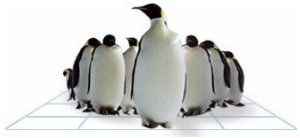
Linux on IBM System z Security

Security, here today, ready for tomorrow!

IBM Systems

Trademarks



The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

DB2*
e-business logo
HiperSockets
IBM*
IBM eServer
IBM logo*
MQSeries*
RACF*
Redbooks*
S/390*
System z
System z
Tivoli*
WebSphere*
z/OS*
z/VM*
zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a registered trademark of the Intel Corporation in the United States, other countries or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

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

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

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

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

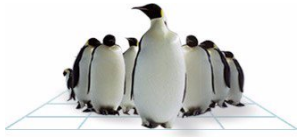
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Linux for System z is not …

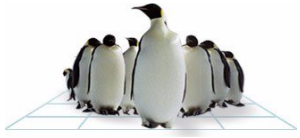


Linux® for IBM System z™ is not z/OS®

Linux for System z is not RACF®

Linux for System z is not ICSF

Linux is ...



Linux for System z has security-rich features.

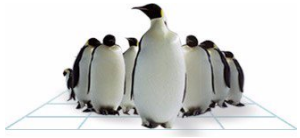
Linux for System z is open, no security through obscurity; anyone can see flaws and fix them.

Linux has a large active developer base enabling a thorough code review.

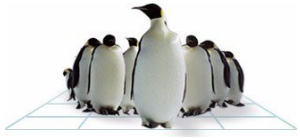
Linux has a worldwide user base which allows testing on a wide range of hardware and diverse scenarios.

Linux benefits from almost immediate response to security advisories and rapid implementation of new technologies.

Linux Security Objectives

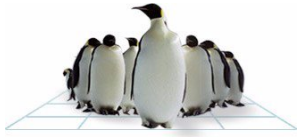


- Provide System Integrity of the Linux for System z Kernel.
- Allow the Linux for System z offering to take advantage of and not be excluded from current security offerings available on other Linux platforms. These offerings may be available in the open source community, requiring little or no modification to run on Linux for System z, or may need to be developed internally.
- Provide that the Linux for System z offering to take advantage of System z cryptographic offerings.
- Provide security solutions as needed to enable Linux for System z to take advantage of or complement the overall System z Security Strategy and Architecture.



Key Technologies

Key Technologies Available on Linux



Cryptography

Firewall

User Management

Image Isolation

Image Hardening

Intrusion Detection

Directory Services

Secure Network Communication

Digital Certificates

Anti-Virus

Access Control

PAM

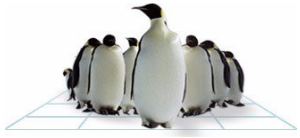
Pluggable Authentication Modules

Linux on System z Security Building Blocks

Access Control Lists	**SELinux, AppArmor, IBM Tivoli® Access Manager & WebSeal, CA's eTrust Access Control & Web Access**
Anti-Virus/Anti-Spam	**ClamAV, OpenAntiVirus, AmaViS, MIMEDefrag, TrendMicro (ServerProtect & ScanMail), Network Associates, Roaring Penguin's CanIt**
Directory Services	**Open LDAP, NIS/NIS+, IBM Directory, CA's eTrust Directory, PADL's XAD, Quest's VAS**
Digital Certificates	**Freeware PKI, z/OS PKI Services**
Firewall	**IPTables/NetFilter, zGuard, StoneGate, webApp.Secure**
Intrusion Detection	**Snort, Snare, PortSentry, TripWire, LIDS, IPLog,** **IBM Tivoli Risk Manager (->Tivoli Security Operations Manager), PredatorWatch, SafeZoneNet**

Vendor Product
Open Source Product

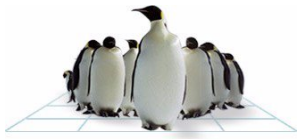
Linux on System z Security Building Blocks



Secure Network Communications	**OpenSSH, PGP, GNU PGP, USAGI IPv6, FreeS/WAN,** **CA's eTrust VPN, StoneSoft's StoneGate VPN, SecureAgent Software**
Secure Socket Layer (SSL)	**OpenSSL, PKCS#11, GSKIT, PKCS#11**
System Hardening	**Bastille, Tiger, Distributions**
Secure Data	**dm-crypt, ppdd, CFS, McAfee's e-Business Server**
Distributed Policy Management	**IBM Tivoli Access Manager, CA's eTrust Directory**
Proxy Server	**Proxy Suite from SuSE, IBM Edge Server**

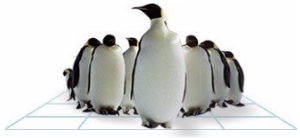
Vendor Product
Open Source Product

Vendor Enablement

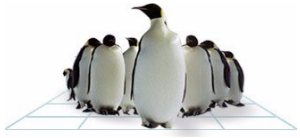


- **Software Developer Products for Linux for System z**
  - **ibm.com**/zseries/solutions/s390da/linuxproduct.html
  - Currently 374 Participating Vendors
  - Currently 1017 Vendor Applications
- **Data Encryption**
  - Network Associates' E-Business Server offers PGP encryption and compression for data transfer and storage
- **Patch Management**
  - BMC Software's SystemCheck
- **User Management**
  - Blockade Systems' Syncserv
  - IBM Tivoli Identity Management

Distributions Embracing Security

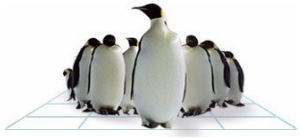


- Hardening
- Secure shell
- Virtual Private Network
- Enhanced Audit Capability
- Enhanced Authentication Options
- Enhanced Firewall Management
- Intrusion Detection Systems
- Cryptographic Libraries and Access to Hardware
- Host and Network Scanning Tools
- Certifications



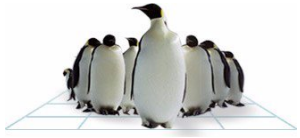
Certification

Isolation and Certification



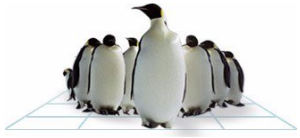
- **LPAR**
  - IBM eServer™ zSeries® 900 (z900) - 12/02 CC EAL4/EAL5
  - IBM eServer zSeries 800 (z800) - 5/03 CC EAL4/EAL5
  - IBM eServer zSeries 990 (z990) - 10/04 CC EAL4/EAL5
  - IBM eServer zSeries 890 (z890) - 6/05 CC EAL4/EAL5
  - IBM System z9™ 109 – 3/06 CC EAL5
  - IBM System z9 Enterprise Class (z9 EC) & Business Class (z9 BC) – 8/06 CC EAL 5
- **z/VM®**
  - Statement of System Integrity
  - Common Criteria
    - Status: z/VM 5.1 certified 2Q 2005
    - EAL 3+
      - LSPP – Labeled Security Protection Profile
      - CAPP – Controlled Access Protection Profile

Linux on System z Certification

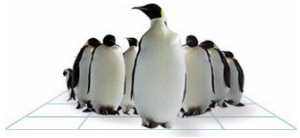


- **Common Criteria**
  - CAPP
    - Controlled Access Protection Profile
    - Created by NSA
    - Audit, Access Control, etc.
  - LSPP
    - Labeled Security Protection Profile
    - Mandatory Access Control
    - Multilevel Security (MLS)
  - Evaluation Assurance Level
    - EAL 3 = methodically tested and checked
    - EAL 4 = methodically designed, tested and reviewed
    - + = Maintenance (Flaw Reporting Procedures)
- **DIICOE**
  - Defense Infrastructure Information/Common Operating Environment
  - US Only
- **FIPS**
  - OpenSSL – FIPS 140-2 Level 1 Validated
  - CP Assist
    - SHA-1 validated for FIPS 180-1
    - DES & TDES validated for FIPS 46-3

Linux for System z Certifications by Distribution

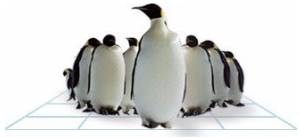


Version	Certification Level	Status
Novell SUSE		
SLES 8	**CAPP – EAL 3 +**	**Complete**
SLES 9	**CAPP – EAL 4 +**	**Complete**
SLES 10	**CAPP – EAL 4 +**	**In evaluation**
RedHat		
RHEL 3	**CAPP – EAL 3 +**	**Complete**
RHEL 4	**CAPP – EAL 4 +**	**Complete**
RHEL 5	**CAPP / LSPP – EAL 4 +**	**In evaluation**



crypto

Crypto Hardware Matrix



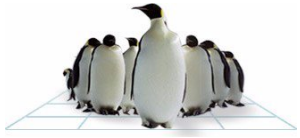
PCI Cards

Name	Supported HW	Linux Support	Remarks
PCICC	G5, G6, z900, (not z800)	Clear Key SSL only	1 processor/card
PCICA	z900 GA 2, z800, z990	Yes	5 processors/card
PCIXCC	z990 GA 2, z890	Clear Key SSL only	1 card per adapter
CEX2C	z990 GA 4, System z9	Clear Key SSL only	2 cards per adapter (cards same as PCIXCC)
CEX2 (Coprocessor & Accelerator)	System z9 EC, System z9 BC	Clear key SSL + secure key	2 cards per book, each card can have a 2A or 2C personality

Instructions

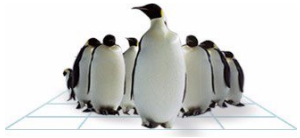
Name	Supported HW	Linux Support	Remarks
CCF	G5, G6, z900, z800	No	Replaced by CP Assist in z990
CP Assist Instructions	z990, z890	Yes	DES, TDES, SHA-1
CP Assist Instructions	System z9 EC/BC	Yes	AES-128, SHA- 256, PRNG

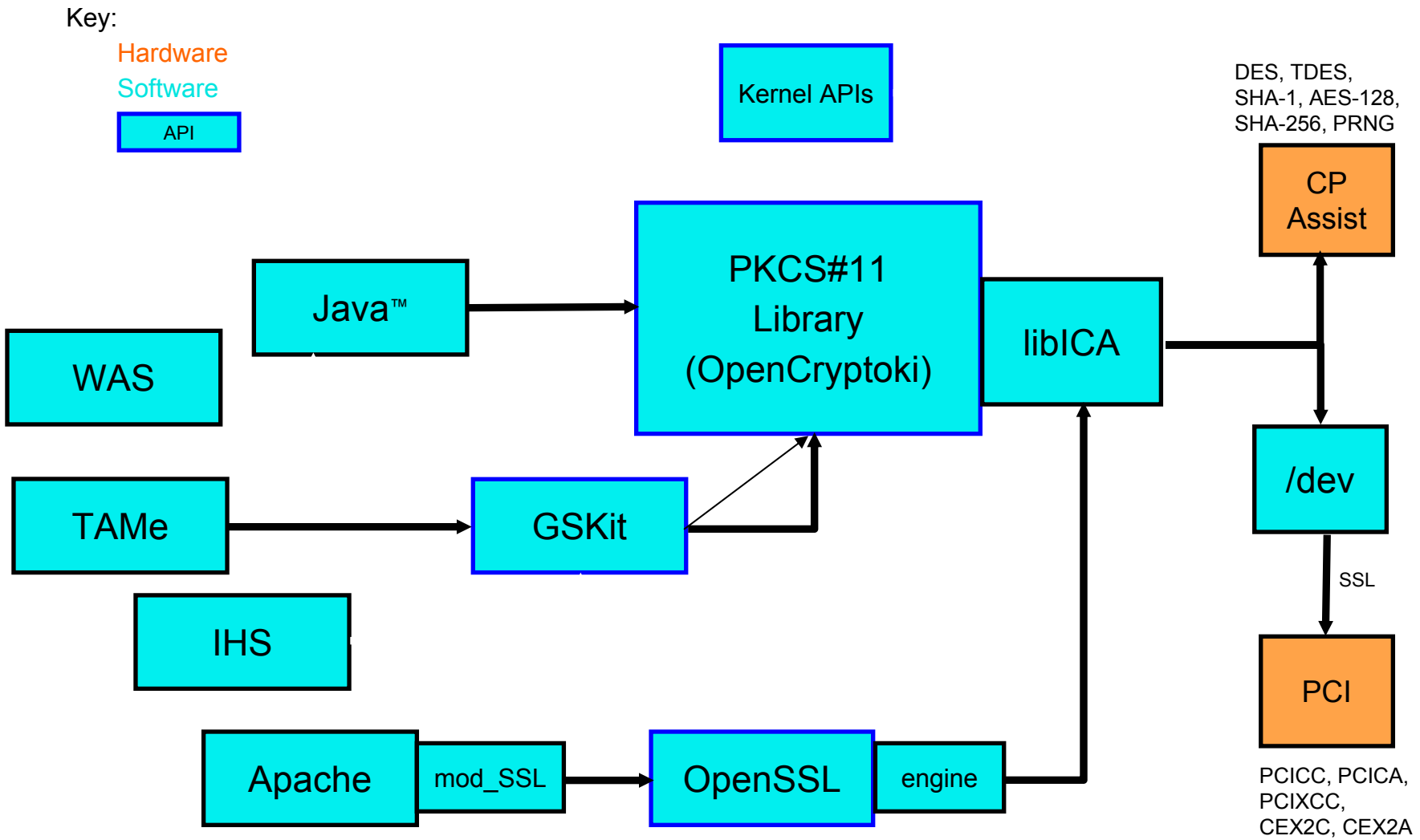
Cryptography – Clear Key



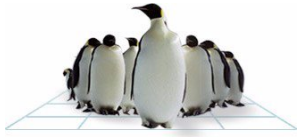
- **Hardware Acceleration**
  - **Asymmetric**
    - RSA handshake
      - PCICC with ~200 handshakes/second/card
      - PCICA with 2 cards ~
        - 1000 handshakes/second/card
        - 2000 handshakes/second/feature
      - PCIXCC with ~ 1000 handshakes/second/card
      - CEX2C with ~ 2000 handshakes/second/card
      - CEX2A w/one accelerator ~ 3000 handshakes/second/card
      - CEX2A w/two accelerators ~ 6000 handshakes/second/feature
  - **Symmetric**
    - DES, TDES, AES, SHA-1 and SHA-256
  - **PRNG**
- **Software Libraries for crypto access**
  - Kernel APIs
  - OpenSSL
  - PKCS#11
  - GSKit

Clear Key Crypto Solution



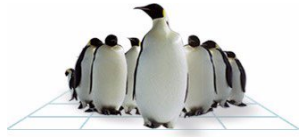


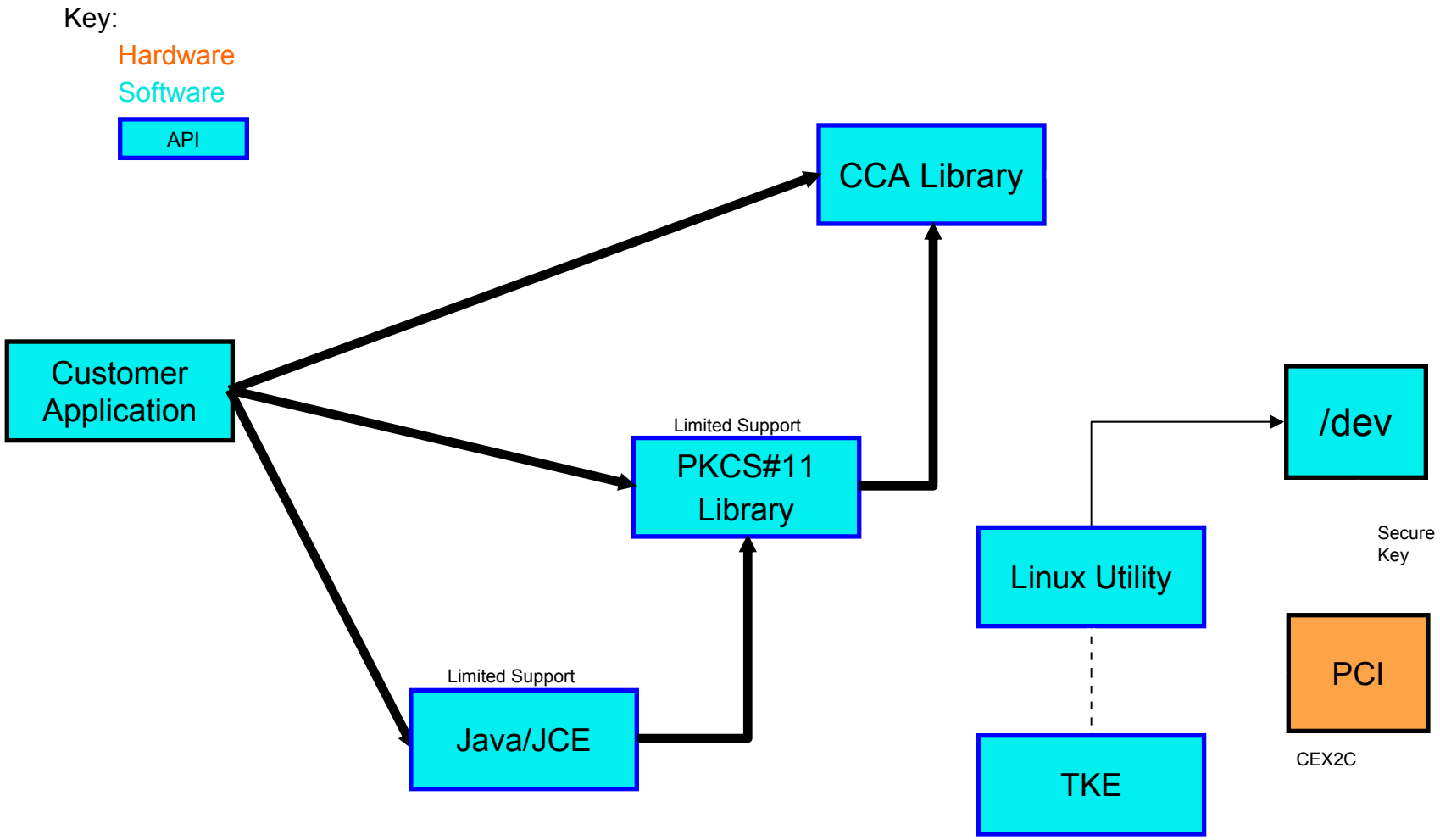
Cryptography – Secure key



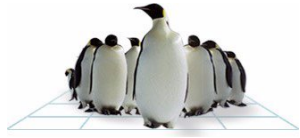
- **Hardware Acceleration**
  - Asymmetric and Symmetric
    - CEX2C
- **Software Libraries for crypto access**
  - CCA – Common Cryptographic Architecture
  - PKCS#11 – Limited
    - Key generation/encrypt/decrypt for TDES & RSA
  - Java/JCE – Limited as above
- **Card Management**
  - Trusted Key Entry (TKE)
  - Linux CCA utility
  - Configure via z/OS then re-assign to Linux

Secure Key Crypto Solution

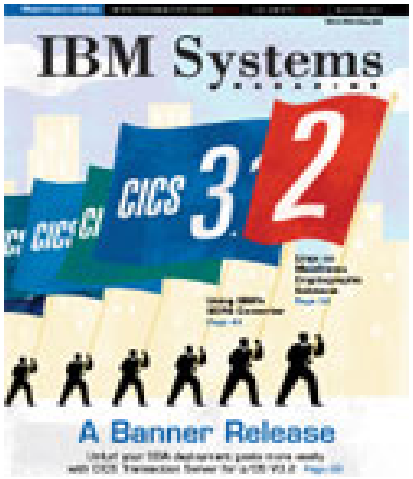




Further Reading

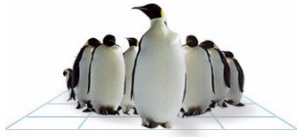


IBM Systems Magazine: Mainframe edition
May/June 2007



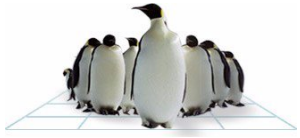
Cutting-Edge Cryptography

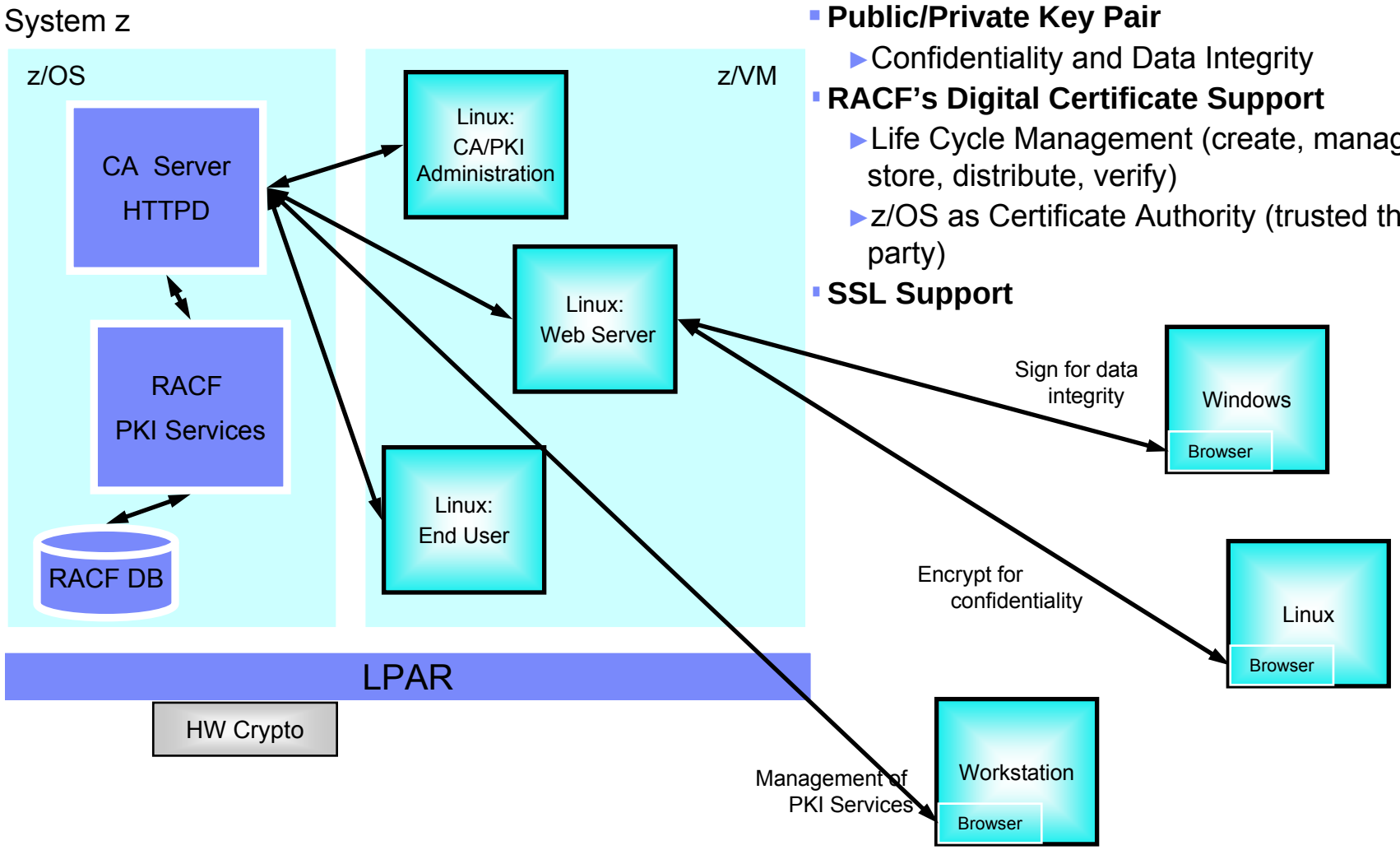
http://www.ibmsystemsmag.com/Mainframe/May07/Spera



Platform Synergy

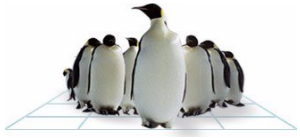
Public Key Infrastructure (PKI)

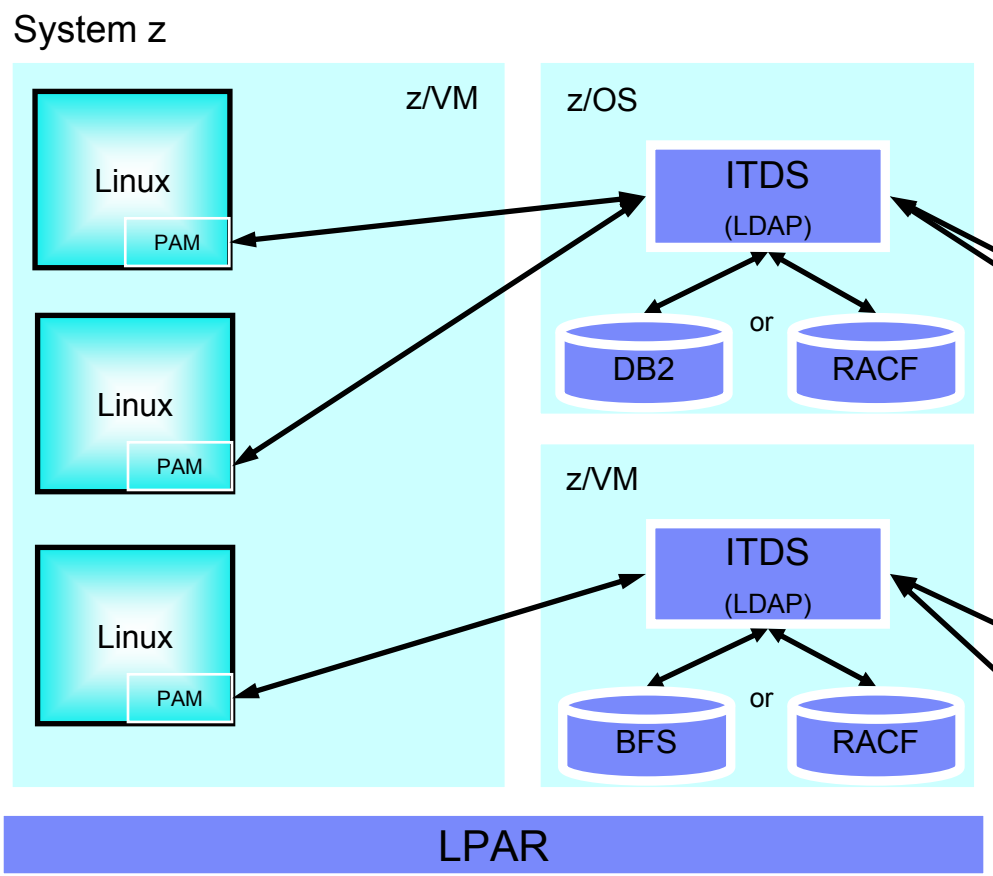




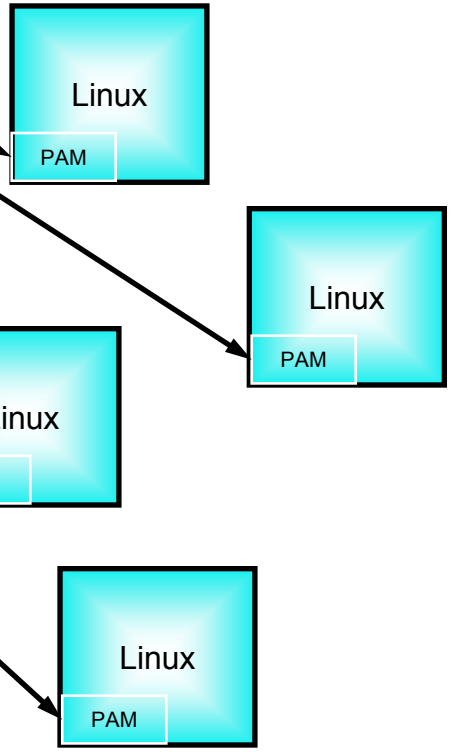
- **Public/Private Key Pair**
  - Confidentiality and Data Integrity
- **RACF's Digital Certificate Support**
  - Life Cycle Management (create, manage, store, distribute, verify)
  - z/OS as Certificate Authority (trusted third party)
- **SSL Support**

Centralized Authentication

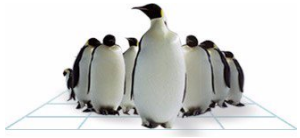




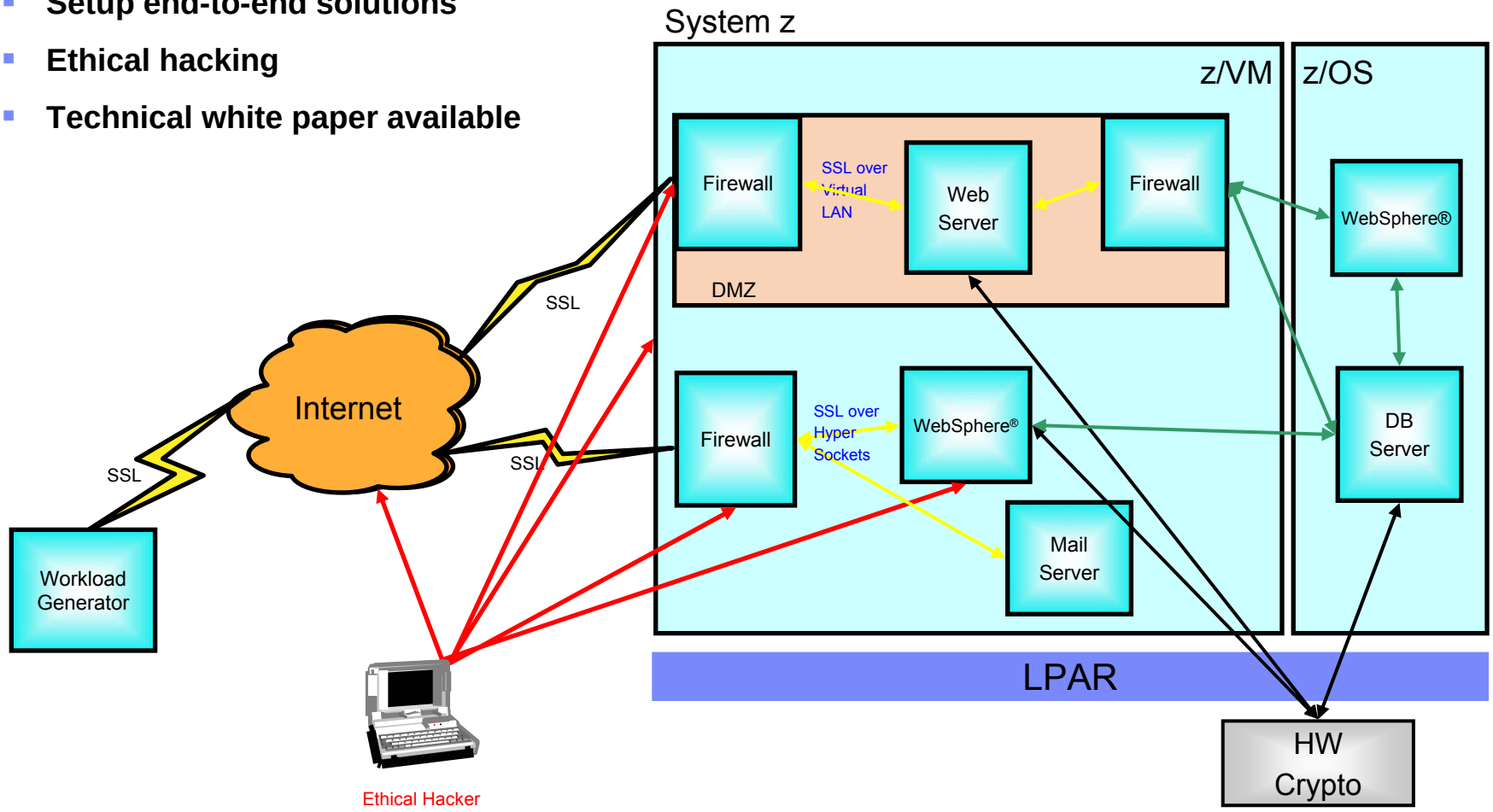
- **Common Client – PAM**
- **Integrated LDAP Server on z/OS and coming on z/VM**
- **LDAP backed by RACF or DB2®**



Ethical Hacking

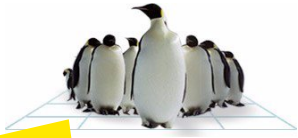


- **Setup end-to-end solutions**
- **Ethical hacking**
- **Technical white paper available**



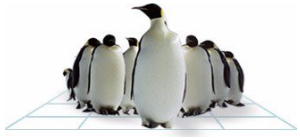
For details see:

- Linux Security: Exploring Open Source Security for a Linux Server Environment (GM13-0636-00)
- zSeries Platform Test Report for z/OS and Linux Virtual Servers



zDMZ

Demilitarized Zone (DMZ)



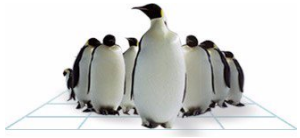
Definition:

A DMZ is a perimeter network between an external network and a private or protected network that provides isolation for a publicly available service, with the ultimate goal of protecting the private network and private services in the enterprise. The DMZ is often bounded by two firewalls.

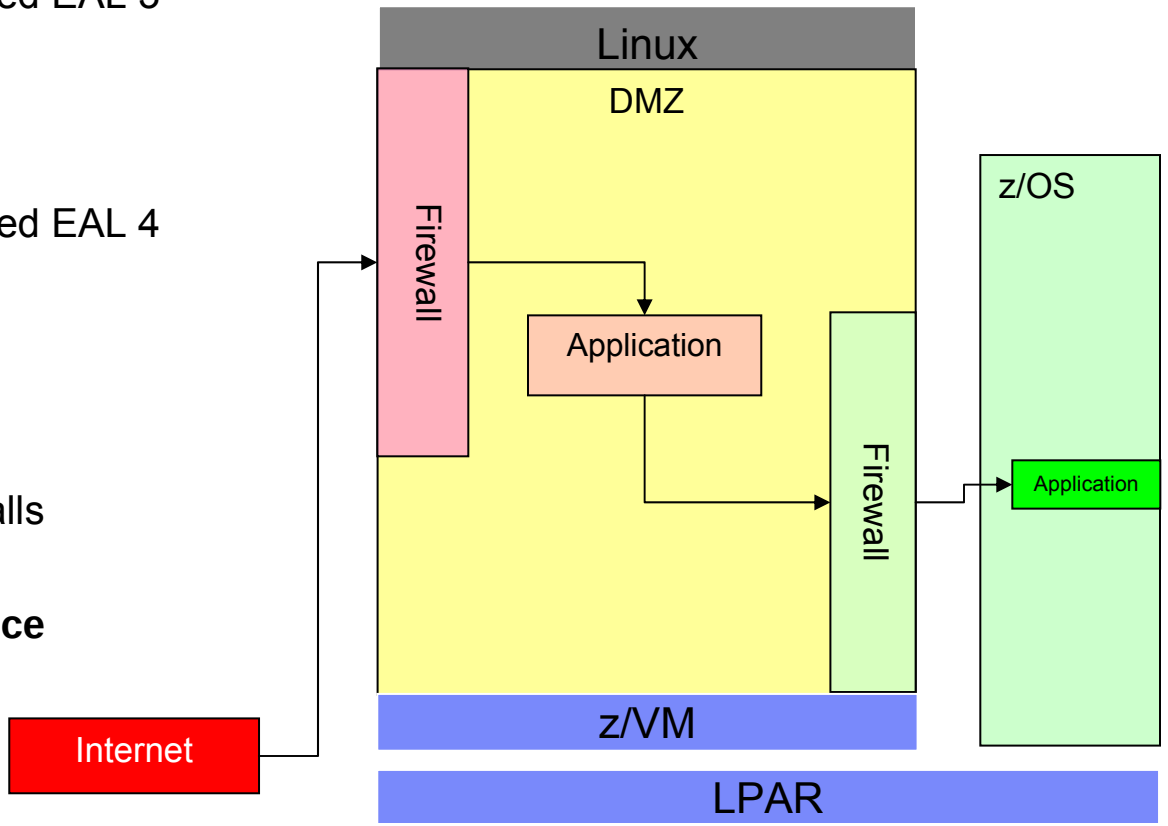
Scenario:

A Web server that is available to the Internet would need to be isolated, via DMZ, from the enterprise's internal network and/or transaction and data services.

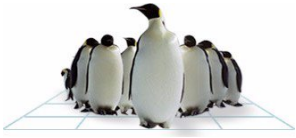
Anatomy of a DMZ on System z



- **Isolation with LPAR**
  - Common Criteria Certified EAL 4/5
- **z/VM**
  - Common Criteria Certified EAL 3
  - Integrity Statement
  - RACF
- **Linux**
  - Common Criteria Certified EAL 4
- **Networking**
  - HiperSockets™
  - Virtual LANs
- **Demilitarized Zone**
  - Bastion & Choke Firewalls
  - Hot -> Caution -> Safe
- **Application or public service**
- **Auditability**



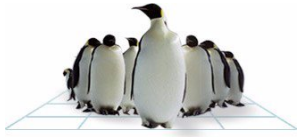
Further Reading



IBM Systems Magazine: Mainframe edition
January/February 2007

Living Next Door to the DMZ

http://www.ibmsystemsmag.com/Mainframe/Jan07/Spera

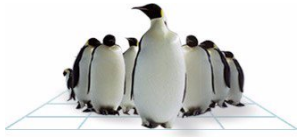


Utility Services for System z

Utility Services

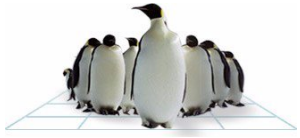
- **Software Appliances**
- **Tools to build DMZ**
  - Firewall
  - Application Firewall
  - Centralized User Authentication
- **Utility Services encompass:**
  - Inherent value for z/OS
  - Documentation
  - Testing
  - Marketing messages

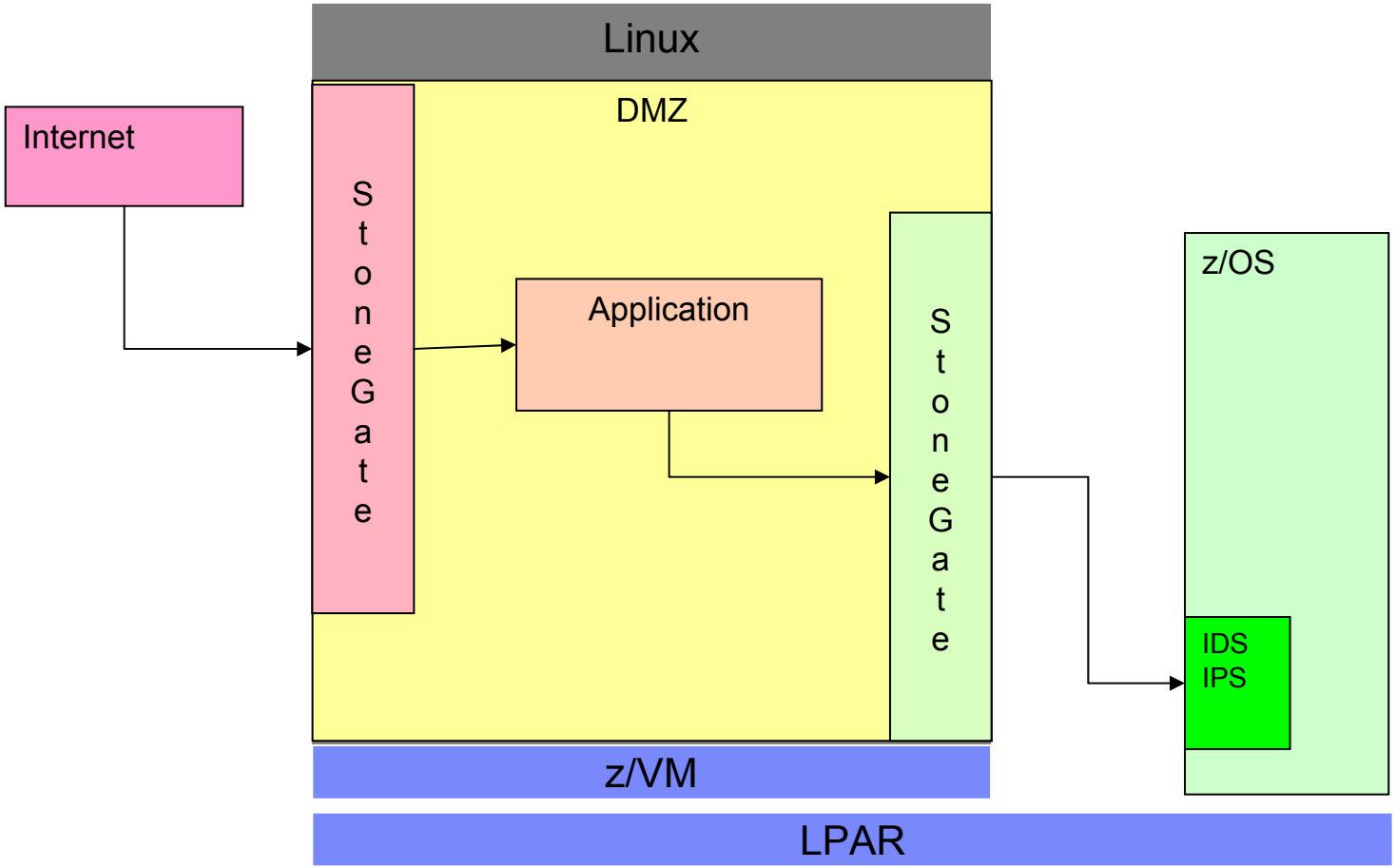
StoneGate Utility Service



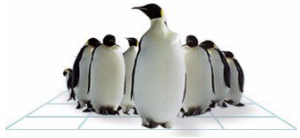
- **Compatible with and complimentary to z/OS, IPSec and IDS**
- **Full function firewall - simple IP filtering to complex packet interrogation**
- **Includes a VPN for management and secure communication**
- **Centralized enforcement and management of diverse security policies across all deployed firewall instances**
- **Provides real time surveillance of firewall traffic with IPS (Intrusion Prevention System) capability**
- **Includes support for HiperSockets, QDIO and CTC, providing physically secure communications to z/OS**
- **Workload balanced *Firewall Farm* can meet load peaks and high availability requirements without additional hardware**

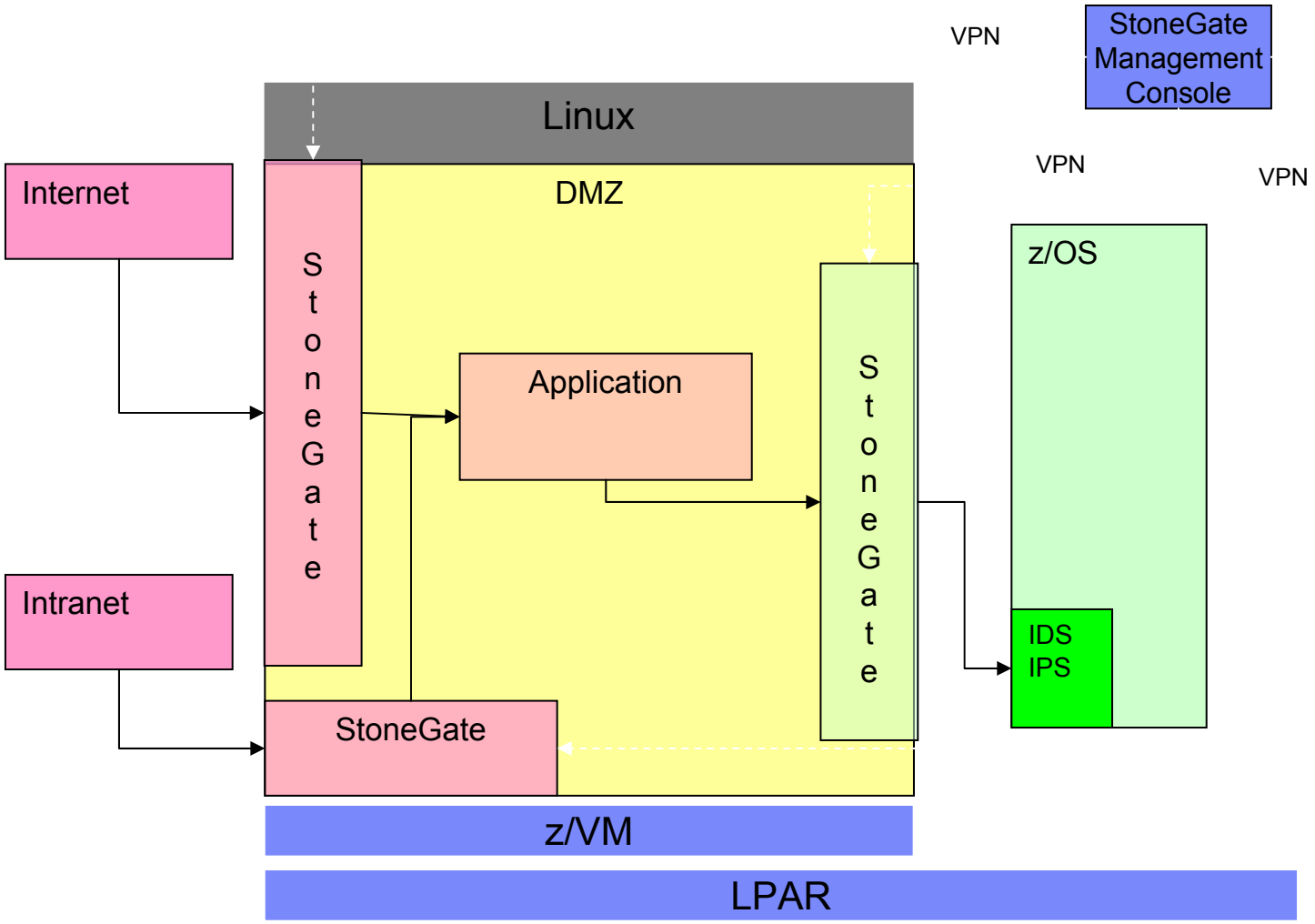
Basic Distributed DMZ



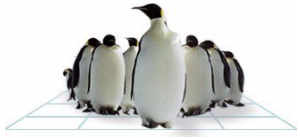


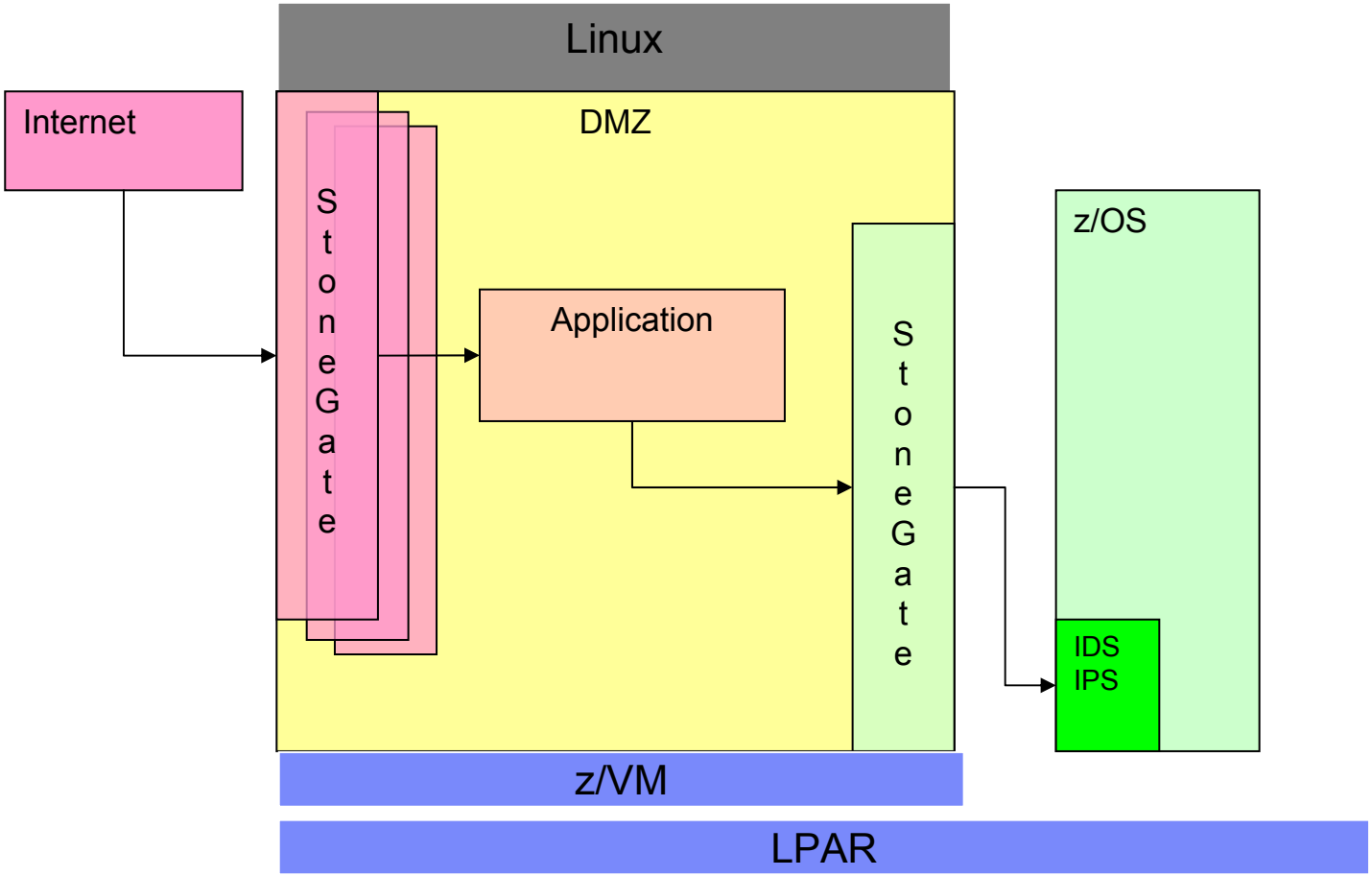
Diverse DMZ (various policies)



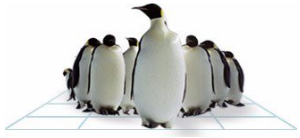


High Availability DMZ



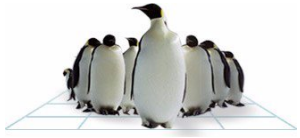


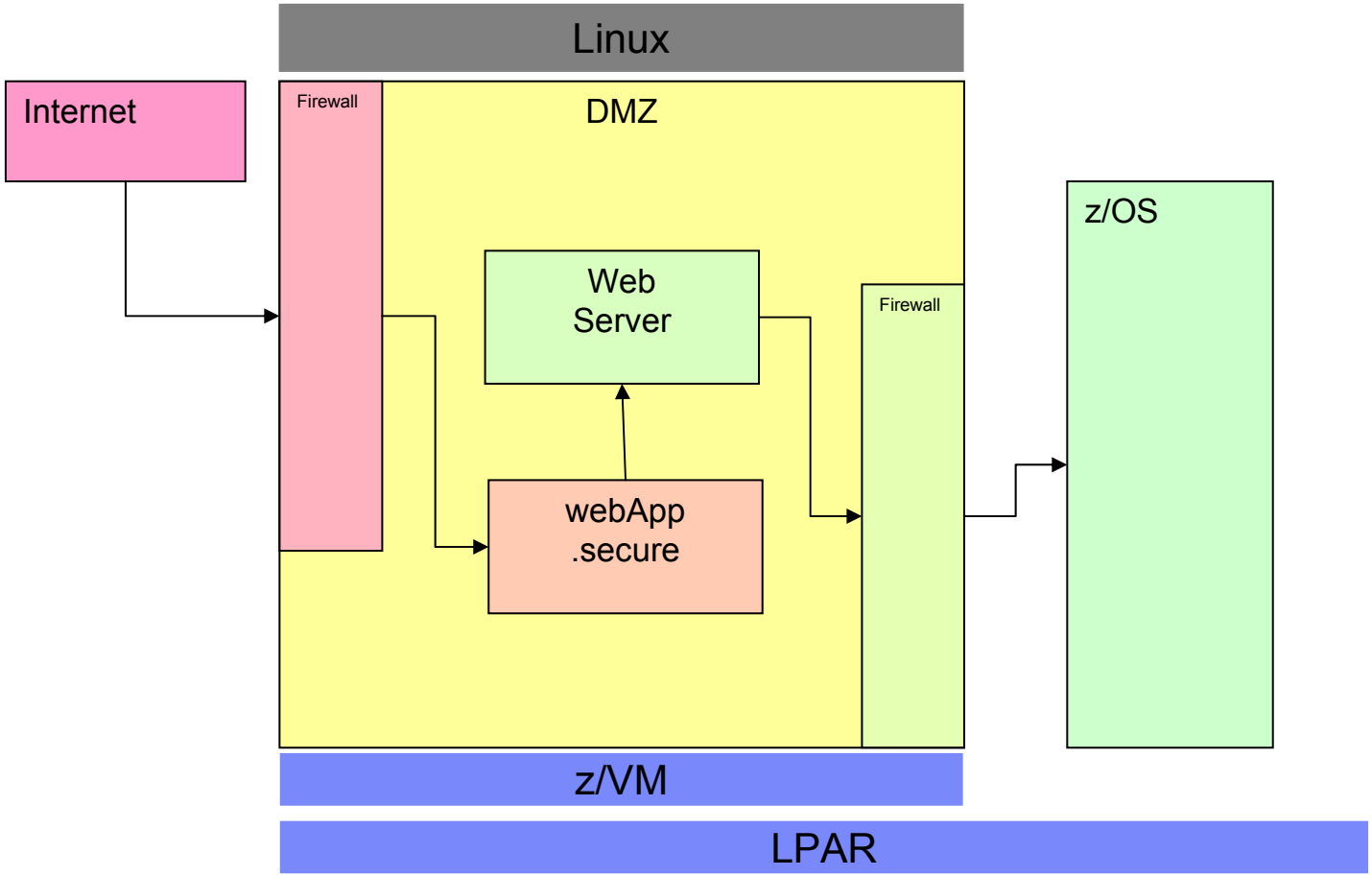
webApp.secure Utility Service



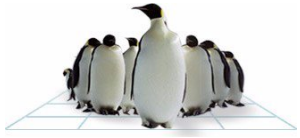
- Network security in some cases is not enough; webApp.secure protects Web applications from attack
- Application Firewalls are strategic
- Should be used in conjunction with traditional firewall/perimeter security
- webApp.secure in conjunction with z/OS ensures that transaction content is validated
- Inserted in the DMZ, before the Web server, protecting z/OS from the growing threat of application attacks
- Ensures that Web site guidelines, policies and rules are enforced and auditable

webApp.secure



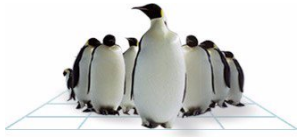


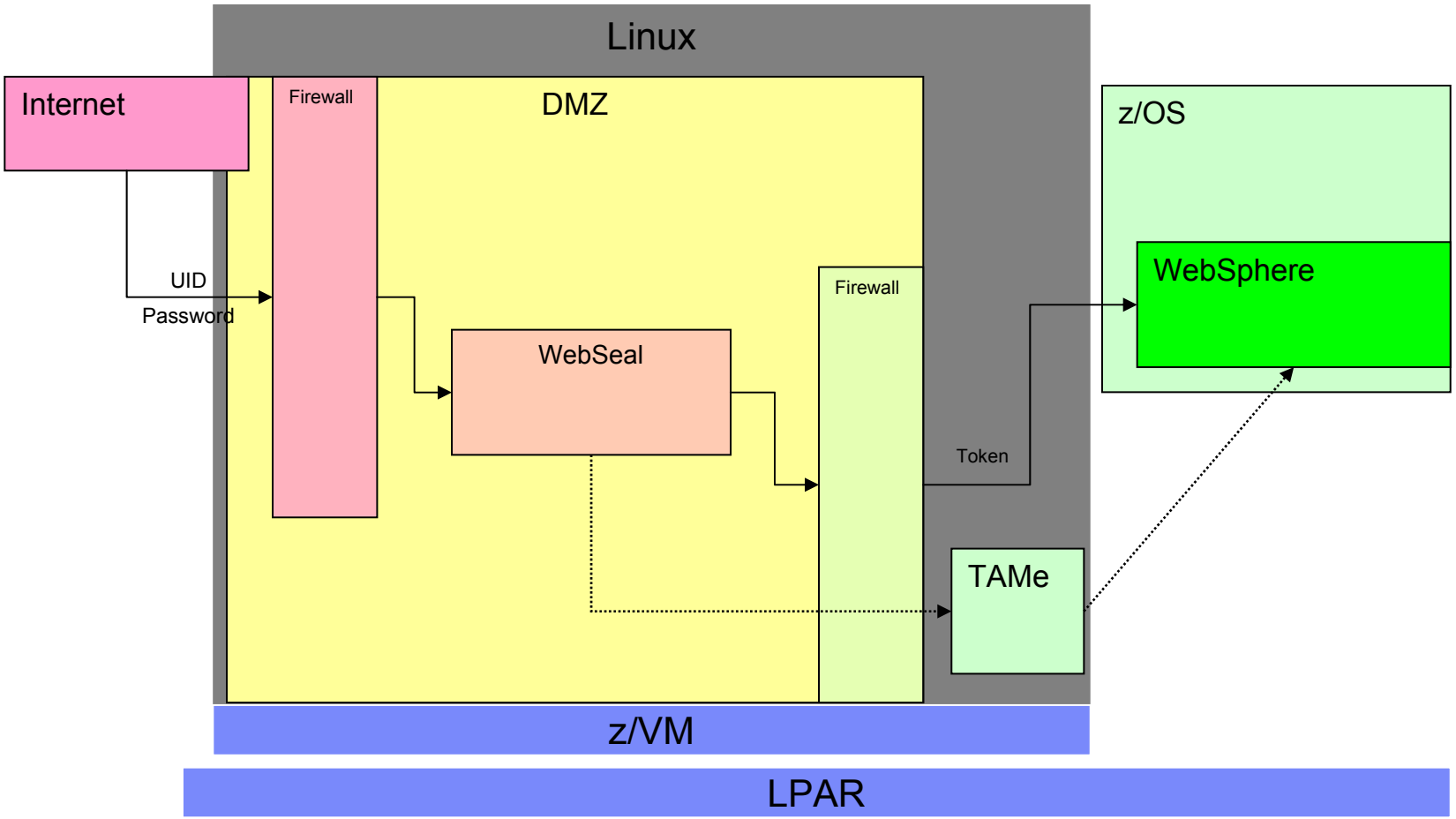
WebSeal Utility Service

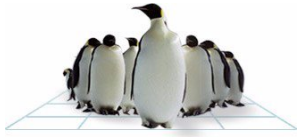


- **WebSeal, together with Tivoli Access Manager and WebSphere® residing on z/OS provide end-to-end, centralized authentication and single sign on capability for secure transactions**
- **z/OS remains safely isolated from Internet traffic and threats**
- **A client would be authenticated by WebSeal via user ID and password, and a token would be assigned and associated to the transaction for the remainder of the communication**
- **There is no WebSeal offering for z/OS**
- **Can take advantage of hardware crypto acceleration for SSL**

WebSeal

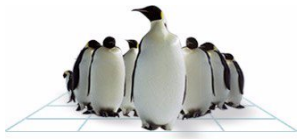



Linux
Internet
Firewall
DMZ
z/OS
UID
Password
WebSeal
Firewall
WebSphere
Token
TAMe
z/VM
LPAR



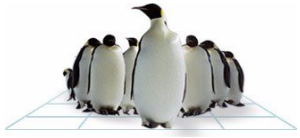
References

System z Advantage Summary



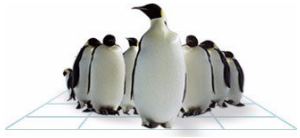
- **Image Isolation**
  - LPAR
  - z/VM
- **Common Criteria Certification**
- **Hardware Encryption**
  - Asymmetric Algorithm provides SSL performance enhancements
  - Symmetric Instructions - DES, TDES, AES-128, SHA-1 and SHA-256
  - Secure key cryptography
- **HiperSockets Provide Physical Security**
- **Qualities of Service**
- **Integration with IBM Software**
  - IBM Director
  - Tivoli Access Manager and AM-OS provide enforcement and management of security policy across platforms
  - Tivoli MQSeries®
  - Tivoli Risk Manager provides Host, Network and Web IDS
  - Tivoli Identity Manager
  - Tivoli Federated Identity Manager

Sources of General Linux Information



Linux for System z	**ibm.com**/zseries/linux/
z/VM and Linux on System z Resources	**ibm.com**/zseries/vm/linux/
Linux for System z Redbooks®	publib-b.boulder.**ibm.com**/cgi-bin/searchsite.cgi?query=Linux+AND+zSeries

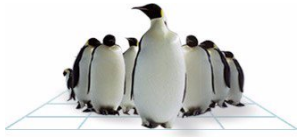
Linux for System z Security Resources



- Linux on zSeries Security (White paper, March 2005)
  - GM13-0488, **ibm.com**/zseries/library/techpapers/pdf/gm130488.pdf
- Linux Security: Exploring Open Source Security for a Linux Server Environment (White paper, June 2004)
  - GM13-0636, ftp://ftp.software.**ibm.com**/eserver/zseries/misc/literature/pdf/whitepapers/gm130636.pdf
- z/VM Security and Integrity (White paper, April 2005)
  - GM13-0145, **ibm.com**/zseries/library/techpapers/pdf/gm130145.pdf
- Linux on IBM eServer zSeries and S/390®: Best Security Practices (Redbook, May 2004)
  - SG24-7023, publib-b.boulder.**ibm.com**/abstracts/sg247023.html?Open
- Security Web pages for Linux on zSeries (April 2005)
  - **ibm.com**/zseries/os/linux/security/
- Linux Utilities for IBM System z
  - **ibm.com**/systems/z/os/linux/utilities/
- Request a quote from the Linux on zSeries Web page
  - **ibm.com**/zseries/os/linux/getquote/
- Platform Test Reports
  - **ibm.com**/servers/eserver/zseries/zos/integtst/

Secure Key Crypto - Information & Download

- **Crypto Cards – select “PCI-X Cryptographic Coprocessor”**
  - www-03.**ibm.com**/security/cryptocards/
  - Hardware Overview
    - www-03.**ibm.com**/security/cryptocards/pcixcc/overview.shtml
  - Hardware Summary
    - www-03.**ibm.com**/security/cryptocards/pcixcc/overproduct.shtml
  - CCA Overview
    - www-03.**ibm.com**/security/cryptocards/pcixcc/overcca.shtml
  - Programmer's Guide
    - www-03.**ibm.com**/security/cryptocards/pcixcc/library.shtml
  - CCA Library Download
    - www-03.**ibm.com**/security/cryptocards/pcixcc/ordersoftware.shtml
  - Hardware Order Information
    - www-03.**ibm.com**/security/cryptocards/pcixcc/order.shtml
  - Crypto Support
    - www-03.**ibm.com**/security/cryptocards/pcixcc/support.shtml



Peter Spera
spera@us.ibm.com

- **Questions?**
- **Comments!**
- **Suggestions?**