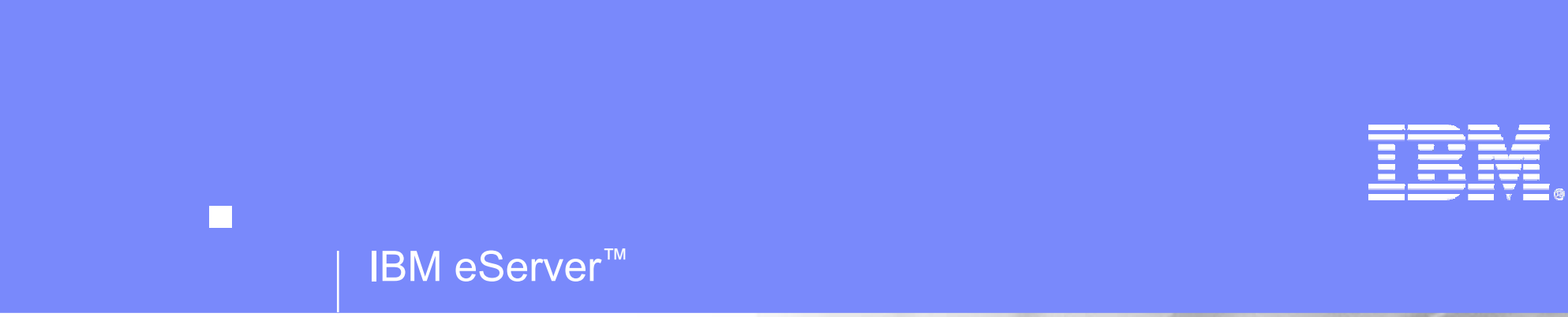


IBM eServer™

Linux for zSeries
Security

Linux Security Design

ON DEMAND BUSINESS™

Trademarks

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

DB2*
developerWorks*
Domino
HiperSockets
IBM*
IBM eServer
IBM logo
Lotus*
RACF*
RACF*
S/390*
Tivoli*
WebSphere*
z/OS*
z/VM*
zSeries*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

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 zSeries is not …

Linux® for IBM eServer™ zSeries is not z/OS®

Linux for zSeries is not RACF®

Linux for zSeries is not ICSF

Linux is …

Linux for zSeries has security-rich features.

Linux for zSeries 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.

Key Technologies Available on Linux

- Access Control
- Anti-Virus
- Cryptography
- Digital Certificates
- Directory Services
- Firewall
- Hardening
- Image Isolation
- Intrusion Detection
- Pluggable Authentication Modules (PAM)
- Security-rich Network Communication
- User Management

Linux Security on All Platforms

Access Control Lists	**SELinux, LoMac, Best Bits, IBM Tivoli® Access Manager & WebSeal, CA's eTrust Access Control & Web Access**
Anti-Virus/Anti-Spam	**ClamAV, OpenAntiVirus, AmaViS, MIMEDefrag, CA's eTrust AntiVirus, TrendMicro, REA Internet F-PROT, Roaring Penguin's CanIt**
Directory Services	**Open LDAP, IBM Directory, CA's eTrust Directory, NIS/NIS+**
Digital Certificates	**Freeware PKI, z/OS PKI Services**
Firewall	**IPTables/NetFilter, zGuard, StoneGate**
Intrusion Detection	**Snort, Snare, PortSentry, TripWire, LIDS, IPLog,** **IBM Tivoli Risk Manager, ISS RealSecure, PredatorWatch, SafeZone**

Vendor Product
Open Source Product

Linux Security for All Platforms

Security-rich 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, GSKIT, PKCS#11**
System Hardening	**Bastille, Tiger, Distributions**
Secure Data	**CFS, TCFS, ppdd, 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 zSeries**
  - **ibm.com**/zseries/os/linux/apps/sec.html or **ibm.com**/zseries/solutions/s390da/linuxproduct.html
  - 244 Participating Vendors
  - 636 Vendor Applications
- **Data Encryption**
  - McAfee's E-Business Server offers PGP encryption and compression for data transfer and storage
- **Patch Management**
  - BMC Software's SystemCheck
- **User Management**
  - Blockade Systems' Syncserv

AntiVirus

- **Communigate Pro Messaging Server**
  - Antivirus and anti-spam
- **McAfee**
  - Virus scanning
- **TrendMicro**
  - ServerProtect - HTTP, FTP & file serving
  - ScanMail for Lotus® Domino™
- **RAE Internet / F-PROT AntiVirus**
  - Mail and file serving
  - Message Processing Platform (MPP)

Firewall

- **IP Tables**
  - basic IP filtering
- **StoneGate**
  - from StoneSoft
  - High availability
  - IDS (scriptable)
  - VPN
- **zGuard**
  - From fbit/becom
  - Virus scanning
  - Basic IDS (logging and reporting)
  - VPN

Intrusion Detection

- **SafeZoneNet**
  - from LG N-SYS
- **PredatorWatch Auditor**
  - from PredatorWatch, Inc.
- **Tivoli Risk Manager**
  - From IBM
  - Web, Network & Host support

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

Linux Security Objectives

- Enable the System Integrity of the Linux for zSeries Kernel.
- Allow the Linux for zSeries 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 zSeries or may need to be developed internally.
- Enable that the Linux for zSeries offering to take advantage of zSeries cryptographic offerings.
- Provide security solutions as needed to enable Linux for zSeries to take advantage of or complement the overall zSeries Security Strategy and Architecture.

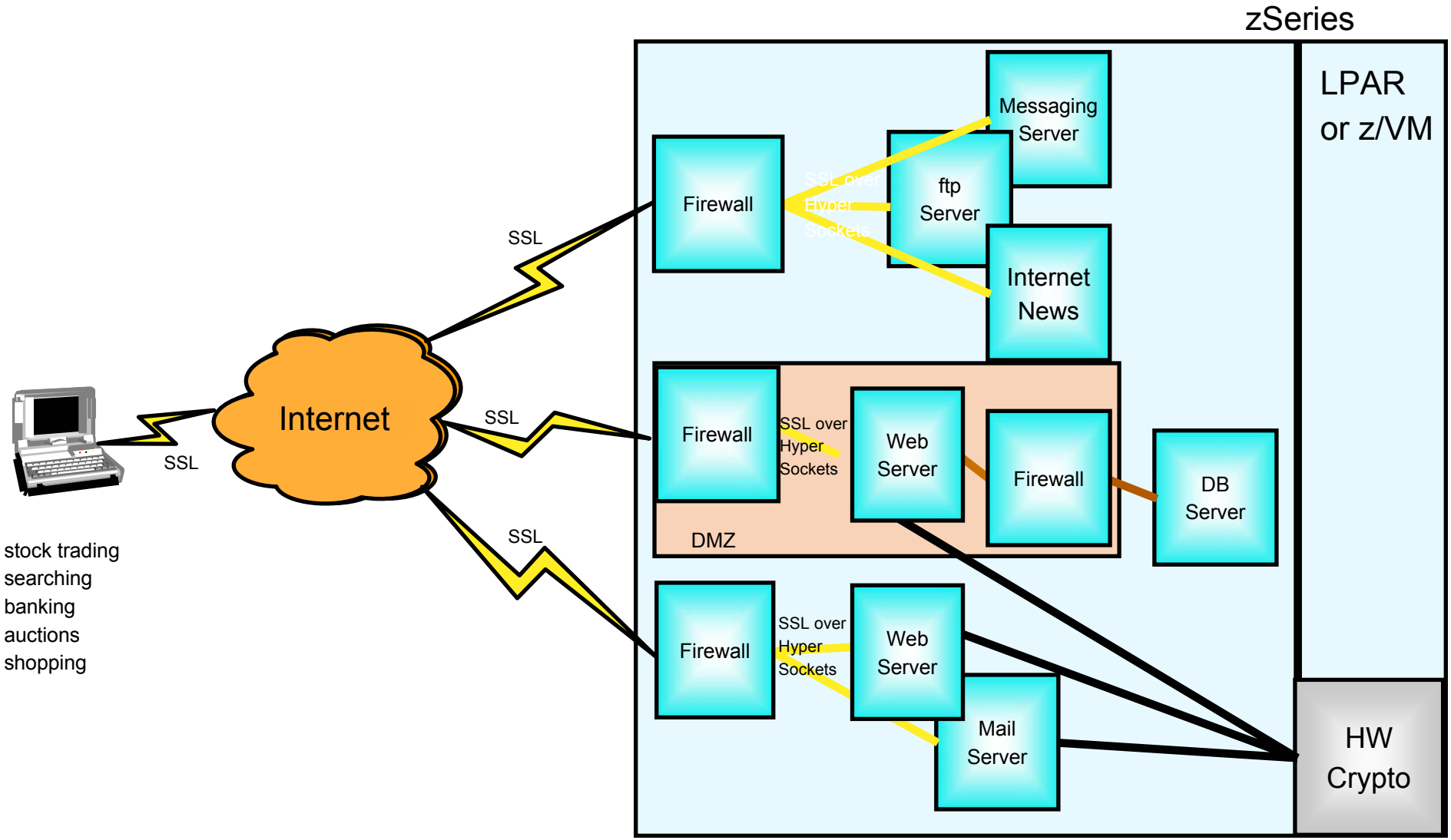
zSeries Advantage

- **Image Isolation**
  - LPAR
  - z/VM®
- **Hardware Encryption**
  - Asymmetric Algorithm (SSL) provides performance enhancements
  - PCICC, PCICA PCIXCC and CEX2C
  - Symmetric Instructions - DES, TDES and SHA-1
- **HiperSockets™ Provide Physical Security**
- **IBM Directory**
- **Tivoli's Access Manager and AM-OS provide enforcement and management of security policy across platforms**
- **Tivoli's MQSeries®**
- **Tivoli's Risk Manager provides Host, Network and Web IDS**

Synergy with z/OS

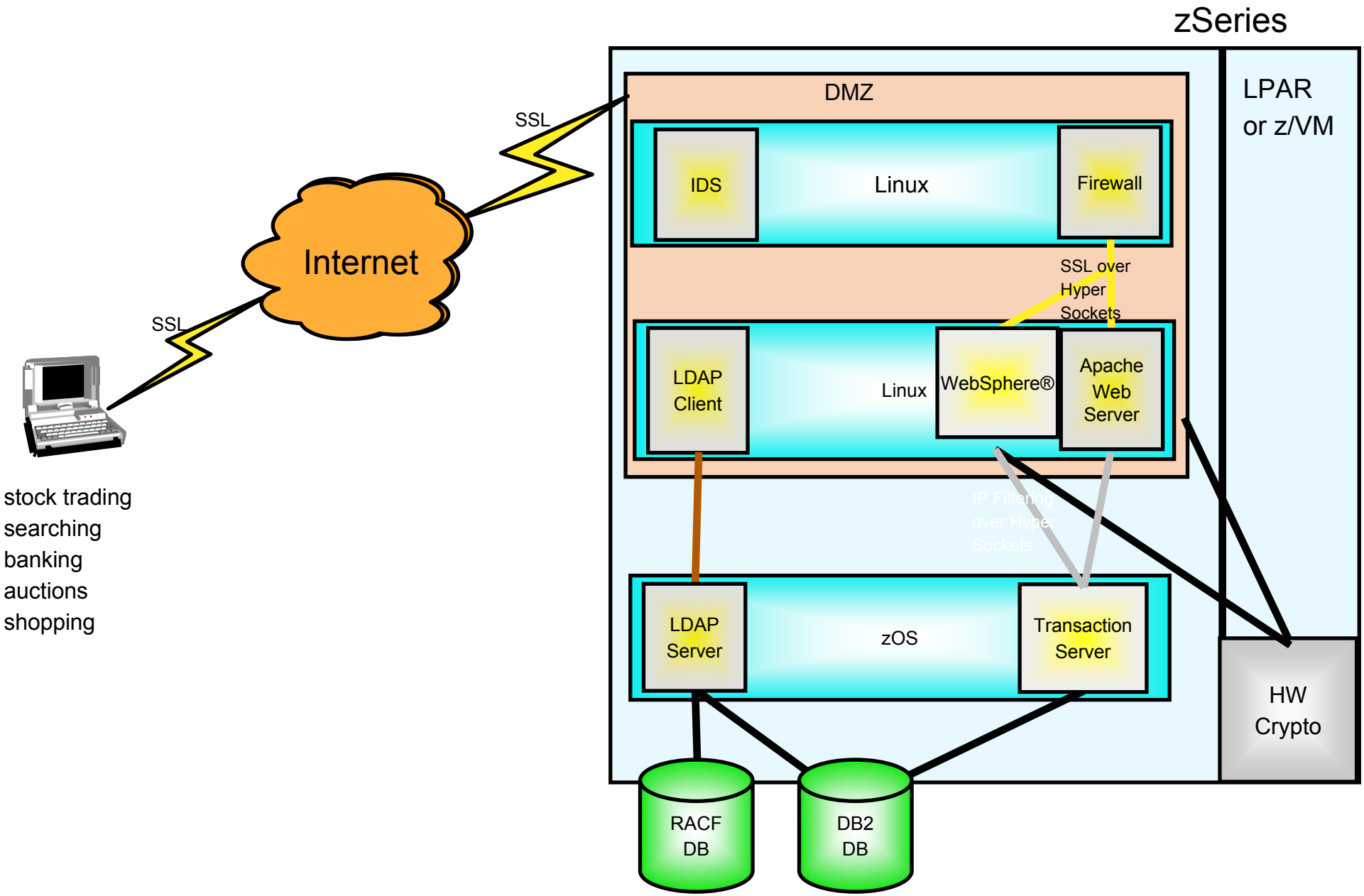
- **Centralized Authentication**
  - Integrated LDAP
  - Backed by RACF or DB2®
- **Public Key Infrastructure (PKI)**
  - Public/Private Key Pair
    - Confidentiality and Data Integrity
  - RACF's Digital Certificate Support
    - Life Cycle Management (create, manage, store, distribute, verify)
    - z/OS as Certificate Authority (trusted third party)
  - SSL Support

Application Server Integration Example



Server Farms: Single purpose Internet-related servers

Network Integration Example



stock trading
searching
banking
auctions
shopping

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
- **z/VM**
  - Statement of System Integrity
  - Common Criteria
    - Status: in evaluation
    - EAL 3+
      - LSPP – Labeled Security Protection Profile
      - CAPP – Controlled Access Protection Profile

Linux on zSeries Certification

- **Common Criteria**
  - CAPP
    - Controlled Access Protection Profile
    - Created by NSA
    - Audit, Access Control, etc.
  - Evaluation Assurance Level
    - EAL 3 = methodically tested and checked
    - EAL 4 = methodically designed, tested and reviewed
    - + = Maintenance
- **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

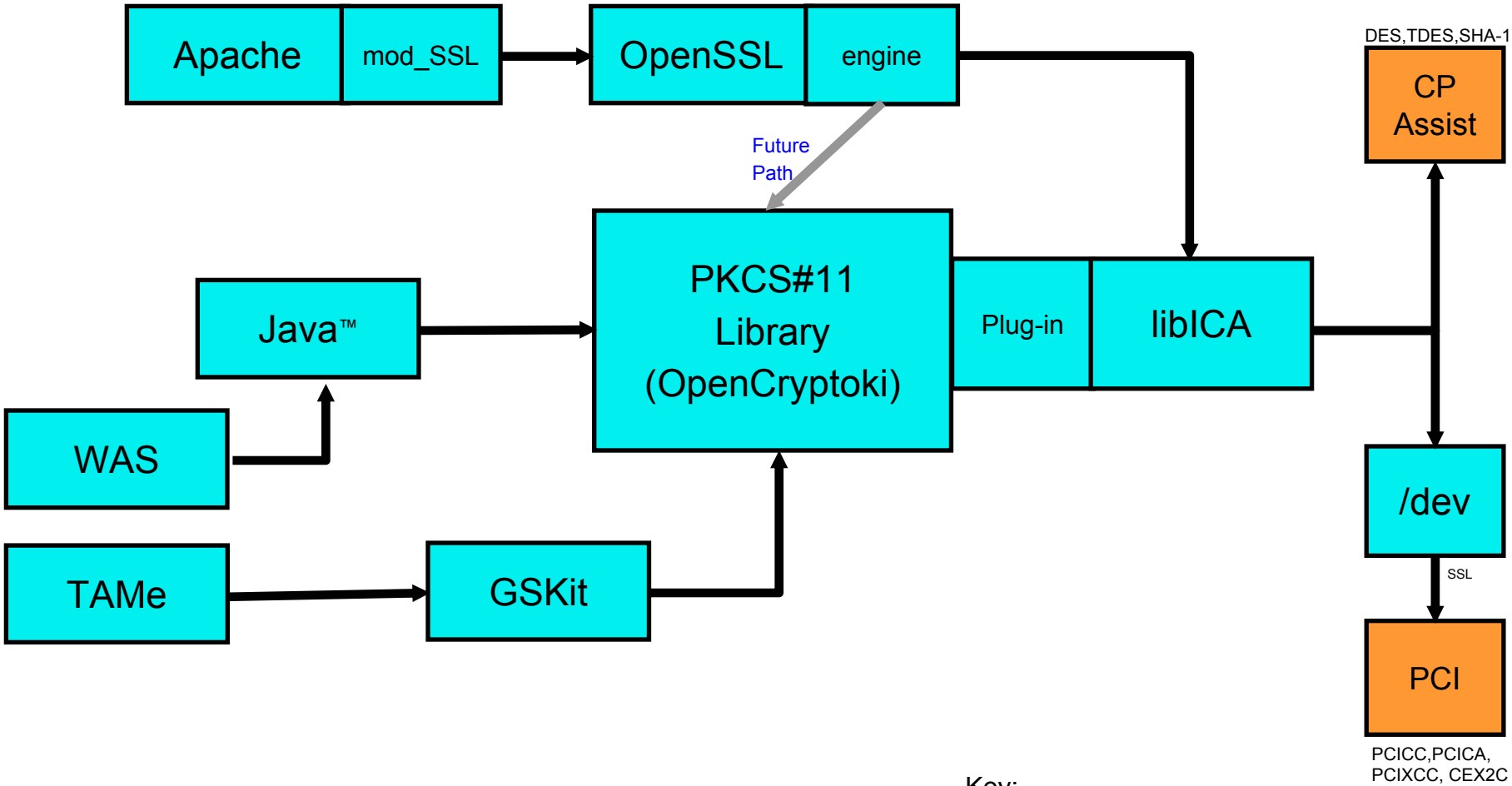
Linux Technology Center

- **Crypto Support**
  - developerWorks®
    - www.**ibm.com**/developerworks
    - z990 Crypt Device Driver
    - OpenSSL patches
    - libICA
    - OpenCryptoki (PKCS#11)
- **Enterprise Identity Mapping (EIM)**
  - www.**ibm.com**/servers/eserver/security/eim/
- **Certifications**
  - CC, DIICOE, FIPS software

Cryptography

- **Hardware**
  - Asymmetric
    - RSA handshake
      - PCICC with ~200 handshakes/second/card
      - PCICA with ~1000 handshakes/second/card
      - PCIXCC with ~ 1000 handshakes/second/card
      - CEX2C with ~ 1000 handshakes/second/card
  - Symmetric
    - DES
    - TDES
    - SHA-1
- **Software Libraries for crypto access**
  - OpenSSL
  - PKCS#11 library
  - GSKit

Hardware Crypto Exploitation



Future Direction

- **Parts**
  - AV, Hardware Crypto, Firewall, IDS, etc.
- **Synergy**
  - z/VM integration
  - z/OS synergy
  - Security-rich management of operating environment - ssh, VPN (IPSec), etc.
  - Security-rich management of user domain - LDAP, RACF, Tivoli, etc.
  - Continued certification of Linux for zSeries and applications
  - Tooling, both hardware and software, to build a secure operating and application environment in support of Web applications, Web hosting, e-Utilities, on-demand, firewall, IDS, Enduring Value, etc.
  - End-to-end solutions and ethical hacking

zSeries Security White Papers and Redbook

- ***Linux on zSeries Security White Paper***
  - GM13-0488
- ***Linux Security: Exploring Open Source Security for a Linux Server Environment***
  - GM13-0636
- ***z/VM Security and Integrity***
  - GM13-0145
- ***Linux on IBM eServer zSeries and S/390: Best Security Practices***
  - SG24-7023

Security Sites

- **General Security**
  - www.linuxsecurity.com
  - www.securityportal.com
  - www.ibm.com/developerworks
- **Security Vendors**
  - www.raeinternet.com
  - www.trendmicro.com
  - www.stonesoft.com
  - www.zguard.de
  - ca.com/solutions/linux
- **Secure Distributions**
  - nsa.gov/selinux
  - www.immunix.org
  - www.rsbac.org
- **Security Related Tools**
  - www.apache-ssl.org
  - www.bastille-linux.org
  - www.openssl.org
  - www.tripwire.org
  - www.tripwiresecurity.com
  - linux-firewall-tools.com/linux

Questions

To: Peter Spera
IBM Corp.
2455 South Road, MS P328
Poughkeepsie, NY 12601
spera@us.ibm.com