Vanguard Security Solutions & RACF User Training
Session RTB 13
June, 2008

z/OS Security Componentry Today, plus Trends and Directions

Rich Guski CISSP
IBM Senior Technical Staff Member
zSeries Software Security Architecture

ON DEMAND BUSINESS™

Abstract

RACF, PKI, Kerberos, LDAP, Communications Server, WebSphere, and heritage applications; this presentation takes a survey view of z/OS security and the rich set of functions that have evolved in reflection of the flexibility and richness of z/OS itself. Besides adding clarification to your understanding of the topology of z/OS security today, the presenter will discuss important trends that are expected to affect the future.

Trademarks

See url http://www.ibm.com/legal/copytrade.shtml for a list of IBM trademarks

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

BSAFE
Identrus
IdenTrust
Vanguard Products

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

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.

Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

Agenda

- ➡ **Our corner of the industry**
- **Topology of security on z/OS®**
  - Cryptography
  - RACF® and LDAP (z/OS Directory Server)
  - Security Functions for Communications (Servers and Protocols)
  - Adding users and resources to the picture
  - WebSphere® Application Server (WAS) – Connection to the Internet
  - Role of Tivoli® products
  - Role of Vanguard products
- **Survey of z/OS recent security enhancements**
- **z/OS Certifications**
- **z/OS Security Strategic Objectives**
- **Directions**
- Closing remarks

Our corner of the Industry

Fundamental Computer Security Disciplines

- **Identification & Authentication (implies: user registry, authenticators)**
  - Identify users, allows for accountability
- **Access Control (implies: resource registry, access rules, resource managers)**
  - Controlling access to logical objects (files, programs, methods, HW interfaces, etc.)
- **Auditing**
  - Verification of security policy enforcement, intrusion detection (log files, procedures)
- **Cryptography**
  - Data Confidentiality: security-rich environment for storage and transport of information (banking industry, Internet applications)
  - Advanced user authentication (Kerberos, PKI, PassTickets)
- **System Integrity**
  - Security mechanisms designed so that they cannot be illegitimately bypassed
- **Intrusion Defense**
  - Inhibit malicious attacks against computing infrastructure

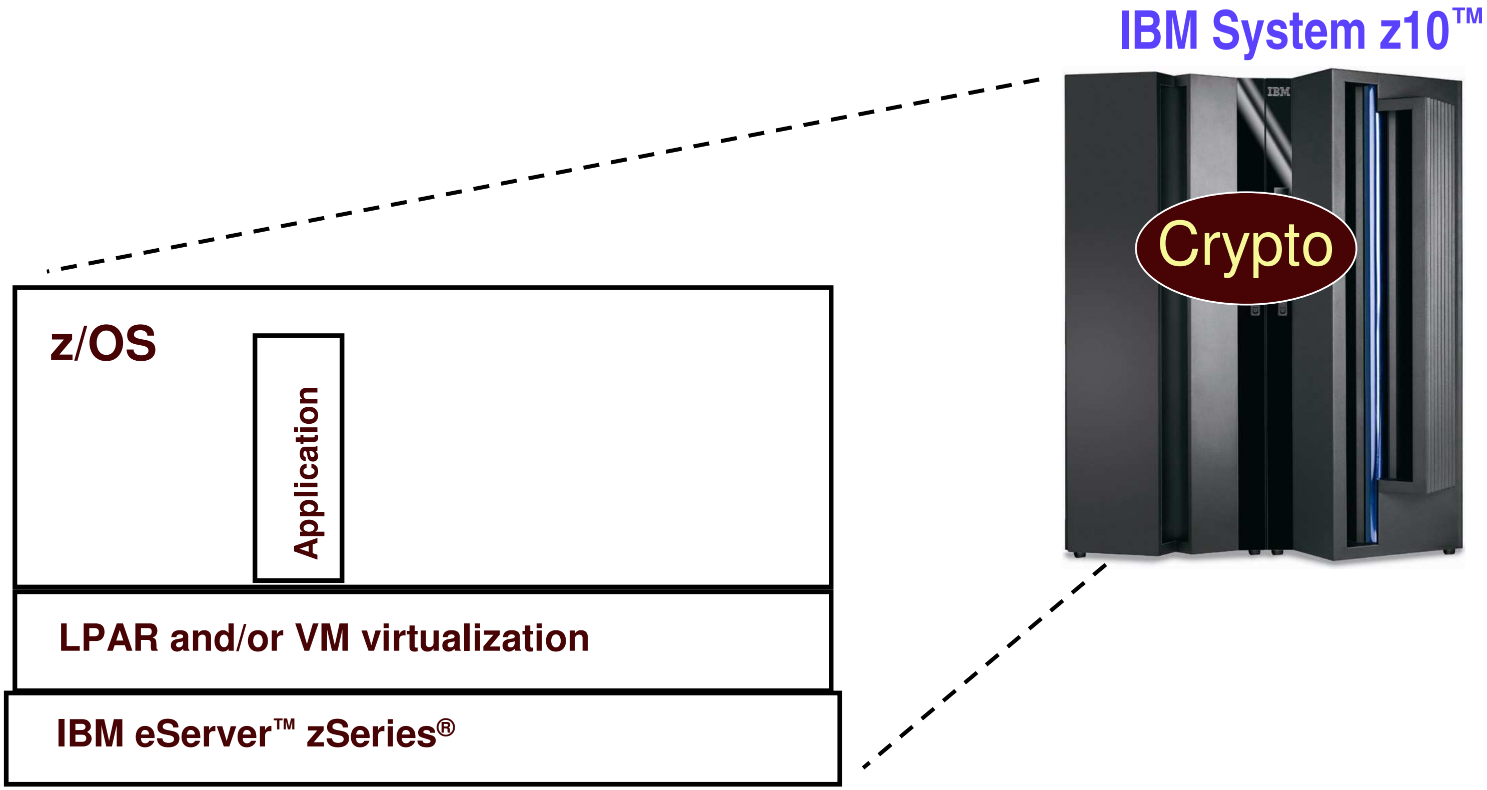
Applying Security Disciplines to:

- **Platforms, networks, middleware, applications**

Agenda

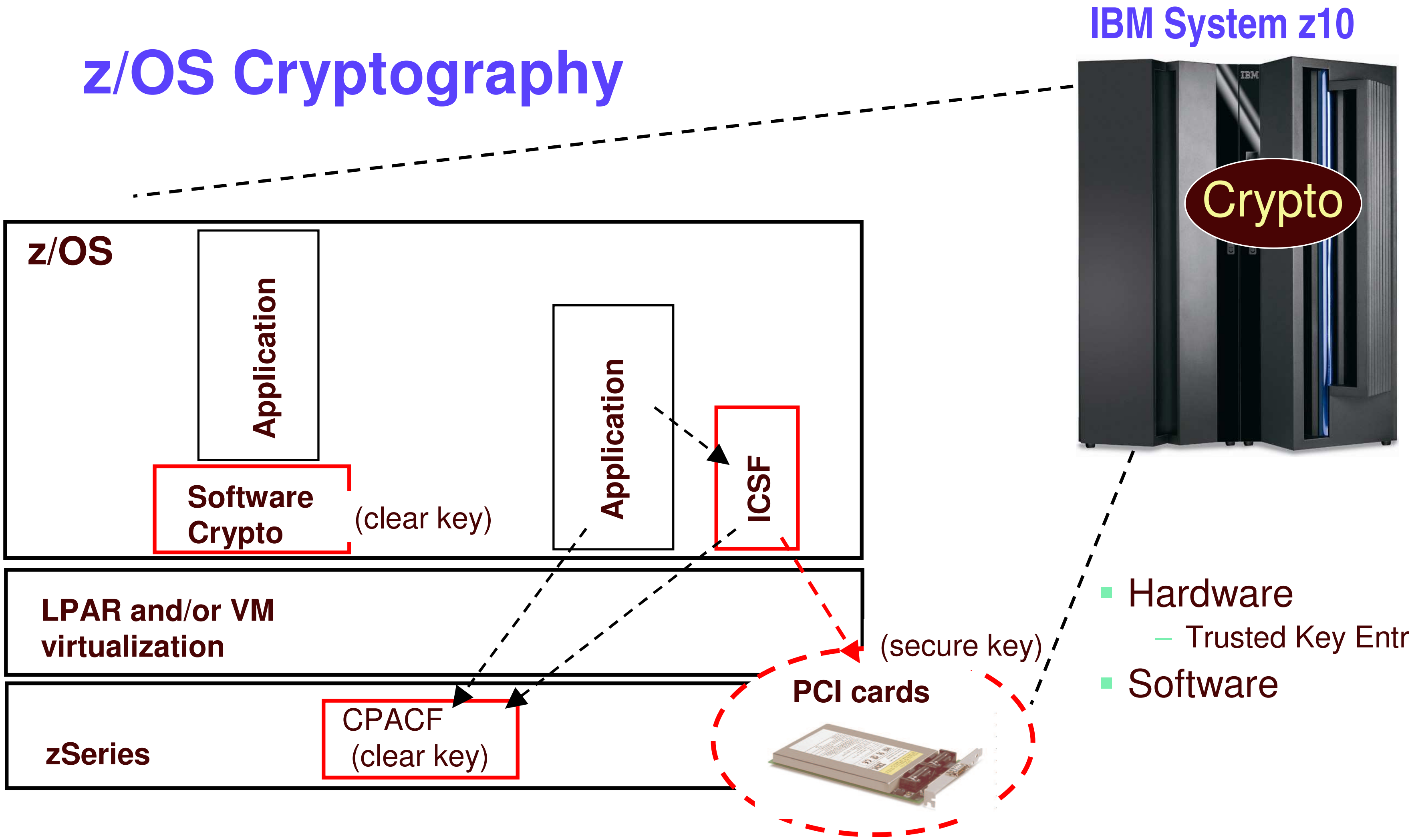
- Our corner of the industry
- Topology of security on z/OS
  - Cryptography
  - RACF and LDAP (z/OS Directory Server)
  - Security functions for Communications (Servers and Protocols)
  - Adding users and resources to the picture
  - WAS – Connection to the Internet
  - Role of Tivoli Products
  - Role of Vanguard products
- Survey of z/OS recent security enhancements
- z/OS Certifications
- z/OS Security Strategic Objectives
- Directions
- Closing remarks

z/OS security starts with hardware that had security designed in from the beginning



- Storage protection keys
- EAL5 Certified LPARs
- Hardware Cryptography

z/OS Cryptography



- Hardware
  - Trusted Key Entry
- Software

Crypto accessible via multiple language paths; from assembler for clear key crypto to CCA, OCSF, and Java™ interfaces to secure key HW assisted crypto.

Explaining the z/OS 3 crypto sweet spots

(clear key)

Software Crypto

Engines:
- BSAFE
- CDSA-OCSF
- RACF
- ICSF

Functions:
- RSA (encrypt, decrypt)
- Diffie-Hellman
- SHA
- DSA
- AES

Exploiters:
- SSL
- LDAP
- RACF
- Etc..

Internet business requires functions that may be supported in SW

(clear key)

CPACF

Functions:
- Very high performance
  - AES-128, DES, TDES
  - SHA

Very high performance needed e.g. by SSL

ICSF

(secure key)

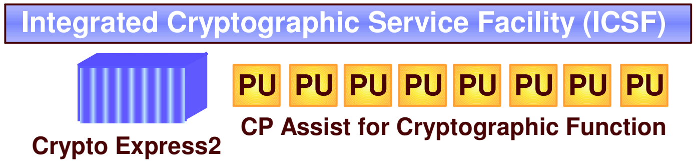
PCI (CEX2)

Functions:
- ATM support
- DES, TDES
- SHA
- Trusted Key Entry

Exploiters:
- Banking Industry
- RACF

Banking industry and possible government markets are expected to require security of HW

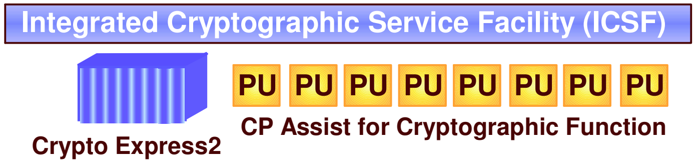
Z10 EC CPACF Support


Integrated Cryptographic Service Facility (ICSF)
Crypto Express2
PU PU PU PU PU PU PU PU
CP Assist for Cryptographic Function

- **CP Assist for Cryptographic Function (CPACF)**
  - Available for CPs and IFLs
    - 1 CPACF for every 2 CPs
  - High performance clear key symmetric encryption/decryption
    - Advanced Encryption Standard (AES) - 192 bit and 256 bit NEW
    - Triple DES / DES
    - Requires no charge enablement feature
  - High performance clear key hashing
    - Secure Hash Algorithm (SHA)-512 NEW
    - SHA-1
    - Shipped enabled on all systems
  - High performance Pseudo Random Number Generator (PRNG)
    - Requires no-charge enablement feature
    - Not exploited by ICSF
  - Called via ICSF API or Problem State Instructions
  - Performance information for z9 EC/BC and earlier can be found on www-03.ibm.com/servers/eserver/zseries/security/cryptography.html

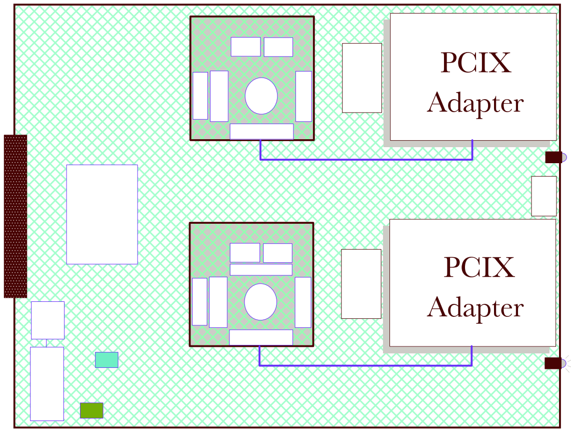
* Performance is in External Throughput Rate (ETR) based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, 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 rates stated here.

Z10 EC Cryptographic Coprocessor


Integrated Cryptographic Service Facility (ICSF)
Crypto Express2
PU PU PU PU PU PU PU PU
CP Assist for Cryptographic Function

Crypto Express2 Coprocessor (CEX2C)

- Default configuration for Crypto Express2 feature
  - Provides secure-key cryptographic coprocessor functions
  - Provides cryptographic key management
  - Provides SSL acceleration
- Scalable - 0 to 8 features
  - Minimum purchase increment is two
- Configurable via HMC (Hardware Management Console)
  - 0, 1, or 2 coprocessors per feature
  - Individually by PCIX adapter, see options below
- Current applications expected to run without change
- Connection to STI interface; no external cables
- Fully programmable, User Defined Extensions (UDX) support
- Designed for FIPS 140-2 Level 4 Certification (Cert #661)
- Trusted Key Entry (TKE) 5.0 support
  - Supports Crypto Express2 coprocessor
  - Smart Card Reader support
- Note: PCIXCC cannot be carried forward to z9, or z10
  - Replaced by Crypto Express2 Coprocessor



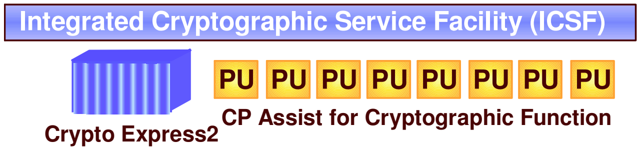
Configuration Options

- **Coprocessor / Coprocessor**
- **Coprocessor / Accelerator**
- **Accelerator / Accelerator**

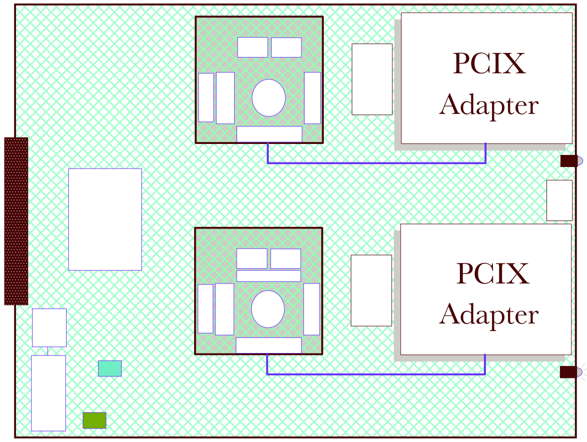
Accelerator discussed on next chart

All z10 cryptographic features are managed under z/OS by ICSF for optimum performance!

Z10 EC Cryptographic Accelerator

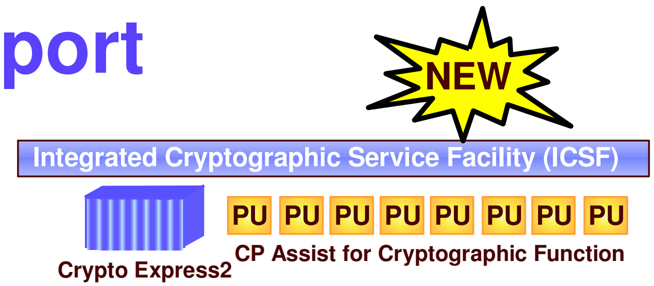

Integrated Cryptographic Service Facility (ICSF)
PU PU PU PU PU PU PU PU
CP Assist for Cryptographic Function
Crypto Express2

- **Crypto Express2 Accelerator (CEX2A)**
  - Non-default configuration for Crypto Express2 feature
    - Provides SSL acceleration functions only
  - Scalable - 0 to 8 features
    - Minimum purchase increment is two
  - Configurable via HMC
    - 0, 1, or 2 accelerators per feature
    - Individually by PCIX adapter
  - High performance public key (RSA) acceleration
  - Hardware acceleration for Secure Sockets Layer (SSL transactions)*
    - Greater than 3,000 SSL handshakes/sec. (single accelerator)
    - Greater than 6,000 SSL handshakes/sec. (single feature w/ 2 accelerators)
  - Connection to STI interface; no external cables
  - Note: PCIXCC cannot be carried forward to z9, or z10
    - Replaced by Crypto Express2 Accelerator



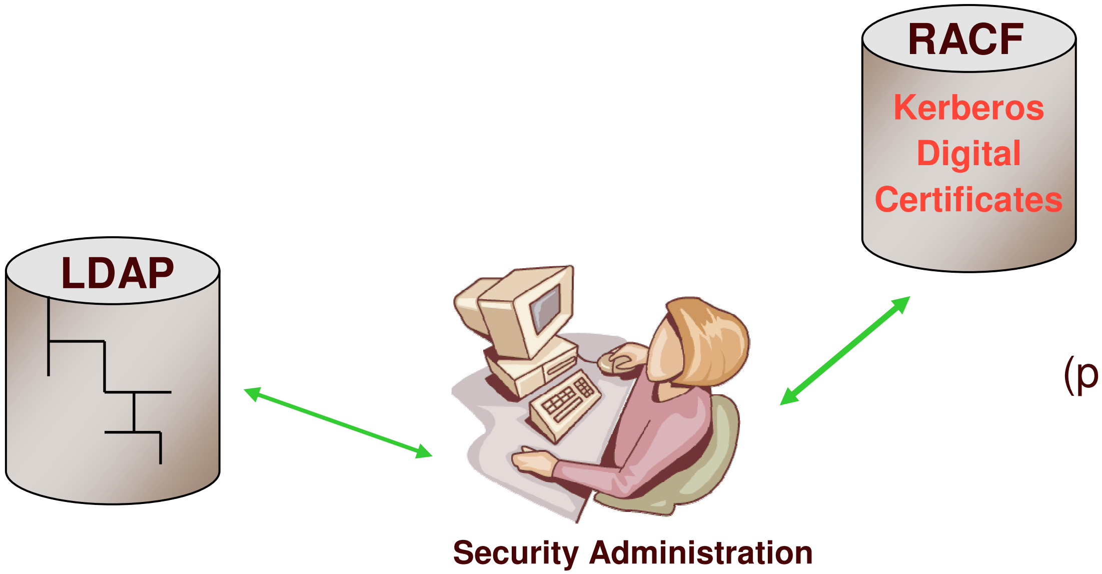
* Performance is in External Throughput Rate (ETR) based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, 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 rates stated here.

ATM Remote Key Loading Support


NEW
Integrated Cryptographic Service Facility (ICSF)
PU
PU
PU
PU
PU
PU
PU
PU
Crypto Express2
CP Assist for Cryptographic Function

- **ATM Remote Key Loading**
  - The ability to securely load initial keys to an ATM from a remote location
  - Enhanced capabilities for exchanging keys with non-CCA cryptographic systems
    - **Uses new ISO 16609 CBC Mode TDES MAC service**
- **Remote Loading of Initial ATM Keys**
  - Distribution of initial key encrypting keys (KEKs) to a newly installed ATM.
  - Distribution of operational keys or replacement KEKs, enciphered under a KEK currently installed in the ATM.
- **Automatic Teller Machines and POS Standards:**
  - ISO/IEC 11770-3: Information Technology, Security Techniques, Key Management, Part 3: Mechanisms Using Asymmetric Techniques.
  - ANS X9.24-2 : Retail Financial Services, Symmetric Key Management, Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Key
- **System z9 EC/BC and System z10**
- **Code for Enhancements to Cryptographic Support for z/OS V1R6/R7**
  - (ICSF Web Deliverable)

z/OS Security Server (RACF) and z/OS Directory Server (LDAP)



RACF
(priced feature)

- ✓ Users
  - Groups & Roles
- ✓ Resources
  - Access rules
    - DAC, MLS
  - Audit controls

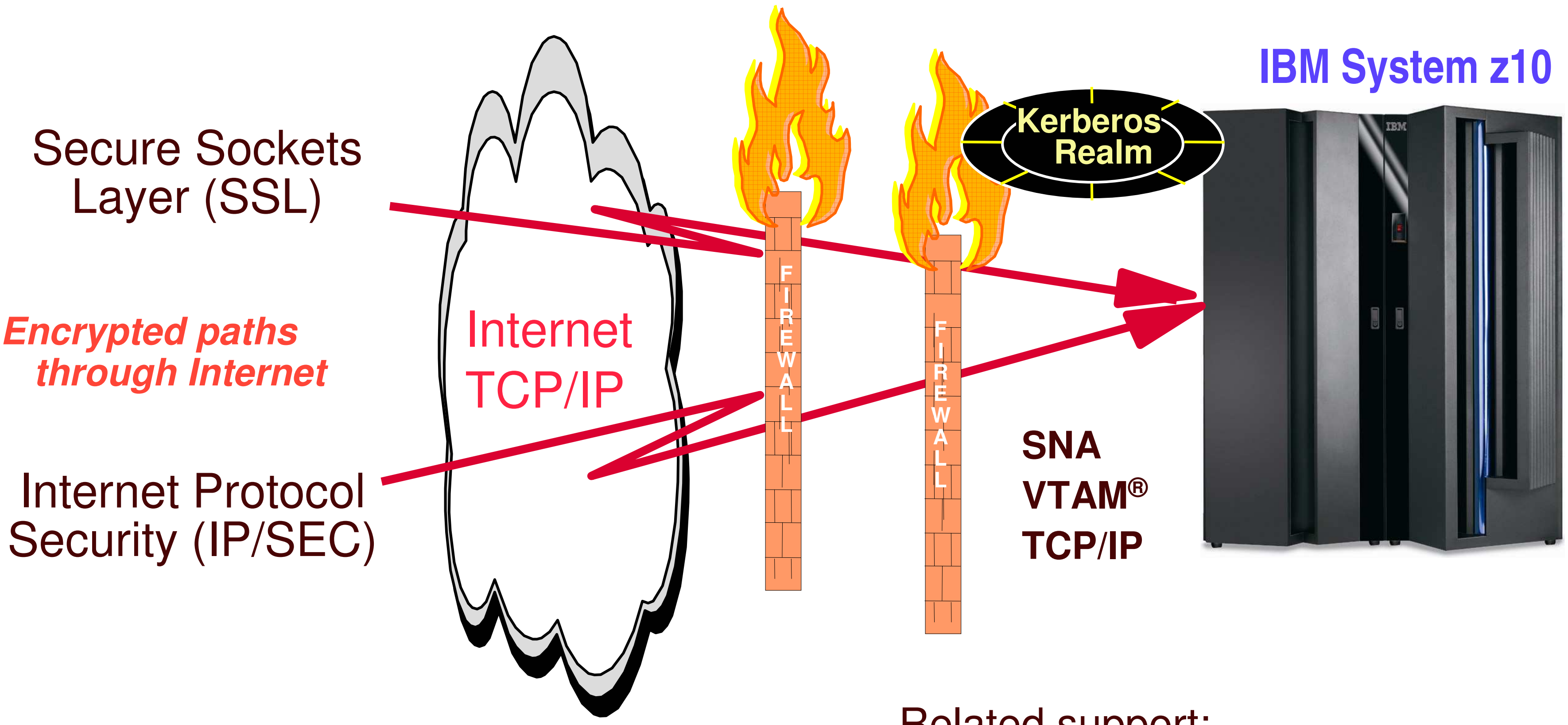
- Identification
- Access Control
  - **Who** (user identification)
  - Has access to **What**
- Auditing
- Administration

z/OS Directory Server

- Light Directory Access Protocol (LDAP)
- Distributed directory services
- Where users and servers are in the distributed world
- Distributed authentication
- "Communication protocol", to other registries and into RACF

DAC = Discretionary Access Control
MLS = Multi-Level Security

Communication Protocols and Security



Secure Sockets Layer (SSL)

Encrypted paths through Internet

Internet Protocol Security (IP/SEC)

Internet TCP/IP

IBM System z10

Kerberos Realm

SNA
VTAM®
TCP/IP

Z/OS Communications Server Function

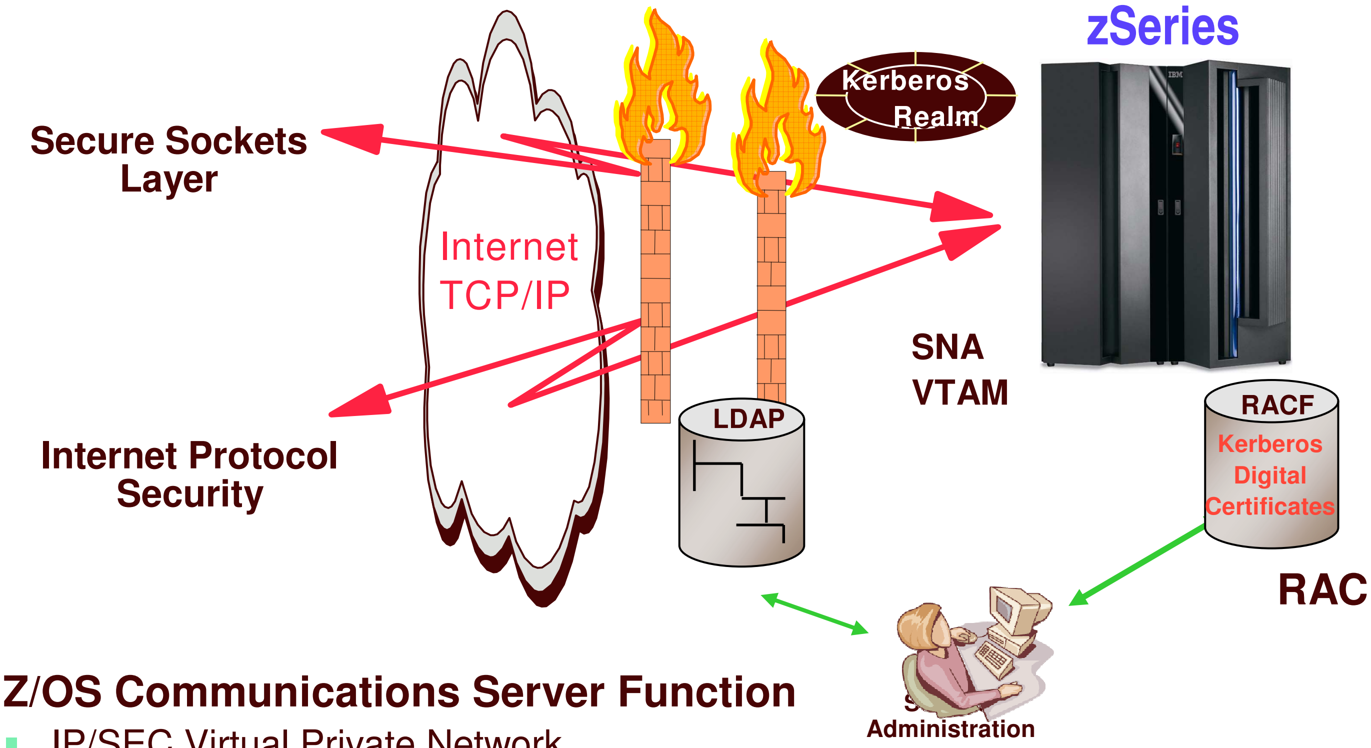
- IP/SEC Virtual Private Networking
- Z/OS Firewall function
- Intrusion Defense

Related support:

✓Kerberos and GSSAPI
✓PKI

Putting things together so far

(Typical z/OS “baseline” security functional environment)



RACF

- ✓ Users
  - Groups & Roles
- ✓ Resources
  - Access rules
    - DAC, MLS
  - Audit controls

Z/OS Communications Server Function

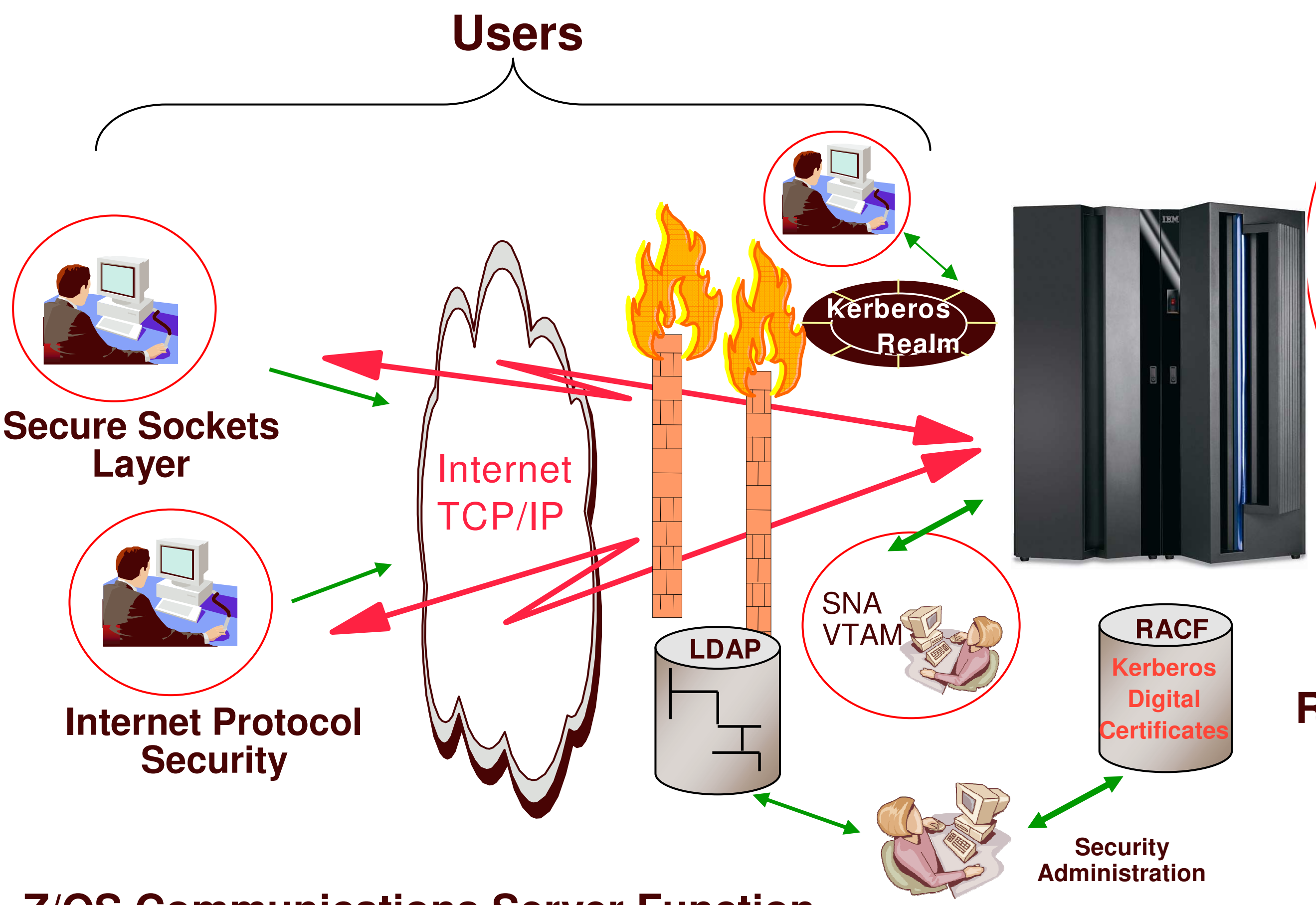
- IP/SEC Virtual Private Network
- Z/OS Firewall function
- Intrusion Defense

Light Directory Access Protocol

- Distributed directory services
- Where users and servers are in the distributed world

- Identification
- Access Control
  - **Who** (user identification)
  - Has access to **What**
- Auditing
- Security Administration

Adding users and resources…



Resources

- ✓ Applications
  - WebSphere, MQ, etc.
- ✓ Transactions
  - CICS®, IMS™
- ✓ Databases
  - DB2®
- ✓ Programs
- ✓ Files etc..

RACF

- ✓ Users
  - Groups & Roles
- ✓ Resources
  - Access rules
    - DAC, MLS
  - Audit controls

Z/OS Communications Server Function

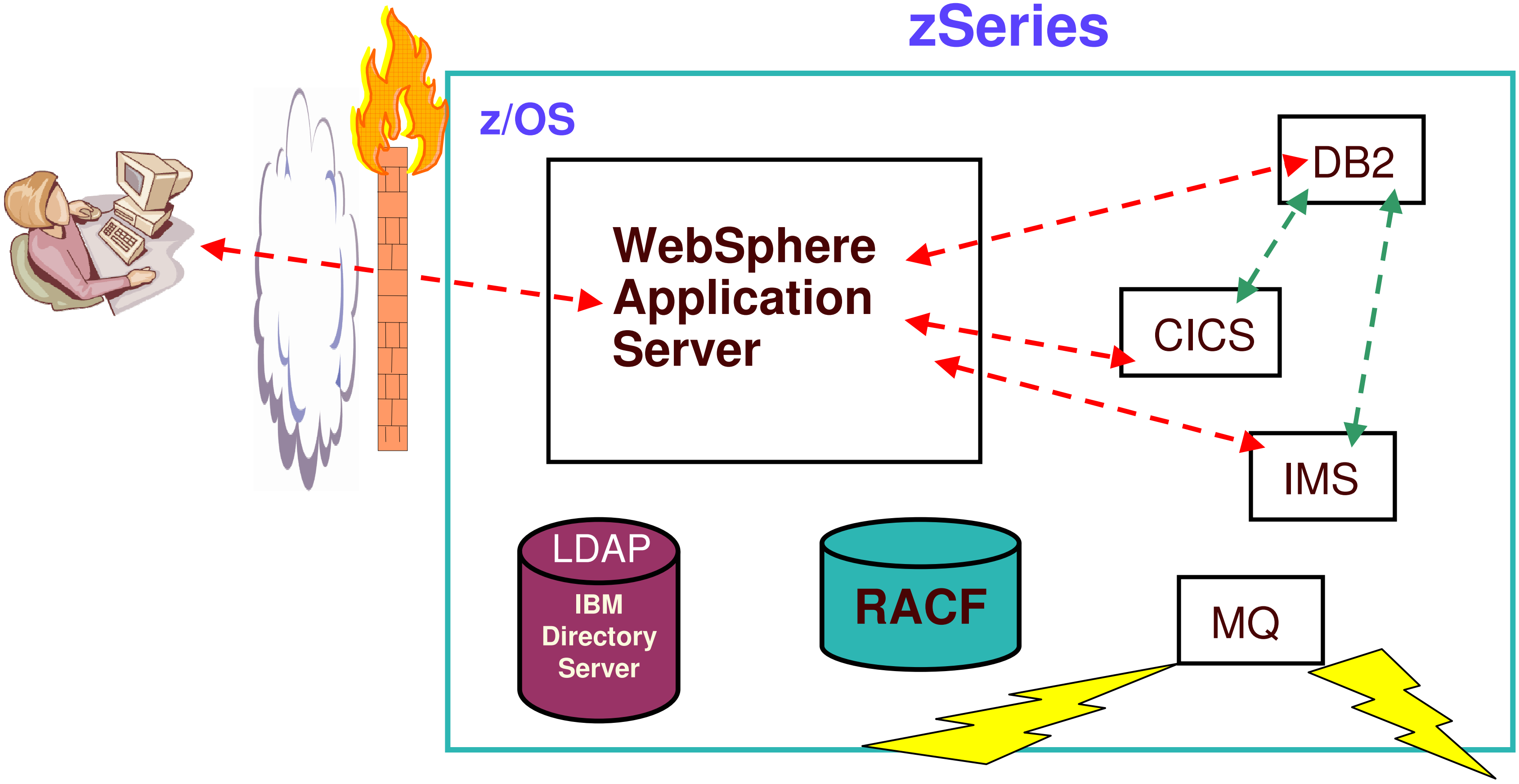
- IPsec Virtual Private Network
- Z/OS Firewall function
- Intrusion Defense

Light Directory Access Protocol

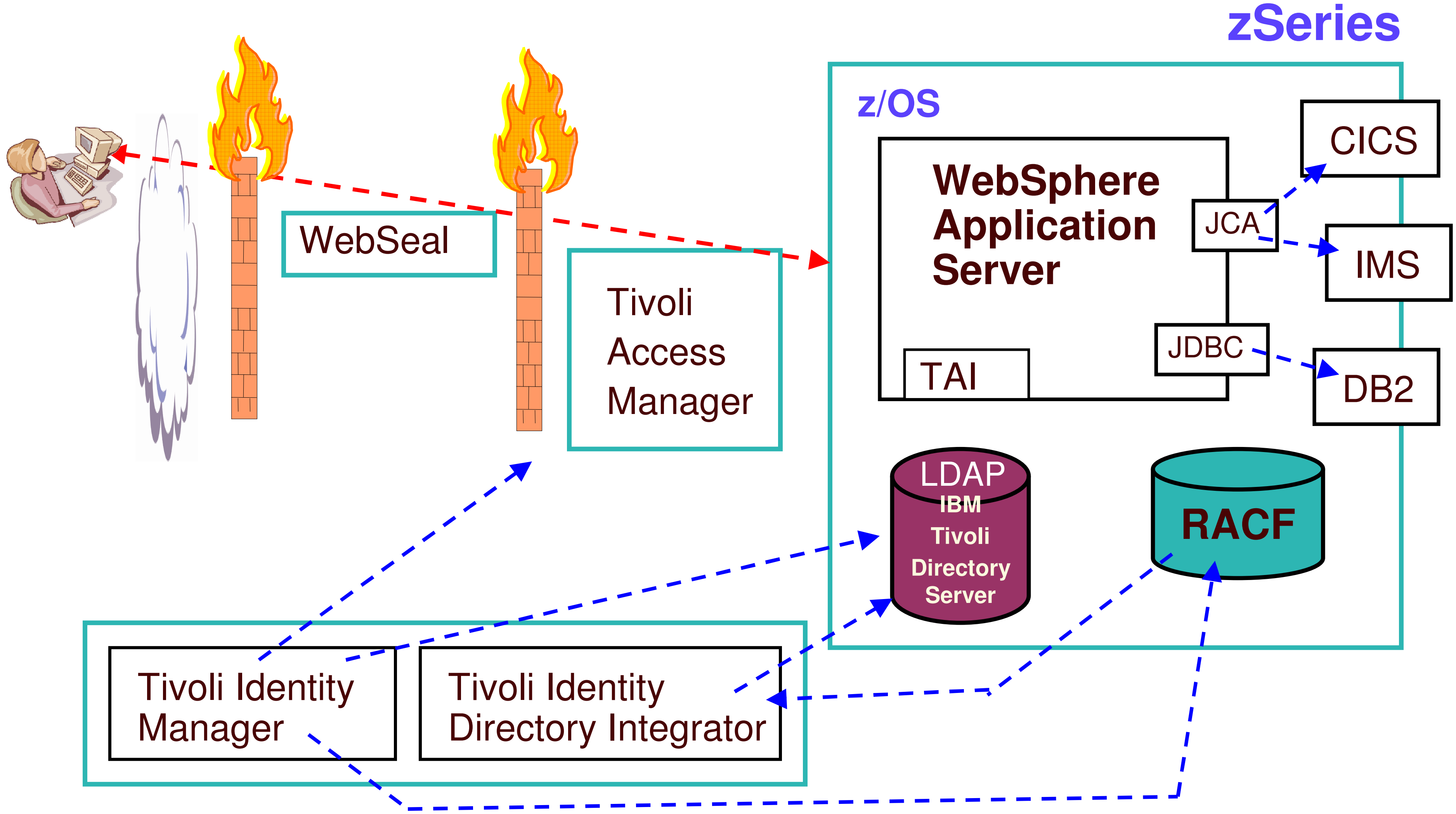
- Distributed directory services
- Where users and servers are in the distributed world

- Identification
- Access Control
  - **Who** (user identification)
  - Has access to **What**
- Auditing
- Security Administration

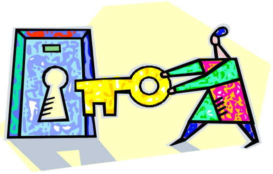
WAS – a connection to the Internet



Role of Tivoli products


zSeries
z/OS
WebSphere Application Server
JCA
JDBC
TAI
CICS
IMS
DB2
LDAP
IBM Tivoli Directory Server
RACF
WebSeal
Tivoli Access Manager
Tivoli Identity Manager
Tivoli Identity Directory Integrator

Leveraging Tivoli products for Administration



IBM Tivoli Solutions

Tivoli Federated Identity Manager

- Share identity and policy data about users and services
- A federated model simplifies administration and enables companies to extend identity and access management to third-party users and third-party services

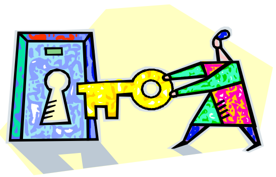
Tivoli Access Manager (TAM) for e-business

- Single Sign On and additional protection for z/OS Web servers
- Use of the IBM Directory Server on z/OS, with the option of authenticating users through RACF, TopSecret, or other security service-providing products

IBM Tivoli® Directory Integrator

- Synchronizes identity data residing in directories, databases, collaborative systems, applications used for human resources (HR), customer relationship management (CRM), and Enterprise Resource Planning (ERP), and other corporate applications

Leveraging Tivoli products for Administration



IBM Tivoli Solutions

Tivoli Federated Identity Manager

- Share identity and policy data about users and services
- A federated companies to extend identity and d third-party services

Tivoli Acce

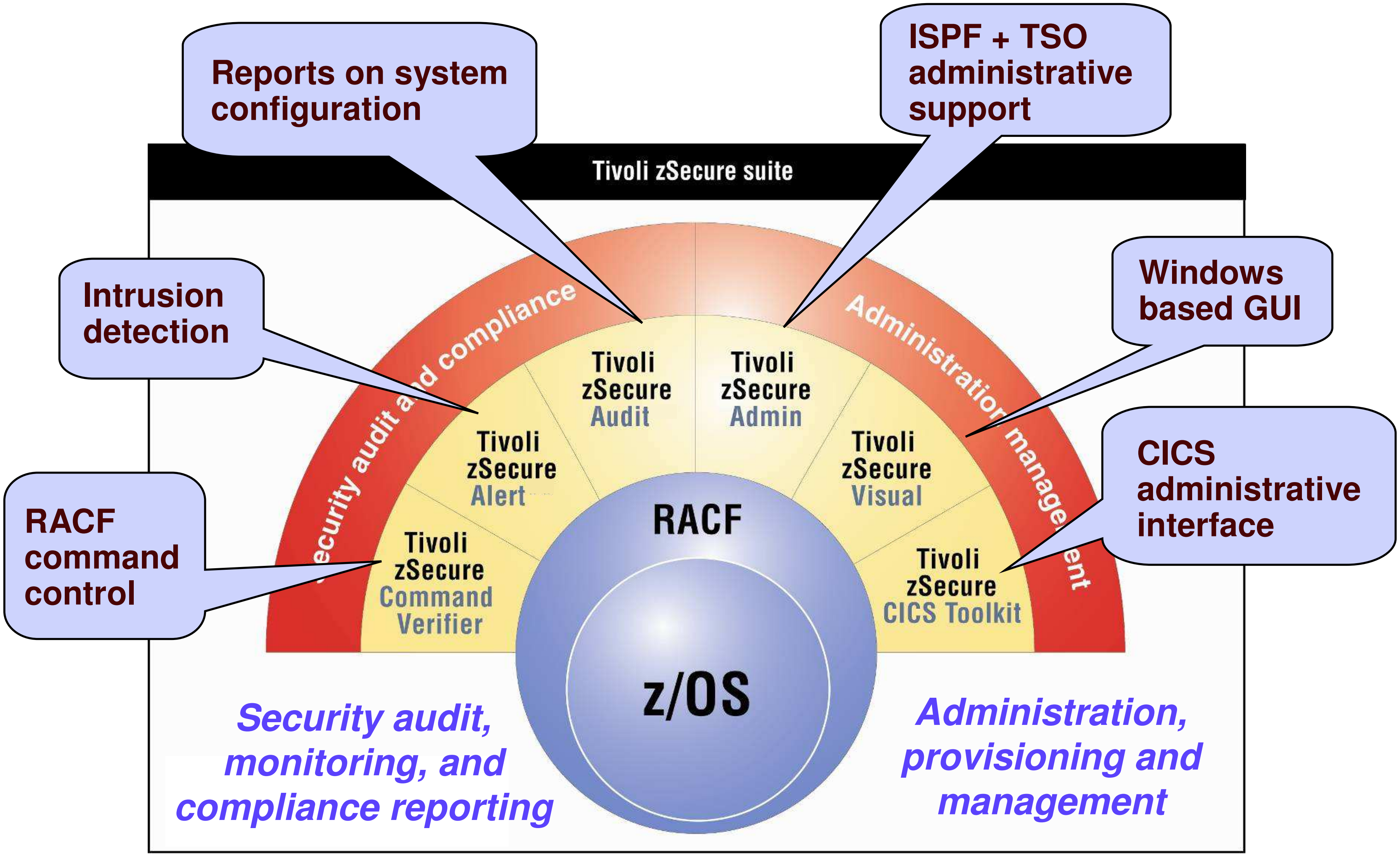
- Single Sign (servers
- Use of the IBM Directory Server on z/OS, with the option of authenticating users through RACF, TopSecret, or other security service-providing products

Repeated for page 2 of notes. Chart is hidden…

IBM Tivoli® Directory Integrator

- Synchronizes identity data residing in directories, databases, collaborative systems, applications used for human resources (HR), customer relationship management (CRM), and Enterprise Resource Planning (ERP), and other corporate applications

IBM Tivoli zSecure Suite


Tivoli zSecure suite
Security audit and compliance
Administration management
Tivoli zSecure Audit
Tivoli zSecure Admin
Tivoli zSecure Alert
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS Toolkit
RACF
z/OS

Reports on system configuration

ISPF + TSO administrative support

Intrusion detection

Windows based GUI

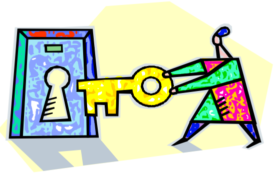
RACF command control

CICS administrative interface

Security audit, monitoring, and compliance reporting

Administration, provisioning and management

Leveraging Vanguard Administration



Vanguard Solutions

Designed to:

Help organizations comply with security regulations, help reduce the complexities of RACF administration, eliminate user errors, and enforce best practices

- **Vanguard Administrator** can help simplify and enhance RACF administration
- **Vanguard Analyzer** is designed to assist with risk assessment and threat analysis audits
- **Vanguard Enforcer** provides a host based option for intrusion detection and management
- **Vanguard Advisor** is designed to provide Event Detection, Analysis and Reporting capabilities for z/OS and RACF
- **Vanguard Security Center** offers browser-based RACF and DB2 security administration on z/OS

Summary of z/OS Security Elements

🟦 Crypto and Key Management

🟩 Network Security

🟧 Security management

🟪 Standards-audit-compliance

⬛ Resource Access Control

🟢 User I & A

Security Server (RACF)

🟧 🟪 ⬛ 🟦 🟩 🟢

ICSF / TKE

🟦

TIDS (LDAP)

⬛ 🟧 🟪 🟩 🟢

EIM

🟧

Tivoli TIM & TAM zSecure

🟧 🟪 ⬛

z/OS Communications Server

🟩 🟪

Kerberos

🟩 🟢

SSL

🟩 🟢

z/OS Encryption Facility

🟦

PKI and Digital Certificates

🟩 🟢

Encrypting Tape Drives & EKM

🟦

Resource Managers

CICS

MQ

IMS

HoD

JES

DB2

TSO

WebSphere Java programming

Web Services Security

Agenda

- Our corner of the industry
- Topology of security on z/OS
  - Cryptography
  - RACF and LDAP (z/OS Directory Server)
  - Security Functions for Communications (Servers and Protocols)
  - Adding users and resources to the picture
  - WAS – Connection to the Internet
  - Role of Tivoli Products
  - Role of Vanguard products
- **Survey of z/OS recent security enhancements**
- z/OS Certifications
- z/OS Security Strategic Objectives
- Directions
- Closing remarks

Survey of z/OS R9 Security Enhancements

Looking at recent enhancements can shed light on emerging trends

General Availability was October of 2007

- **PKCS #11 support** (alternative to proprietary CCA)
  - **ICSF**
  - **RACF**

- PKCS (Public Key Cryptography Standards) is offered by RSA Laboratories of RSA Security Inc. (TM) PKCS #11, also known as Cryptoki, is the cryptographic token interface standard. It specifies an application programming interface (API) to devices, referred to as tokens. The PKCS #11 API is an industry-accepted standard commonly used by cryptographic applications. PKCS #11 applications developed for other platforms can be recompiled and run on z/OS.

continued ↘

Survey of z/OS R9 Security Enhancements…

- **RACF**
  - **Java Interface to administer / query RACF user / group profiles**
  - **Password Phrase extension**
    - **9-13 characters will be supported when activated by a RACF exit**
    - **Sample exit provided**
- **Network Authentication Service (Kerberos)**
  - **AES added to crypto suite**
- **System SSL**
  - **Tuning capabilities for CRL checking**
  - **Callback re-handshake notification**
  - **Hostname validation granularity**
  - **Notification on switch from HW crypto to software**

continued ↘

Survey of z/OS R9 Security Enhancements…

- **PKI Services**
  - **Writable SAF keyrings**
  - **Support of certificates with two byte UTF8 chars** (that can be mapped to code page 1047)
  - **e-mail notification for the PKI administrator for pending certificate requests**
  - **Max limit of certificate validity period - change from 3650 days to 9999 days**
  - **Query on expiring certificates based on the number of days until expiration**
  - **Automated certificate renewal to send renewal certificates via e-mail when the expiration dates for older certificates are approaching**
  - **A new REFRESH reminder message is planned to be issued after changes made to a certificate or a certificate filter profile through the RACDCERT command, to indicate that a refresh to the DIGTCERT or DIGTMAP class is needed after the affected RACDCERT commands when the DIGTCERT or DIGTNMAP class is RACLISTed**
  - **The generation of unused serial numbers will be avoided in the event of an ICSF failure when the PKI CA has a hardware key**

continued ↘

Survey of z/OS R9 Security Enhancements…

- z/OS Communications Server
  - Network Security Services function providing:
    - centralized IPSec certificate services
  - IKE Daemon to be configurable as a Network Security client

- FTP server, FTP Client, and TN3270
  - Application Transparent TLS (AT-TLS) to manage security

z/OS R10 Preview Announce Security Enhancements

z/OS V1.10 plans include:

- **RACF (Resource Access Control Facility)**
  - **Password phrase**
    - Introduced in V1.8, enhanced V1.9 (0-100 chars possible)
      - password change logging and enveloping functions for password phrases
      - expiration warning like done today for passwords
    - Exploitation expected by: TSO/E Logon, z/OS Unix Kernel, z/OS UNIX Shell and Utilities su and passwd commands, C run-time functions login(), __passwd(), pthread_security_np() and getpass(), Network Authentication Service support for Kerberos, IBM Tivoli Directory Server (LDAP) for z/OS SDBM backend support
    - ***RACF users can now effectively have longer passwords with fewer character restrictions*** (such as can currently exist on Windows and UNIX systems)
    - Allows considering implementation of enterprise-wide password synchronization (using, for example, IBM Tivoli Directory Integrator)
  - **Custom Fields (for RACF user and group profiles)**
    - You define new fields as you need, and assign labels to your new fields
    - Administration supported by RACF commands, panels, and LDAP

* Statements regarding IBM future direction and intent are subject to change or withdrawal, and represents goals and objectives only.
**With appropriate HW

z/OS R10 Preview Announce Security Enhancements…

- **RACF continued**

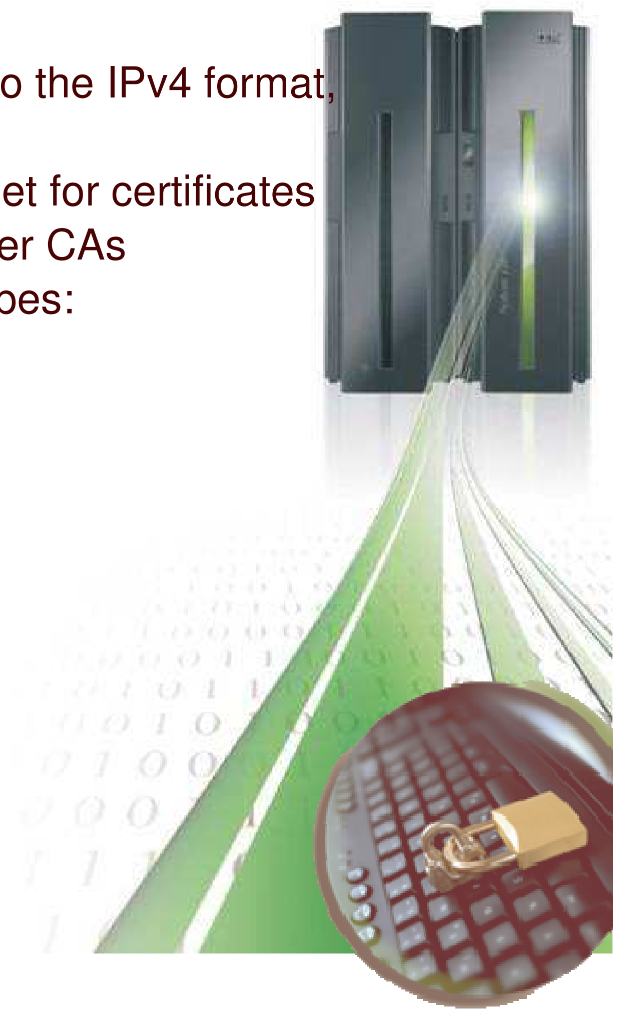
  – **Selective authority for resetting passwords**
  - Grant authority to individual to reset passwords for individual(s) or members of a specific group(s)
    – Not necessary to have system-wide SPECIAL or access within the system-wide IRR.PASSWORD.RESET profile in FACILITY class
    – Authority scoped by the owner of the RACF user or users that are within a selected RACF group tree
  - Help desk personnel will be able to do password resets without granting them additional authorizations

  – **RACDCERT (Digital Certificate support in RACF) enhanced to:**
  - Generate and display the IPv6 type IP address, in addition to the IPv4 format, in the certificate Subject Alternate Name extension
  - The BSAFE crypto provider that is presently imbedded within RACDCERT, will be replaced with the IBM Crypto Library in C (CLiC)

* Statements regarding IBM future direction and intent are subject to change or withdrawal, and represents goals and objectives only.

**With appropriate HW

z/OS R10 Preview Announce Security Enhancements…



- **Public Key Infrastructure (PKI) Services**
  - Generate and display the IPv6 type IP address, in addition to the IPv4 format, in the certificate Subject Alternate Name extension
  - Support for additional characters from the UTF8 character set for certificates
    - improves interoperability with certificates created by other CAs
  - Support for three additional Distinguished Name attribute types:
    - Domain Component,
    - Distinguished Name Qualifier, and
    - User ID

- **System SSL (Secure Sockets Layer)**
  - Utilize hardware support for RSA digital signature **
  - SHA-224, SHA-256, SHA-384, and SHA-512 algorithms **

- **z/OS Communications Server**
  - **<u>IPSec RFC Currency</u>:**
    - IPV6 standards,
    - RFCs 4301-4305, 4308

* Statements regarding IBM future direction and intent are subject to change or withdrawal, and represents goals and objectives only.
**With appropriate HW

z/OS R10 Preview Announce Security Enhancements…

- **ICSF (Integrated Cryptographic Service Facility)**
  - 4096-bit RSA key support (with z10 EC, z9 EC and z9 BC)
  - IBM: SHA-224, SHA-384**, and SHA-512**
  - AES-192 and AES-256 algorithms **
  - ISO Format-3 PIN Block support (meets ISO 9564-1 Banking standard) (with z10 EC, z9 EC and z9 BC)
  - Also, random number callable service

- **ITDS (IBM Tivoli Directory Server) for z/OS**
  - New extended operation to support group access checking in addition to user access checking
    - "Roll back" PTFs for z/OS V1.8 and V1.9 via APAR OA23078
  - Improved compatibility for z/OS
    - Configured plug-ins can be used to extend the capabilities of ITDS for z/OS. Pre-operation, post-operation and client operation plug-ins are supported

* Statements regarding IBM future direction and intent are subject to change or withdrawal, and represents goals and objectives only.

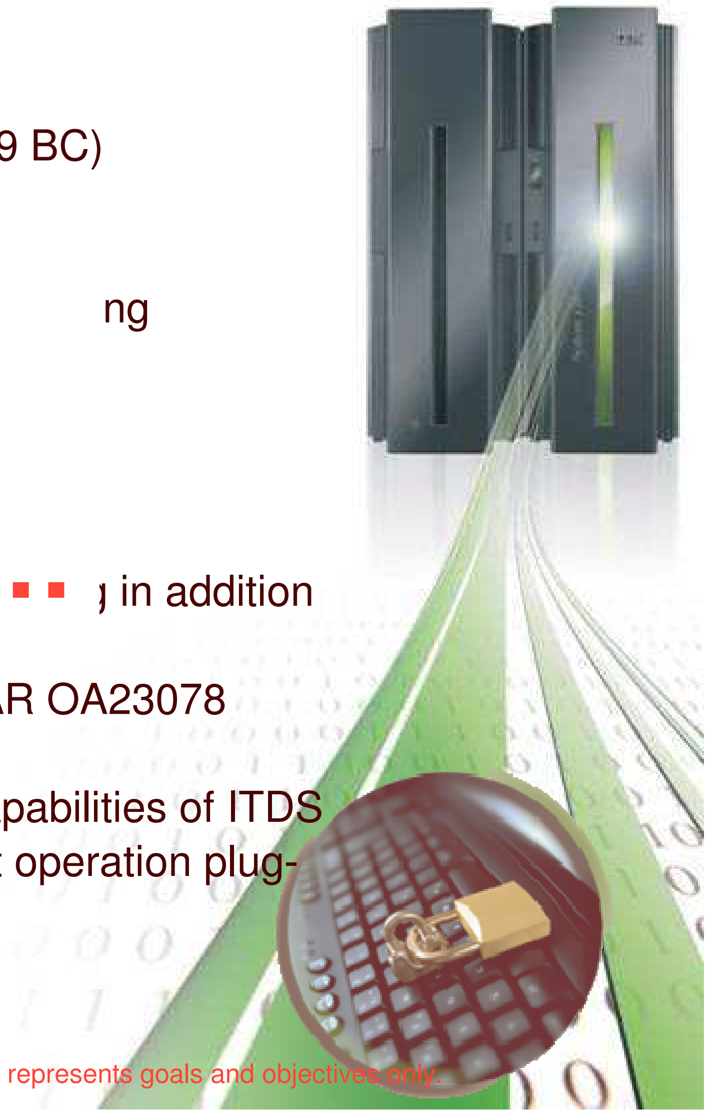
**With appropriate HW

z/OS R10 Preview Announce Security Enhancements…

- **ICSF (Integrated Cryptographic Service Facility)**
  - 4096-bit RSA key support (with z10 EC, z9 EC and z9 BC)
  - IBM: SHA-224, SHA-384**, and SHA-512**
  - AES-192 and AES-256 algorithms **

Repeated for page 2 of notes. Chart is hidden…

  - ISO Form ng standard)
  - Also, ran
- **ITDS (IBM**
  - New exte in addition to user access checking
    - "Roll back" PTFs for z/OS V1.8 and V1.9 via APAR OA23078
  - Improved compatibility for z/OS
    - Configured plug-ins can be used to extend the capabilities of ITDS for z/OS. Pre-operation, post-operation and client operation plug-ins are supported



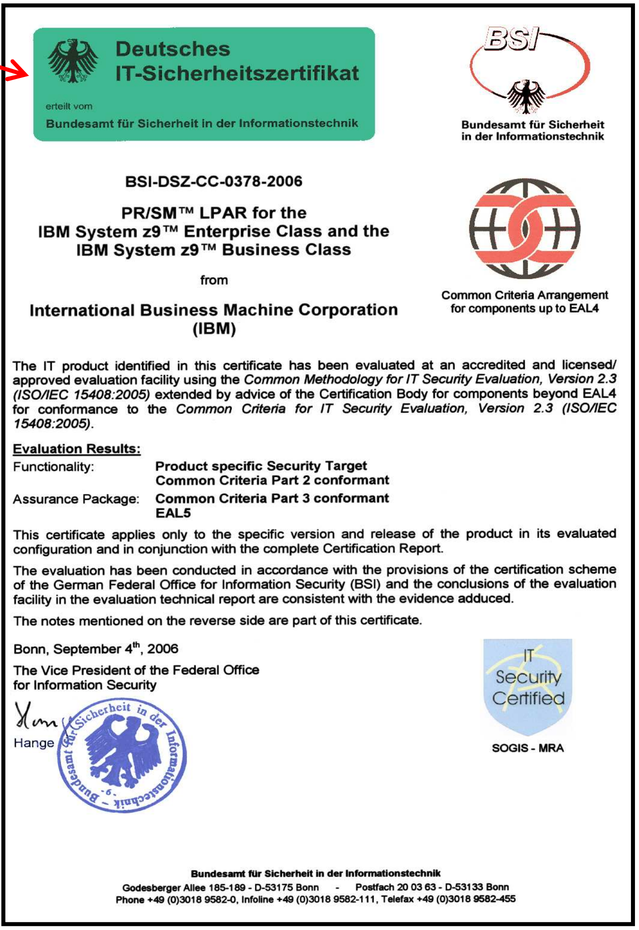
* Statements regarding IBM future direction and intent are subject to change or withdrawal, and represents goals and objectives only.
**With appropriate HW

Agenda

- Our corner of the industry
- Topology of security on z/OS
  - Cryptography
  - RACF and LDAP (z/OS Directory Server)
  - Security Functions for Communications (Servers and Protocols)
  - Adding users and resources to the picture
  - WAS – Connection to the Internet
  - Role of Tivoli Products
  - Role of Vanguard products
- Survey of z/OS recent security enhancements
- ➡ z/OS Certifications
- z/OS Security Strategic Objectives
- Directions
- Closing remarks

z/OS and System z9 Certifications

- **September 2006, EAL5 awarded to PR/SM LPAR for IBM System z9 Enterprise Class and IBM System z9 Business Class computers**
- **March 2008, EAL4+ awarded to z/OS 1.9 with RACF**
  - Encompasses:
    - CAPP (Controlled Access Protection Profile) EAL4+, and
    - LSPP (Labeled Security Protection Profile) EAL4+
- **z/VM 5.3 in evaluation for EAL4+**
- **IdenTrust certification for z/OS PKI**
  - Note: Identrus recently renamed to IdenTrust



Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0378-2006

PR/SM™ LPAR for the
IBM System z9™ Enterprise Class and the
IBM System z9™ Business Class

from

International Business Machine Corporation
(IBM)

Common Criteria Arrangement
for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)* extended by advice of the Certification Body for components beyond EAL4 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL5**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, September 4th, 2006

The Vice President of the Federal Office
for Information Security

Hange

Bundesamt für Sicherheit in der Informationstechnik -6-

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)3018 9582-0, Infoline +49 (0)3018 9582-111, Telefax +49 (0)3018 9582-455

For more, see http://www-03.ibm.com/security/standards/st_evaluations.shtml

EAL = Evaluated Assurance Level

Z/OS V1.9 with RACF now at EAL4+ for CAPP and LSPP

Once again delivering on our commitment to provide customers higher levels of security certification, IBM is proud to announce that its flagship operating system z/OS V1.9 with the RACF optional feature has achieved EAL4+ for Controlled Access Protection Profile (CAPP) and Labeled Security Protection Profile (LSPP).

This prestigious certification indicates that z/OS V1.9 has gone through a rigorous testing process and conforms to standards sanctioned by the International Standards Organization and officially recognized by many governments worldwide. Achieving EAL4 may further enable z/OS to be adopted by governments and government agencies for mission-critical and command-and-control operations.

Certification to the Common Criteria EAL4 requires in-depth analysis of product design and development methodology, backed by extensive testing. EAL4 certificates are currently recognized by the following countries: United States, Canada, Australia, New Zealand, France, Germany, Finland, Greece, Israel, Italy, The Netherlands, Norway, Spain and the United Kingdom.

The evaluation was completed by atsec information security GmbH, one of the world's leading vendor-independent IT security consulting companies, and accredited in Germany by the Federal Office for Information Security (BSI).

What is “z/OS PKI Services” ?

- PKI (Public Key Infrastructure) Services support the “**life cycle management**” of large numbers of ***Digital Certificates***
  - Digital Certificates, based on public key encryption technology, provide a foundation for a security-rich and scalable user identification and authentication, and security-rich and verifiable data exchange.
- PKI Services is technology that allows our z/OS customers to act as their own ***Certificate Authority (CA)*** for their internal and external users, issuing and administering digital certificates in accordance with their organizational policies
  - Value: z/OS customers do not have to buy digital certificates or similar services from other sources or run CAs on other platforms
- IdenTrust Certified

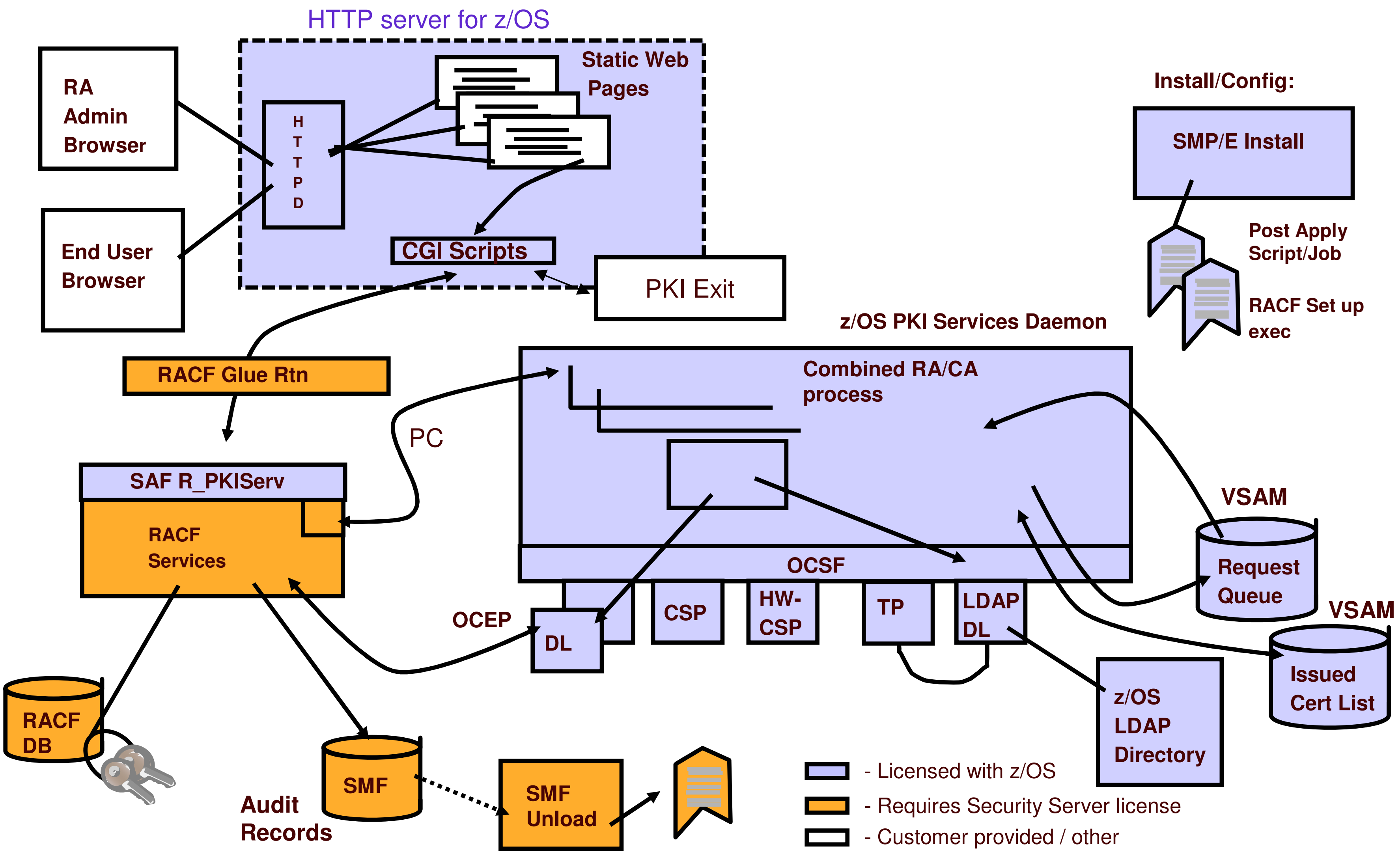
http://www.**ibm.com**/servers/eserver/zseries/zos/pki/

http://w3.itso.ibm.com/redpieces/abstracts/sg247470.html?Open

IdenTrust Certified PKI Services

- z/OS PKI Services certified as an IdenTrust compliant Certificate Authority (CA)
  - Technology capable of IdenTrust compliance
- z/OS Banking customers now have an IdenTrust compliant Certificate Authority and related PKI services available to them via the z/OS operating system plus an external security manager such as RACF (or equivalent)

z/OS PKI Services Architecture



🟪 - Licensed with z/OS

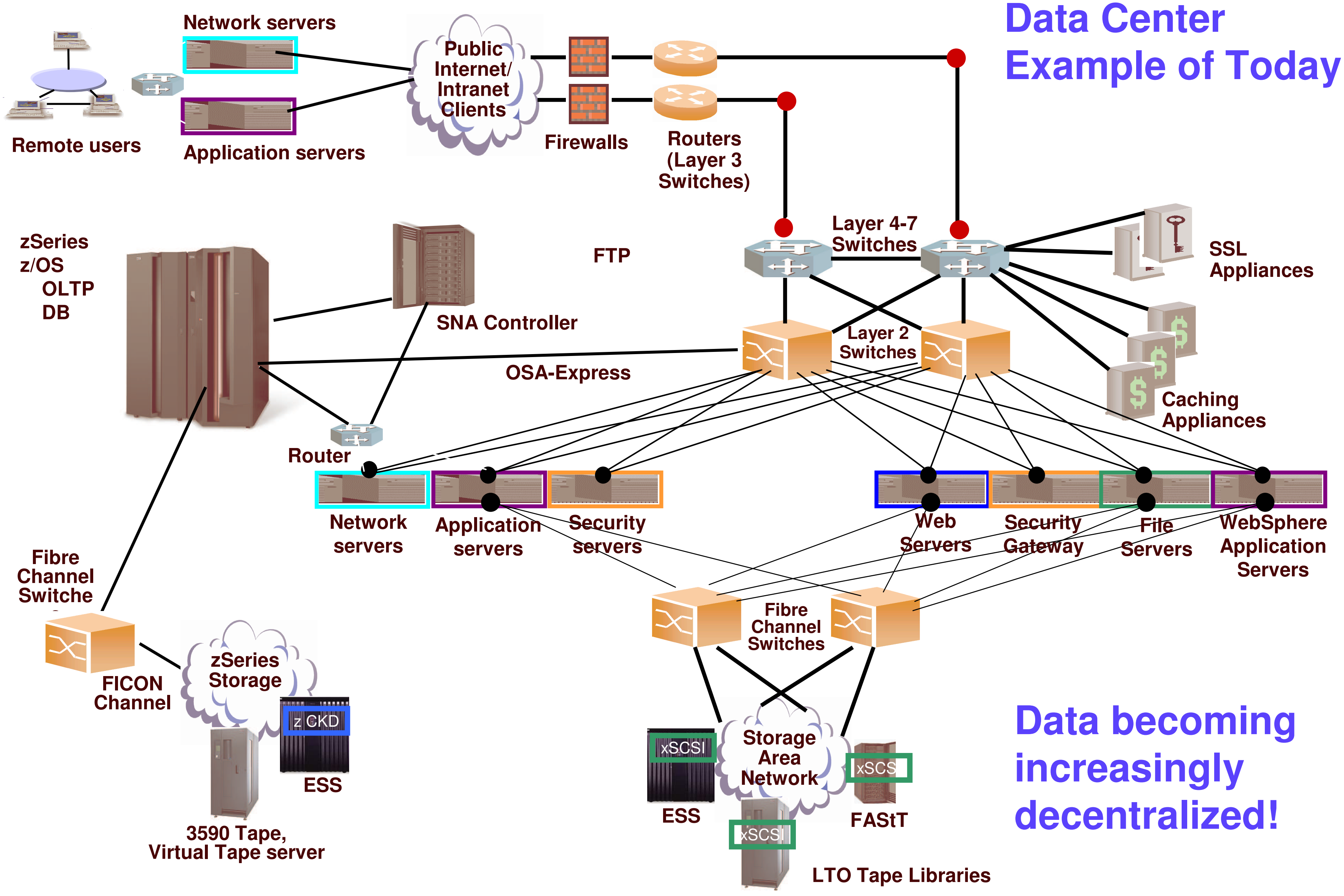
🟧 - Requires Security Server license

□ - Customer provided / other

Agenda

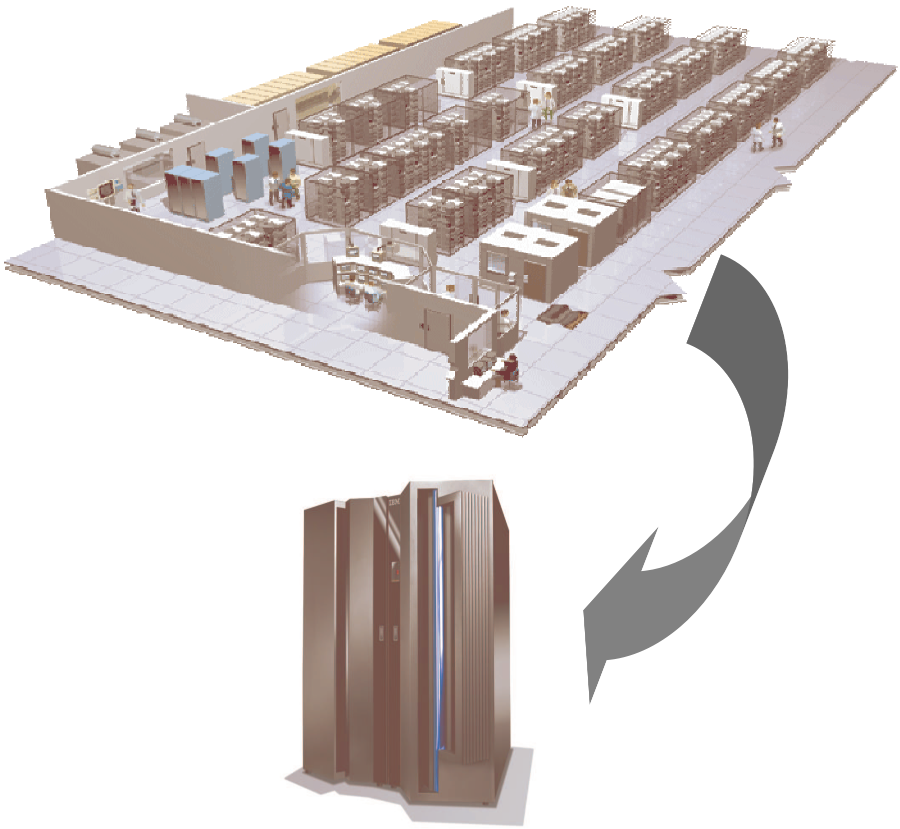
- Our corner of the industry
- Topology of security on z/OS
  - Cryptography
  - RACF and LDAP (z/OS Directory Server)
  - Security Functions for Communications (Servers and Protocols)
  - Adding users and resources to the picture
  - WAS – Connection to the Internet
  - Role of Tivoli Products
  - Role of Vanguard products
- Survey of z/OS recent security enhancements
- z/OS Certifications
- **z/OS Security Strategic Objectives**
- Directions
- Closing remarks

Data Center Example of Today



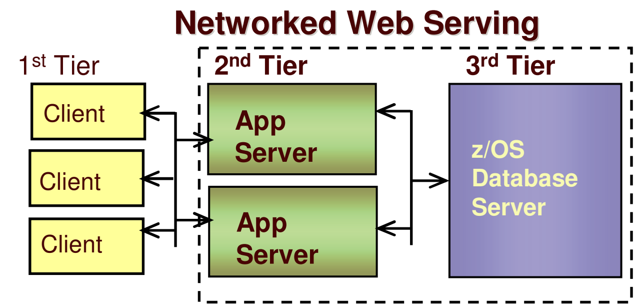
Data becoming increasingly decentralized!

Mainframe optimization starts with a Data Center in a box…not a server farm

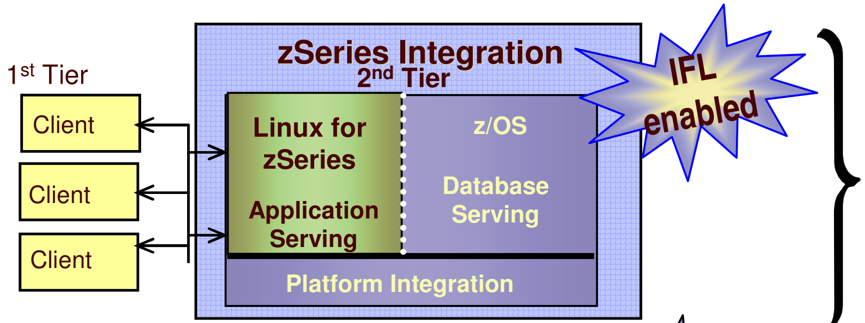


- IBM has invested billions of dollars in Hardware and Software Development to make System z9 an industry leading platform.
- System components are integrated and tested to enable optimal synergies
- Powerful and scalable capacity
- Hundreds of support processors
- Central point of management
- High resource utilization
- May offer lower cost of operations
  - **Less Servers**
  - **Fewer SW Licenses**
  - **Fewer resources to manage**
  - **Less energy, cooling and space**
- Fewer intrusion points help provide tighter Security
- Fewer points of failure help provide greater Availability

Simplify and improve TCO by integration

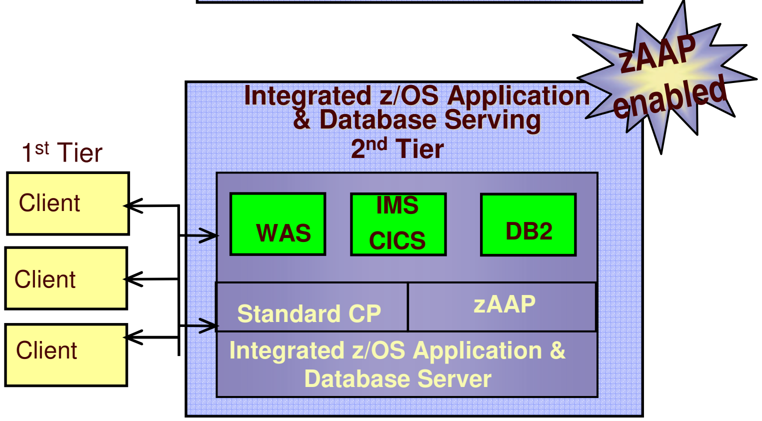


Advantages of consolidating your application and data serving



Better Production Value

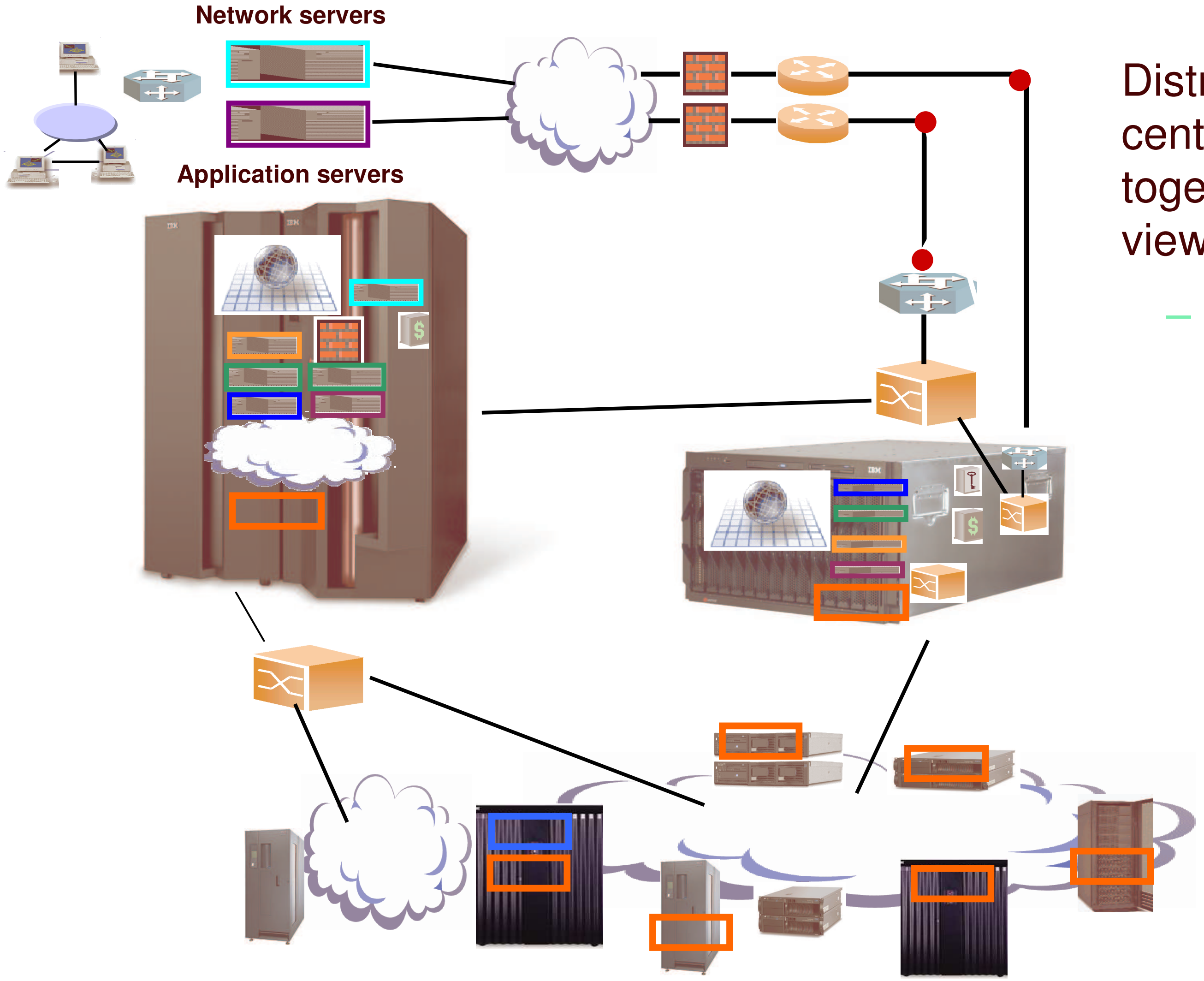
✓Security	Fewer points of intrusion
✓Resilience	Fewer Points of Failure, better mean time between failure
✓Performance	Avoid Network Latency
✓Operations	Fewer parts to manage
✓Environmentals	Less Hardware
✓Capacity	Easier to dynamically add


zAAP enabled
Integrated z/OS Application & Database Serving
2nd Tier
1st Tier
Client
Client
Client
WAS
IMS
CICS
DB2
Standard CP
zAAP
Integrated z/OS Application & Database Server

Best Production Value

✓Security	Fewer points of intrusion
✓Resilience	Fewer Points of Failure
✓Auditability	Consistent identity
✓Performance	Avoid Network Latency
✓Utilization	Efficient use of resources
✓Scaleability	Batch and Transaction Processing
✓Operations	Fewer parts to manage
✓Simplification	Problem Determination/diagnosis
✓Transaction Integrity	Automatic recovery/rollback
✓Environmentals	Less Hardware

z/OS Objective: simplified business process infrastructure

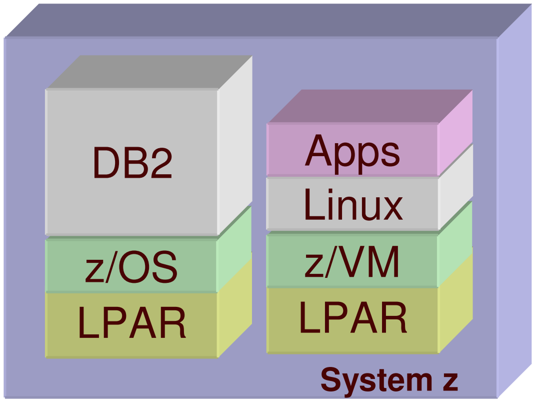


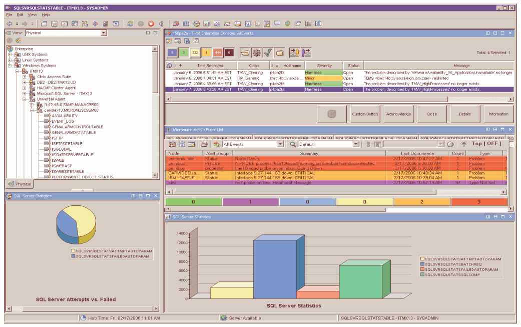
Distributed servers and centralized servers can work together with a centralized view of data

- Importantly, there are political considerations:
  - Manage by business process or by server role (glass house vs. LOB)

z/OS Simplification Strategy

- **Deployment: packages vs. piece-parts**
  - **Hardware, software, middleware viewed as an entity; designed and packaged to work together, out of the box.**
  - **New components are easy to plug in and swap out**
- **Platform management:**
  - **Task automation - reduces skill requirements**
  - **Modern user interface that is consistent across IBM; based on Tivoli console technology**
  - **Open management interfaces that accelerate the development of new management applications and automation**
- **Application development:**
  - **Modern, Eclipse-based environment that make z/OS look cool to kids coming out of school**
  - **Tools that accelerate the design and development of new business applications – and the modernization of existing ones**

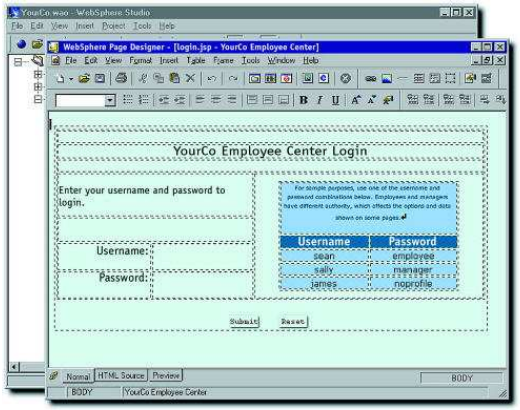




Time Received	Class	Hostname	Severity	Status	Message
January 6, 2006 6:51:49 AM EST	TMW_Clearing	p4pa2kk	Harmless	Open	The problem described by 'VMwareAvailability_IVI_ApplicationUnavailable' no longer
January 6, 2006 7:04:51 AM EST	ITM_Generic	itmx14b.tivlab.ral...	Minor	Open	TEMS <itmx14b.tivlab.raleigh.ibm.com> restarted
January 7, 2006 4:33:59 AM EST	TMW_Clearing	p4pa2kk	Harmless	Open	The problem described by 'TMW_HighProcesses' no longer exists.
January 7, 2006 5:43:26 AM EST	TMW_Clearing	p4pa2kk	Harmless	Open	The problem described by 'TMW_HighProcesses' no longer exists.

Node	Alert Group	Summary	Last Occurrence	Count	Type
warrenw.ralei...	Status	Node Down.	2/17/2006 10:47:27 AM	1	Problem
omnibus	PROBE	A PROBE process, tme10tecad, running on omnibus has disconnected	2/17/2006 9:38:00 AM	1	Problem
omnibus	probestat	tme10tecad probe on omnibus: Going Down ...	2/17/2006 9:38:00 AM	2	Problem
EAPVIDEO.ra...	Status	Interface 9.27.144.163 down. CRITICAL	2/17/2006 10:48:34 AM	1	Problem
IBM-Y1A5FJ6...	Status	Interface 9.27.144.169 down. CRITICAL	2/17/2006 10:29:04 AM	1	Problem
kiwi		nv7 probe on kiwi: Heartbeat Message	2/17/2006 10:57:19 AM	97	Type Not Set

0	1	0	0	2	3


YourCo.wao - WebSphere Studio
File Edit View Insert Project Tools Help
WebSphere Page Designer - [login.jsp - YourCo Employee Center]
File Edit View Format Insert Table Frame Tools Window Help
Normal
HTML Source
Preview
BODY
BODY
YourCo Employee Center

YourCo Employee Center Login

Enter your username and password to login.

Username:

Password:

For sample purposes, use one of the username and password combinations below. Employees and managers have different authority, which affects the options and data shown on some pages.

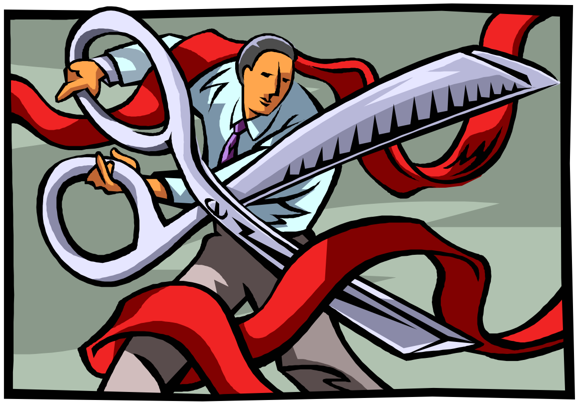
Username	Password
sean	employee
sally	manager
james	noprofile

Submit Reset

Simplifying z/OS management – today!

Multiple initiatives; my focus is security

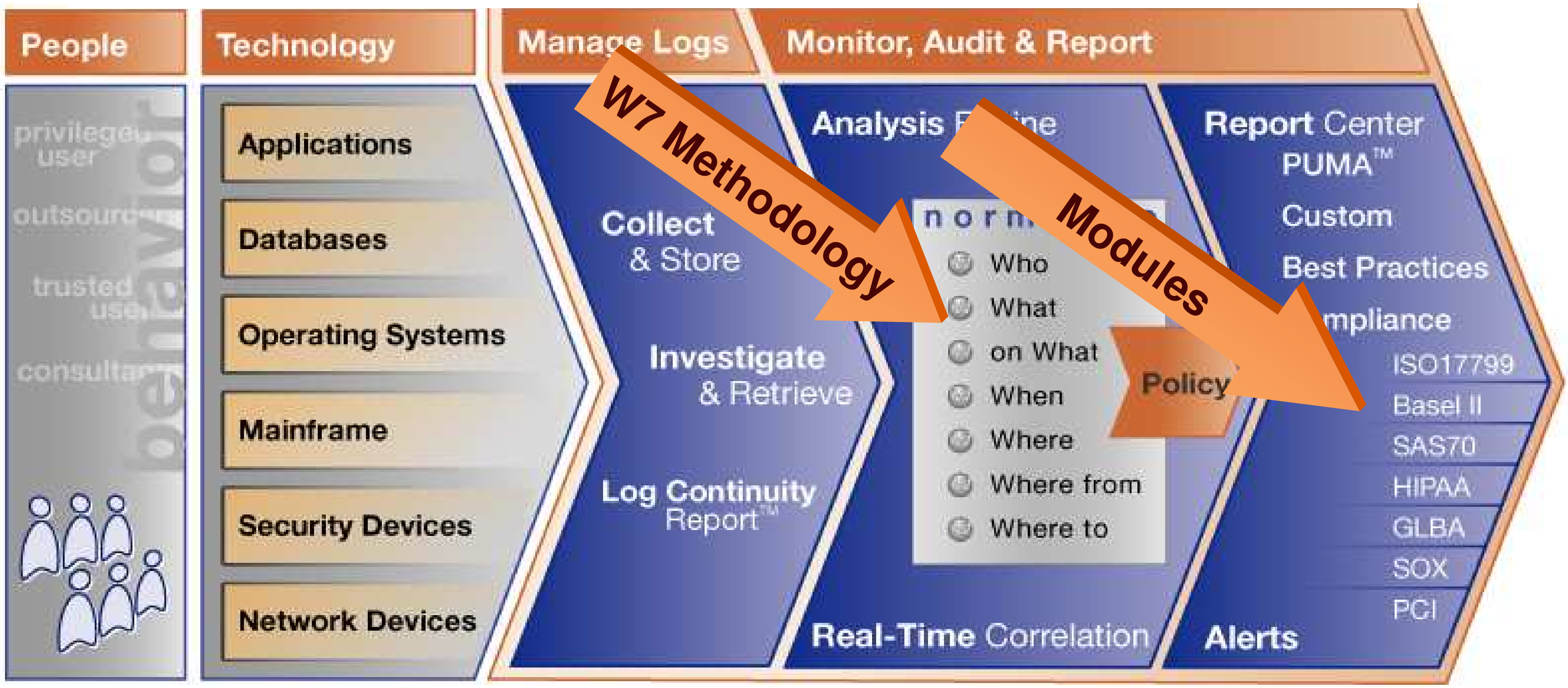
- **Operations**:
  - **IBM OMEGAMON® z/OS Management Console for system health monitoring**
- **Configuration**:
  - **Health Checker for z/OS to help configure with best practices**
  - **Hardware Configuration Manager can simplify I/O configuration and planning**
- **Maintenance**:
  - **SMP/E Internet Service Delivery can automate service acquisition**
  - **ShopzSeries can help you manage your inventory**
- **Security:**
  - **RACF®-based products to help you administer security & monitor compliance**
    - **New Tivoli products**
      - **IBM has acquired Consul**
- **Networking**:
  - **IBM Configuration Assistant for z/OS Communications Server (formally named the z/OS Network Security Configuration Assistant)**



Compliance monitoring, auditing, and reporting

Patent-pending W7 methodology and out-of-the box compliance support modules to help accelerate clients' policy, and compliance initiatives

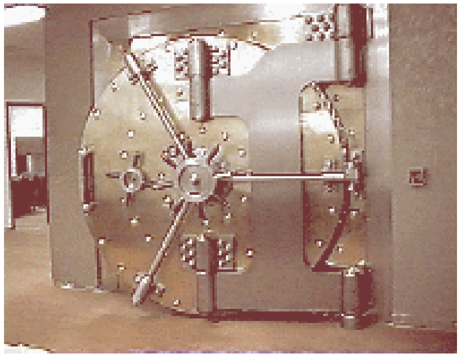
Tivoli Compliance Insight Manager



On Demand Differentiation

z/OS Strategy:

- **Map applications to data – "Vaults" data in a centralized, controlled location, collocated with applications intended to help**
  - **Reduce operational complexity**
  - **Reduce management/monitoring costs**
  - **Prioritize system redundancy around workflow**



z/OS Security Strategy:

- **Whatever is necessary to support and enhance the value to customers of the afore mentioned z/OS strategy**
  - **Advanced treatment of runtime identities**
  - **State of the art: encryption, PKI, user I&A, access control**
  - **Etc..**

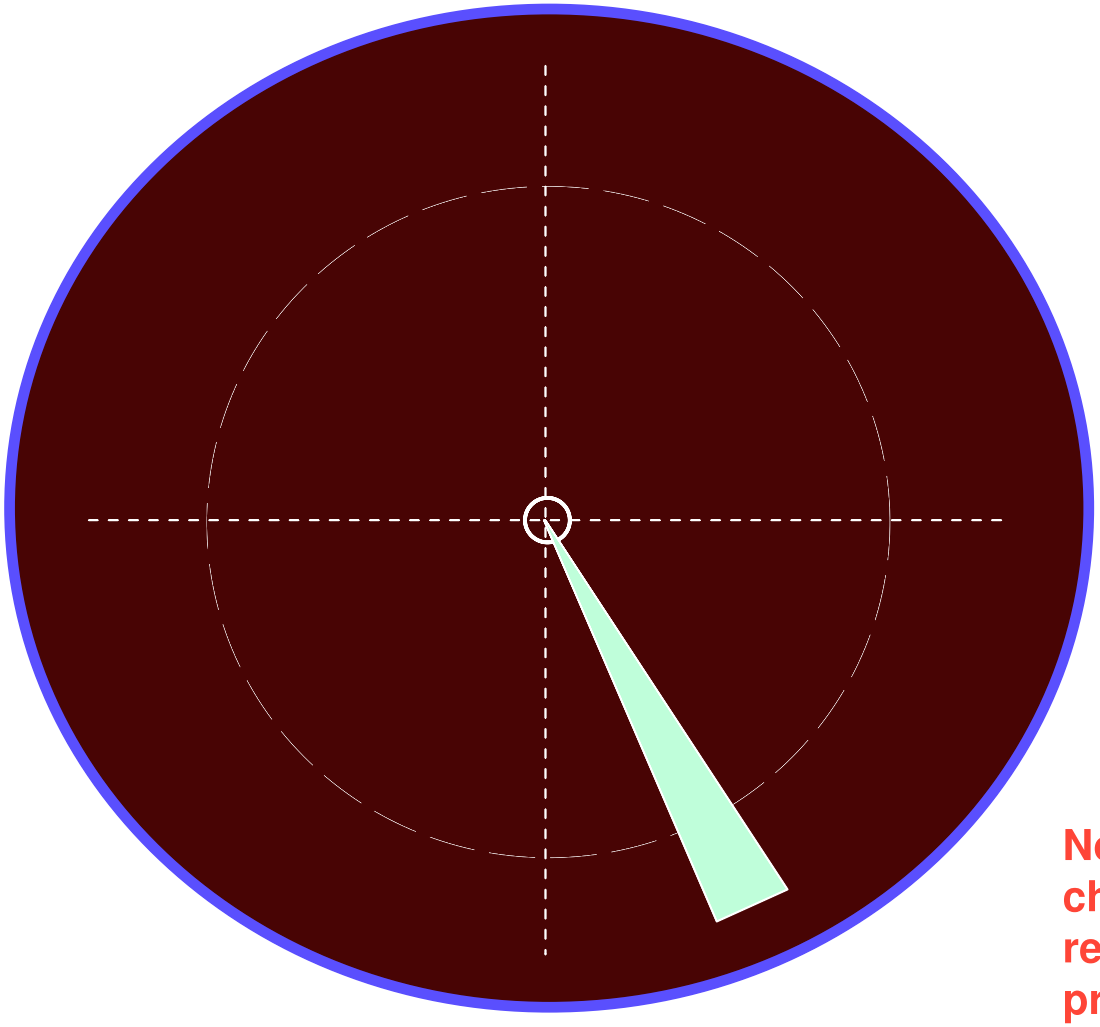
z/OS, be the Enterprise data vault for the ON DEMAND environment

Agenda

- Our corner of the industry
- Topology of security on z/OS
  - Cryptography
  - RACF and LDAP (z/OS Directory Server)
  - Security Functions for Communications (Servers and Protocols)
  - Adding users and resources to the picture
  - WAS – Connection to the Internet
  - Role of Tivoli Products
  - Role of Vanguard products
- Survey of z/OS R6 security enhancements
- z/OS Certifications
- z/OS Security Strategic Objectives
- Directions
- Closing remarks

Security Role in Support of z/OS Objectives

RADAR
SCOPE



Note: Items on this chart are not reproduced in presentation copies

Agenda

- Our corner of the industry
- Topology of security on z/OS
  - Cryptography
  - RACF and LDAP (z/OS Directory Server)
  - Security Functions for Communications (Servers and Protocols)
  - Adding users and resources to the picture
  - WAS – Connection to the Internet
  - Role of Tivoli Products
  - Role of Vanguard products
- Survey of z/OS R6 security enhancements
- z/OS Certifications
- z/OS Security Strategic Objectives
- Directions
- ➡ **Closing Remarks**

Security Role in Support of z/OS Objectives

✓ zSeries and z/OS security functions leveraged from zLinux

✓ Evaluations and certifications, e.g. EALn

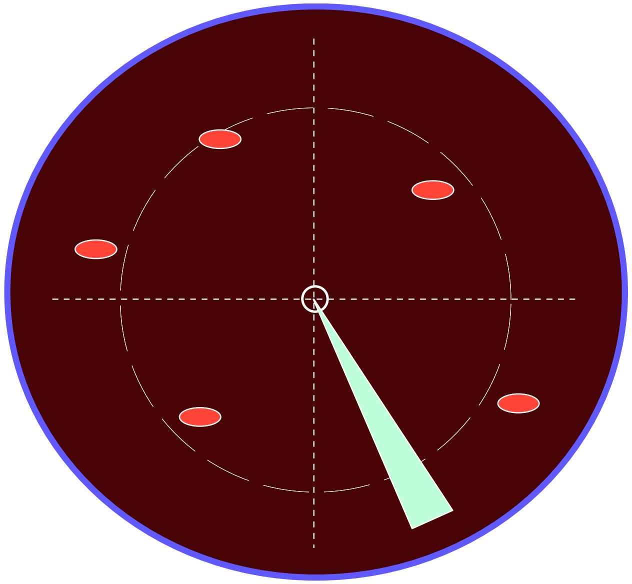
✓ Use of message signature and verification in selected situations

✓ More exploitation of Password Phrase

✓ Enhanced handling of user identities between distributed world and z/OS, exploiting XML and SOAP

✓ Enablement of ‘synchronization’ of user and group definitions between z/OS RACF and z/VM RACF

z/OS Security Radar Scope



Note: Items on this chart are not reproduced in presentation copies

Summing Up

- **Security Disciplines**
- **z/OS Security Baseline**
- **Recent Enhancements**
- **Strategy and directions**

? ? ? ? ? ? ? ? ? ? ? ?

Time for Questions

z/OS Security Information on the Web

- **z/OS Web Sites**
  - http://www.**ibm.com**/servers/eserver/zseries,
  - http://www.**ibm.com**/servers/eserver/zseries/zos

- **RACF Home Page**

  http://www.ibm.com/RACF
  - Latest release information on RACF
  - Links to announcement letters
  - Sample code
    - DBSYNC to compare/sync. two RACF databases
    - RACFICE to create audit/analysis reports
    - OS390ART for a Web-based reporting tool
    - RACTRACE tracing facility
    - RACFDB2 Conversion Utility
    - PKIServ (replacement for CA Servlet)
  - Frequently Asked Questions
  - RACF user group information
  - RACF-L information

IBM System z Security

- http://www.ibm.com/systems/z/security/

IBM Systems Journal articles on z/OS Security, via the Web at http://www.research.**ibm.com**/journal

- Search for "Security on z/OS: Comprehensive, current, and flexible" , and
- "Using RACF to Secure DB2 Objects"

Security: always work left to do

Thank you for your attention

Backup charts follow

ON DEMAND BUSINESS™

Survey of z/OS R8 Security Enhancements

Looking at recent enhancements can shed light on emerging trends

General Availability was October of 2006

- Support for Password Phrases from 14 to 100 characters in length
  - In addition to current support for passwords
  - Password Phrases allow for an exponentially greater number of possible combinations of characters and numbers than do passwords
  - Currently, no exploitation of Password Phrase; RACF supports future exploitation
- Significant enhancements to Identrus-certified support for Digital Certificates including multiple CA and SCEP support
  - Including the ability to have multiple Certificate Authorities on a single z/OS image
  - (SCEP) Simple Certificate Enrolment Protocol
- Support for Advanced Encryption Standard (AES) for IPSec

Survey of z/OS R8 Security Enhancements…

- **Support for SAF Identity Tokens**

- **Support for Virtual Key Rings**

- **Support for defining Intrusion Detection Services (IDS) policies in a policy agent configuration file as well as an LDAP Server**

- **New option for securing tape data sets via SAF**
  - **DATASET class without activating TAPEDSN for TAPEVOL classes, specifies:**
    - **That all data sets on a volume have common authorization, and**
    - **If users are authorized to overwrite existing files on a tape volume**

Survey of z/OS 1.7 Security Enhancements

- **RACF USER-related enhancements:**
  - ✓ Mixed-case passwords
  - ✓ Detect or Prevent password recycling
  - ✓ Changes to REVOKE – RESUME
- **RACF Availability enhancement:**
  - ✓ Automatic RVARY SWITCH to backup for some errors
- **Programming:**
  - ✓ R_admin functions to extract USER, GROUP, and CONNECT information
- **Server security:**
  - ✓ Delegated Resources
- **PKI Services enhancements**

More info on Tivoli security products

- **Tivoli Identity Manager**
  - http://www-3.**ibm.com**/software/tivoli/products/identity-mgr/
- **Tivoli Access Manager**
  - http://www-3.**ibm.com**/software/tivoli/products/access-mgr-e-bus/
  - http://www-3.**ibm.com**/software/tivoli/products/access-mgr-bus-integration/
  - http://www-306.**ibm.com**/software/tivoli/products/access-mgr-operating-sys/
- **Tivoli Privacy Manager**
  - http://www-3.**ibm.com**/software/tivoli/products/privacy-mgr-e-bus/
- **Tivoli Security Compliance Manager**
  - http://www-3.**ibm.com**/software/tivoli/products/security-compliance-mgr/
- **Tivoli Risk Manager**
  - http://www-3.**ibm.com**/software/tivoli/products/risk-mgr/
- **IBM Tivoli Directory Server**
  - http://www-3.**ibm.com**/software/tivoli/products/directory-server/
- **IBM Tivoli Directory Integrator**
  - http://www-3.**ibm.com**/software/tivoli/products/directory-integrator/

Encryption Facility V1.2 Details Capabilities and Value

- **Using OpenPGP support, the customer can:**
  1. Passphrase based encrypt/decrypt
  2. Public/Private key based encrypt/decrypt
  3. Digitally sign data/Verify signatures
  4. Compress Data
  5. Exchange key material in OpenPGP certificates
  6. Generate key pairs and OpenPGP/X.509 certificates
- **Value:**
  1. Additional data integrity services
     - Multiple algorithms for each service
  2. Existing open source tooling
  3. Exchange one payload with multiple partners
  4. RACF, ICSF, or Java keystore repository
  5. Special text processing

Encryption Facility V1.2 Details…

Usage & Invocation

- **Invocation from an OMVS login**
  - java –jar /usr/lpp/encyryptionfacility/CSDEncryptionFacility.jar [*–homedir dir]* [*options] commands [input file…]*
- **Invocation from batch**
  - Sample JCL, environment member, PROC
- **Messaging/Tracing**
  - Messages →STDOUT
  - Tracing (when active) → STDERR
  - XML Logging (when activate) → zFS file
- **Configuration File**
  - Sample shipped: /usr/lpp/encryptionfacility/ibmef.config
  - Default Search Location: /etc/encryptionfacility

Encryption Facility V1.2 Details…
Usage & Invocation cont …

- **Data I/O**
  - zFS
  - PDS, PDSE, Sequential Data Sets
    - Output of encrypt/sign/compress must be VB
    - Syntax Example
      - '//HLQ.PDS.HLQ1(Mem)'
      - //HLQ.SEQ.HLQ
      - //DD:ddNAME
- **OpenPGP Key Ring**
  - Default: /var/encryptionfacility/ibmpkring.ikr
- **Keystores**
  - RACF, RACF+ICSF, ICSF
    - Require H/W crypto provider
    - RACF – read only
  - Java JKS, Java JCEKS

Encryption Facility V1.2 Details…

Public Key vs. Passphrase

- **Passphrase**
  - Con: Must securely exchange passphrase
  - Pro: Simpler
    - No public key management
    - No public key verification
- **Public Key**
  - Pro: Eliminate need to exchange passphrase
  - Con: Key management
    - 1 key per recipient

Encryption Facility V1.2 Details…

Certificates: X.509 vs. OpenPGP

- **Support X.509 through keystore**
  - RACF key rings
  - Certificate Authority simplifies Trust establishment
- **Support OpenPGP**
  - Original approach for key exchange and OpenPGP
  - Trust not as straightforward

Encryption Facility V1.2 Details…
Interactions & Dependencies

- **Hardware Dependencies**
  - z800,z900,z890,z990, z9
  - Using H/W crypto,
    - OpenPGP support requires the same H/W as EF 1.1.
      - CPACF
      - RSA, HW Key Generation → Crypto Coprocessor:
        - CEX2C
        - PCIXCC
        - PCICC
        - CCF
- **Software Dependencies**
  - z/OS 1.6 and above
  - 31 Bit Java SDK 5 SR 4 and above
  - ICSF HCR7720 and above
    - APAR OA19177

Security Headlines Daily

Is Anything More Important to the Success and Survival of Your Business?

More Than 90% Of Companies Regularly Expose Employee And Customer Data[1]

FBI – Businesses Reluctant To Report Cyber Attacks[2]

One In Four Identity-Theft Victims Never Fully Recover[3]

PCI: Card Associations Unite to Fight Fraud With Collaborative Standard[4]

[1] Reconnex Insider Threat Index August 2005
[2] 2005 CSI/FBI Computer Crime and Security Survey
[3] Nationwide Mutual Insurance Co. Survey July 2005
[4] Green Sheet Inc. August 2005 Issue 2

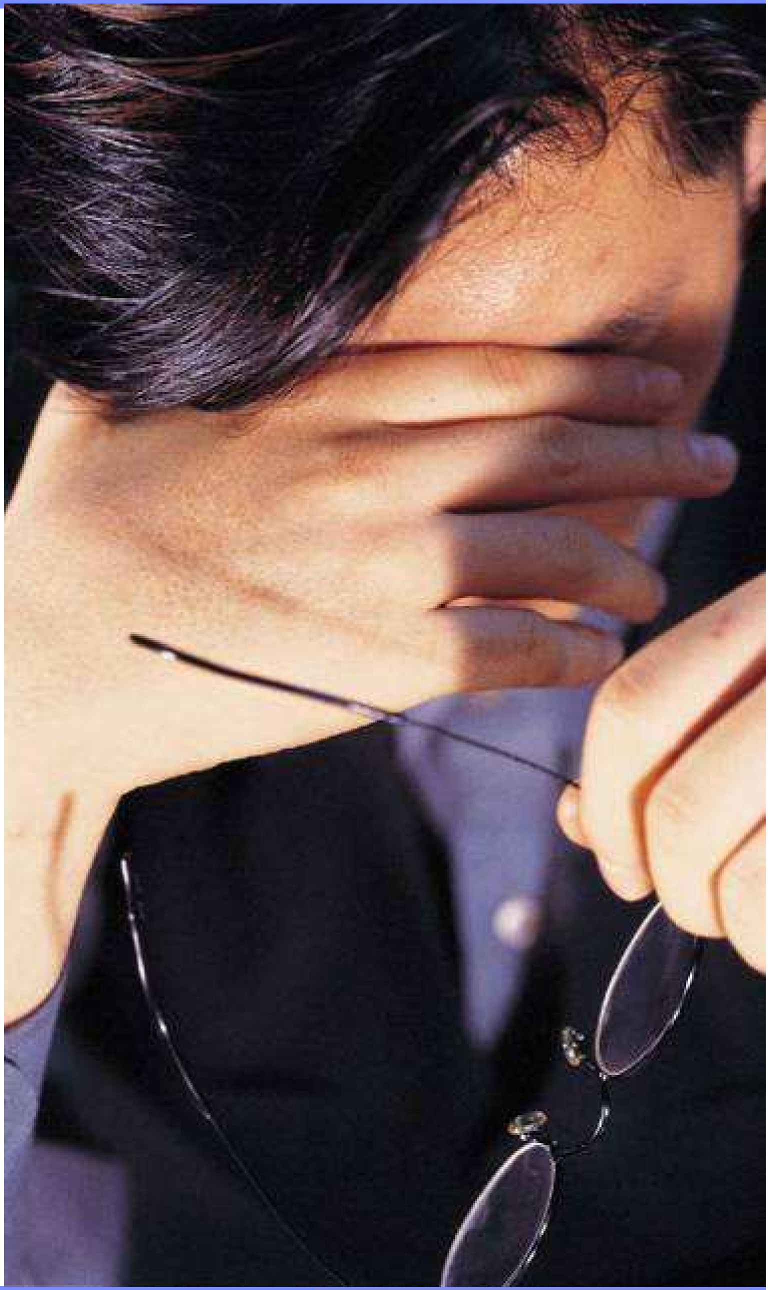
Regulatory and Compliance Considerations

- Gramm-Leach-Bliley Financial Services Modernization Act (GLBA)
- Sarbanes Oxley (SOX)
- European Union Data Protection Directive (EUPA)
- International IT Security Standard (ISO 17799)

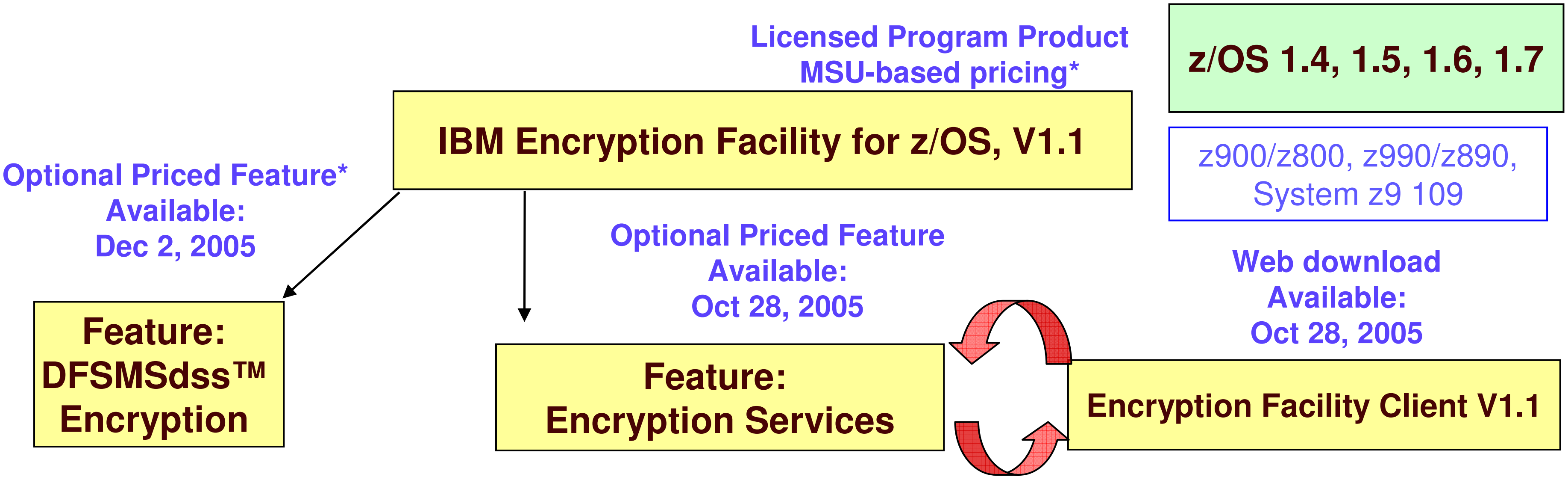
Potential Costs of a Security Breach

- $ Cost of research and recovery
- $ Cost to notify customers
- $ Lost customers/business
- $ Problem solution or remediation
- $ Claims from trusted vendors and business partners

$$ ***Damage to brand image***



z/OS Encryption Facility



Licensed Program Product
MSU-based pricing*

IBM Encryption Facility for z/OS, V1.1

z/OS 1.4, 1.5, 1.6, 1.7

z900/z800, z990/z890,
System z9 109

Optional Priced Feature*
Available:
Dec 2, 2005

Feature:
DFSMSdss™
Encryption

Optional Priced Feature
Available:
Oct 28, 2005

Feature:
Encryption Services

Web download
Available:
Oct 28, 2005

Encryption Facility Client V1.1

- Allows encryption and compression of dump data sets created by DFSMSdss
- Supports decryption and decompression during RESTORE process
- Leverages z/OS centralized key management and IBM mainframe cryptographic and compression capabilities

- Supports encrypting and decrypting data files
- Leverages z/OS centralized key management and access authentication capabilities
- Uses IBM mainframe server cryptographic and compression capabilities
- Can use either Public Key/Private keys or passwords to create secure exchange between partners

- Java technology-based code that allows client systems to decrypt and encrypt tapes for exchange with z/OS systems
- Must be used in conjunction with z/OS systems using the Encryption Services feature
- Can be used on any Java-enabled system

Leverages z/OS centralized key management and PKI function, plus IBM mainframe cryptographic and compression capabilities

* Variable Workload License Charges (VWLC), Entry Workload License Charges (EWLC), zSeries Entry License Charges™ (zELC), Parallel Sysplex License Charges (PSLC)

z/OS Encryption Facility…

Encryption Facility Client V1.2 Web Download

NEW

- Decryption client added June 2, 2006 – allows partners, who have z/OS, to decrypt (with compression) files encrypted and compressed on a z/OS system with Encryption Facility 1.1
- Cannot be used for encryption

z/OS Encryption Facility V1.2

NEW

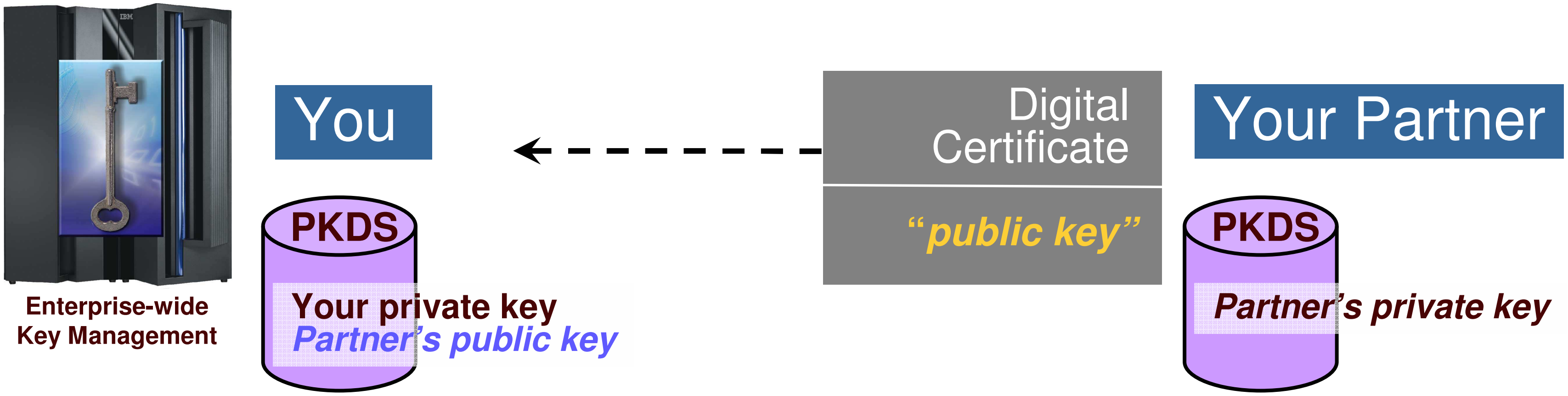
Highlights of January 16, 2007 announce

- More flexibility for exchanging encrypted files with business partners
- Support for OpenPGP standard, RFC 2440
- Continued support for the System z format for encrypting files, which offers performance advantages above the Open PGP format
- Planned Availability March 16, 2007

z/OS Encryption Facility…

Security for data exchanged based on: Password, Digital Certificates, or OpenPGP

Example: Using Digital Certificates to establish a key management environment with your partners



Enterprise-wide Key Management

You

PKDS

Your private key

Partner's public key

Digital Certificate

"public key"

Your Partner

PKDS

Partner's private key

1. Your partner acquires a Digital Certificate (and with it, associated RSA public-private keys)
   - z/OS can be a Digital Certificate Authority using z/OS PKI Services
   - Partner may already have a Digital Certificate
   - Partner may use third party Digital Certificate Authority
2. You invoke RACDCERT to store Dig Cert in RACF and RSA public key in ICSF PKDS
3. You use the public key, via its ICSF label, to encrypt data with Encryption Facility

z/OS Encryption Facility…

Example of encryption flow (using RSA public key)

Enterprise-wide
Key Management

You

Encryption Facility for z/OS feature: ***Encryption Services***

Invoked via JCL

1. Random generation of data key for either AES128 or TDES encryption
2. Encrypt data key with RSA public key, and
   - Store encrypted data key in the file header
3. Compress the data (if partner OS is z/OS)
4. Encrypt the data using the data key
5. Send file to partner

Your Partner

Encryption Facility Client

Partner decrypts file

1. Decrypt data key with RSA private key
2. Decrypt the data

If z/OS site: can use *Encryption Facility for z/OS or Encryption Client (Java code)*

If non-z/OS: uses *Encryption Client* (Java code)

* Optionally leverages piping functions in z/OS UNIX Systems Services to help reduce elapsed time for large datasets

- ISS
- Global Services: Security & Privacy Consulting
- IBM Services: Ethical Hacking

- z/OS CommServer (IDS)
- System zAlerts
- SMF & Tivoli zSecure
- z/OS Healthchecker
- DB2 Audit Tool

- Robust Encryption Infrastructure
- Tape encryption
- DB2 & IMS Encryption & Test Tools
- z/OS Encryption Facility V1.2 (Jan 2007)
- Network encryption: SSL/TLS, IPSec, AT-TLS, OpenSSH, NSS
- ISO Format 3 Pin Block (1.9)

- System Integrity
- RACF MLS
- z/OS PKI Services
- Tivoli Identity Manager (TIM)
- Tivoli Federated Identity Manager (TAM)
- Tivoli zSecure

- EAL 5 for z9 LPAR
- EAL(1.8) & FIPS Certifications
- Linux on System z as DMZ
- z/OS CommServer Security