egress)*

Network Traffic:

- *Authentication*
- *Encapsulation*

SA - Security Association