System z Security Update

Share 11253
Anaheim, CA August 2012

Greg Boyd (boydg@us.ibm.com)

With Thanks to Jack Jones

Trademarks

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

IBM*	FICON*	System z*
IBM (logo)*	IMS	System z10
ibm.com*	Lotus*	Tivoli*
AIX*	POWER7	WebSphere*
BladeCenter*	ProtecTIER*	XIV*
DataPower*	RACF*	zEnterprise
CICS*	Rational*	z/OS*
DB2*	System Storage	z/VM*
DS4000*	System x*	z/VSE

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* 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.

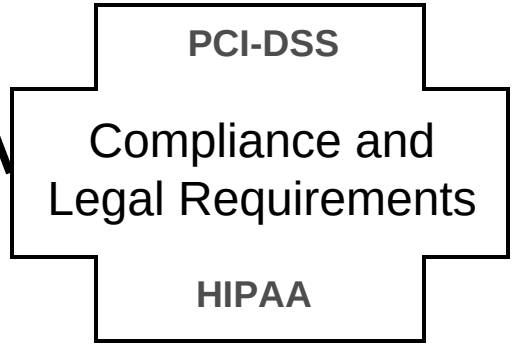
Agenda

- System z, z/OS, and z/VM Security Strategy
  - Most Securable System
  - Protecting the Borders of System z and its Data
  - Extending System z's Quality of Service (Security) to the Enterprise
- Some of the Current Security Features
  - RACF for z/OS and z/VM
  - z/OS Communication Server and its Tools for Cybersecurity
  - System z Hardware Encryption Features
    - Providing Protection for Data in Transit
    - Encrypting Data at Rest and Backups
  - Managing Digital Certificates with z/OS PKI Services
  - Extending Identity Management and Auditing with LDAP (z/OS and z/VM)

The z196 and zEnterprise preserve and enhance the industry renown strengths of the IBM Security Framework

without requiring changes of the current core business applications.

IBM continues to leverage and enhance the leading security capabilities provided by the z/OS and z/VM operating system to build the tightest IT Security Hub, and further enhance their enterprise security through new technology in Authentication, Authorization, Encryption, Auditing, and Administration.



System z Integrity Statements

Designed to help protect your system, data, transactions, and applications from accidental or malicious modification

- **System integrity is the inability to bypass the security on system resources**
- **IBM will always take action to resolve if a case is found where the above can be circumvented**

System z integrity statements and the Common Criteria certifications can be helpful proof points in addressing compliance requirements.

ibm.com/servers/eserver/zseries/zos/racf/zos_integrity_statement.html

http://www.vm.ibm.com/security/zvminteg.html

First Issued in 1973 – Over 3 decades !!

For System z Security has been a state of mind from design to delivery

IBM's commitment to z/OS System Integrity reaffirmed in September 2007

What do you think of the Mainframe (System z)?

Forrester Survey –

"*Please rank which operating system category you feel is inherently more secure?"*

April 10, 2007
Operating System Vendors: Do More To Help Users With Server Security
by Jennifer Albornoz Mulligan

	Rank	
More secure	1	Mainframe
	2	Unix
	3	Macintosh
	4	Linux
Less secure	5	Windows

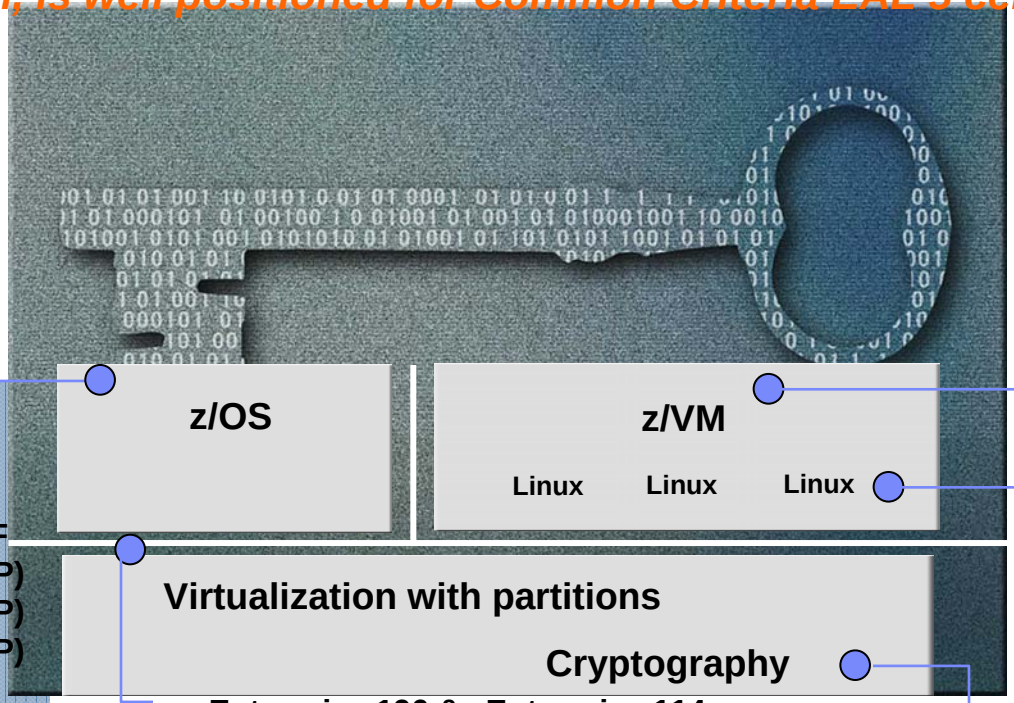
Figure 3 - Security Decision-Makers' Opinions On OSes' Security

- Source: Forrester Research, Inc. 41887
- Base: 75 decision-makers responsible for server security

System z Evaluations & Certifications

… z196, by design, is well positioned for Common Criteria EAL 5 certification !

The Common Criteria program establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/OS

- Common Criteria EAL4+
  - with CAPP and LSPP
  - z/OS 1.7 → 1.10 + RACF
  - z/OS 1.11 + RACF (OSPP)
  - z/OS 1.12 + RACF (OSPP)
  - z/OS 1.13 + RACF (OSPP)
- Common Criteria EAL5
  - z/OS RACF 1.12 (OSPP)
- z/OS 1.10 IPv6 Certification by JITC
- IdenTrust™ certification for z/OS PKI Services
- FIPS 140-2
  - System SSL z/OS 1.10 →1.12 & 1.13
  - z/OS ICSF PKCS#11 Services – z/OS 1.11, 1.12, 1.13
- Statement of Integrity

z/VM

- Common Criteria
  - z/VM 5.3, 6.1
  - EAL 4+ for CAPP and LSPP
- System Integrity Statement

Linux on System z

- Common Criteria
  - SUSE SLES10 certified at EAL4+ with CAPP
  - Red Hat EL5 EAL4+ with CAPP and LSPP
- OpenSSL - FIPS 140-2 Level 1 Validated
- CP Assist - SHA-1 validated for FIPS 180-1 - DES & TDES validated for FIPS 46-3

- zEnterprise 196 & zEnterprise 114
  - Common Criteria EAL5+ with specific target of Evaluation – LPAR: Logical partitions
- Crypto Express2 & Crypto Express3 Coprocessors
  - FIPS 140-2 level 4 Hardware Evaluation
  - Approved by German ZKA
- CP Assist
  - FIPS 197 (AES)
  - FIPS 46-3 (TDES)
  - FIPS 180-3 (Secure Hash)

How does System z fulfill its security strategy:

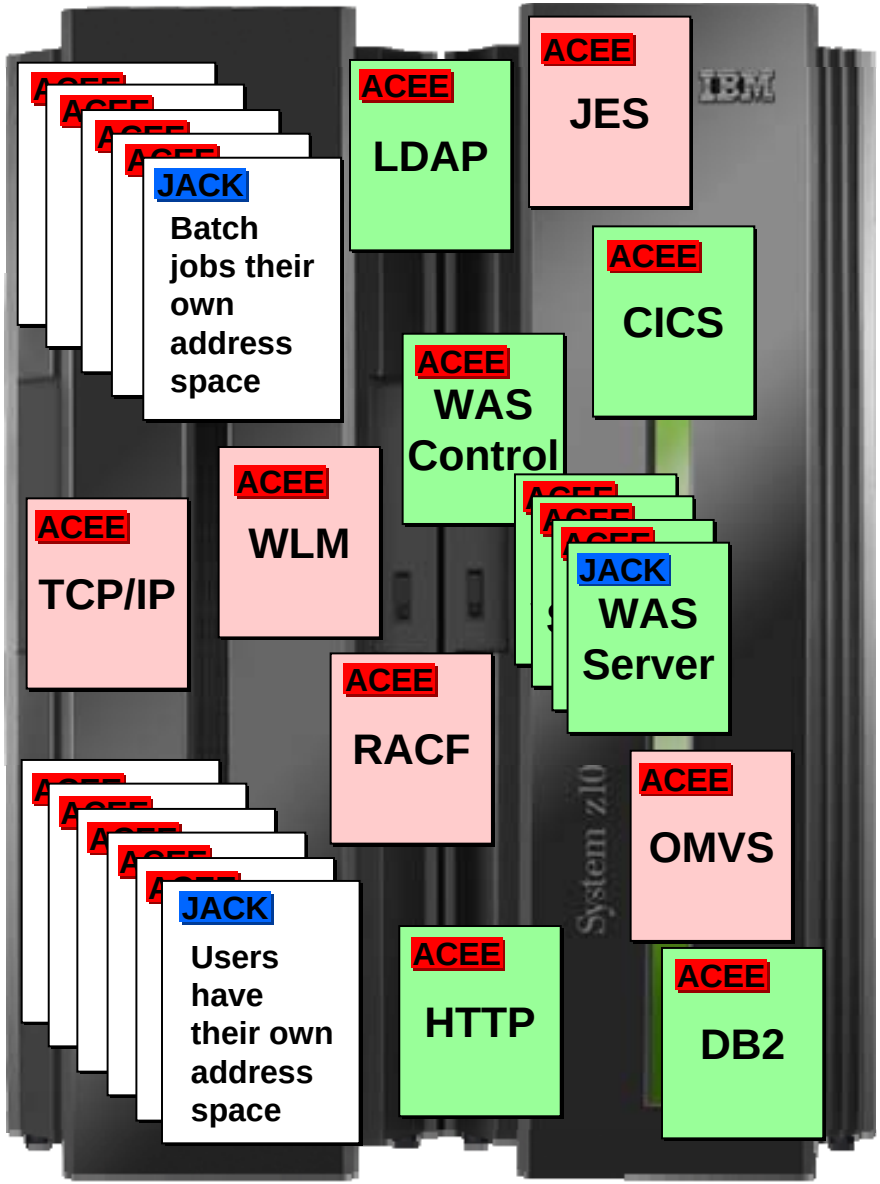
- ENHANCE its own host protection – a continuous process with advancements in digital certificates, RACF in both z/OS and z/VM, tighter integration between Linux for System z, z/OS, and z/VM – strengthening its compliance, auditing, and monitoring capabilities
- PROTECT the host interfaces and boundaries (this includes identities and data passing across these borders) – additions of technologies such as the security features of the z/OS Communication Server, Tivoli Directory Server (LDAP) on both z/OS and z/VM, kerberos enhancements, and PKI Services for z/OS
- EXTEND the security Quality of Service into the enterprise – Encryption Facility for z/OS (to secure data if it has to leave the vault), Network Security Services and Policy Agent (for managing network security policies), z/VM Guest LANs & Virtual Switches, Linux audit plug-in as well as the PAM with LDAP, TKLM and Tivoli Insight (IBM's SOA security is Websphere, Tivoli, and vendor products, most of which can run on System z)
- SIMPLIFY the design, implementation, administration, and monitoring – z/OS Management Facility (z/OSMF) and IBM Security zSecure for example

Remember that address space concept?

Transactions and requests from other systems

External Users
Already Authorized?
ID Propagation

Interactive Users
TSO and USS
Some Privileged

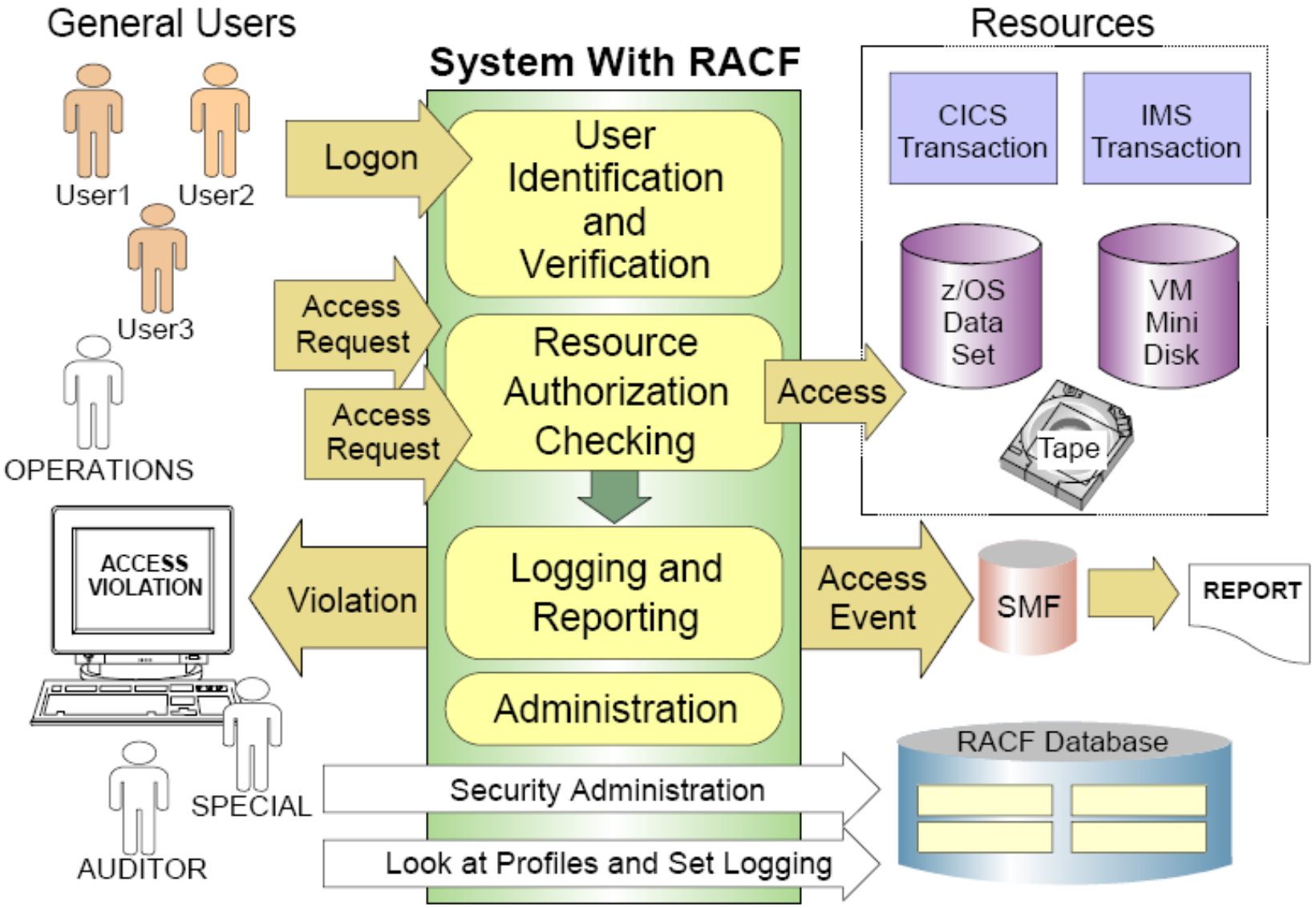


System Files
APF Libraries
RACF Database
Master Catalog

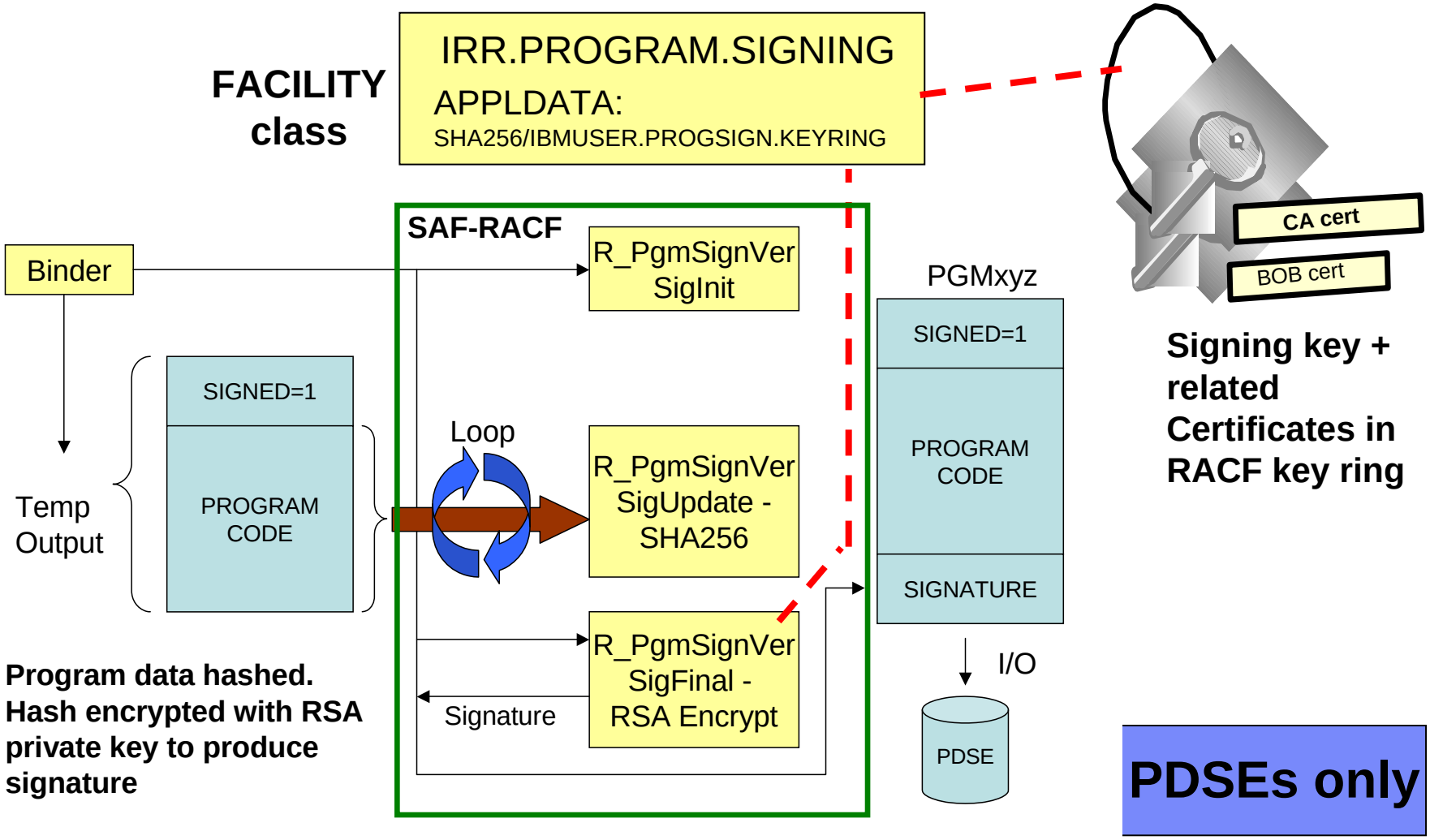
Applications Programs

Data and Databases

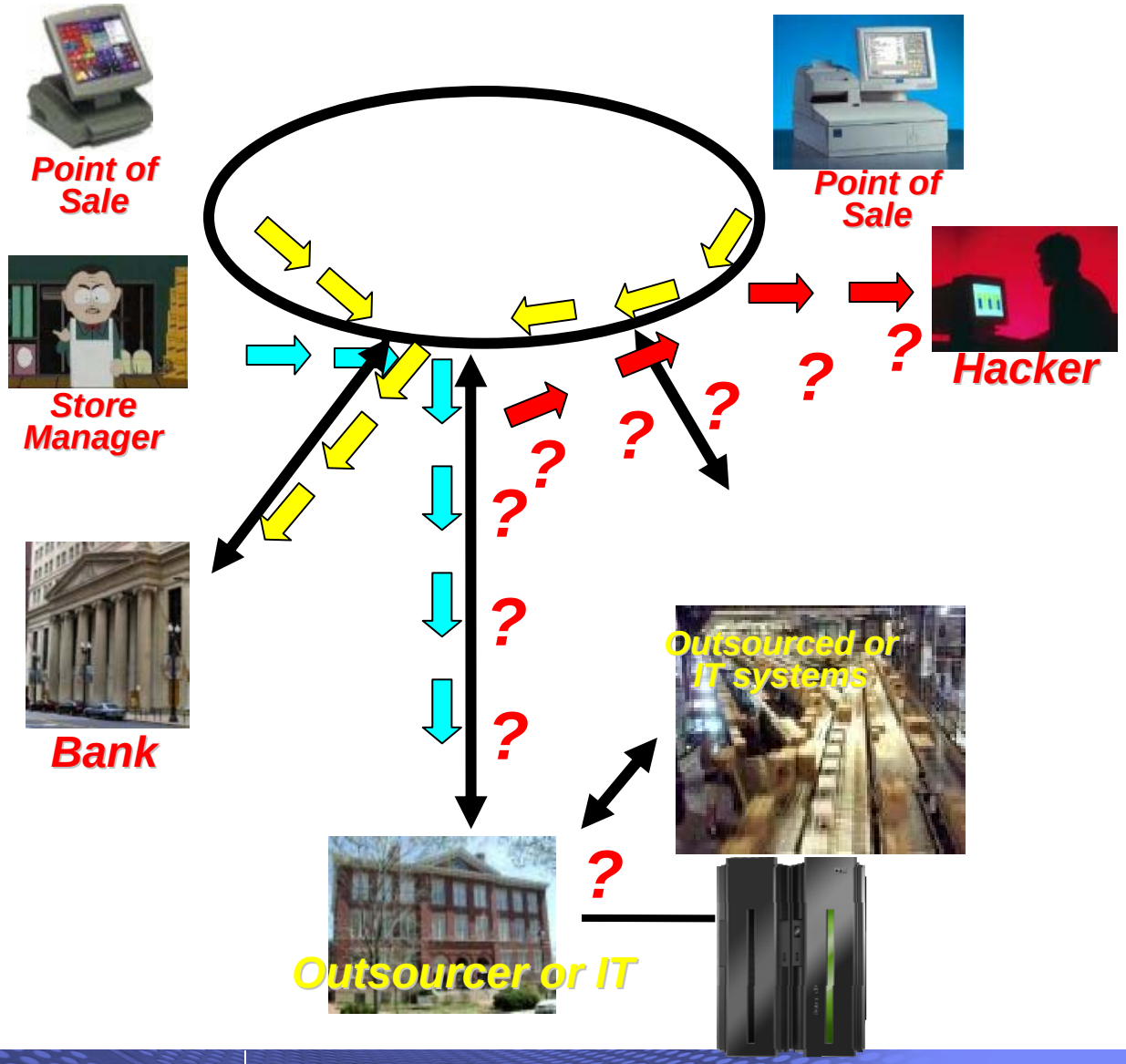
Basic Security Features and Functions



Example: Protecting Sensitive Code



Real Customer Problem – is this a technical hack?



- Store uses WEP wireless for Point of Sale devices
- POS processes cards with banks
- Common password on all store systems
- Security patches not applied to store systems
- Hacker plugs in and gets copies of all transactions
- Problem detected and store systems are getting fixed
- Mainframe folks are happy they are bullet proof
- Hypothesis: Mainframe could help secure stores if they use good procedures
- Store managers run inventory transactions to mainframe
- No encryption on sign in
- No audit records analyzed

Security Features with the z/OS TCP/IP
A view of the protocol stack

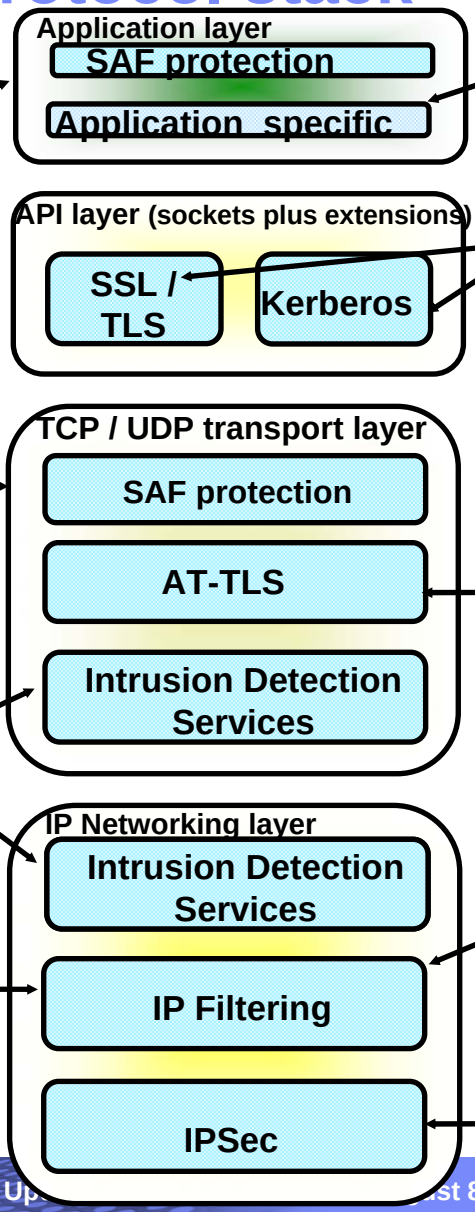
Protect the system

z/OS CS TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources.

The SAF SERVAUTH class is used to prevent unauthorized user access to TCP/IP resources (stack, ports, networks)

Intrusion detection services protect against attacks of various types on the system's legitimate (open) services. IDS protection is provided at both the IP and transport layers.

IP packet filtering blocks out all IP traffic that this systems doesn't specifically permit. These can be configured or can be applied dynamically as "defensive filters."



Protect data in the network

Examples of application protocols with built-in security extensions are SNMPv3 and OSPF.

Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these security functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

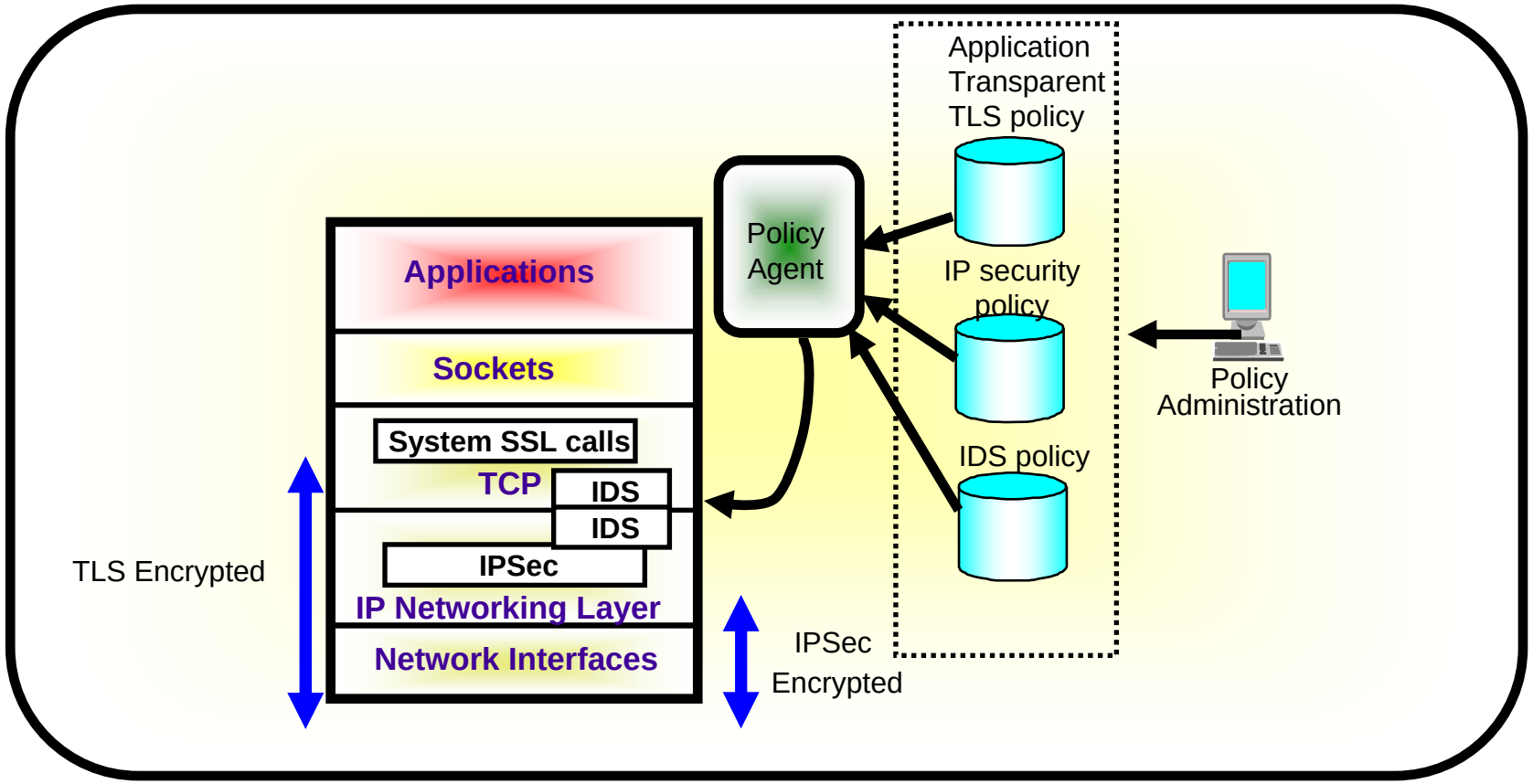
AT-TLS is TCP/IP stack service that provides SSL/TLS services at the TCP transport layer and is transparent to upper-layer protocols. It is avaliable to TCP applications in all programming languages except PASCAL.

IP packet filters specify traffic that requires IPSec

IPSec resides at the networking layer and is transparent to upper-layer protocols, including both transport layer protocol and application protocol.

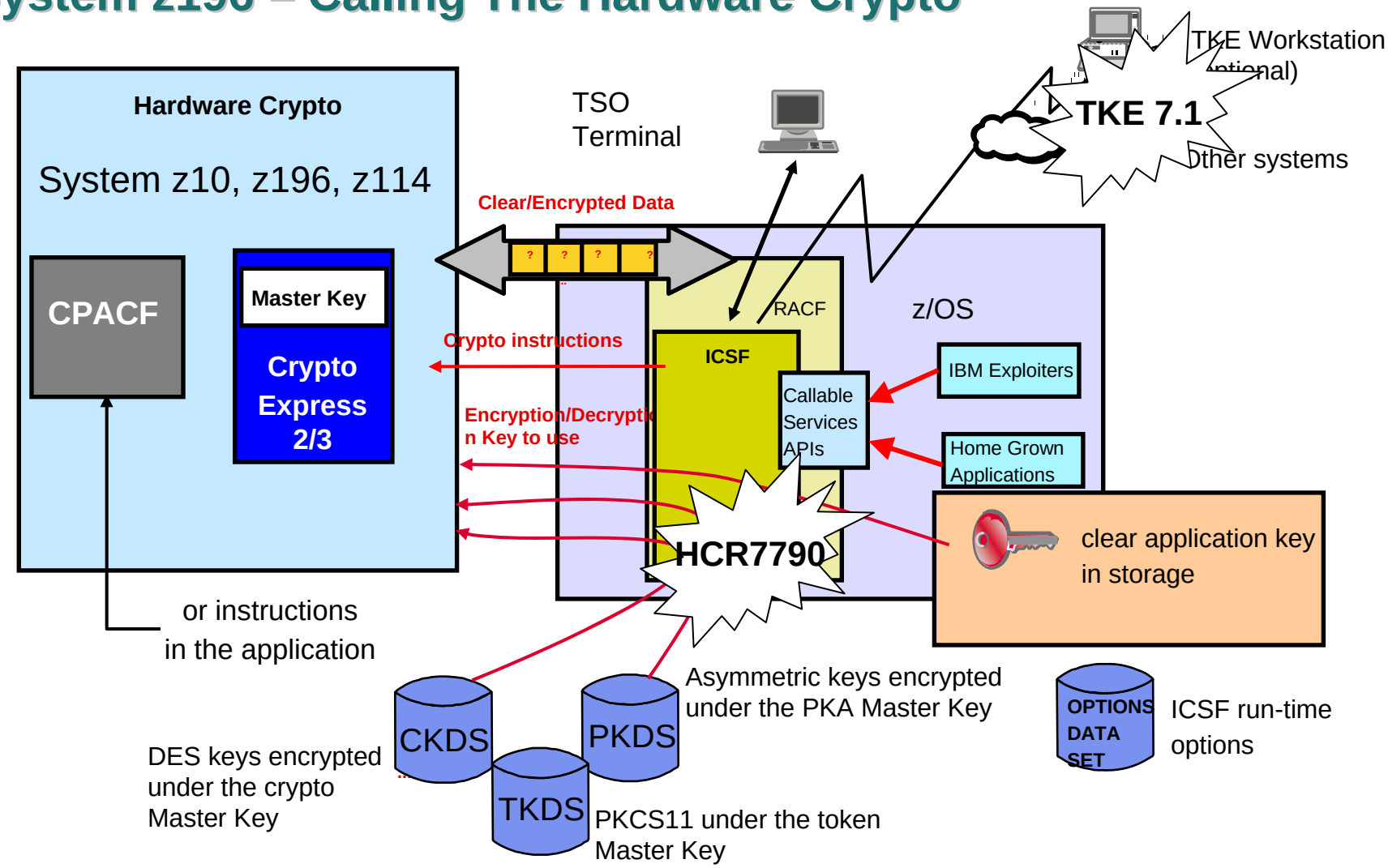
And, of course, you need to Audit the z/OS TCP/IP Configuration Definitions as well …

- The z/OS network security policy is implemented via the Configuration Assistance Utility (now part of zOSMF).
- The network security features that are implemented (IPSec, AT-TLS, etc.) can be viewed via this tool, as well as the rules for each of these features can be reviewed or printed.



Z10 and z196 Crypto Hardware

System z196 – Calling The Hardware Crypto



Access to the cryptographic services and keys can be controlled by RACF with the CSFSERV and CSFKEYS classes

Linux on System z Crypto Stack

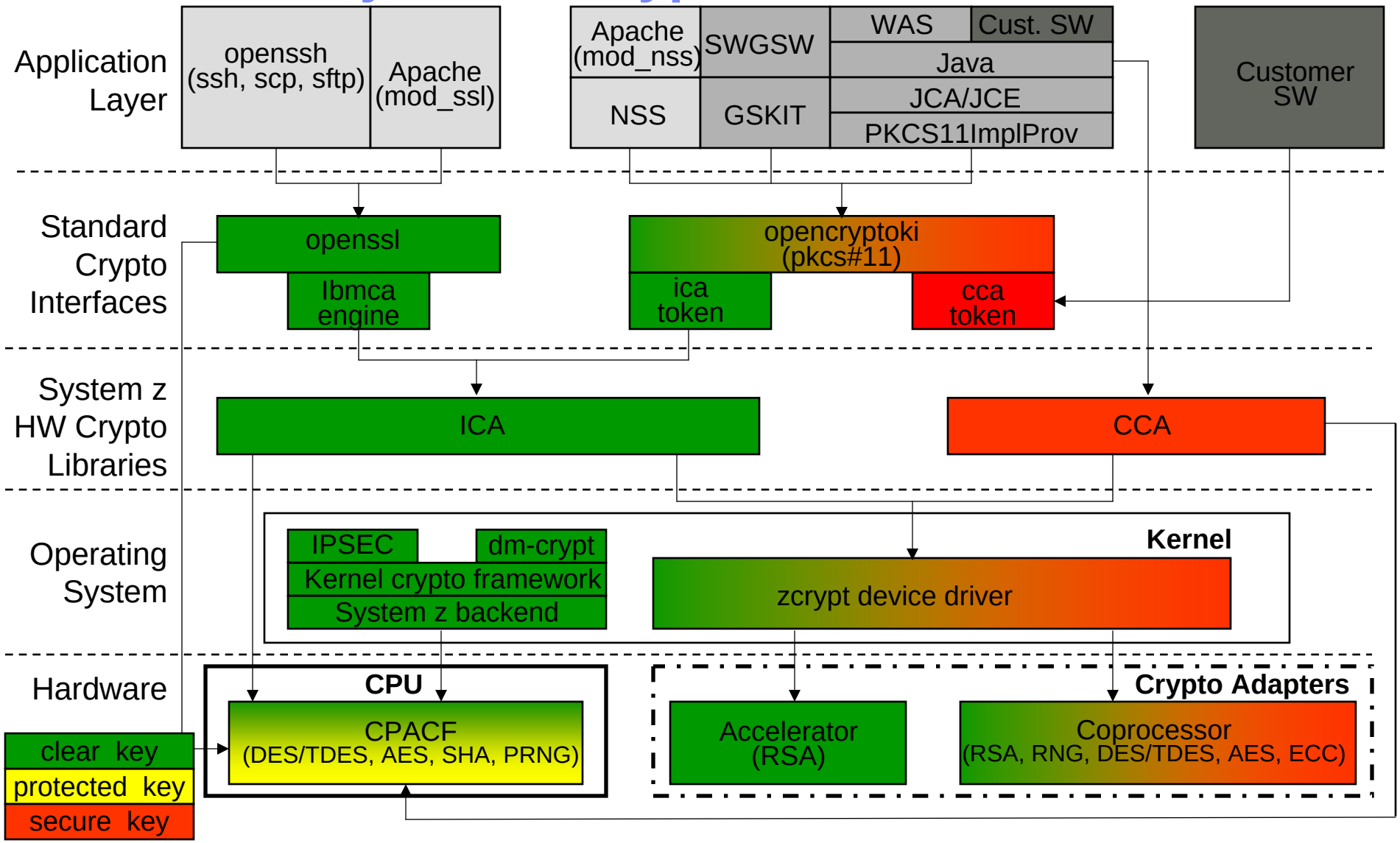
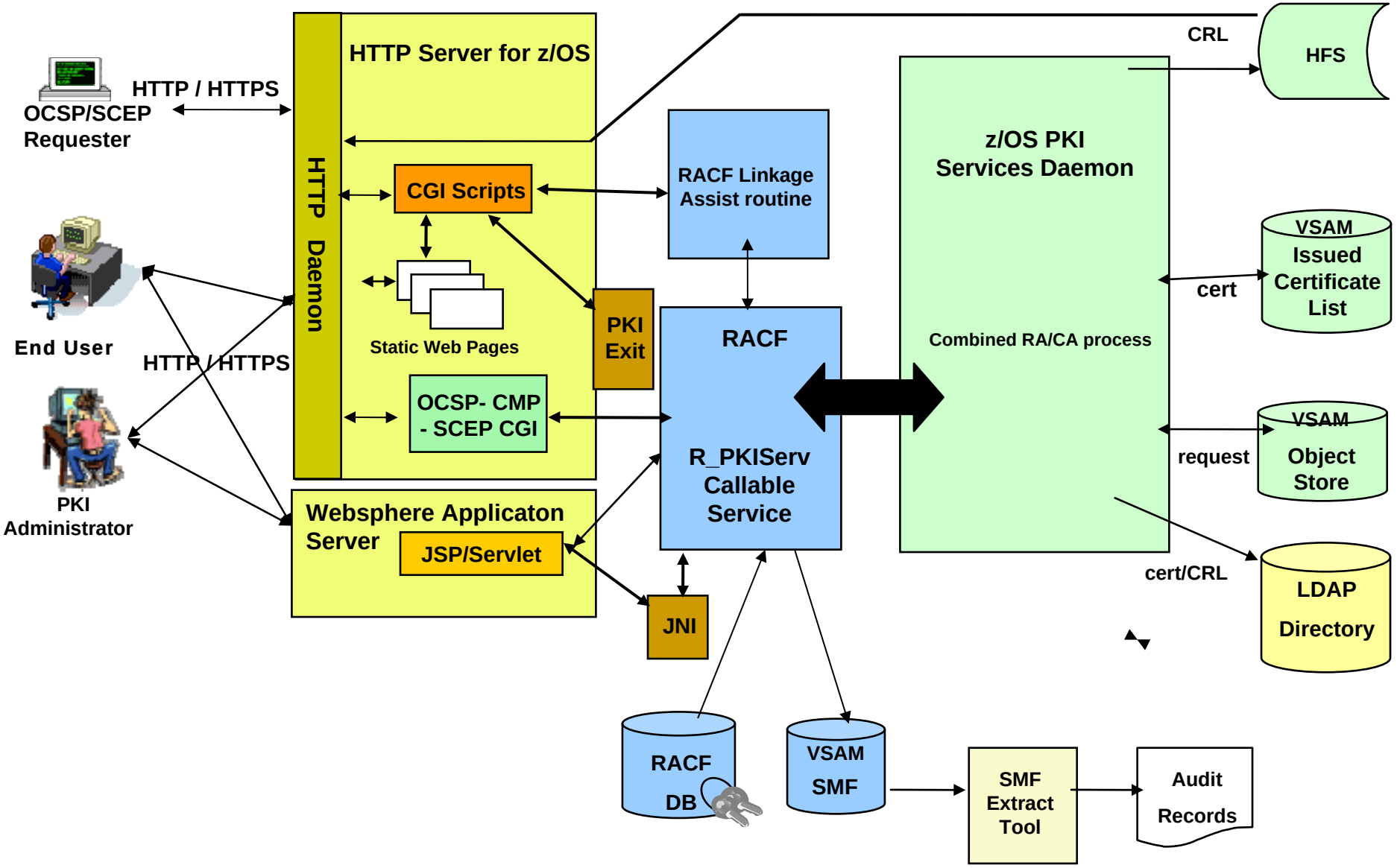
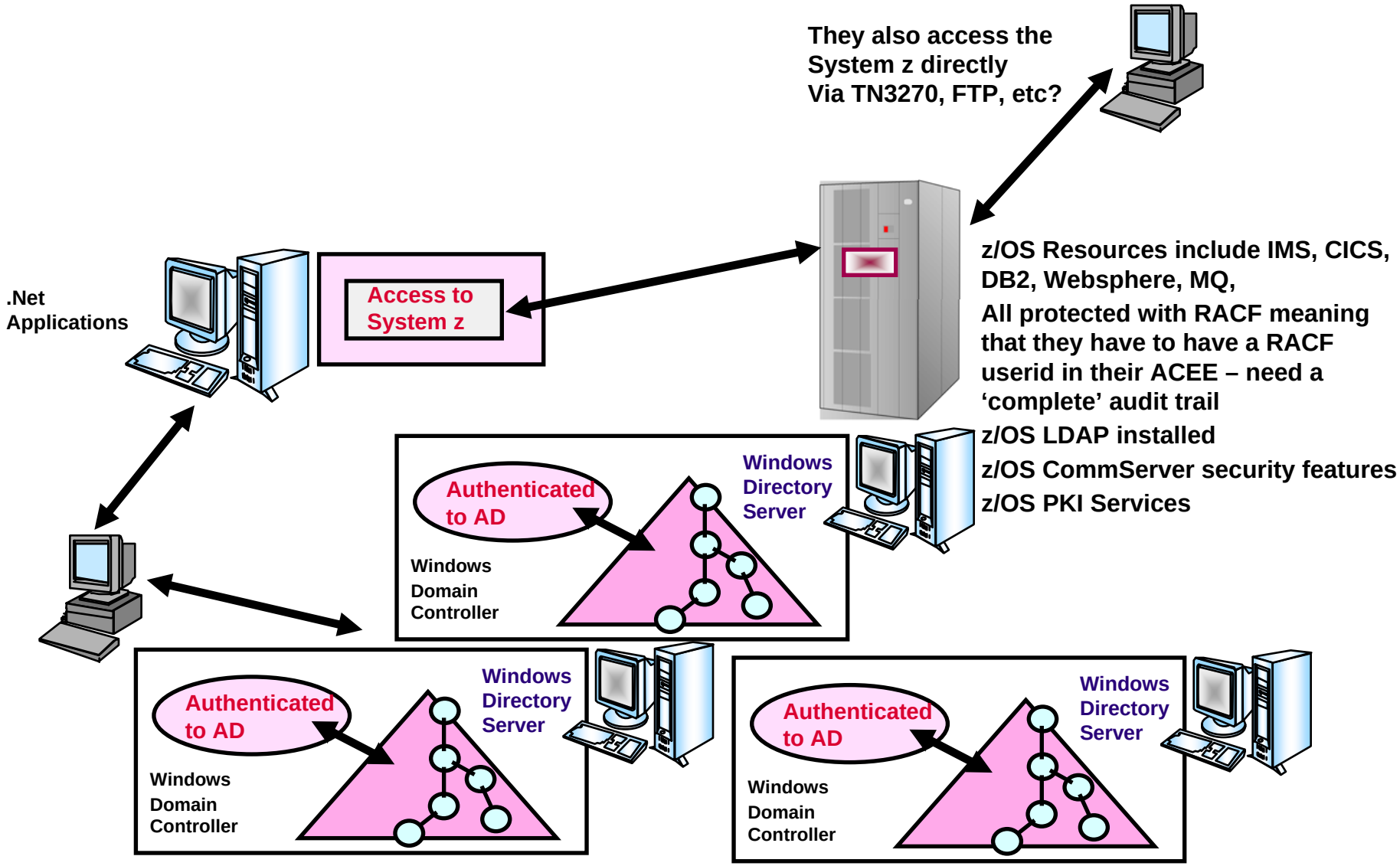


*Chart from Reinhard Buendgen

z/OS PKI Services Structure



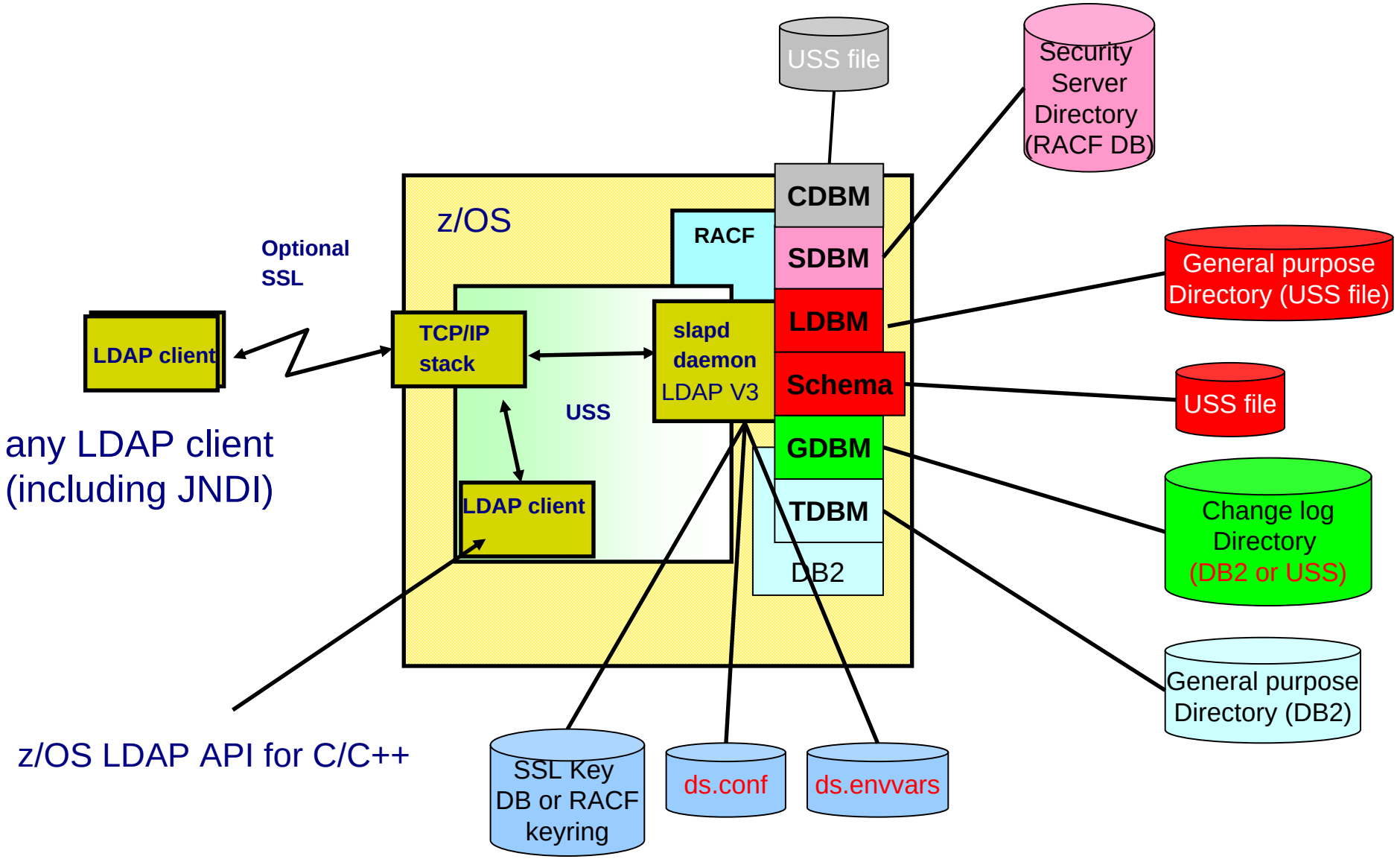
Other Options for Identity Translation/Propagation/Synchronization



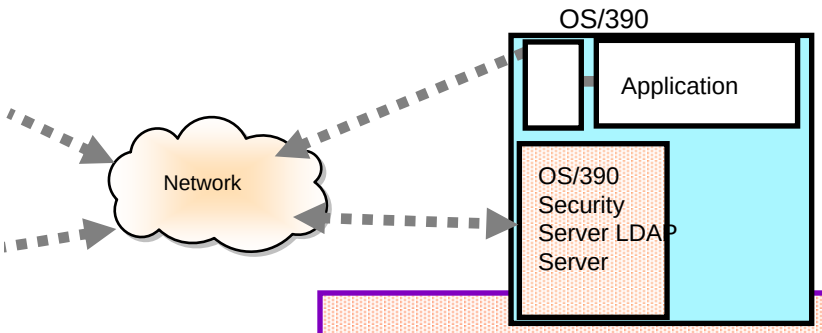
Identify and Access Management

- **Imbedded with the z/OS features:**
  - **Tivoli Directory Services (TDS – commonly called LDAP) extending System z security as well as allowing for propagation of RACF information**
  - **Digital Certificates and z/OS PKI Services**
  - **Kerberos (within the RACF domain and building trust across separate KDC – WAS & SPNEGO)**
  - **Passtickets**
  - **ID Propagation**
- **zSecure for Admin and Audit (plus Command Verifier)**
- **Federating Identities with Tivoli Federated Identity Manager (TFIM) for web services**
- **Tivoli Access Manager (eb (ebusiness) for web security – bi for business integration)**
- **Managing Identities on System z or Across the Enterprise with Tivoli Identity Manager (TIM)**

IBM TDS Overview



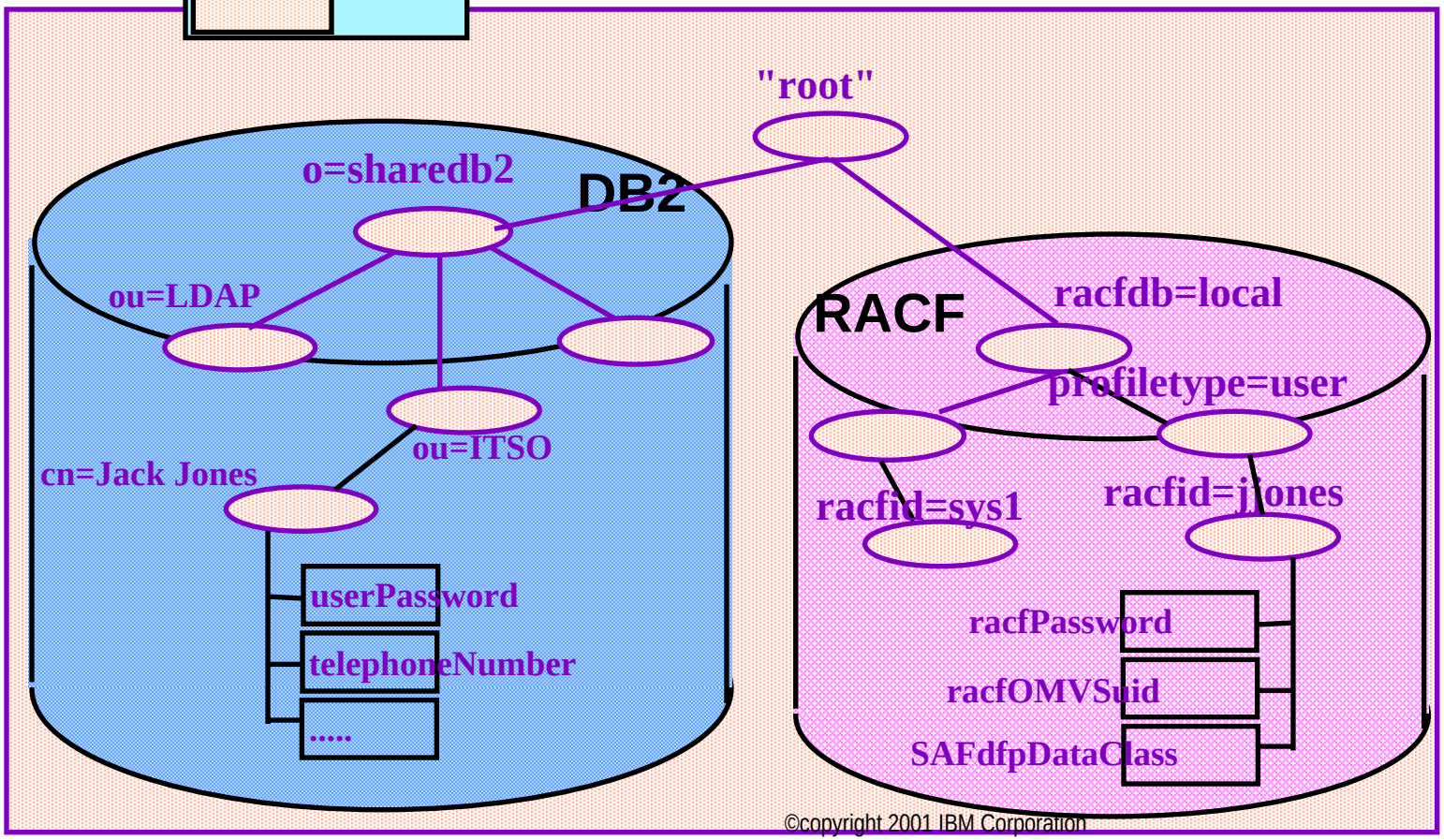
SDBM & TDBM Backends



Slapd.conf:

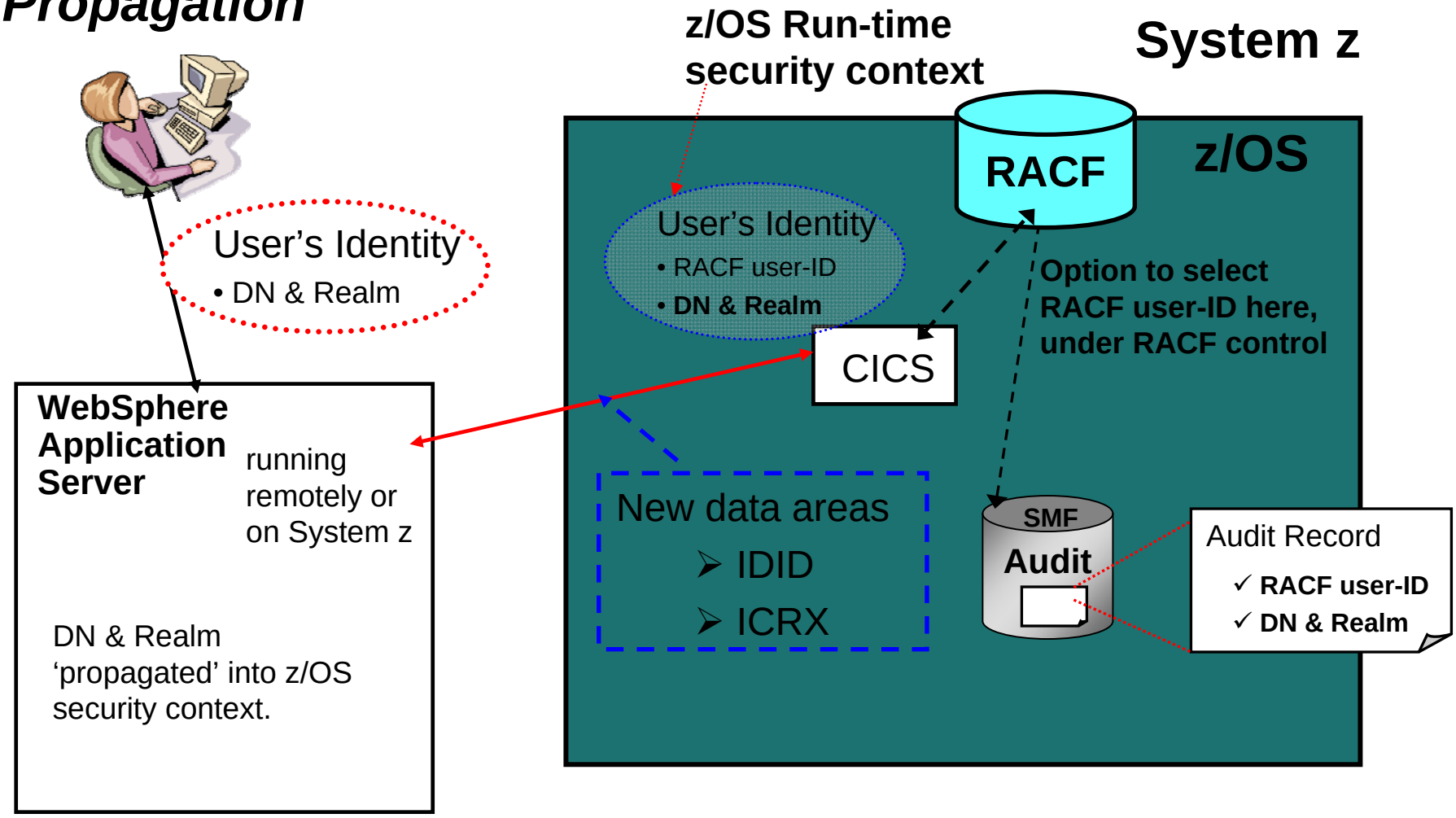
database tdbm gldbtdbm
suffix o=sharedb2

database sdbm gldbsdbm
suffix racfdb=local



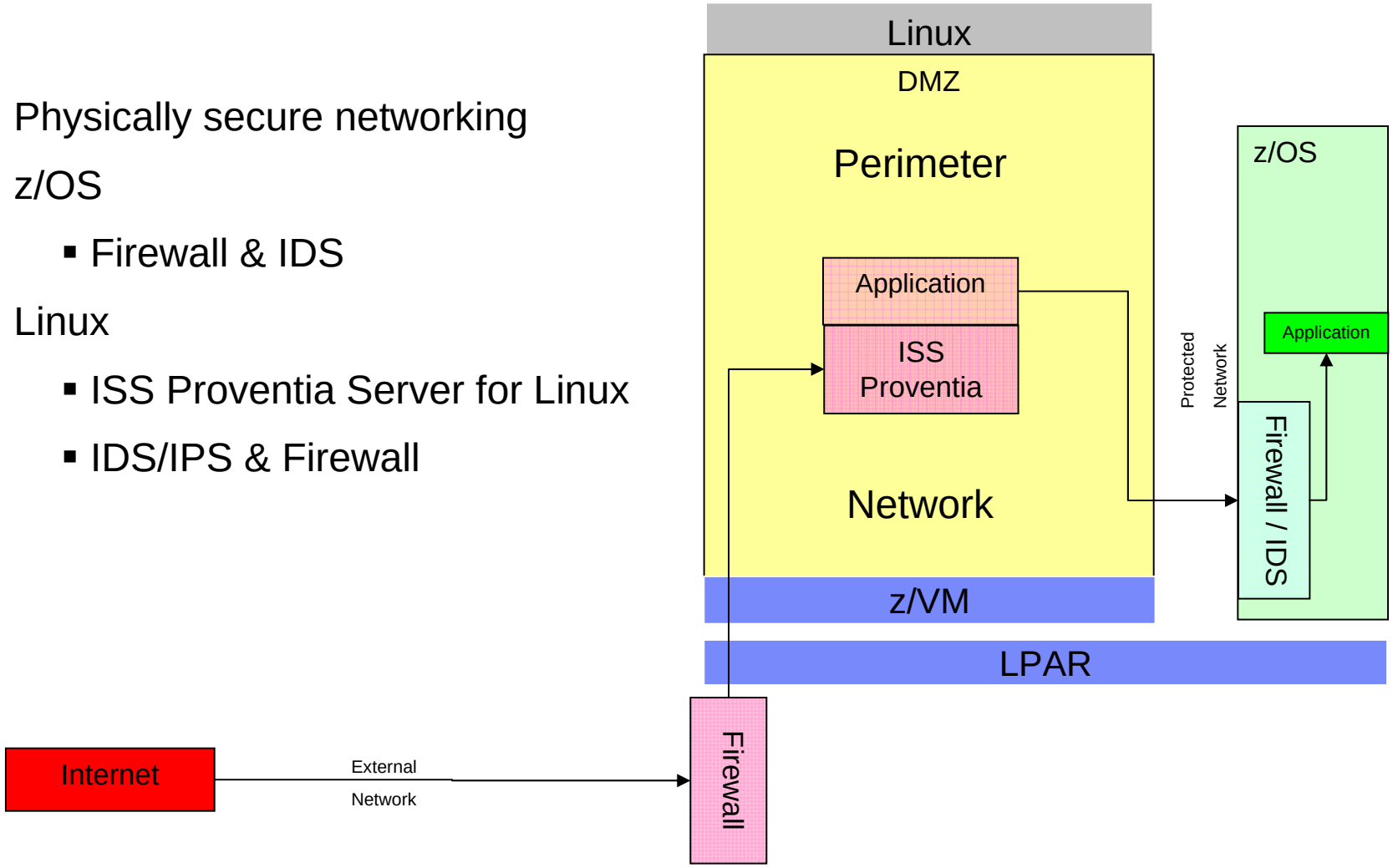
IDENTITY & ACCESS MANAGEMENT

With z/OS Identity Propagation



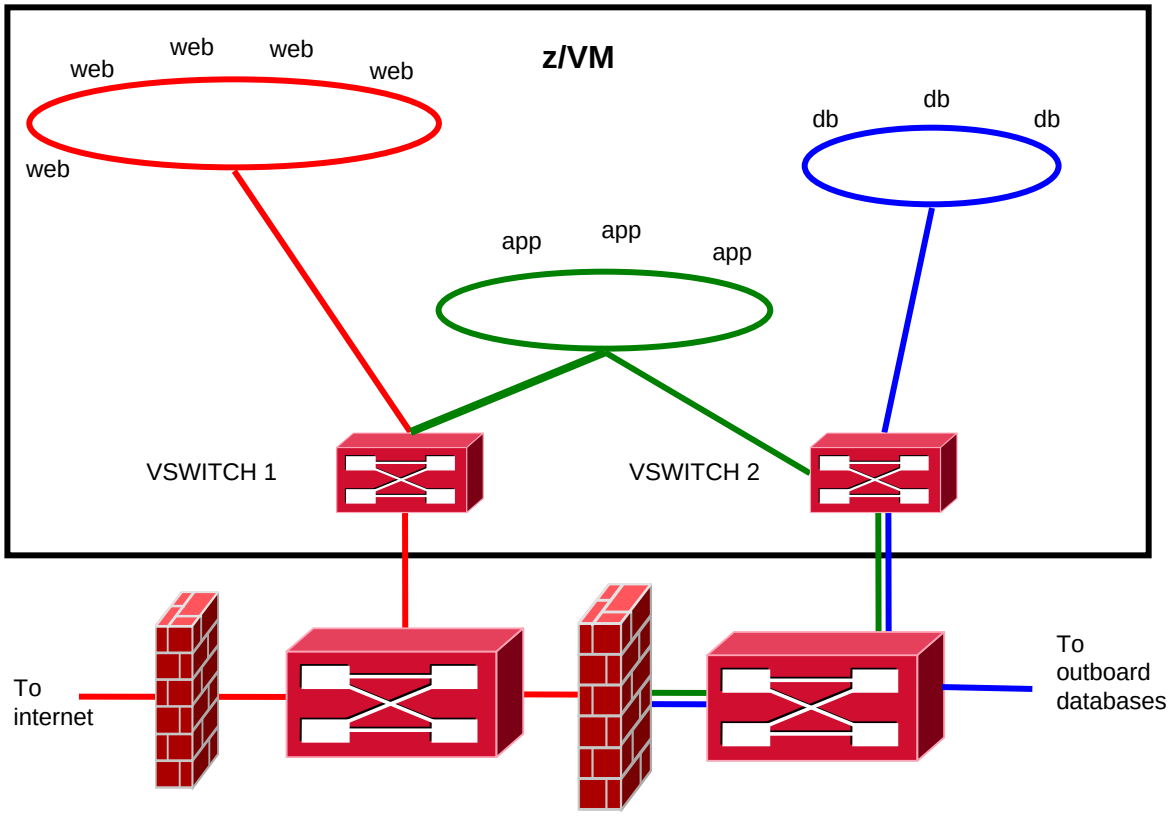
Host Firewalls

- Physically secure networking
- z/OS
  - Firewall & IDS
- Linux
  - ISS Proventia Server for Linux
  - IDS/IPS & Firewall



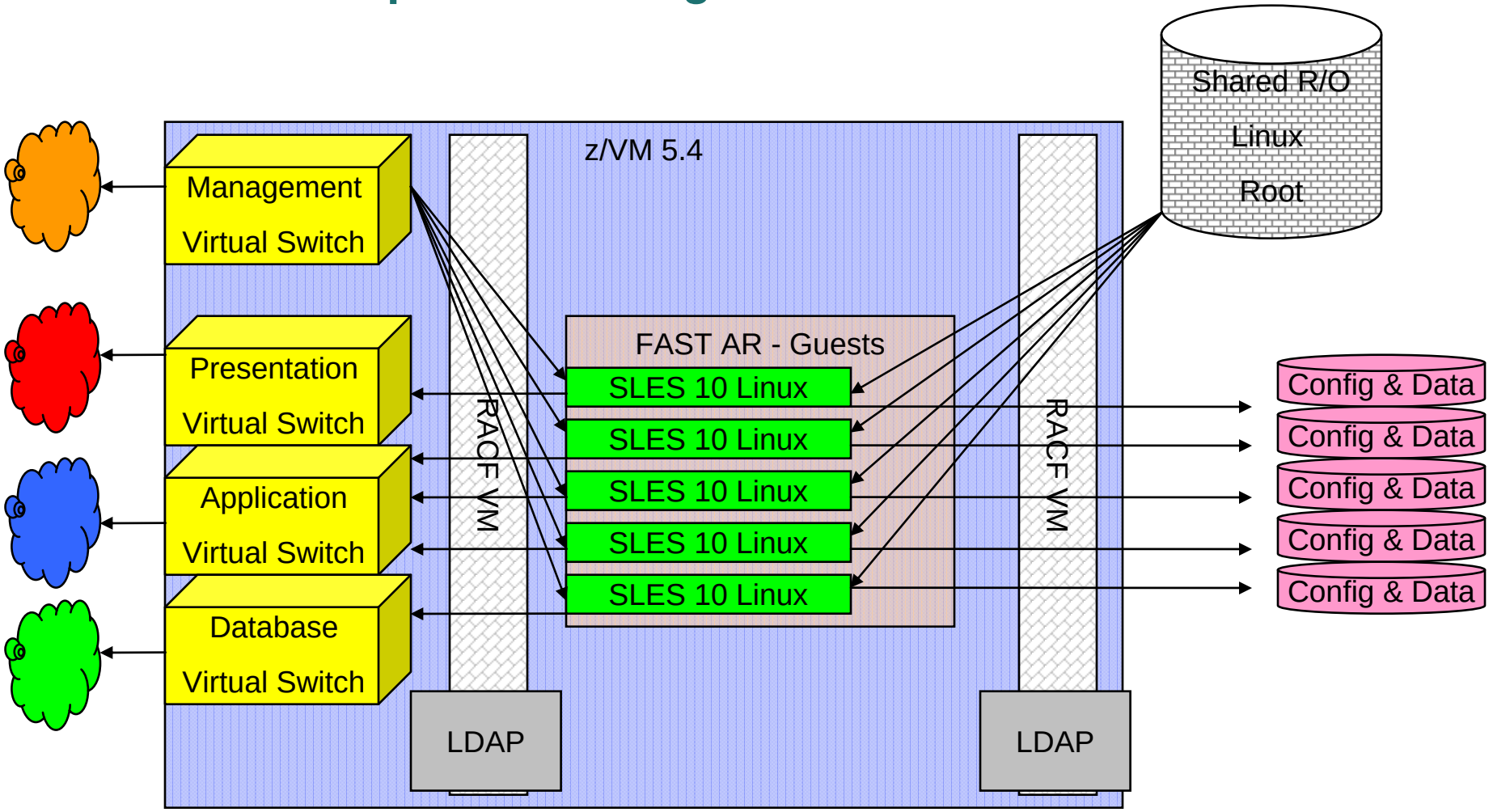
Virtual Network Management
Multiple Security Zones

Use z/VM RACF Security Server to control and audit Linux and other virtual server access to networks.



- **Control access to Virtual Switch (VSWITCH)**
- **Control access to specific VLANs on a VSWITCH**
- **Control and audit guest sniffing of virtual networks**
- **Better control of multi-tenant environments**

Customer Example of Utilizing RACF zVM and LDAP zVM



Linux guest access to a variety of different virtual switches and VLANs are controlled by RACF controls

Architecture overview for Identity Management

Developers

e-Business Users

z/VM

Linux

Linux PAM Directory

RACF

LDAP

ITIM RACF/VM Agent

WebSeal

IBM Tivoli Identity Manager

ITIM Server

ITIM TAM Agent

Tivoli Access Manager

Policy Server

Replica ACL

Master ACL

z/OS

CICS

WebSphere App Server

z/OS Services

ITIM RACF Agent

LDAP Server

App 1 DATA

App 2 DATA

App 3 DATA

App n DATA

RACF Database

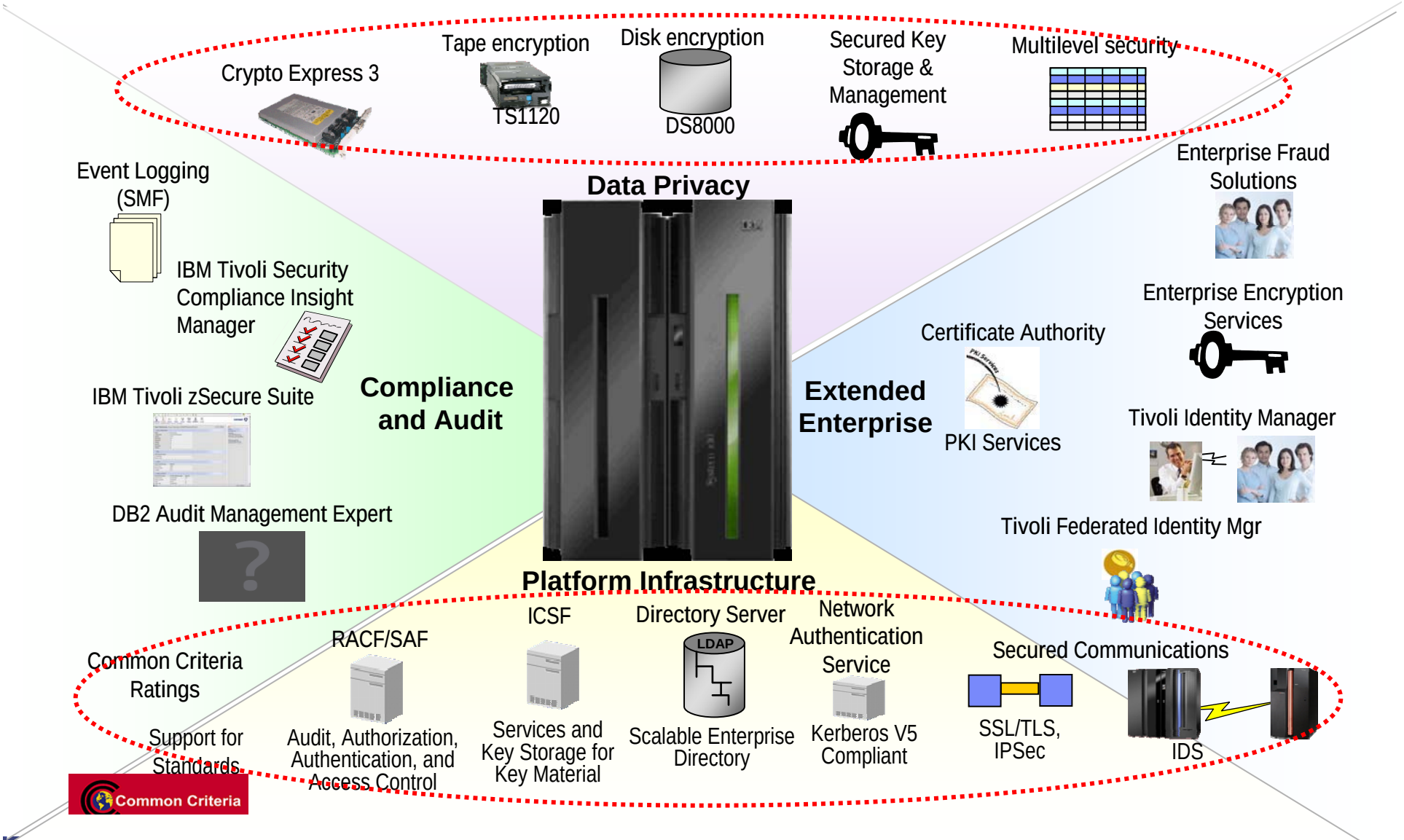
Other User Registry(s)

DMZ

Mgmt/Dev Zone

TRUSTED Zone

Elements of Enterprise Security



References

- **REDP-4528-01 Introducing the IBM Security Framework and the IBM Security Blueprint to realize Business Driven Security**

www.ibm.com/security

