Pulse2011

Enterprise Security (R)Evolution

System z Security – “Secure by Design”

Steve Talbot-Walsh

Senior Technical Architect (SWITA) – System z Architect

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list pricesand performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

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

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance 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 or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

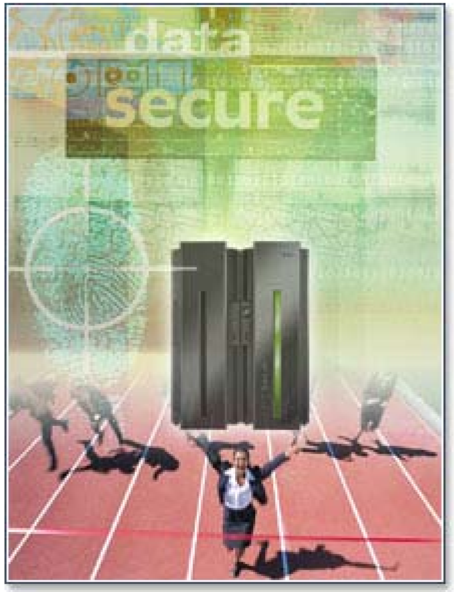
Agenda

- Questions to Consider
- Security Concerns of Mainframe Customers
- Why Security Management for System z?
- System z, z/OS, and z/VM Security Strategy
- Identity & Access Management (zSecure, TIM, FIM)
- Security for UNIX and Linux Environments

Some questions for you to Consider:

- What security system are you currently using on your mainframe?
- How are you proving regulatory compliance today? Is it meeting your needs?
- What is the status of your de-centralized security management?
- Do you need to report, monitor, or assess on compliance with regulatory mandates?
- What audit and regulatory concerns do you have?
- On average, how long would you say it takes to identify a new security vulnerability?
- How was your last company security audit? What was the impact in terms of work disruption? Time? Cost?
- Do you need to enhance the audit, reporting, or administrative capabilities of your current security system?
- Are your security initiatives disjointed? Do you need to define unified security policies?
- Are your security services centralized?
- How much of your IT security budget are you spending on mainframe security?
- How long does it take to implement major security policy changes across the company?
- Would you like to do a better job of managing security from a business perspective?

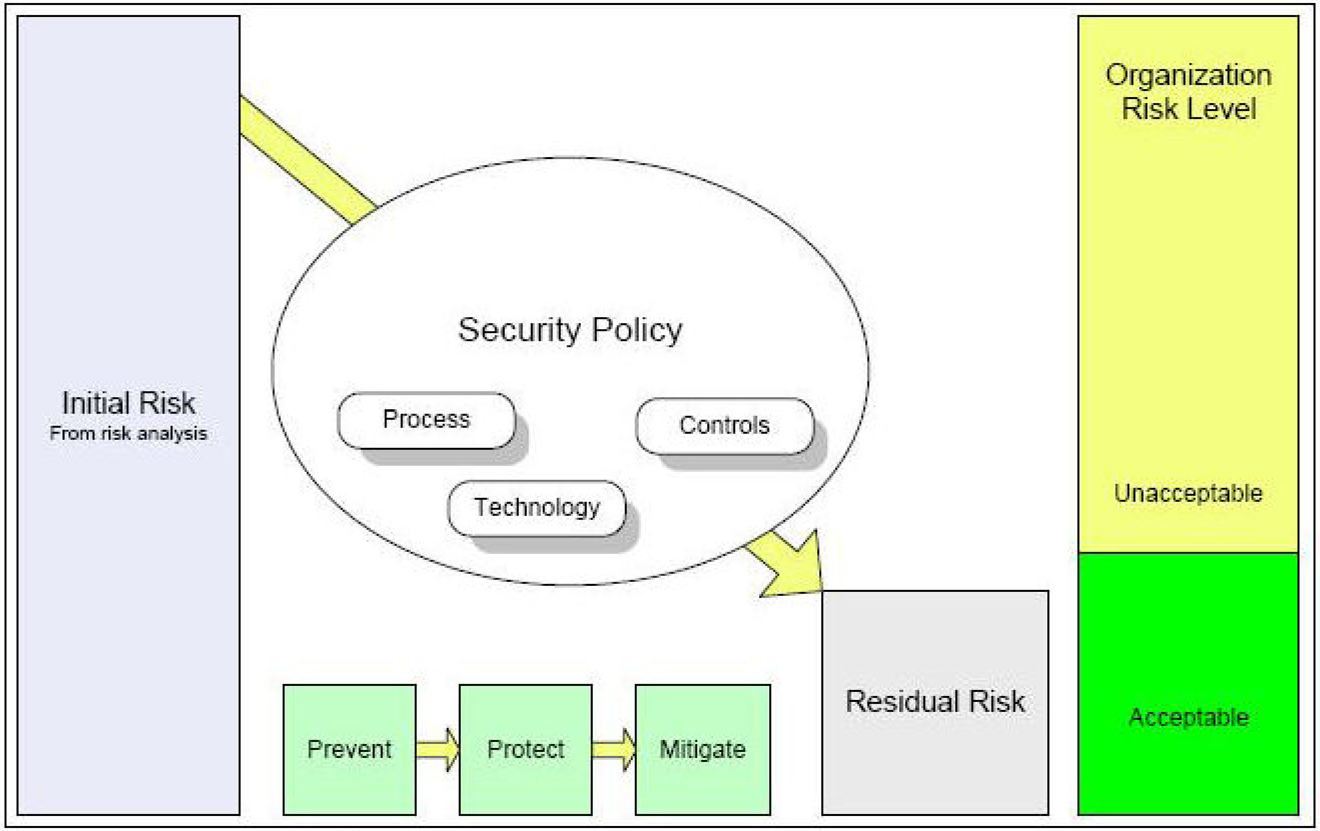
Security Concerns of Mainframe Customers



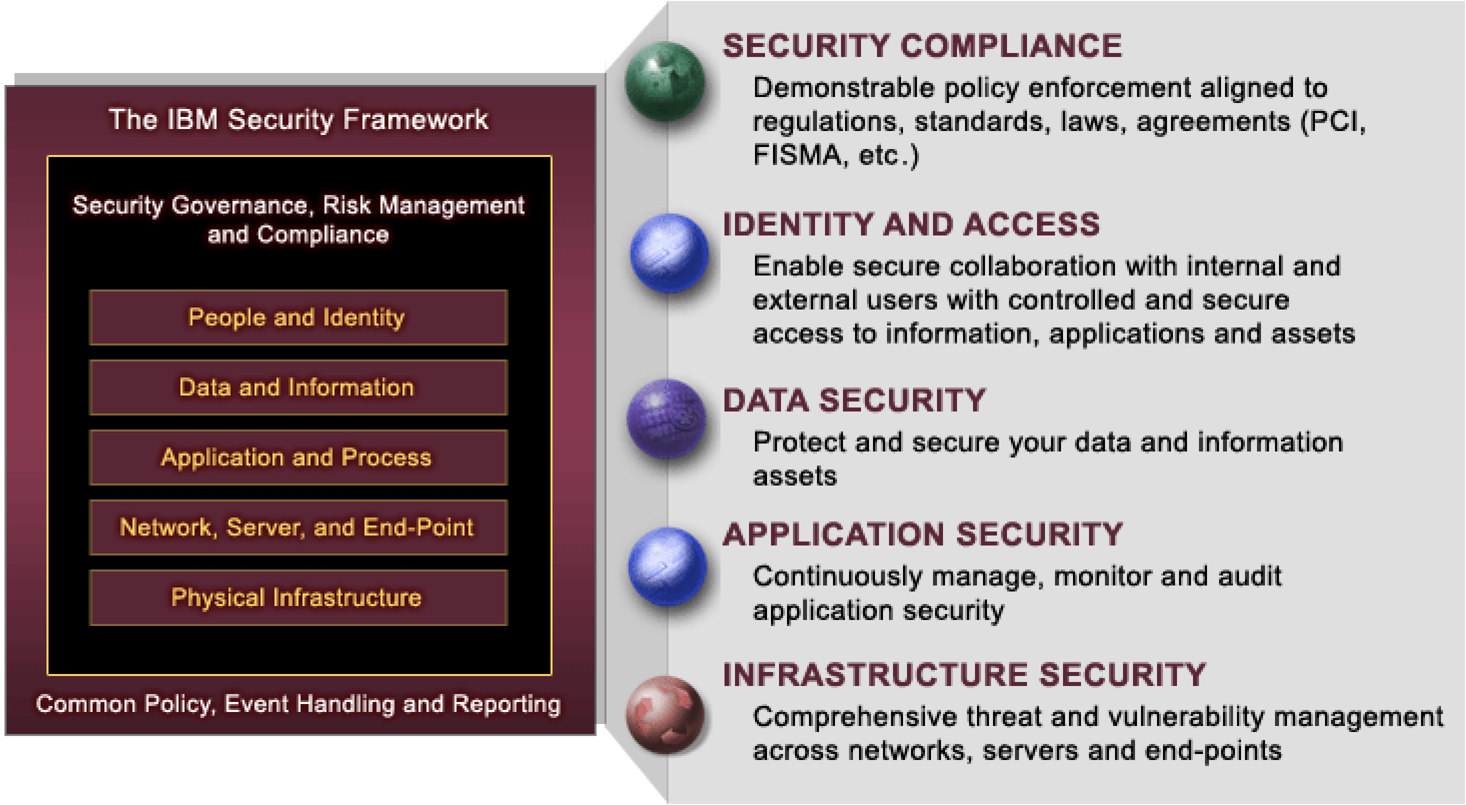
Security Concerns (Overview)

- *Integrity* is the inability to bypass system security controls – the cornerstone of system security
- *Security* is the confidence that systems are operating as expected - is viewed as the boundary of acceptable *risk* for the organization.
- *Compliance* proves that systems operate according to security expectations.

Risk Management



The IBM Security Framework



The IBM Security Framework

Security Governance, Risk Management and Compliance

- People and Identity
- Data and Information
- Application and Process
- Network, Server, and End-Point
- Physical Infrastructure

Common Policy, Event Handling and Reporting

SECURITY COMPLIANCE
Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc.)

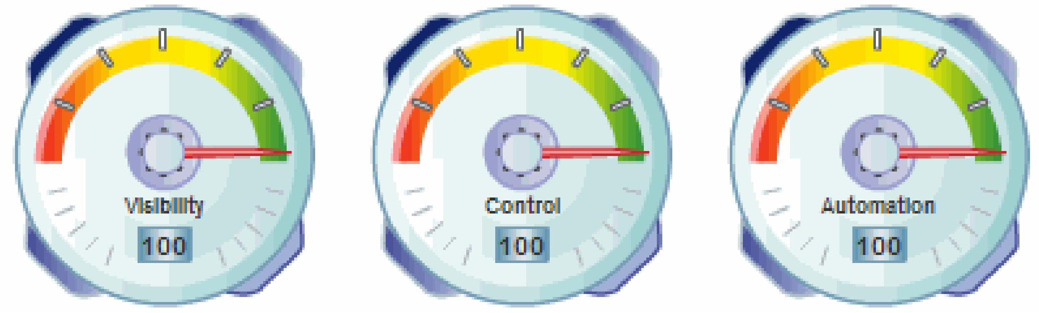
IDENTITY AND ACCESS
Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets

DATA SECURITY
Protect and secure your data and information assets

APPLICATION SECURITY
Continuously manage, monitor and audit application security

INFRASTRUCTURE SECURITY
Comprehensive threat and vulnerability management across networks, servers and end-points

Visibility, Control, and Automation



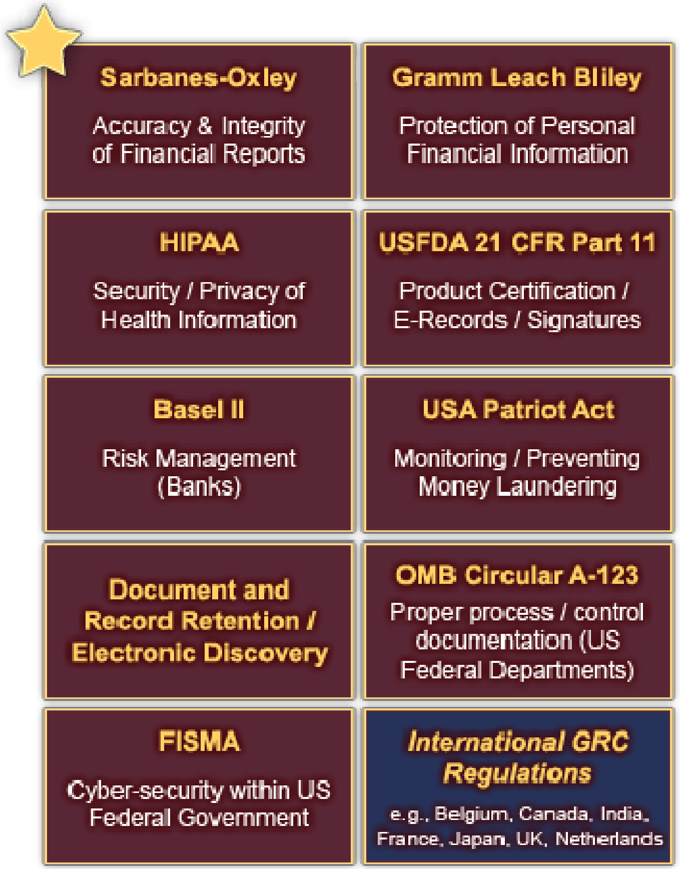
- Visibility: The ability to see everything that is occurring across the environment
- Control: The ability to keep the security environment in its desired state by enforcing policies
- Automation: The ability to manage the ever-increasing size and complexity of infrastructures while controlling cost and quality

Concerns about Security Administrator Retirement

- Security administration is not an easy task!
- RACF® is a component of 86% of System z platforms
- The RACF administrator determines policies and settings to be configured in RACF, monitors and supports security information, and completes many other ancillary tasks.
- The RACF administrator does not have time to be a security administrator.
- As the demand for mainframes continues, so does the demand for RACF administrators. As RACF administrators prepare for retirement, there is an ever-increasing need to transfer their knowledge and provide easier-to-use tooling, such as the zSecure suite of products.

Security Concerns Related to Sarbanes-Oxley and Other Regulatory Compliance

- Information security must demonstrate compliance with different laws and compliance rules among geographies.
- Security compliance is about aligning IT security to business priorities.
- **The current focus on compliance is on PCI-DSS, Sarbanes-Oxley, and Basel II.**
- Additional topics of interest are national data security laws, the European Directive, and security-monitoring solutions.



Sarbanes-Oxley Accuracy & Integrity of Financial Reports	**Gramm Leach Bliley** Protection of Personal Financial Information
HIPAA Security / Privacy of Health Information	**USFDA 21 CFR Part 11** Product Certification / E-Records / Signatures
Basel II Risk Management (Banks)	**USA Patriot Act** Monitoring / Preventing Money Laundering
Document and Record Retention / Electronic Discovery	**OMB Circular A-123** Proper process / control documentation (US Federal Departments)
FISMA Cyber-security within US Federal Government	***International GRC Regulations*** e.g., Belgium, Canada, India, France, Japan, UK, Netherlands

Sarbanes-Oxley Act

- The Sarbanes-Oxley (SOX) Act was a reaction to corporate scandals and lack of investor confidence.
- SOX regulations require quarterly submissions, and large fines are imposed for failure to comply.
- Two sections of SOX are very important to most organizations: **SOX section 302** and **SOX section 404**.

SOX Section 302

- SOX section 302 deals with quarterly reporting of material incidents and deficiencies, and states the requirements for the Management Report on Accuracy of Disclosures.
- The report captures all of the material incidents that occurred during the quarter and that affect the accuracy of financial statement disclosure.
- IT requirements related to SOX section 302 include:
  - Understanding and mitigation of risks associated with finance systems
  - Accurate monitoring and measurement of activities related to finance systems
  - Incident reporting associated with the finance system, such as fraud and unauthorized disclosure

SOX Section 404

- SOX section 404 specifies requirements for the Management Report on Internal Controls and the auditor report on Management's Evaluation on Internal Controls.
- SOX section 404 requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in their annual fiscal reports.
- CIOs are responsible for the security, accuracy, and reliability of the systems that manage and report financial data.
- Independent auditors must attest to and report on the validity of the assessments.

The top five material deficiencies based on the last two years of SOX section 404 filings:

1. Improper change management
2. Insufficient segregation of duties
3. Excessive access to systems, databases, or both
4. Lack of access controls
5. Lack of general monitoring of the security infrastructure

Security Concerns Related to Merger and Acquisition Activities

To achieve a successful transition, these questions, among others, need answers:

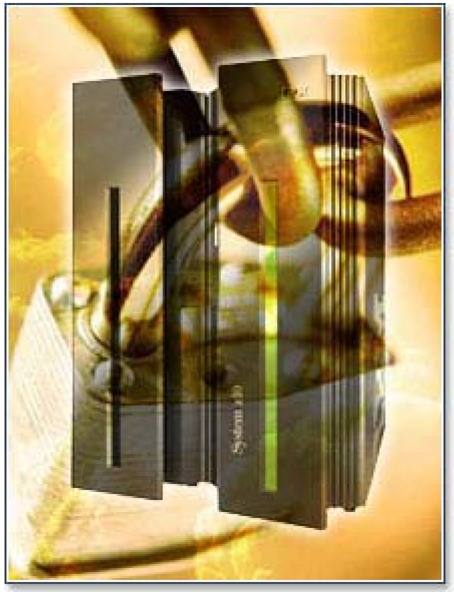
- **Provisioning**
  - is every user account on every resource valid?
  - is user access configured correctly to every resource, and does it stay that way?
- **Productivity**
  - are users efficiently gaining access to valid resources?
- **Access**
  - are access policies and data disclosure rules implemented consistently across every application, data source, and operating system?
- **Audit**
  - how do I find inappropriate access by privileged and trusted users?
  - how do I find inappropriate access to the database management system resources?

Summary: Security Concerns of Mainframe Customers

- Protection of corporate data is a priority at the highest levels of management. A security breach could expose the company to legal and financial penalties and negative publicity.
- Because it is impossible to conduct business without exposure to risk, risk must be managed. Risk management requires analysis to determine the existence of a threat, the probability of occurrence, the potential damage from the threat, and trade-offs to maximize the cost benefit.
- Security administrators are often responsible for so many administrative tasks that the focus on security is blurred. This fact demonstrates a need and an opportunity for more efficient tools that are easier to use.
- Failure of the financial industry to self-regulate has led to government controls that require organizations to comply with very cumbersome and complex rules or face severe financial and legal consequences.
- Mergers and acquisitions are the modern-day preference for growth. This trend introduces many security challenges to integrate processes and databases.

Why Security Management for System z?

Security built in. Not bolted on.



Security for the Mainframe

Why do organizations want mainframe security solutions?

- To protect critical applications and data (over 75% of the world's most critical business data resides on System z)
- To simplify administrative tasks
- To simplify identity and access management
- To gain access to tools that help with compliance efforts
- To reduce costs (TCO)

43% of CFOs think that improving governance, controls, and risk management is their top challenge.

An Analyst's View of Mainframe Security

> *"If IBM has a shortcoming, it's that it hasn't bragged enough about its security capabilities.*
>
> *"Their home turf is the mainframe. That's the Fort Knox of IT today, as it has been the last several decades. That's the most secure environment you will ever find."*
>
> – Bob Djurdjevic
> President of Annex Research

Security: Inherently Built into z/OS

Secure hardware

Secure operating system

Secure storage and encryption

Resource Access Control Facility

Tivoli Security Management for z/OS

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 !!

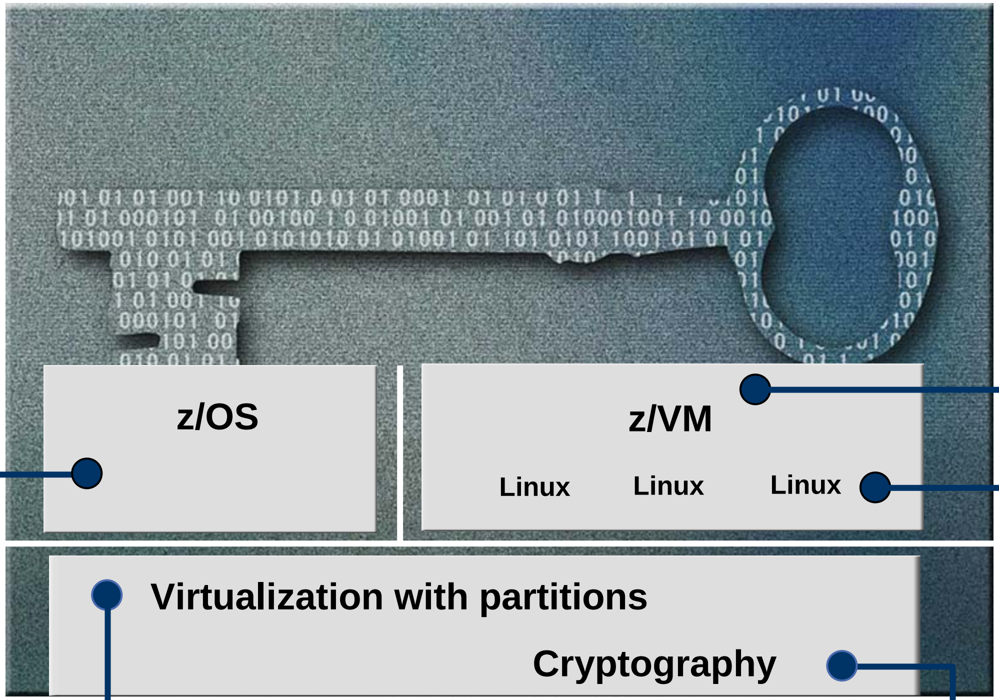
For System z Security has been a state of mind from design to delivery

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

System z Certifications

… the 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 + RACF
  - z/OS 1.8 + RACF
  - z/OS 1.9 + RACF
  - z/OS 1.10 + RACF
- Common Criteria EAL4+
  - With OSPP
  - z/OS 1.11 + RACF
- z/OS 1.10 IPv6 Certification by JITC
- IdenTrust™ certification for z/OS PKI Services

System z10 & z9 EC and BC Servers

- Common Criteria EAL5 with specific target of evaluation for Logical partitions
- Crypto Express 2 Coprocessor
  - FIPS 140-2 level 4 Hardware Evaluation
  - Approved by German ZKA
- Crypto Express 3 Coprocessor
  - Designed for FIPS 140-2 Level 4 compliance
  - Designed for German ZKA compliance
- CP Assist
  - FIPS 197 (AES)
  - FIPS 46-3 (TDES)
  - FIPS 180-3 (Secure Hash)

z/VM

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

Linux on System z

- Common Criteria Certified at EAL 4+
  - Novell SUSE LES10 - with CAPP
  - Red Hat RHEL 5 EAL4+ - CAPP and LSPP
- FIPS
  - OpenSSL - FIPS 140-2 Level 1 Validated

See: www.ibm.com/security/standards/st_evaluations.shtml

How System z fulfills its security strategy:

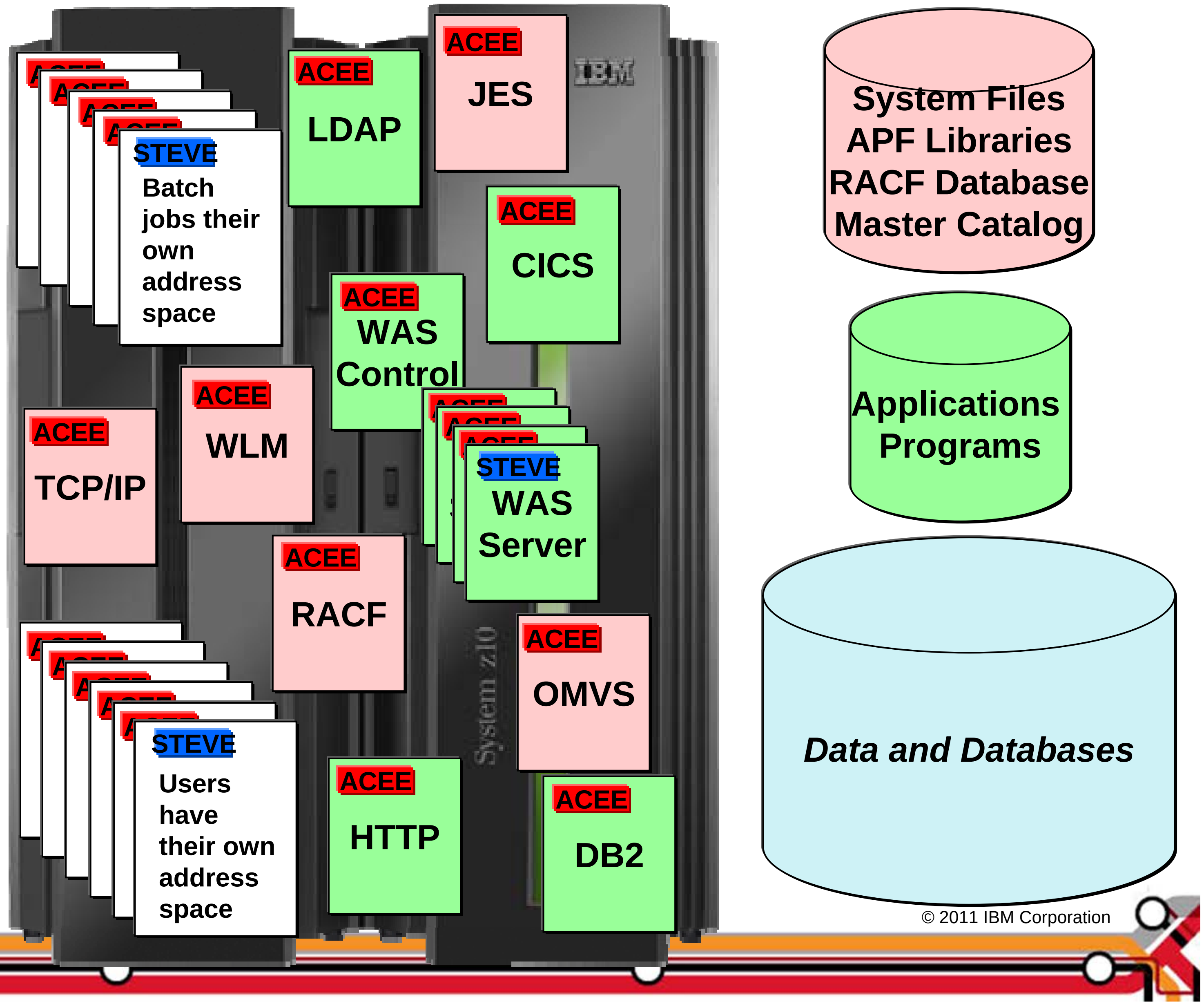
- **ENHANCING AND EVOLVING internal host protection – a continuous process with advancements in Digital Certificates, Encryption, RACF (in both z/OS and z/VM), tighter integration between Linux for System z, z/OS, and z/VM – strengthening its compliance, auditing and monitoring capabilities.**
- **PROTECTING the host interfaces and boundaries (incl. 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 z System z Security QoS into the enterprise – Encryption Facility for z/OS (to secure data if it has to leave the host), 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 Manager (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?

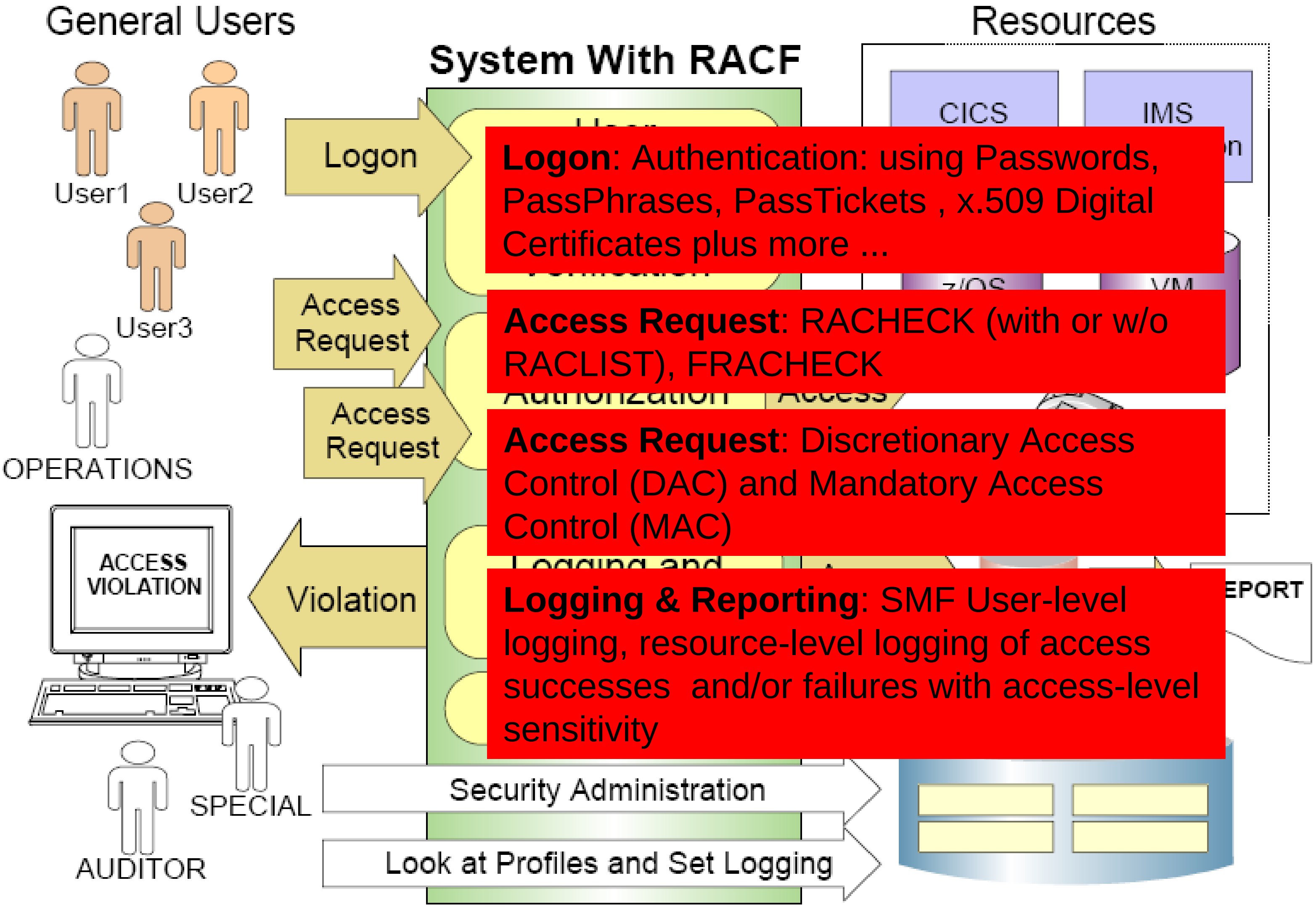
Transactions and requests from other systems

External Users
Already Authorized?
ID Propagation

Interactive Users
TSO and USS
Some Privileged



Basic Security Features and Functions of RACF



Logon: Authentication: using Passwords, PassPhrases, PassTickets , x.509 Digital Certificates plus more ...

Access Request: RACHECK (with or w/o RACLIST), FRACHECK

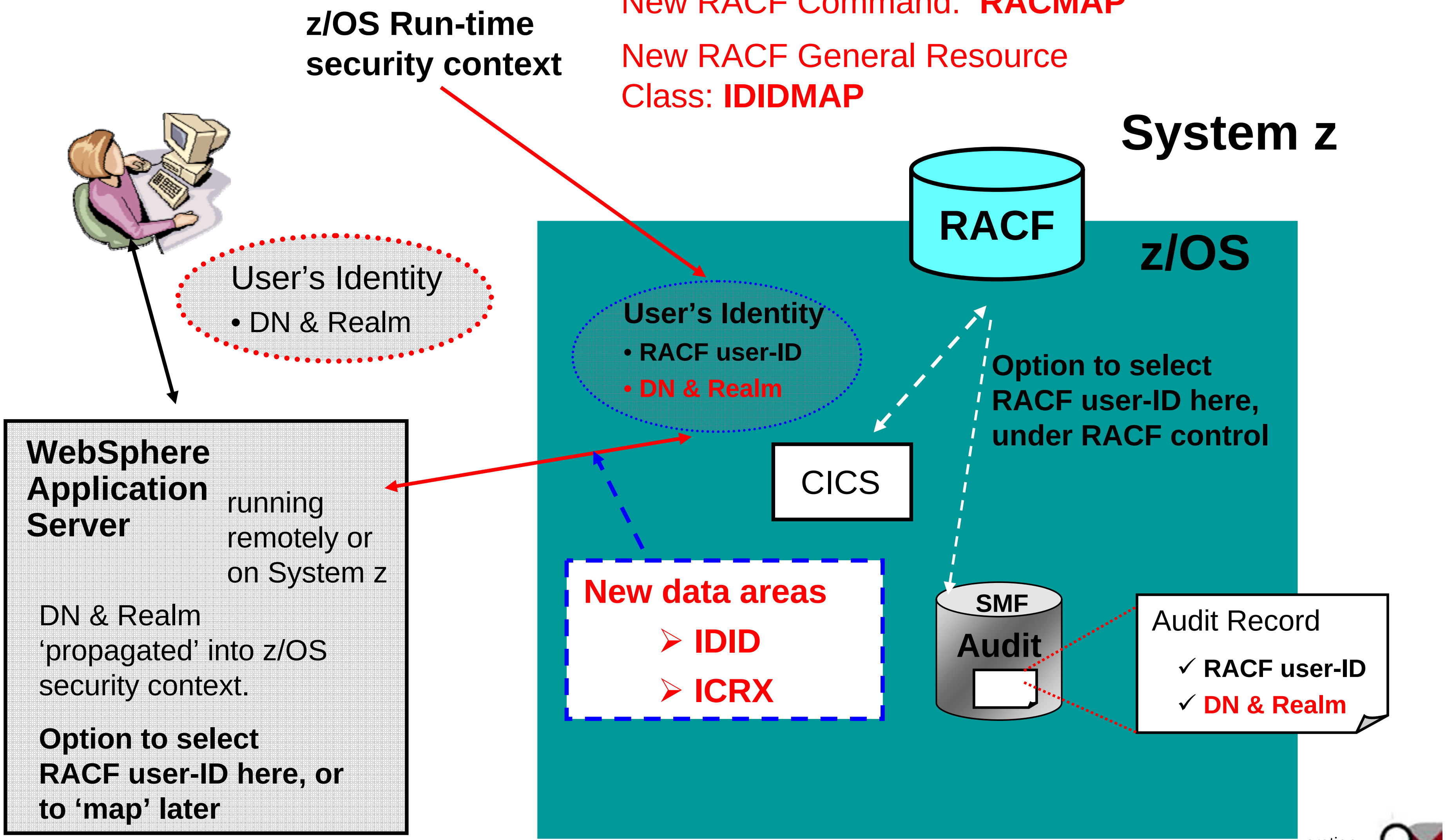
Access Request: Discretionary Access Control (DAC) and Mandatory Access Control (MAC)

Logging & Reporting: SMF User-level logging, resource-level logging of access successes and/or failures with access-level sensitivity

z/OS V1R11: z/OS Identity Propagation

New RACF Command: **RACMAP**

New RACF General Resource Class: **IDIDMAP**



z/OS Run-time security context

System z

RACF

z/OS

User's Identity
- DN & Realm

User's Identity
- **RACF user-ID**
- **DN & Realm**

Option to select RACF user-ID here, under RACF control

CICS

WebSphere Application Server running remotely or on System z

DN & Realm 'propagated' into z/OS security context.

Option to select RACF user-ID here, or to 'map' later

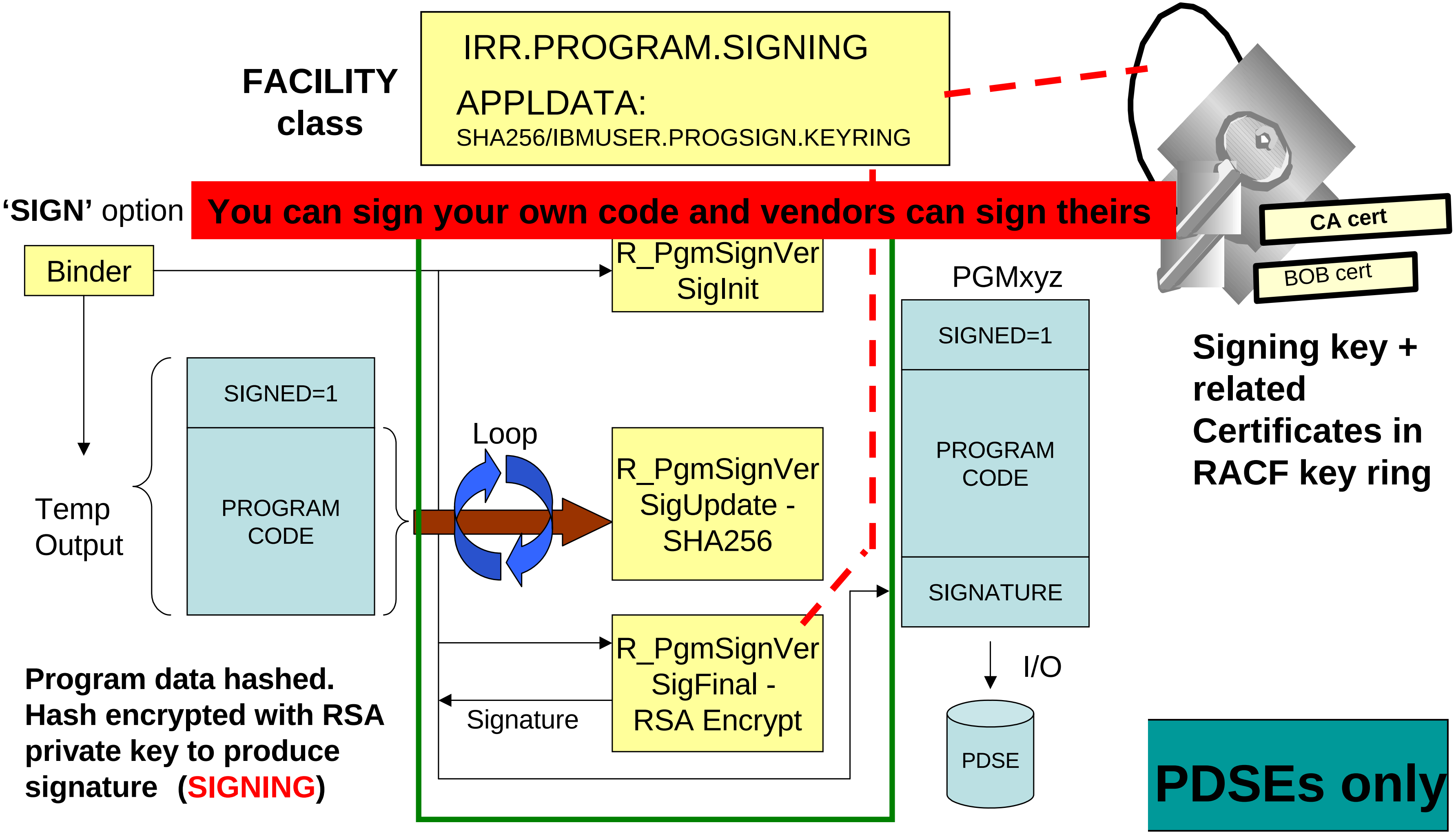
New data areas
- **IDID**
- **ICRX**

SMF

Audit

Audit Record
- ✓ **RACF user-ID**
- ✓ **DN & Realm**

z/OS V1R11: Program Object Signature Verification



Signing key + related Certificates in RACF key ring

Program data hashed. Hash encrypted with RSA private key to produce signature (SIGNING)

PDSEs only

z/OS V1R11: Program Object Signature Verification… Why sign code?

- Belt and braces or ‘defence in depth’. This support is intended to be used in conjunction with existing security mechanisms
- Digitally signing code can help improve the integrity, reliability and security of the system by adding an additional layer of control on executable programs running in the system
- Digitally signing code makes it possible to detect changes to programs due to tampering and/or corruption
- Requiring that certain code be signed makes it easier to enforce change control procedures and protect against accidental changes to program code libraries. This helps avoid errors such as accidently placing 'test' code on a 'production' system.

Security Features within the z/OS TCP/IP Stack

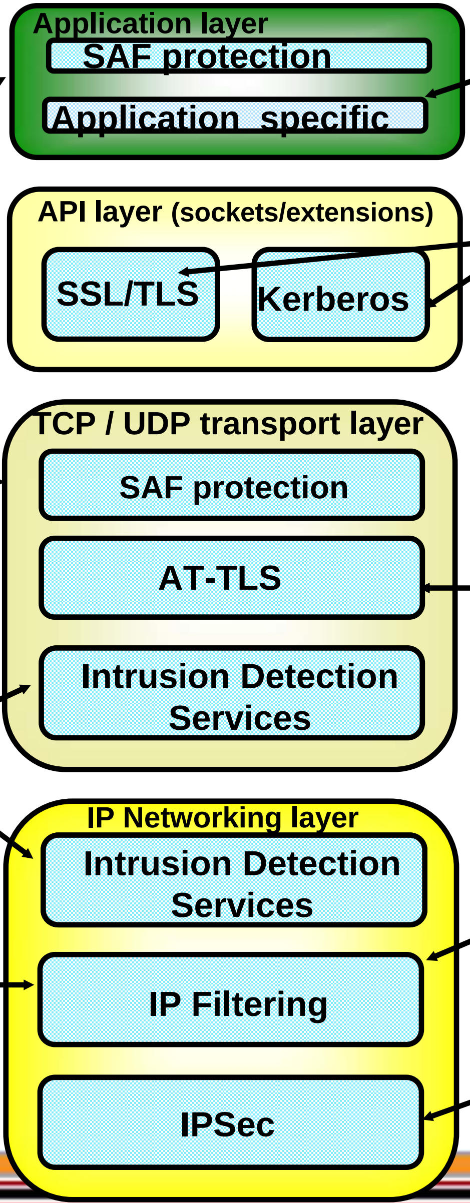
Protect the system

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.

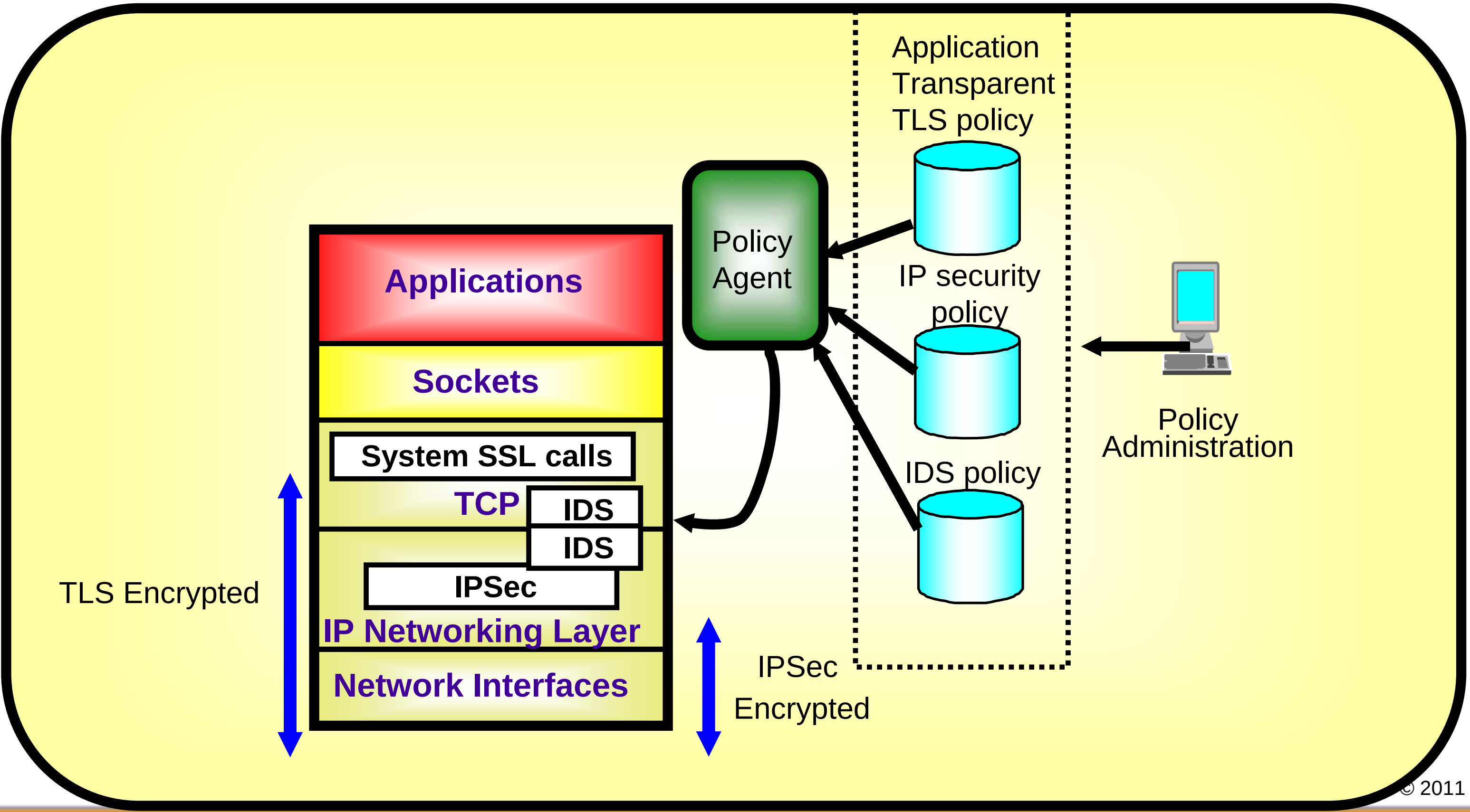
AT-TLS is TCP/IP stack service that provides SSL/TLS services at the TCP transport layer and is transparent to upper-layer protocols. It is available to TCP applications in all programming languages, except PASCAL.

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 z/OSMF).**
- **The network security features implemented (IPSec, AT-TLS, etc.) can be viewed via this tool, and rules for each of these features can be reviewed/printed.**



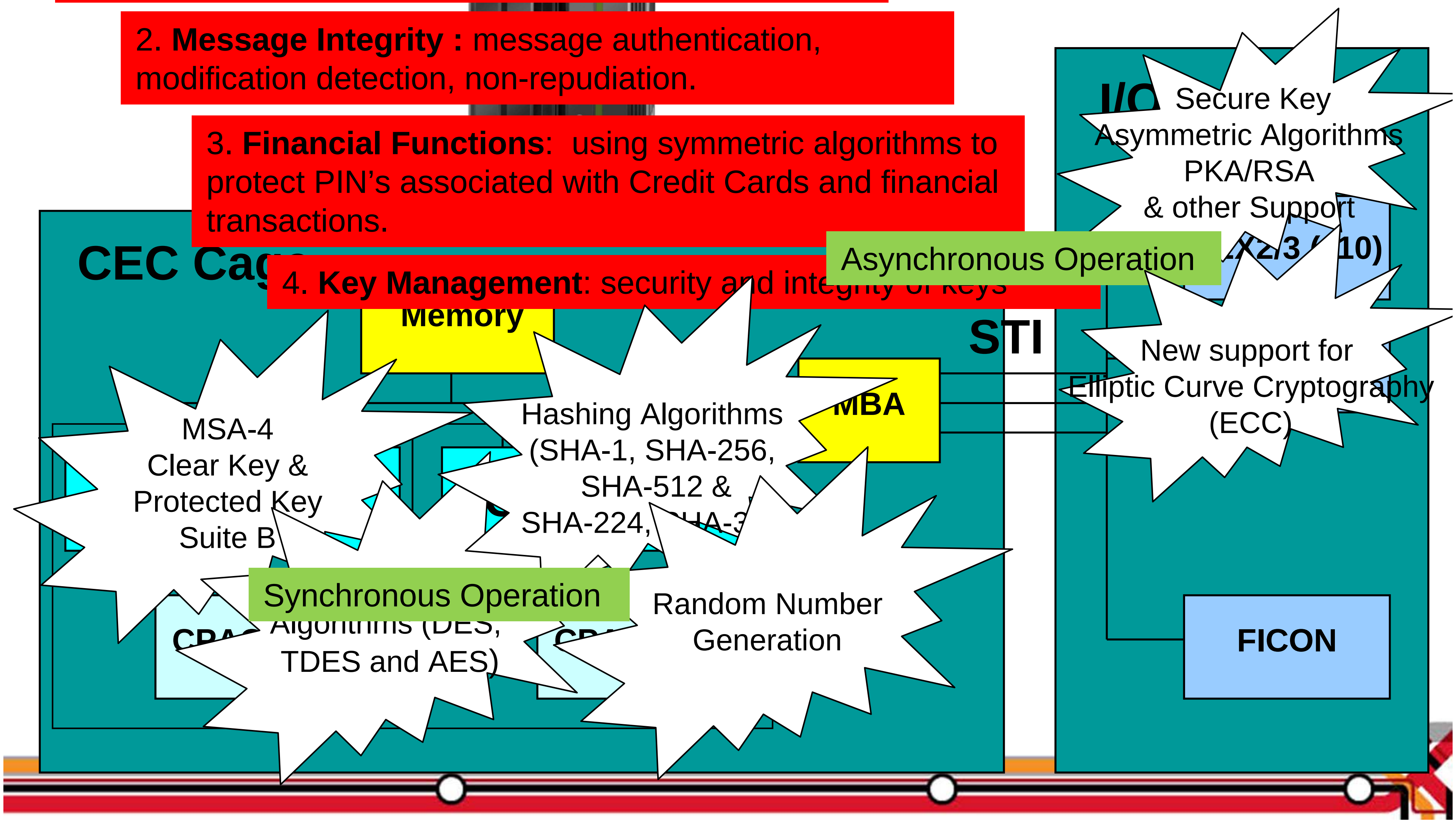
z10 and z196 Cryptographic Hardware

1. **Data Confidentiality**: encrypting/decrypting data using symmetric and/or asymmetric keys

2. **Message Integrity :** message authentication, modification detection, non-repudiation.

3. **Financial Functions**: using symmetric algorithms to protect PIN's associated with Credit Cards and financial transactions.

4. **Key Management**: security and integrity of keys



Secure Key Asymmetric Algorithms PKA/RSA & other Support

Asynchronous Operation

New support for Elliptic Curve Cryptography (ECC)

MSA-4 Clear Key & Protected Key Suite B

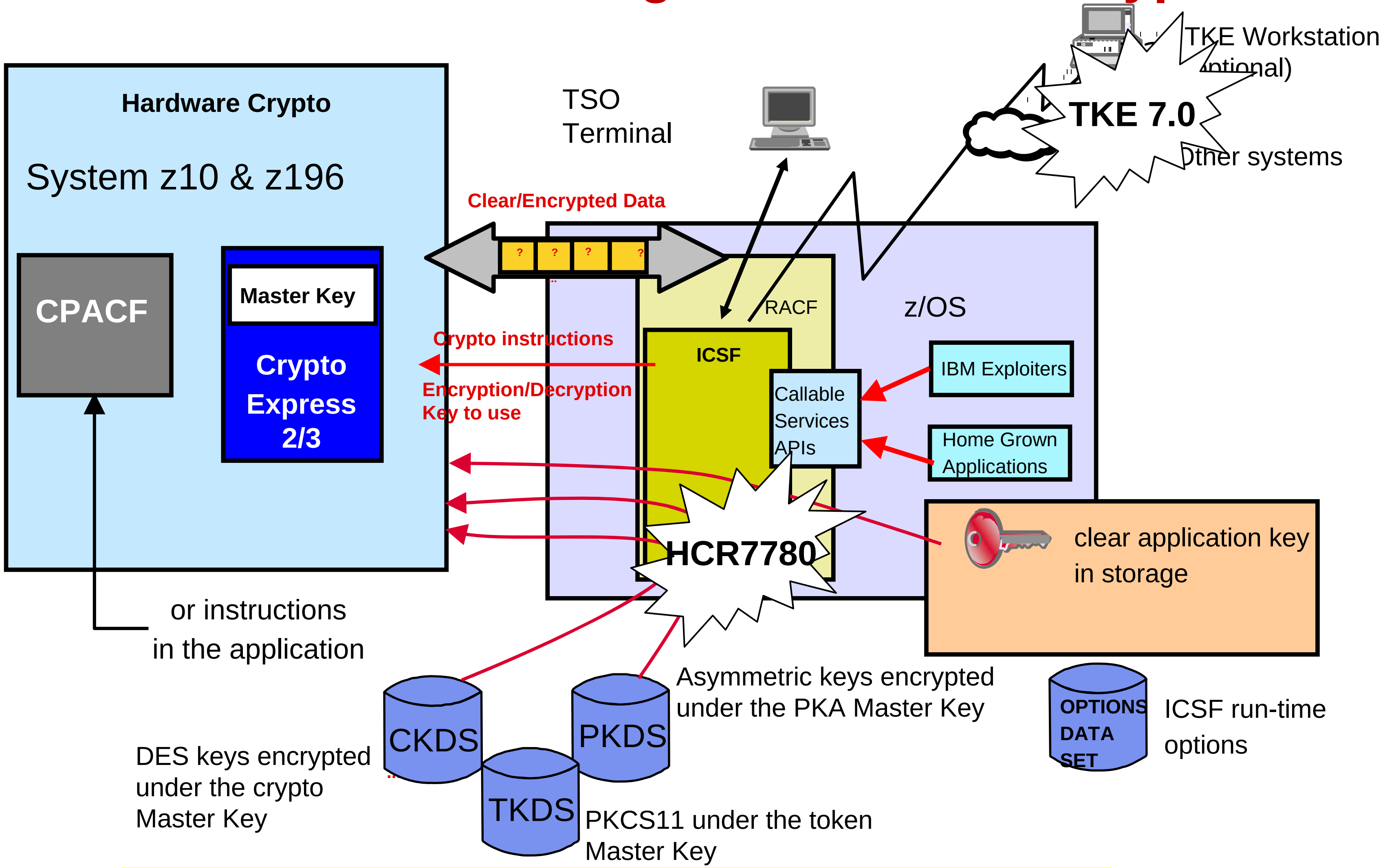
Hashing Algorithms (SHA-1, SHA-256, SHA-512 & SHA-224, SHA-3

Synchronous Operation

Algorithms (DES, TDES and AES)

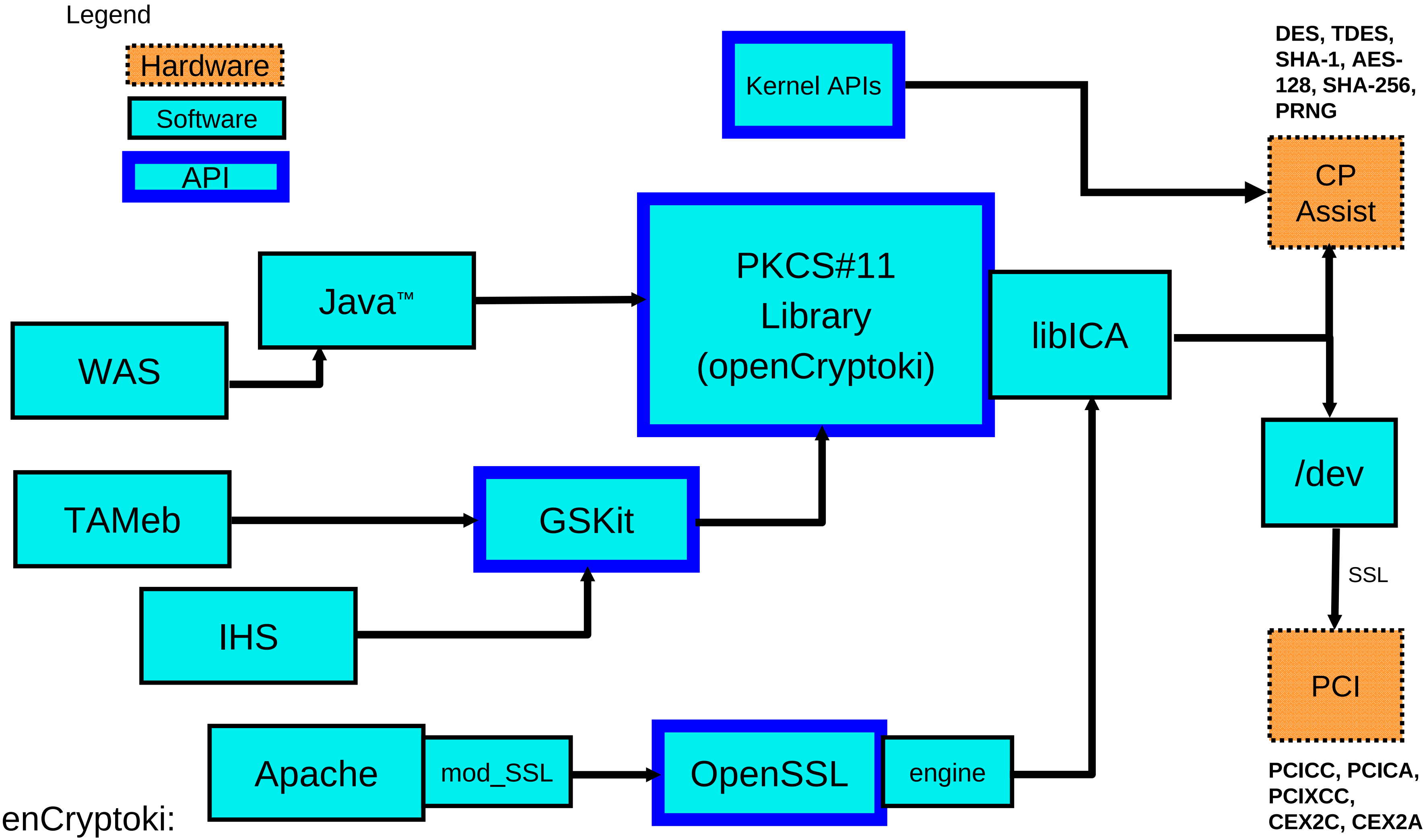
Random Number Generation

System z10 & z196 – Calling The Hardware Crypto



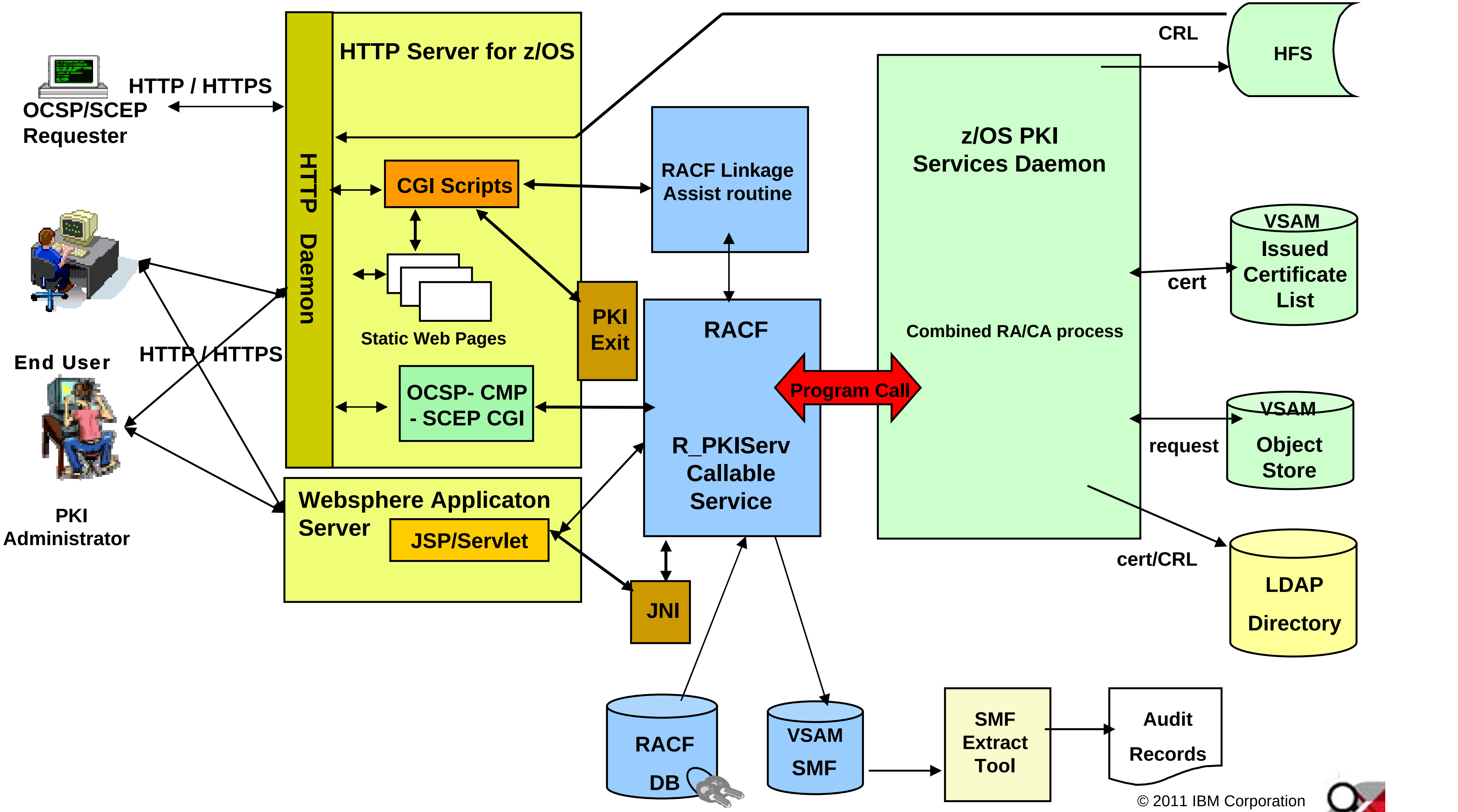
Access to the cryptographic services and keys can be controlled by RACF with the CSFSERV and CSFKEYS classes

Linux on System z – PKCS#11



openCryptoki:
http://www.ibm.com/developerworks/linux/library/s-pkcs/

z/OS PKI Services – “Full-cycle” certificate management



New RACF Features in z/OS v1.12

- RACF adds a new sub-operand called SYMCPACFWRAP to the ICSF operand of the RALTER and RDEFINE commands to allow the security administrator to specify whether certain encrypted symmetric keys are eligible to be rewrapped by CP Assist for Cryptographic Function (CPACF).
- Installations can now use the new GENERICANCHOR operand of the SET command to customize the number of generic profile lists that RACF maintains to keep generic profiles in storage.
- Support to warn, detect and remove “ghost” generic profiles from RACF General Resource Classes.
- RACF enhances support for digital certificates by supporting keys generated with elliptic curve cryptography (ECC) algorithms. Shorter keys generated with ECC algorithms achieve comparable key strengths when compared with longer RSA keys.

New RACF Features in z/OS v1.12 (contd.)

- Digital Certificate enhancements: Long Distinguished Names (DN’s):
  - The ADD and GENCERT functions of the RACDCERT command accept certificates with long distinguished names.
  - RACF callable services R_datalib and initACEE support certificates with long distinguished names.
  - The RACDCERT MAP command supports IDNFILTER and SDNFILTER values of up to 1024 characters.
  - In support of long distinguished names, RACF changes the way that certificate profile names in the DIGTCERT class are formed and stored in the RACF database.
- All functions of the RACDCERT command now support digital certificates with long validity periods.

New RACF Features in z/OS v1.13

- RACF Remote Sharing (RRSF) over TCP/IP
  - AT-TLS required: RRSF will refuse to use an unsecured link
  - Server and client-side authentication will be used
  - Same rule will specify strongest-available encryption method
  - More and better encryption algorithms available in AT-TLS .
    - Note: RRSF via APPC uses 56-bit DES
  - New operand on the RACF TARGET operator command or issued via RAFC subsystem initialisation:
    - PROTOCOL(TCP(ADDRESS(hostname_or_IP_address)))
- SAF-based security for z/OSMF
  - New RACF General Resource Class, ZMFAPLA (similar to EJBROLES class)
  - New RACF Grouping Class, GZMFAPLA for application visibility control
  - Also need to create a ZMFDFLT profile in the REALM class
    - Will be used eventually to allow multiple z/OSMF instances to run with a shared RACF database or a replicated database.

New RACF Features in z/OS v1.13 (contd.)

- z/OS UNIX (USS) file system security:
  - – File system-level access control using SAF with PTF for APAR OA35970)
  - – Optional access control check uses profiles in the new FSACCESS class
  - – When a user is authorized to use a file system, POSIX permission bits and ACLS's are used to control access to individual files and directories
  - – Intended to help improve security administration and auditability
  - – Also available for z/OS v1.12 via PTF
- TN3270 and FTP support for RACF Password Phrases (PASSPHRASES)

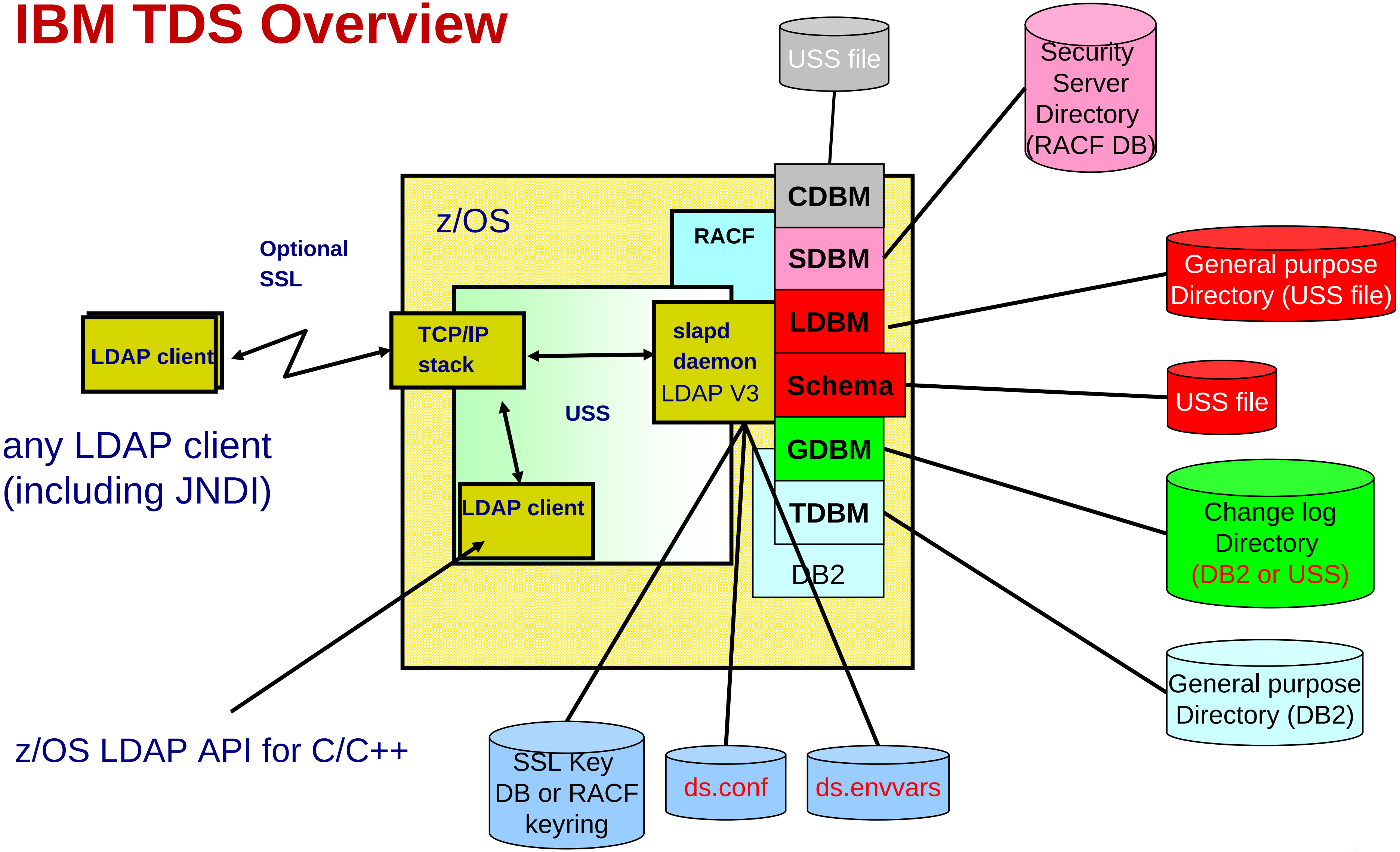
Summary: Why Security Management for System z?

- The majority of the world's critical business data resides on the System z platform and System z addresses today's prominent and growing requirements for IT governance, compliance, and security.
- RACF has been and continues to be the backbone of System z security.
- The IBM Security Framework provides a comprehensive, end-to-end security solution.
- Answering specific security-related questions can help organizations define security needs and determine the best product match.

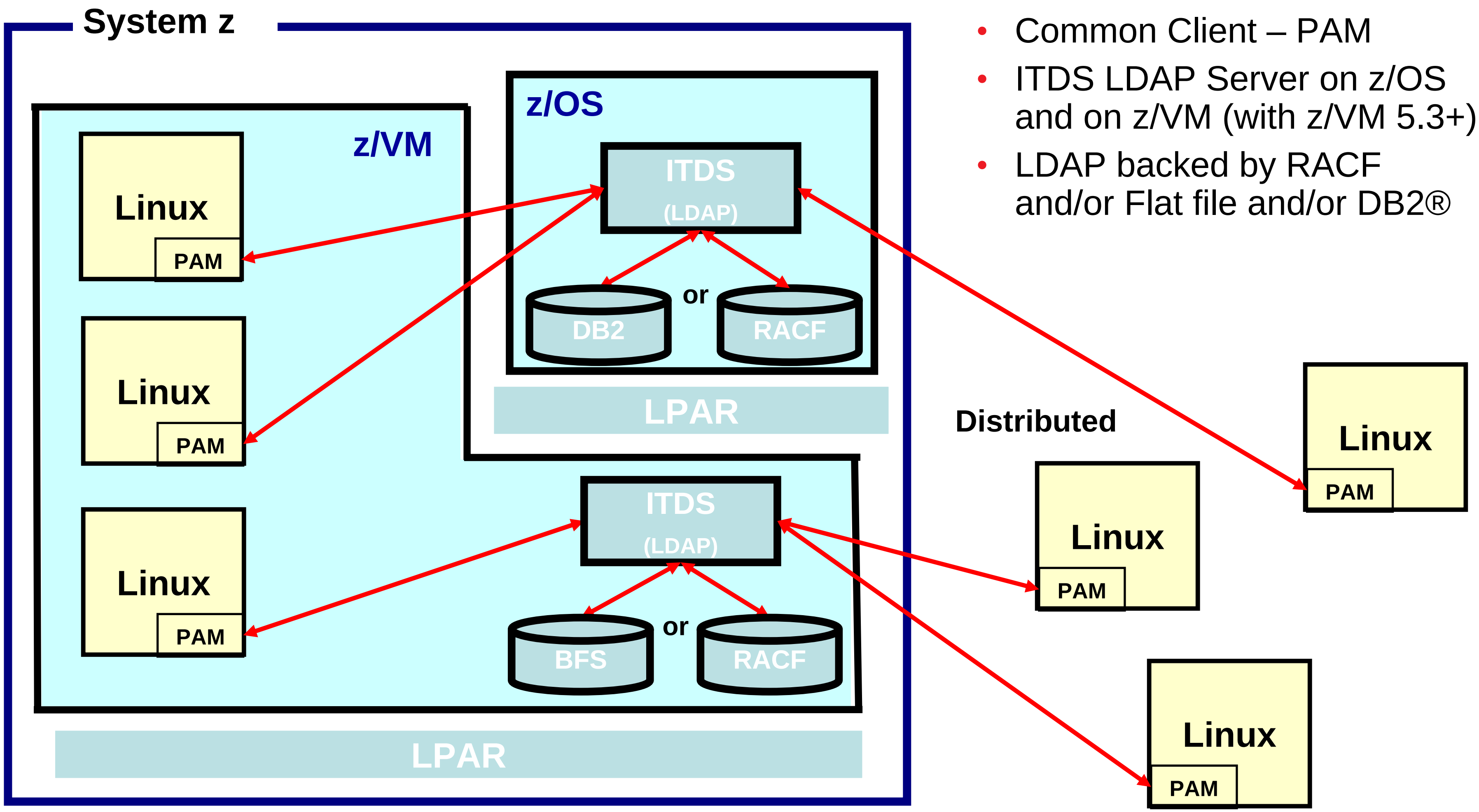
Identity & Access Management

- **Features already imbedded within z/OS:**
  - Tivoli Directory Services (ITDS – or LDAP) extending System z security as well as allowing for propagation of RACF information
  - X.509 Digital Certificates and z/OS PKI Services
  - Kerberos
  - Passtickets
  - ID Propagation
    - Using the new SAF services (z/OS 1.11) in Websphere Application Server and CICS
- **Augmented by Tivoli Security Products:**
  - Tivoli zSecure
  - Tivoli Identity Manager (TIM)
  - Tivoli Access Manager (eb for web security – bi for business integration)
  - Tivoli Federated Identity Manager (TFIM) for web services
  - Tivoli Key Lifecycle Manager (TKLM)
  - Tivoli Access Manager for Operating Systems (TAMOS)

IBM TDS Overview

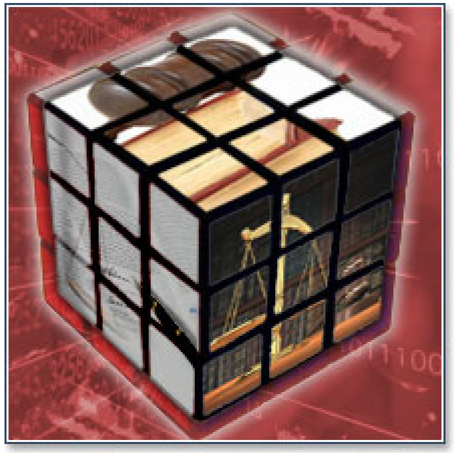

USS file
Security Server Directory (RACF DB)
z/OS
CDBM
RACF
SDBM
General purpose Directory (USS file)
Optional SSL
LDAP client
TCP/IP stack
slapd daemon LDAP V3
LDBM
Schema
USS file
USS
GDBM
any LDAP client (including JNDI)
LDAP client
TDBM
Change log Directory (DB2 or USS)
DB2
General purpose Directory (DB2)
z/OS LDAP API for C/C++
SSL Key DB or RACF keyring
ds.conf
ds.envvars

IBM TDS on z/OS and z/VM



- Common Client – PAM
- ITDS LDAP Server on z/OS and on z/VM (with z/VM 5.3+)
- LDAP backed by RACF and/or Flat file and/or DB2®

Benefits of IBM Security zSecure Products

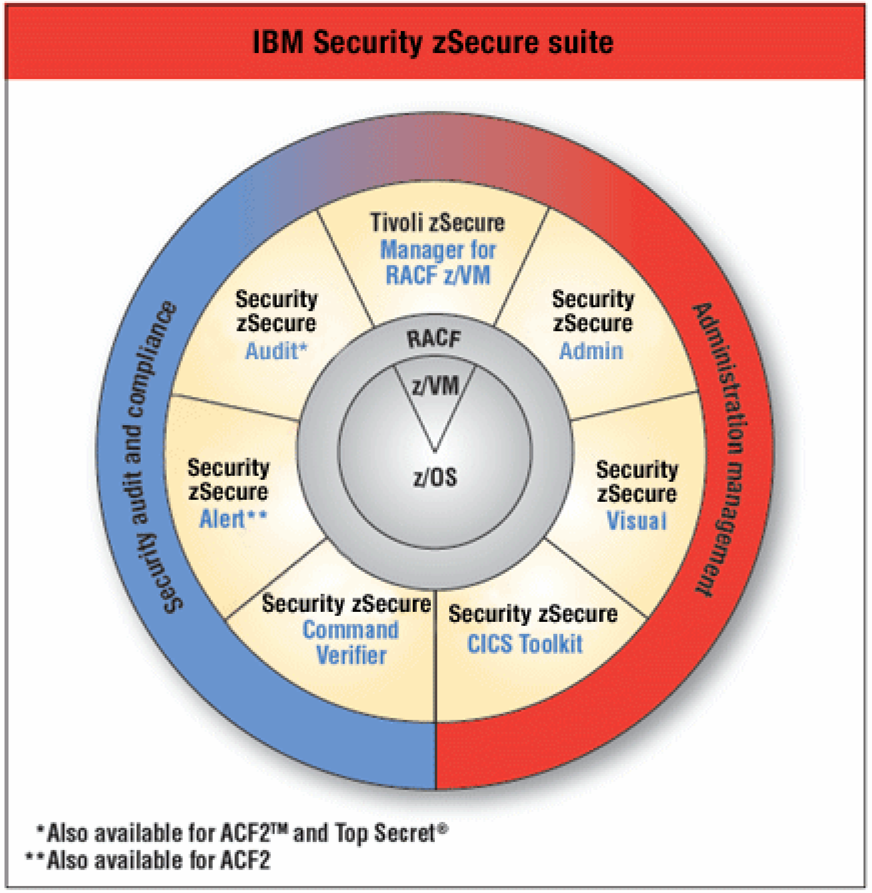


Security Challenges in Today’s Environment

Today’s key security challenges include:

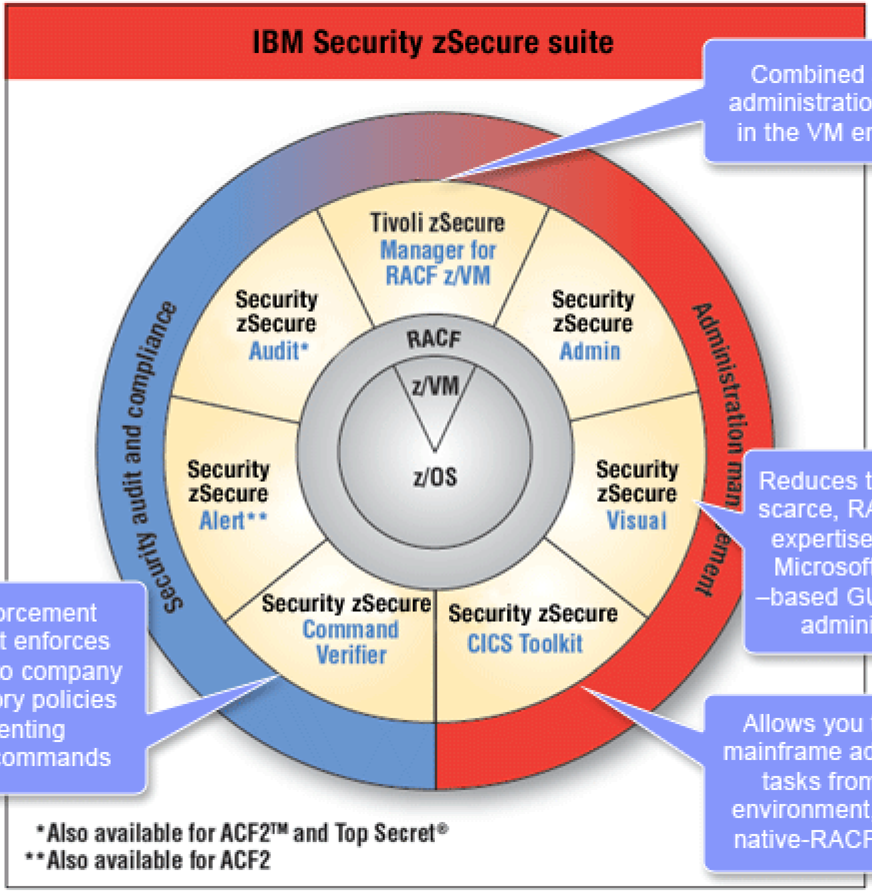
- Increasing requirements that arise through governmental and other external pressures – and internal regulations – that require systems and process compliance
- Increasing complexity of applications and service-oriented architecture (SOA) that increases the complexity of operations management
- Increasing cost pressures to do more with less

The IBM Solution: Security zSecure Suite


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

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

The IBM Solution: Security zSecure Suite (continued)


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

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

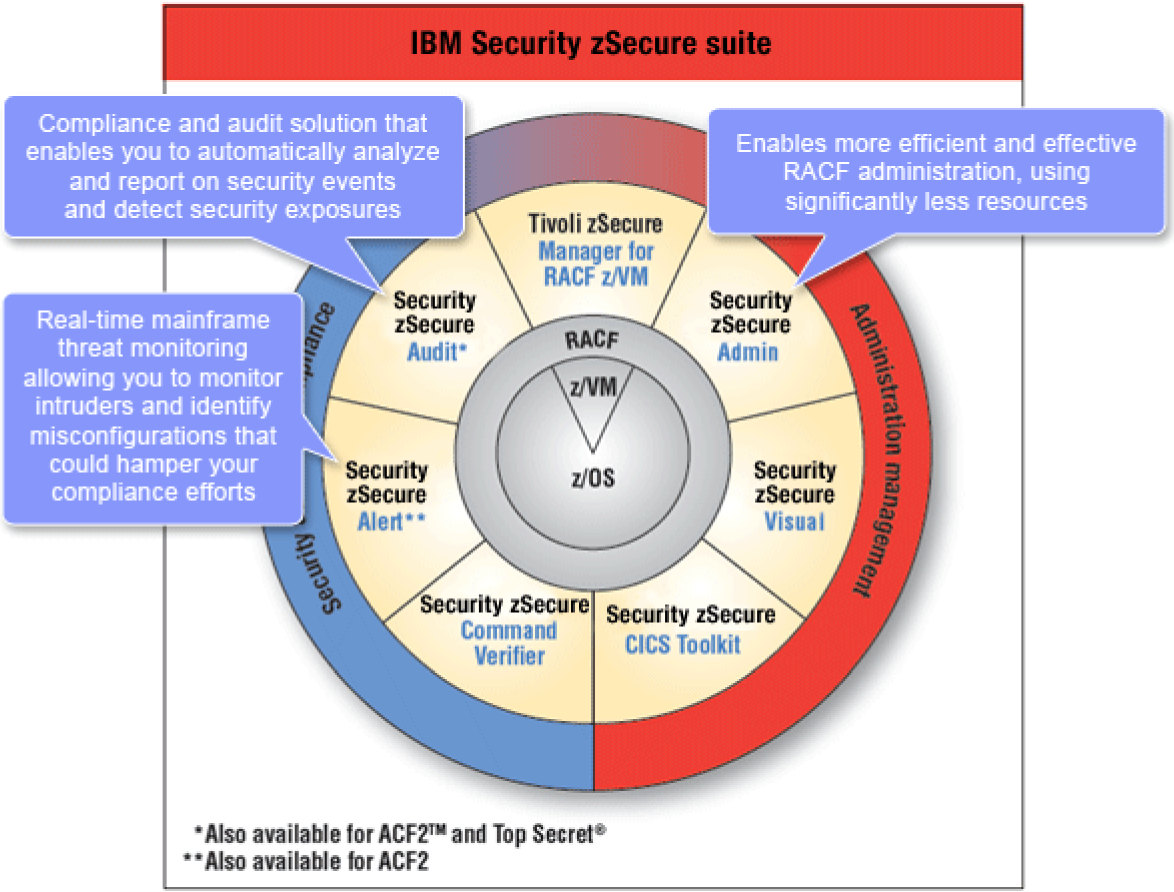
Combined audit and administration for RACF in the VM environment

Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows –based GUI for RACF administration

Policy enforcement solution that enforces compliance to company and regulatory policies by preventing erroneous commands

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

The IBM Solution: Security zSecure Suite (continued)


IBM Security zSecure suite
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS
Security ...ance
Administration management

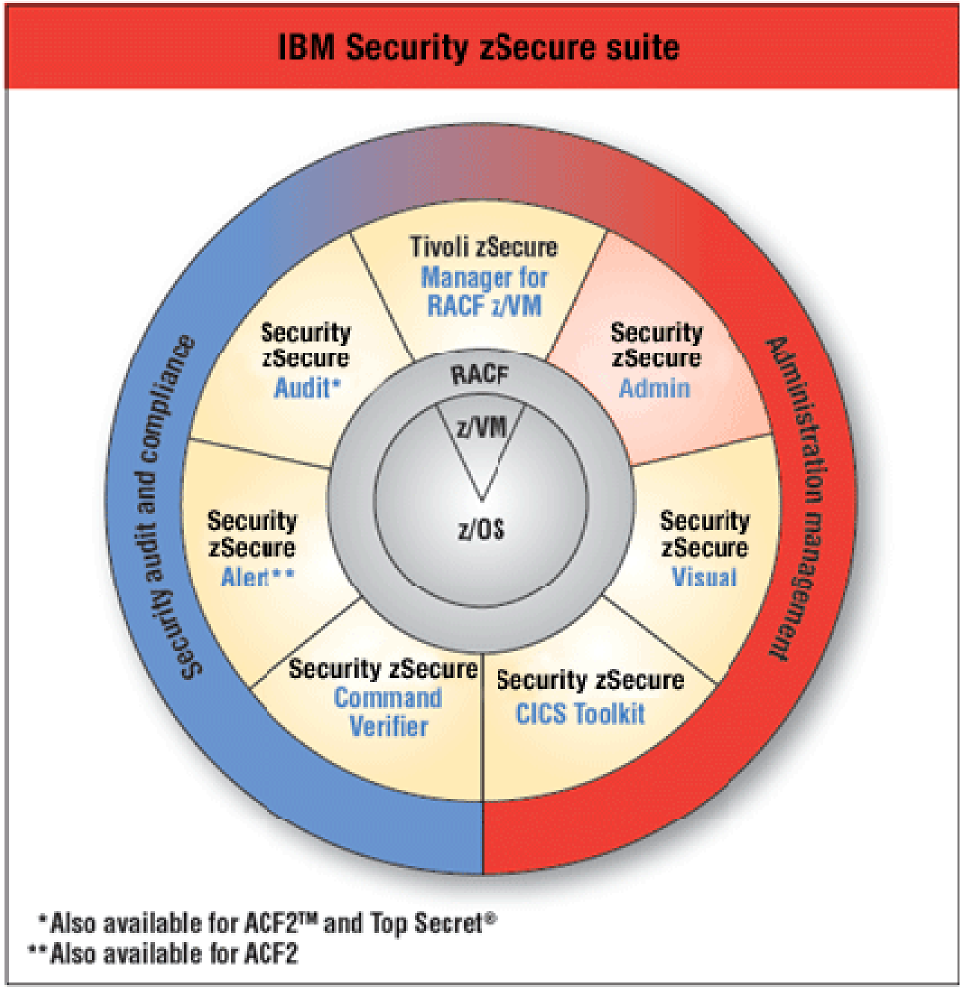
Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

Enables more efficient and effective RACF administration, using significantly less resources

Real-time mainframe threat monitoring allowing you to monitor intruders and identify misconfigurations that could hamper your compliance efforts

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Security zSecure Admin

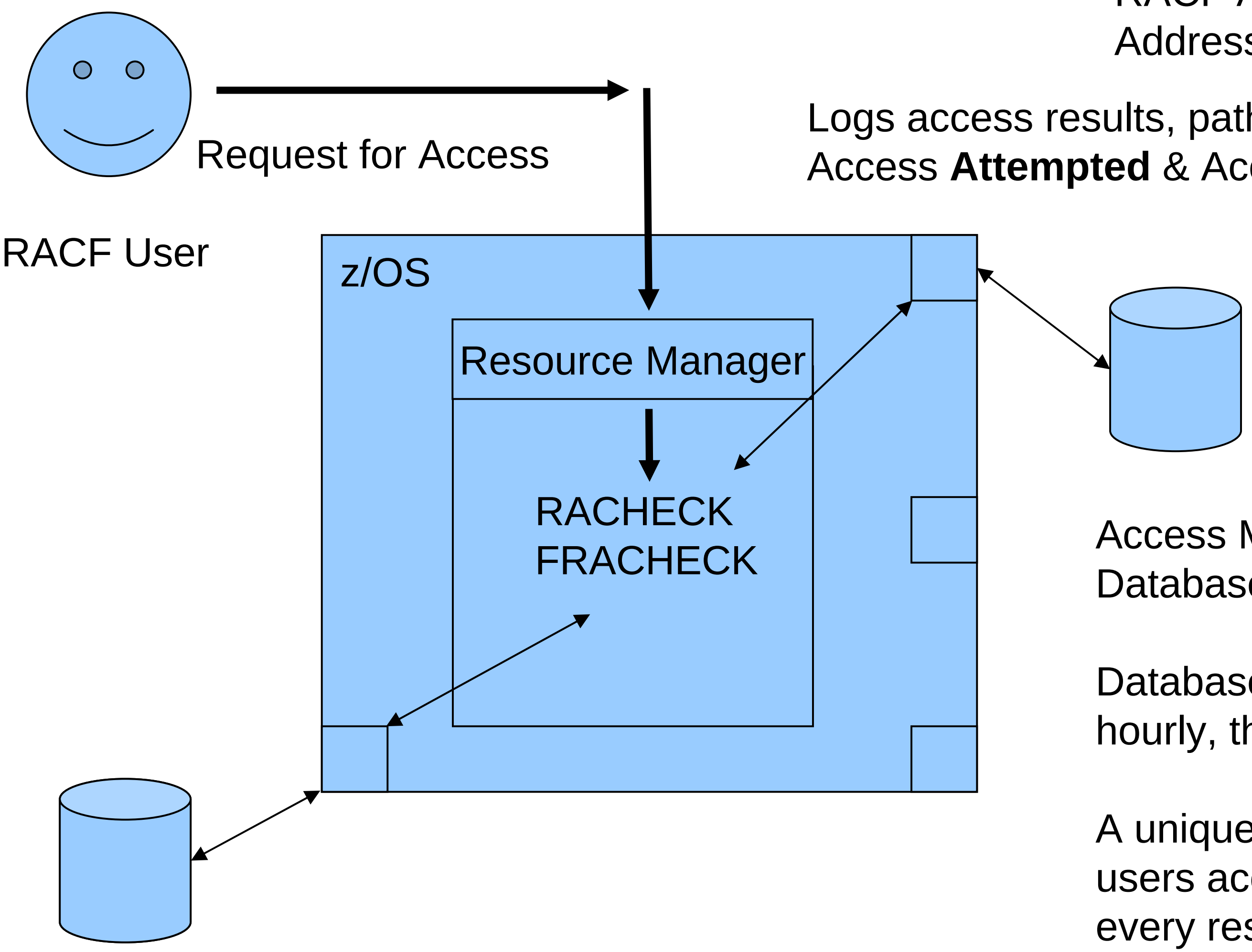

IBM Security zSecure suite
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS
Security audit and compliance
Administration management

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Highlights

- Automates routine tasks
- Identifies and analyzes problems to minimize threats
- Merges databases quickly and efficiently
- Displays data from live RACF database
- Integrates smoothly with zSecure Audit
- Stores non-RACF data to reduce organizational costs
- RACF Access Monitor
- RACF “Offline” feature

The RACF Access Monitor



RACF Access Monitor
Address space

Request for Access

Logs access results, path taken
Access **Attempted** & Access **Allowed**

RACF User

z/OS

Resource Manager

RACHECK
FRACHECK

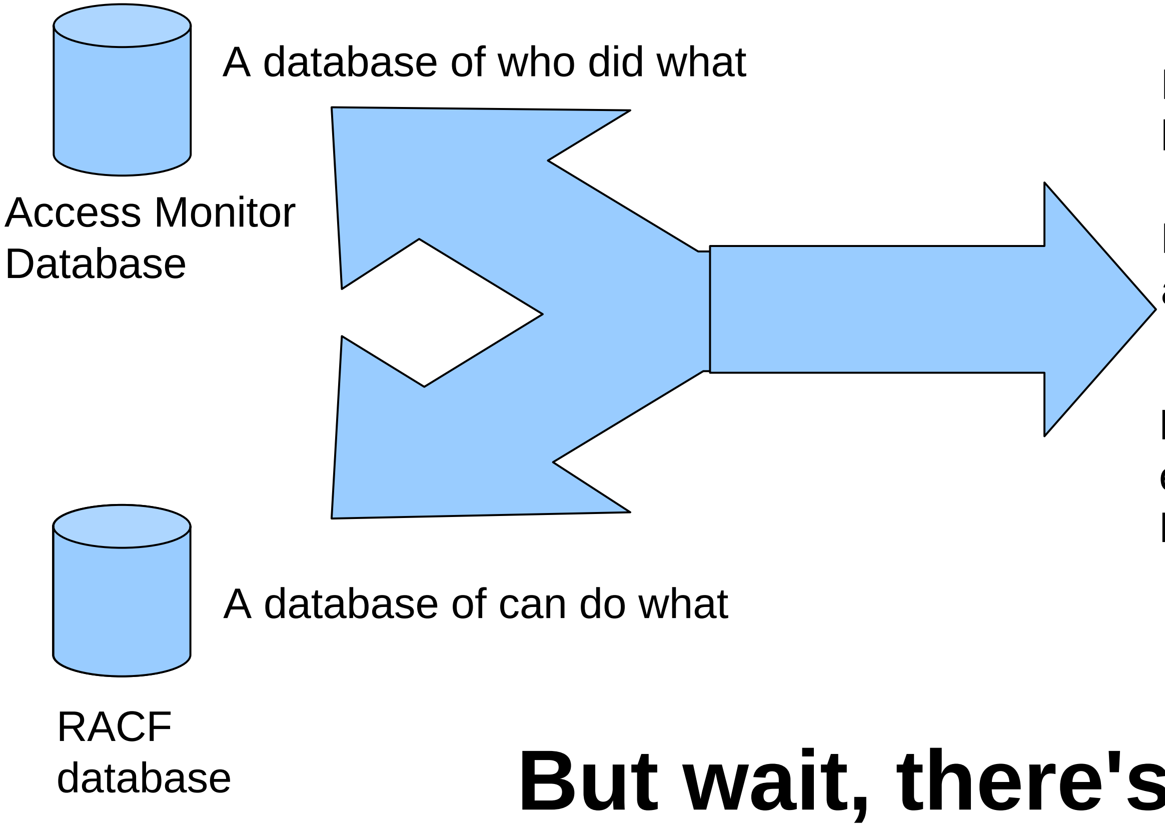
Access Monitor
Database

Database consolidated hourly, then daily etc.

A unique record of every users access used to every resource.

RACF
database

The RACF Access Monitor: RACF Database Cleanup



A database of who did what

Access Monitor
Database

A database of can do what

RACF
database

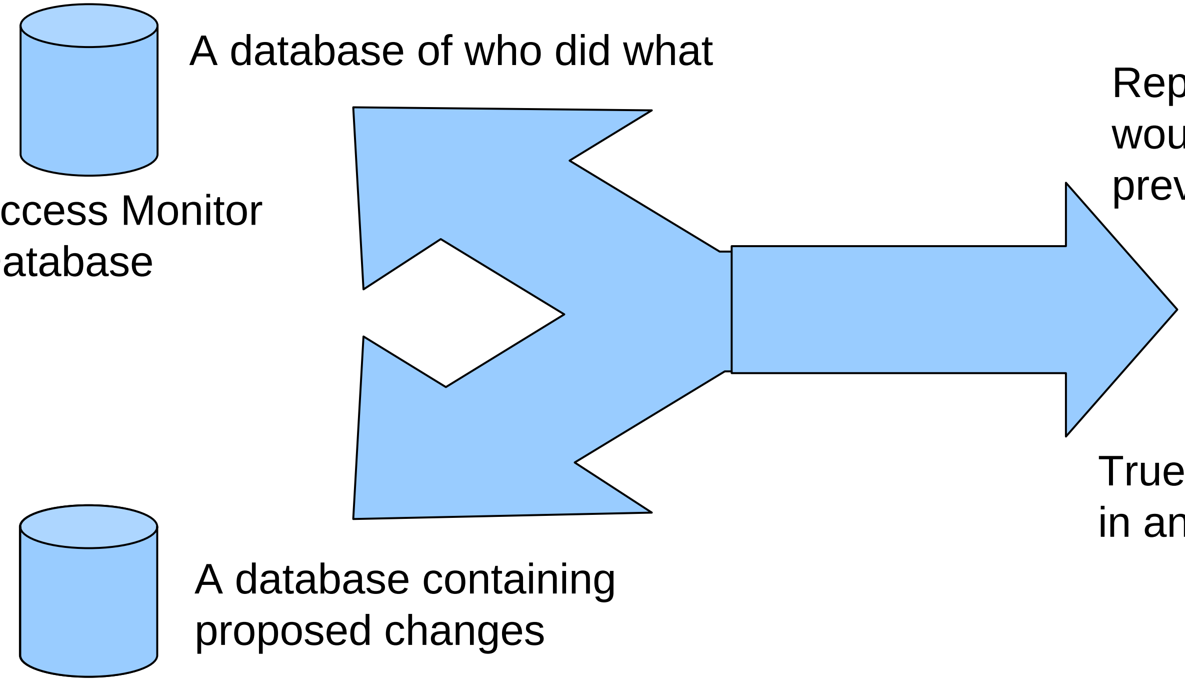
Reports of users who possess higher access than they used.

RACF commands to reduce access to the minimal level used

Reduce privileges to only those exercised – i.e. Principle of Least Privilege

But wait, there's more!

The RACF Access Monitor: RACF Simulation



A database of who did what

Access Monitor Database

A database containing proposed changes

RACF Offline database

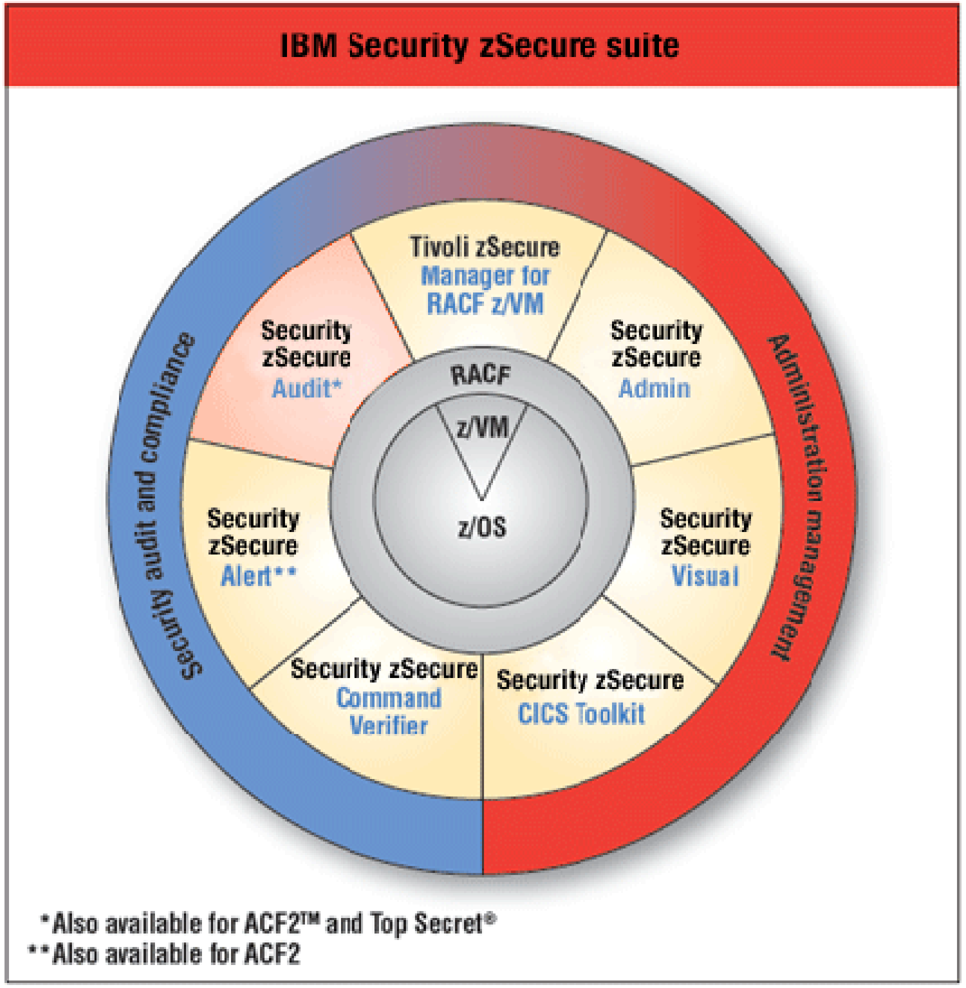
Reports of users whose access would change – i.e. fail where previously they succeeded.

True access modelling – unheard of in any IT security paradigm.

What Customers Ask about zSecure Admin

- **Why do I need zSecure Admin?**
  - Are your security administrators really RACF administrators?
  - The typical answer is that they are spending more time being RACF technicians.
- **What kind of reports do I get?**
  - Many. Any part of the RACF database can be reported on and an e-mail with that information is immediately generated.
  - Standard RACF clean-up and authorization reports are included.
  - Cross-reference access is provided for up to four user IDs.
- **Because information in the RACF database is sensitive, can access within zSecure Admin be restricted?**
  - Yes, although most customers do not install the product this way. zSecure Admin is flexible and supports full control over who can see what parts of RACF.
- **Do I have to give users of zSecure Admin read access to the RACF database?**
  - No! In fact, read access to RACF itself should be very restricted.
  - The beauty of zSecure Admin is that no one needs read access to RACF itself in order to report on any part of RACF.

Security zSecure Audit


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

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

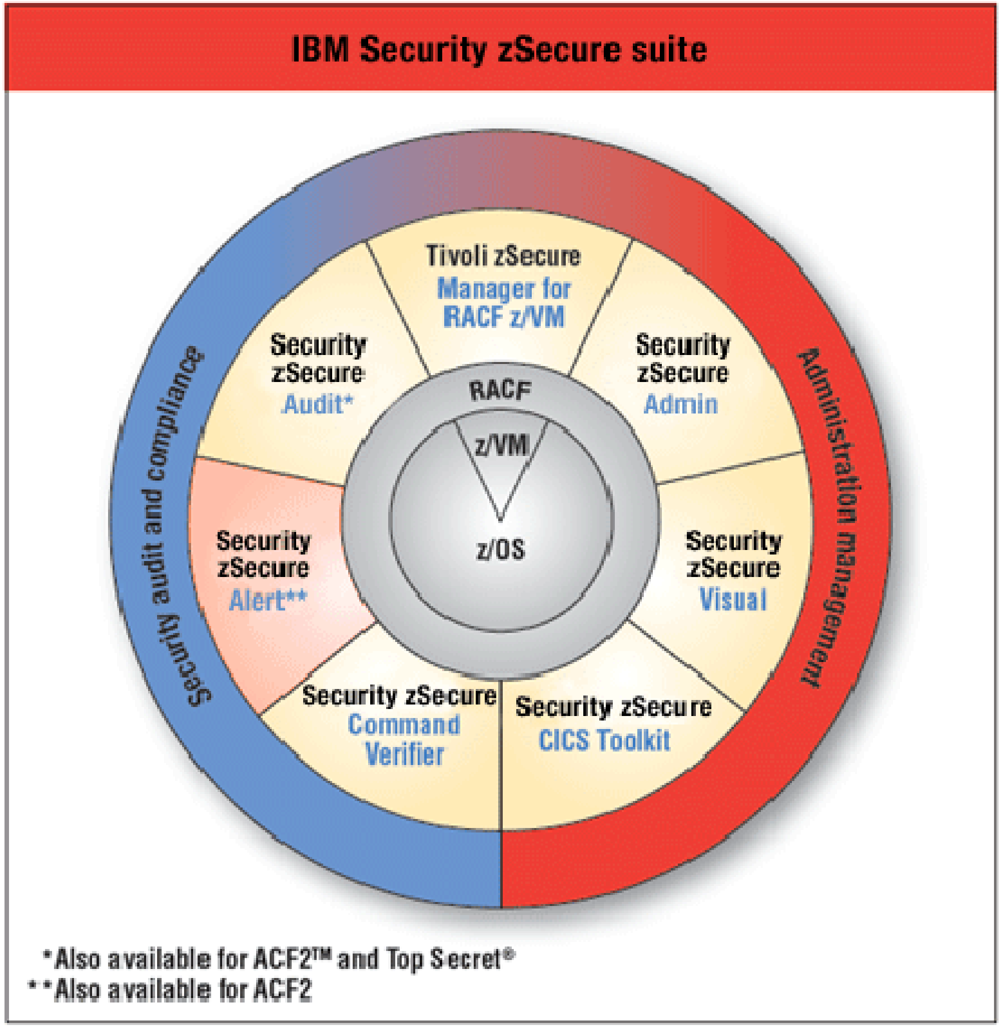
Highlights

- Provides live analysis of critical information
- Customizes reports to meet specific needs
- Analyzes SMF log file to create a comprehensive audit trail
- Analyzes RACF profiles and ACF2 entries
- Detects system changes and integrity breaches to minimize security risks
- Tracks and monitors baseline changes for RACF, ACF2, and Top Secret and selected z/OS components

What Customers Ask about zSecure Audit

- **Why do I need zSecure Audit?**
  - zSecure Audit is audit, compliance, and SMF reporting all rolled into one.
  - Using zSecure Audit, you can determine the state of your mainframe security immediately before the auditor arrives by performing your own audit.
- **Will zSecure Audit tell me which SMF records I need to cut?**
  - zSecure Audit is a comprehensive auditing and reporting product. It will help you determine the auditing settings needed on critical RACF profiles, which does determine the RACF (type 80) SMF records that will be cut.
  - However, zSecure Audit will not tell you that you should have SMF configured to cut record types 80, 81, 83, 102, and so on. Each site has to configure which SMF record types to save to tape.

Security zSecure Command Verifier

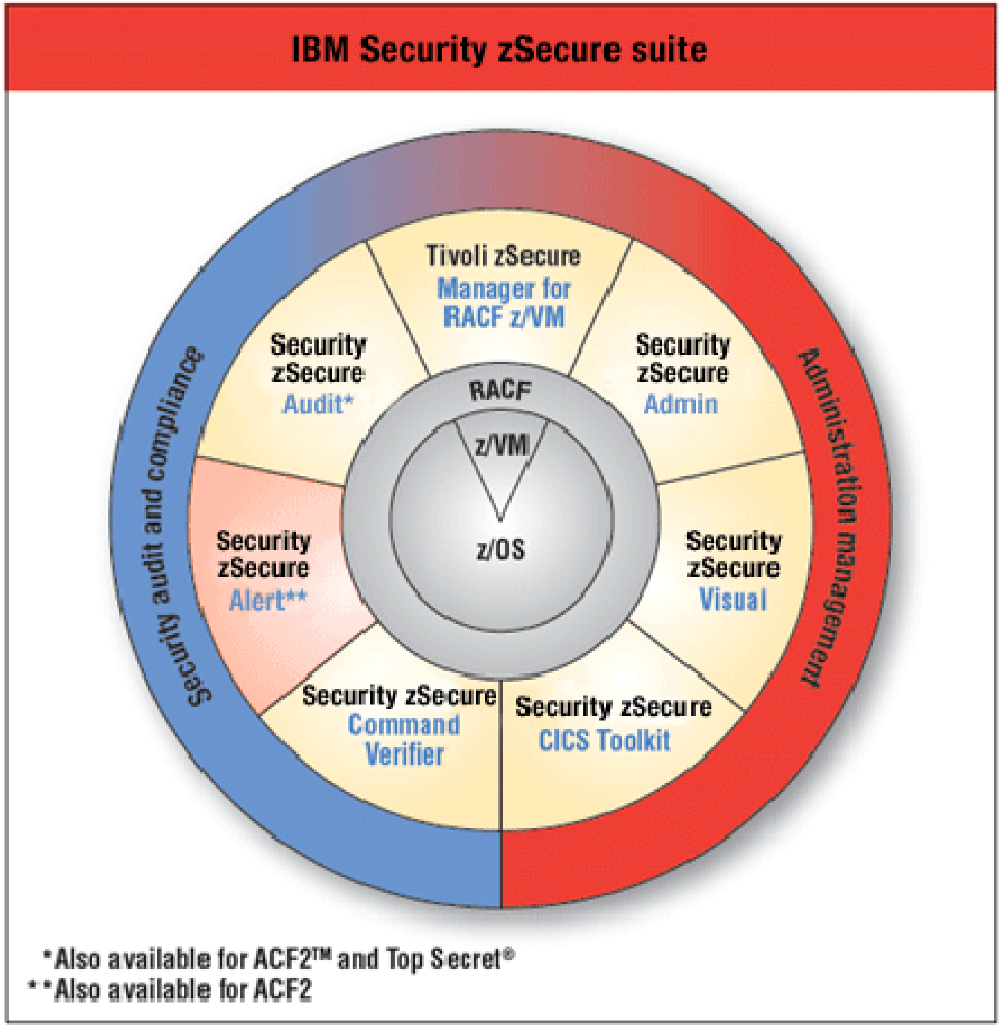

IBM Security zSecure suite
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS
Security audit and compliance
Administration management

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Highlights

- Provides granular control over who can issue RACF commands and keywords
- Verify against RACF profiles and access list
- Apply and enforce local policies and naming standards
- Provides default and enforces mandatory values
- RACF command audit trail – stores recent profile changes in the profile and displays when profile is listed

Security zSecure Alert


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

*Also available for ACF2™ and Top Secret®
**Also available for ACF2

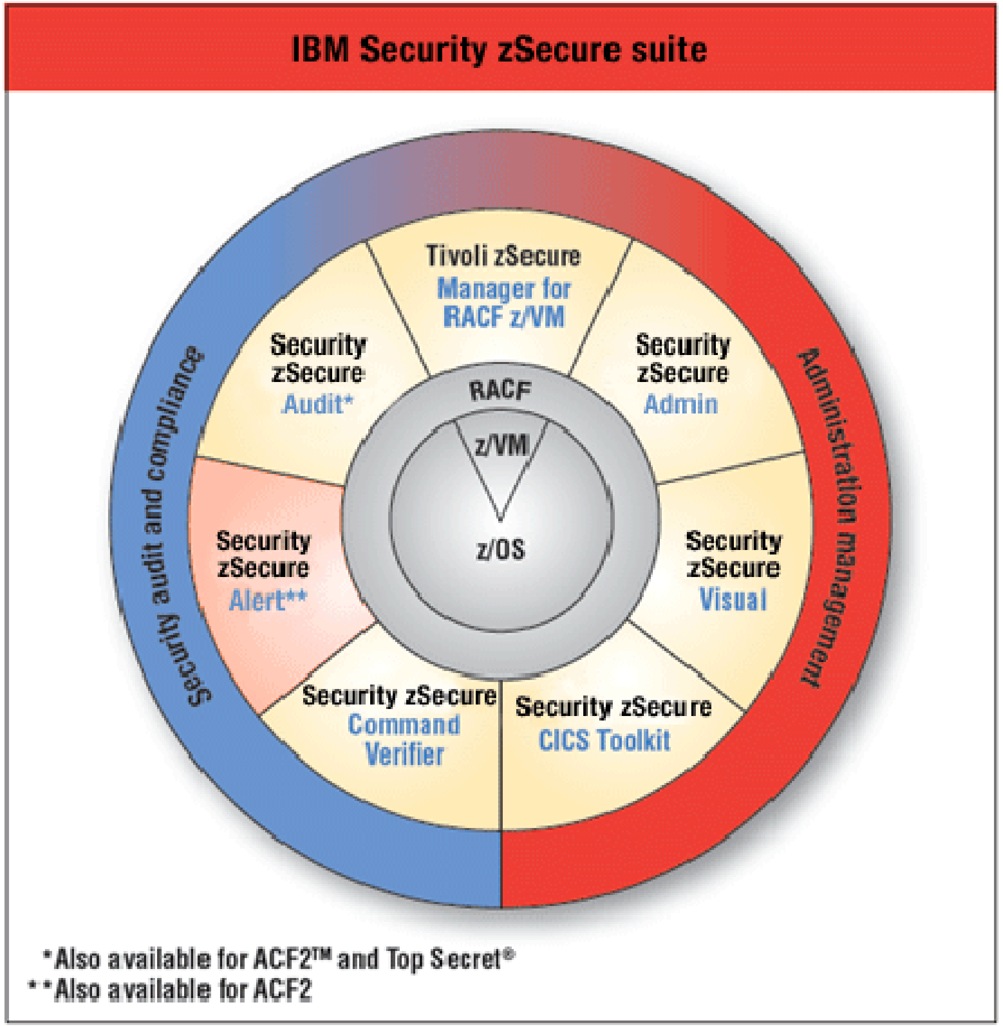
Highlights

- Offers threat knowledge base with parameters from your active configurations
- Alerts on intrusion, mis-configuration, access to critical resources etc.
- Provides a broad range of monitoring capabilities, including monitoring for misuse on z/OS, RACF, CA ACF2, and z/OS UNIX subsystems
- Easily sends critical alerts to enterprise audit, compliance, and monitoring solutions
- Provides integrated remediation with Security zSecure Admin

What Customers Ask about zSecure Alert

- **Why do I need zSecure Alert?**
  - zSecure Alert is beneficial to any organization that has a need to monitor RACF and z/OS in near real time.
  - It is an alternative to lengthy clean-up projects for acquired applications.
  - zSecure Alert supports SOX compliance and compliance with any regulatory requirements.
  - Privileges must be monitored (System Special).
- **Does zSecure Alert really send out alerts in real time?**
  - zSecure Alert sends out alerts every 60 seconds.
- **What if I do not like the default alerting interval?**
  - It can easily be customized to your liking.
- **Will the Alert-started task create a drain on my mainframe's performance?**
  - Absolutely not.
  - zSecure Alert has a test mode so that you can verify how many alerts will be sent out first.
  - Typically, with many alerts coming out of a system, we notice that zSecure Alert adds 1% or 2% of current CPU utilization.

Security zSecure Manager for z/VM



*Also available for ACF2™ and Top Secret®

**Also available for ACF2

Highlights

- Provides selected functionality from zSecure ADMIN & AUDIT components
- Manages the RACF database on z/VM
- Monitor z/VM users in a Linux on System z environment
- Manage z/VM authorities and privileges
- Report on RACF/VM SMF records

Benefits of Using the Mainframe as an Enterprise Security Hub

- **Cost reductions** that are realized through standardized and streamlined security administration and access control
- A single point of control and enhanced audit capabilities that provide the tools to **contain risk**
- Automated audit and compliance reporting, together with comprehensive security policies and enforcement, provide **higher levels of compliance** and **greater ability to demonstrate compliance**

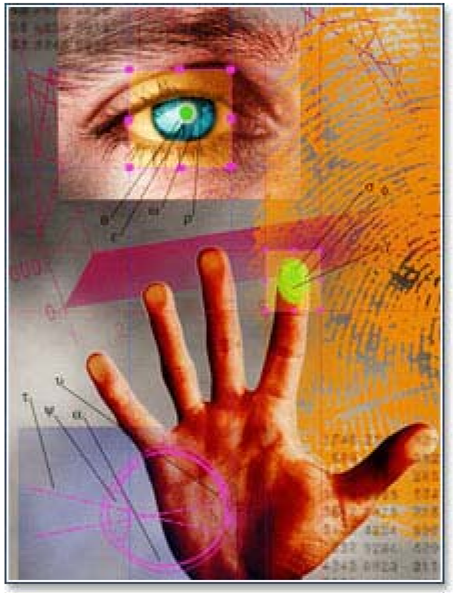
zSecure v1.12 Transforms zEnterprise into a Security Hub

- Arising from the cross-platform, cross-application, cross-resource integration that is available from zEnterprise is another compelling new possibility: **the use of zEnterprise as a security hub.**
- Centrally secure the full spectrum of IT services on multiple platforms. Consolidate distributed Linux servers to the System z environment to **reduce costs** and **improve security**.
- Because zEnterprise supports the ability to run the full spectrum of IT services on multiple platforms, it can also be used to centrally *secure* those services across production systems and test workloads. As organizations consolidate distributed Linux servers to the System z environment to reduce TCO, they can feel confident that overall security will *improve* at the same time—not *decline*. That, in turn, implies many attractive business benefits.
- Instead of fragmented security domains, apply best-in-class security solutions across domains—essentially, multiplying the business value.
- **Implement changes** in the security strategy **faster**, increasing IT agility.
- IBM estimates that when zEnterprise is used as a security hub, auditing overhead can decrease **as much as 70%**—a stunning figure.
- To deliver on this potential, customers will need IBM Security zSecure suite V1.12, a complete package of seven modular, seamlessly-integrated tools that help to secure IT applications, services, and resources from the complete range of security threats.

Summary: Benefits of Security zSecure Products

- The need for data security has increased in priority, scope, and complexity. Data is under threat from internal sources, as well as a myriad of external sources. Compliance challenges can vary across geographical boundaries. Security systems are not considered enhancements that can easily be postponed.
- The IBM Security zSecure suite is an end-to-end security solution that addresses security concerns from access control and provisioning to monitoring and compliance remediation.
- zSecure has several components, including:
  - zSecure Admin, which serves as a “veneer” over RACF and is efficient for mainframe administration’s daily activities
  - zSecure Alert, which provides real-time mainframe awareness of violations and intrusions
  - zSecure Audit, which analyzes and reports security events and detected security exposures

Benefits of TIM, FIM, and TKLM for z/OS

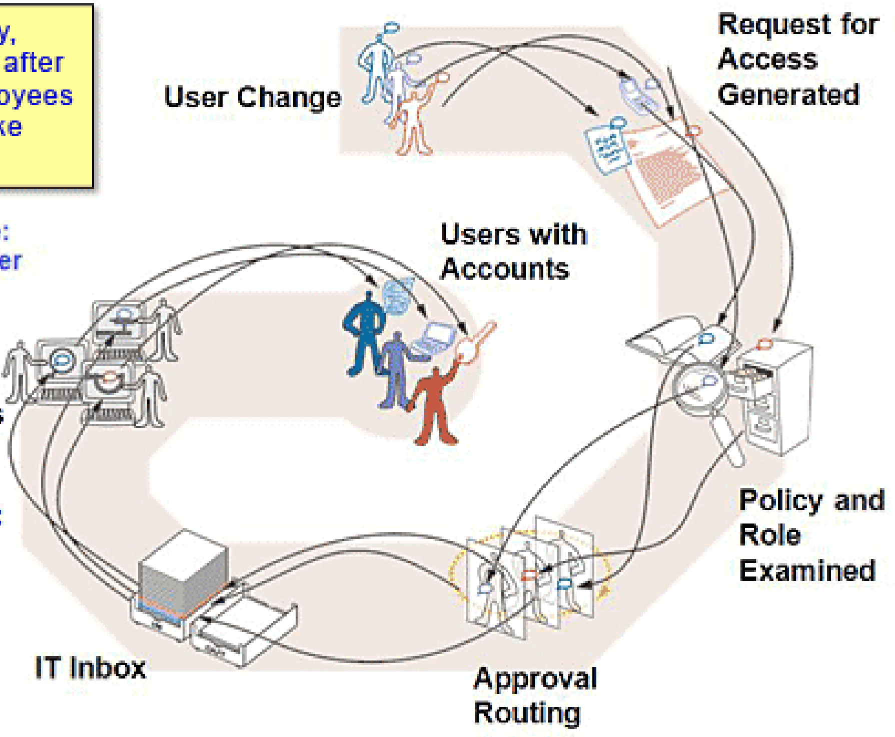


Benefits of Tivoli Identity Manager (TIM)

Life without Identity Management: Relying on the Squeaky and Expensive Wheel

Although slow and costly, initial access is granted after reminder calls. Ex-employees NEVER call and say "take away my access"!

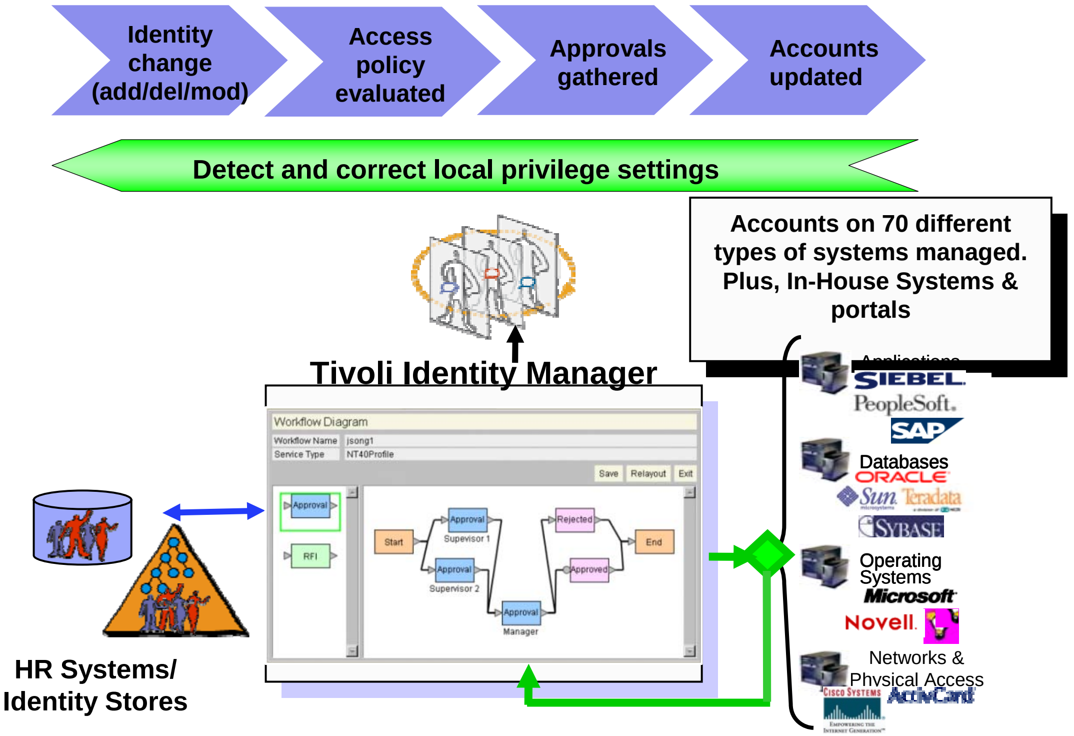
Elapsed turn-on time:
Up to 12 days per user



Account turn-off performance:
30-60% of accounts are invalid

1 FTE user admin only
handles 300-500 users

Tivoli Identity Manager (TIM)



- Know the ***people*** behind the accounts and ***why*** they have the access they do
- Fix non-compliant accounts
- Automate user privileges lifecycle across entire IT infrastructure
- Match your workflow processes

Visibility
See your business
Control
Govern your assets
Automation
Build agility into Operations

Simplify Complexity

- Business-relevant view of security
- Access rights audit & reports

Address Compliance

- On-boarding & recertification workflows
- Closed-loop provisioning

Reduce Costs

- Self-service password reset
- Automated user provisioning & de-provisioning

Quick Setup: TIM – Out of the Box

- Accelerates on-boarding of new applications and users **
- Supports request-based provisioning
- Enables organizations to leverage existing user access business processes
- Immediately removes off-boarded user accounts and privileges **
- Simplifies administration through automation and centralization **
- Provides Web self-service **
- Facilitates compliance by delivering automated audit readiness **
- Automates reconciliation to detect and correct noncompliant accounts **
- Identifies and eliminates dormant and orphan accounts **
- Maintains records of changes related to access rights
- Comes with a “read only” mode for auditors, a full range of compliance-related reports, and integration with IBM Tivoli Compliance Insight Manager for audit reports that map to your regulations and best practices **
- Offers “advanced” mode that provides a graphical drag-and-drop workflow designer

Questions to Think about When Considering TIM

- How do you monitor, enforce, and report on regulatory mandates?
- How are you managing security for privileged users? Is strong authentication required for employees, citizens, or customers?
- Will there be cost reduction efforts in the coming year? If so, how do you plan to reduce costs while also enhancing security?
- Have you recently had layoffs? If so, how are you managing removal of user access?
- To what are your help desk costs primarily due?
- How do you manage integration between physical and logical access?
- Are your users complaining that it is difficult to access the applications?

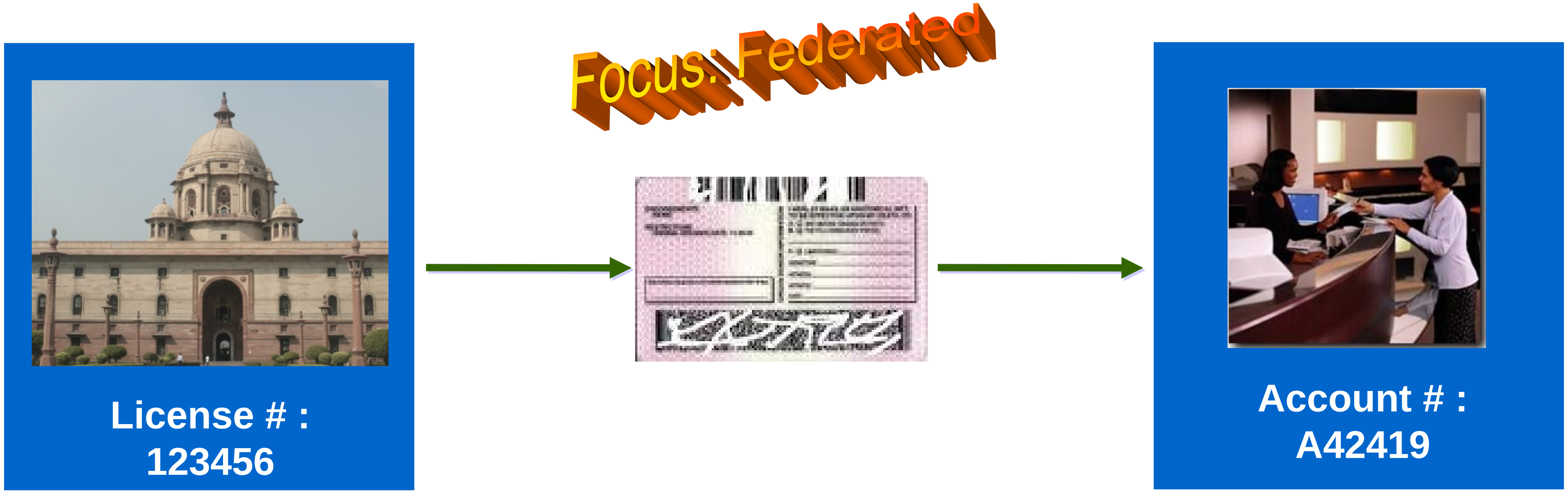
What Is Federation?

- Federation is a means of associating the necessary security context information with services requests so that the right credential format is available at the right times, wherever the services are implemented.
- Federation enables organizations to build security into their service-oriented architectures.

IBM Tivoli Federated Identity Manager (TFIM) can help you manage identity and access to resources that span companies or security domains.

Tivoli Federated Identity Manager Analogy

Similar to presenting a driver’s license to a bank teller, to look up your account number



Focus: Federated

License # : 123456

Account # : A42419

In day-to-day life, it’s proving who you are, as you move from one environment to another.

TFIM addresses this exact paradigm as an identity passes from one domain to another “trusted’’ domain (or one Web service to another).

Benefits of Tivoli Federated Identity Manager

- Reduces cost
- Improves control
- Provides consistency of control
- Provides audit capabilities
- Improves ease of use

Tivoli Key Lifecycle Manager (TKLM) Analogy

If cryptography is the heart of your security infrastructure

TKLM is a tool that looks out for this heart's health

TKLM and PCI-DSS

Have a requirement to meet PCI DSS? TKLM is the essential tool:

Consider:

- Section 3.5.1 Restrict access to keys to the fewest number of custodians necessary
- Section 3.5.2 Store keys securely in the fewest possible locations and forms
- Section 3.6.1 Generation of strong keys
- Section 3.6.2 Secure key distribution
- Section 3.6.3 Secure key storage
- Section 3.6.4 Periodic changing of keys
- Section 3.6.5 Destruction of old keys
- Section 3.6.6 Split knowledge and establishment of dual control of keys
- Section 3.6.7 Prevention of unauthorized substitution of keys
- Section 3.6.8 Replacement of known or suspected compromised keys
- Section 3.6.9 Revocation of old or invalid keys

Benefits of Tivoli Key Lifecycle Manager for z/OS

- Is used to manage IBM storage keys in centralized or distributed fashion
- Reduces encryption management costs related to setup, use, and expiration of keys
- Works with IBM encryption-enabled tape drives and system storage (DASD) devices
- Enables organizations to comply with disclosure laws, discovery rules, and regulations
- Ensures against loss of information due to key mismanagement
- Provides ability to centrally create or import, distribute, back up, archive, and manage enterprise keys
- Adds simplicity and manageability to key life cycle management through an easy-to-use interface

A Security Analyst’s View

> *“What separates IBM from the pack is its ability to provide a complete and extensible storage encryption architecture, including an enterprise key management capability.”*
>
> – Jon Oltsik, Senior Security Analyst
> Enterprise Strategy Group
> August 2008

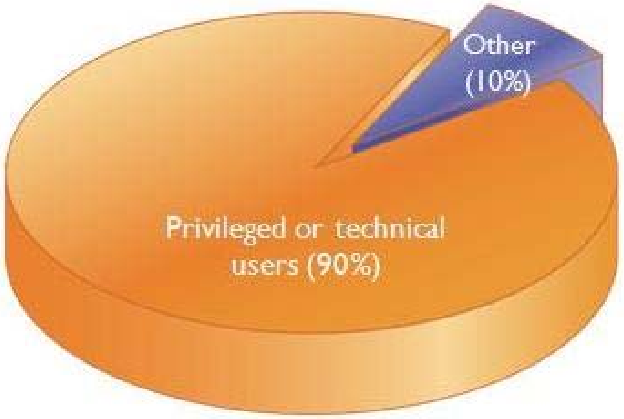
Summary: Benefits of TIM, FIM, and TKLM for z/OS

- IBM Tivoli Identity Manager (TIM) is a policy-based solution that automatically manages user access using (business) roles, accounts, and access permissions.
- IBM Tivoli Federated Identity Manager (FIM) provides a simple, loosely-coupled model for managing identity and access to resources that span companies or security domains.
- IBM Tivoli Key Lifecycle Manager (TKLM) stores and manages encryption keys from the System z platform, reducing integrating key management with System z operations, and automates related key registration, changes, and updates.

Security for UNIX and Linux Environments

The Source of Security Incidents

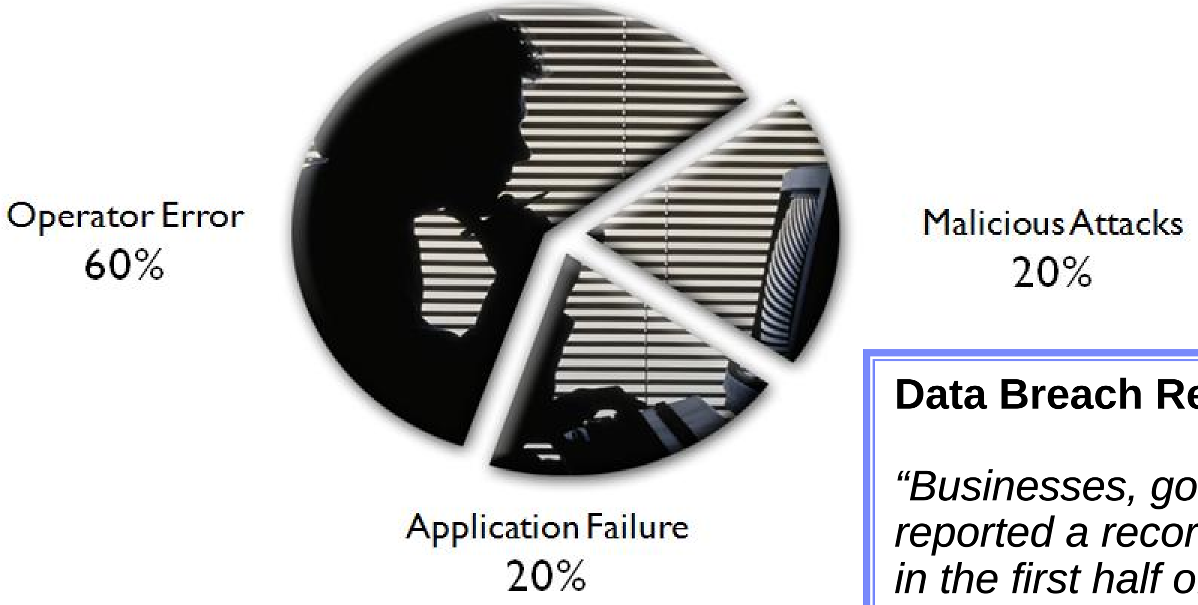
- Privileged or technical users cause 90% of insider incidents.
- Most of these violations are inadvertently caused by:
  - Change management process
  - Acceptable use policy
  - Account management process
- The other violations are deliberate, due to:
  - Revenge
  - Negative events



Sources: Forrester research, IdM Trends 2006; USSS/CERT Insider Threat Survey 2005/6/7/8; CSI/FBI Survey, 2005/6/7; National Fraud Survey; CERT, various documents.

Internal Errors Created by User Groups

Internal attacks cost approximately $11 USD per employee, per day!



Data Breach Reports Up 69% in 2010

“Businesses, governments, and universities reported a record number of data breaches in the first half of this year, a 69 percent increase over the same period in 2009, driven by a spike in data thefts attributed to employees and contractors, according to an analysis by identity theft experts.”

IBM Tivoli Access Manager for Operating Systems (TAMOS)

- Defends against top security threats
- Helps achieve safety of fine-grained authorization for UNIX and Linux systems
- Streamlines management of heterogeneous UNIX and Linux systems with integrated, delegated administration
- Uses extensible, configurable auditing capabilities to document compliance with government regulations, corporate policies, and other security mandates
- Leverages best-practice security policy templates to help minimize implementation effort and time
- Takes advantage of mainframe-class security and auditing in an easy-to-use product

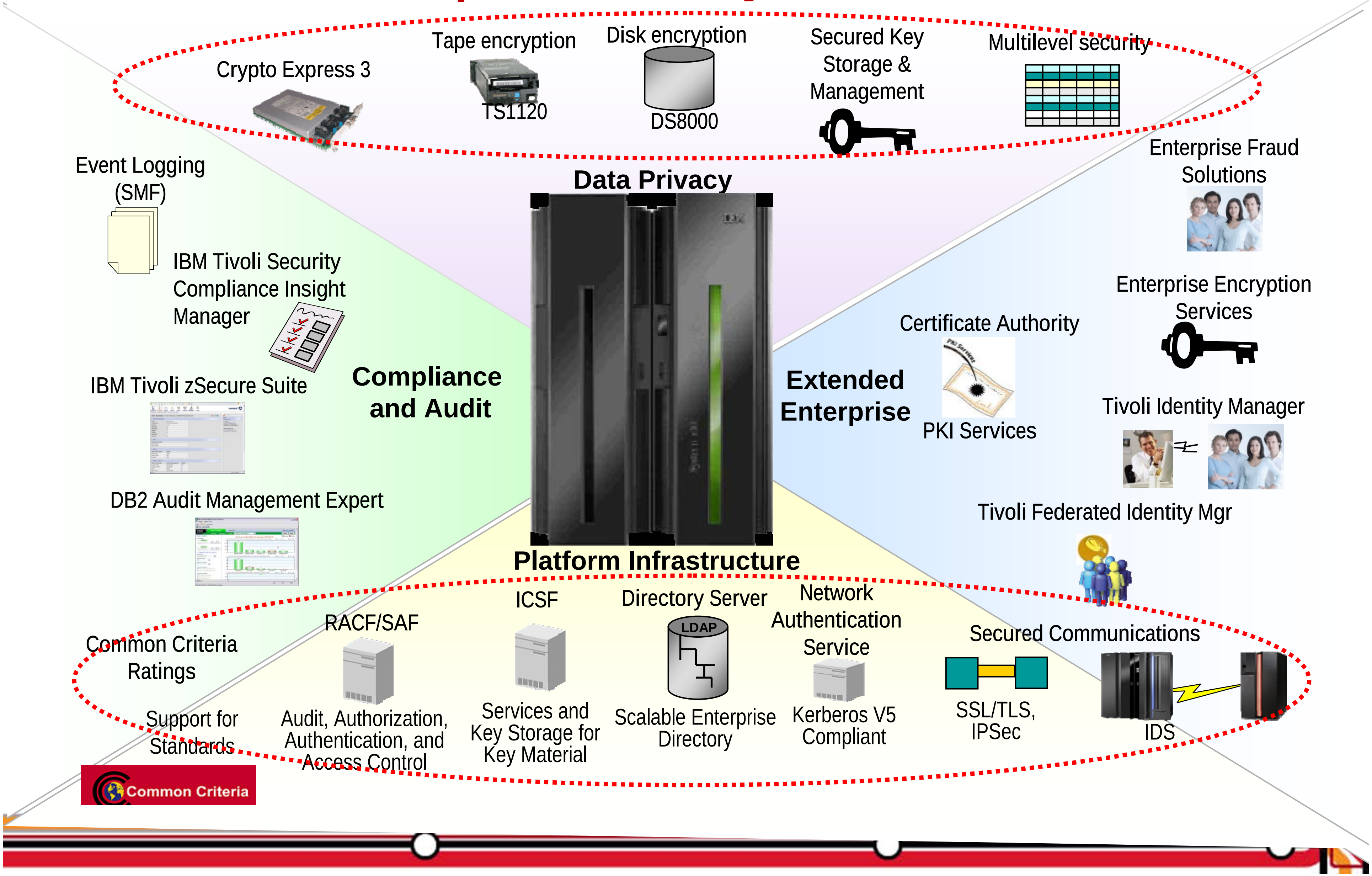
Benefits of TAMOS

- Reduced administration
- Centralized control
- Ease of use
- Integration
- Programming architecture
- Protection

Summary: Security for UNIX and Linux Environments

- TAMOS defends against the top security threats that enterprises face: malicious and fraudulent behavior by internal users and employees. Ninety percent of the security incidents are by privileged or technical users.
- TAMOS is a policy-based access control system for UNIX and Linux operating systems. It securely locks down business-critical applications, files, and operating platforms to help prevent unauthorized access.
- TAMOS can integrate with the other Tivoli security products to offer an end-to-end enterprise security solution.

Elements of Enterprise Security



Data Privacy

Crypto Express 3

Tape encryption

TS1120

Disk encryption

DS8000

Secured Key Storage & Management

Multilevel security

Compliance and Audit

Event Logging (SMF)

IBM Tivoli Security Compliance Insight Manager

IBM Tivoli zSecure Suite

DB2 Audit Management Expert

Extended Enterprise

Enterprise Fraud Solutions

Enterprise Encryption Services

Certificate Authority

PKI Services

Tivoli Identity Manager

Tivoli Federated Identity Mgr

Platform Infrastructure

Common Criteria Ratings

Support for Standards

Common Criteria

RACF/SAF

Audit, Authorization, Authentication, and Access Control

ICSF

Services and Key Storage for Key Material

Directory Server

LDAP

Scalable Enterprise Directory

Network Authentication Service

Kerberos V5 Compliant

Secured Communications

SSL/TLS, IPSec

IDS

www.ibm.com/security

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list pricesand performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

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

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance 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 or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.