IBM
Mainframe Security in the Enterprise

IBM Systems

Agenda

- Managing risk across the enterprise
- IBM mainframe security strategy
- Securing the infrastructure
- Enterprise wide security processes
- Helping to address compliance requirements

Security breaches published regularly demonstrate the spread of the menace

Data theft affects 88 million-plus Americans
SearchSecurity.com, June 21, 2006

MasterCard says 40 million files are put at risk.
New York Times, May 18, 2005

New Trojan Hits Symbian Smartphones
Information Week, July 5, 2005

At least a million machines are under the control of hackers worldwide.
ZDNET March 16, 2005

Phishing attacks against over two dozen European banks were detected by security firm Websense last weekend
The Register, September 20, 2005

Government agencies and companies in the U.K. are under attack by a concerted series of Trojan horses out to steal information.
TechWebNews, June 16, 2005

The number of bank accounts accessed illegally by a New Jersey cybercrime ring has grown to 676,000, according to police investigators.
ComputerWorld, May 20, 2005

Managing risk across the enterprise

The pillars of mainframe security

IT Infrastructure

- Help protect system from compromise
- Help secure access from the Internet
- Help secure data from theft or compromise

Enterprise-wide Business Processes

- Help secure applications that span the enterprise
- Leverage the proven security process of your mainframe

Risk Compliance

- Provide policy based security processes
- Provide audit information
- Enable regulatory compliance
- Detect and prevent a security breach and reduce impact

System z Architecture: Security Built In By Design

- **Enforced Workload Isolation**
  - Each user in a separate address space
  - LPAR separation ensures integrity
  - Supervisor state & system programs protection
- **Authorized program facility (APF)**
  - Executables only accessible to authorized users
- **Storage Protection Keys**
  - Controls access to protected storage
  - Cross memory services prevent unauthorized data access

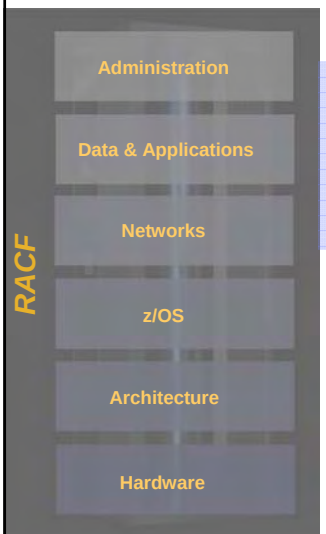
Allows customers to confidently place critical workloads on single z/OS image

Can help prevent intrusion from malware, viruses and worms

Proven with 40 years of secured operations!

The backbone of mainframe security Resource Access Control Facility (RACF)

Authentication
Authorization
Administration
Auditing



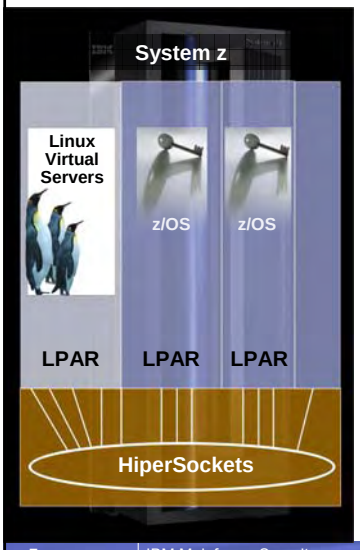
Enables application and database security without modifying applications

Can reduce security complexity and expense:

- Central security process that is easy to apply to new workloads or as user base increases
- Tracks activity to address audit and compliance requirements

- Manage access to encryption key data store
- Integration with distributed system security domain
- Checking for “Best Practices” with z/OS HealthChecker
- Serving mainframe enterprises for over 30 years

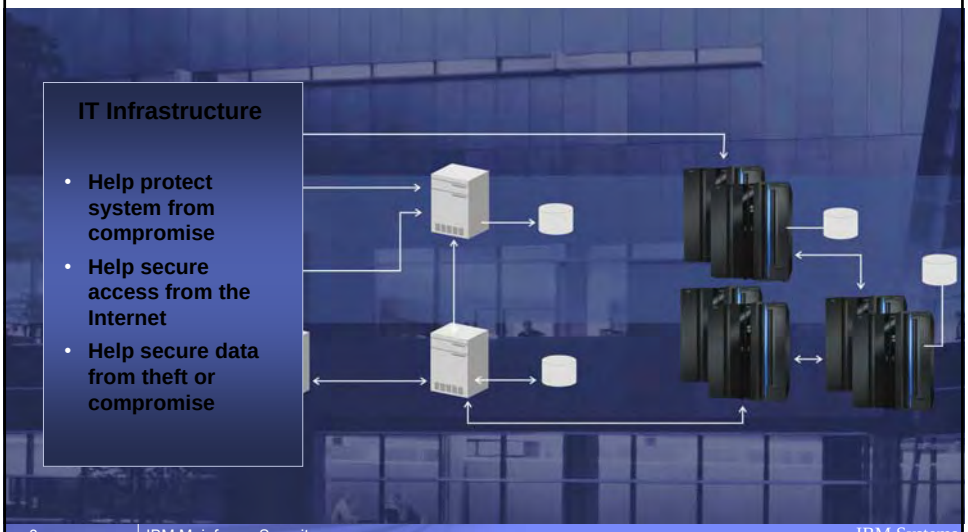
Security through virtualization



- **Virtual servers on a single mainframe: Logical Partitions (LPAR)**
  - Up to 60 isolated system images
  - Flexible dynamic provisioning of hardware resources
  - Highest Common Criteria certification – EAL5
- **Virtual network in the server: HiperSockets**
  - Provides an integrated TCP/IP network through system memory
  - Enables a "Data Center" inside a box with a mixture of z/OS and Linux images.
  - Highly secure connection – no external network exposed

Managing risk across the enterprise

The pillars of mainframe security



The Power of Mainframe Encryption

Helping to reduce risk across your value-net

Helping to protect privacy over the internet

Helping to protect confidential data in databases

Helping to protect data leaving your enterprise

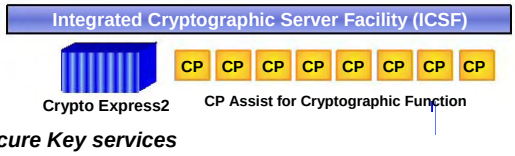
Customer objectives:

- **Only intended party is allowed to decrypt**
- **Availability of the keys and decryption services when you need them**

Enterprise-wide Key Management

Helping to protect archived data

Mainframe Encryption Hardware



Introduced in 1971
Accelerates encryption and provide Secure Key services

CP **CPACF** (z9 EC, z9 BC, z990, z890)

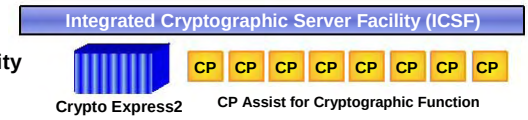
- Support high levels of security for demanding applications
- Very high performance TDES, AES -128* and SHA-256*

CryptoExpress2

- For Secure Key exchanges
- Master keys in “tamper-resistant” package
- Dual control for Master Key management
- Important for finance functions
  - ✓ ATM support, Triple-DES, Trusted Key Entry
  - ✓ CVV validation
- Designed to comply with FIPS 140-2

*** Requires z9 EC or z9 BC**

z/OS Centralized Key Management



Integrated Cryptographic Service Facility (ICSF)

Methodology to help protect and manage keys

- Highly secure and available key data store
- Provides key recovery capabilities
- Long term key management
- Disaster recovery capabilities
- Audit records

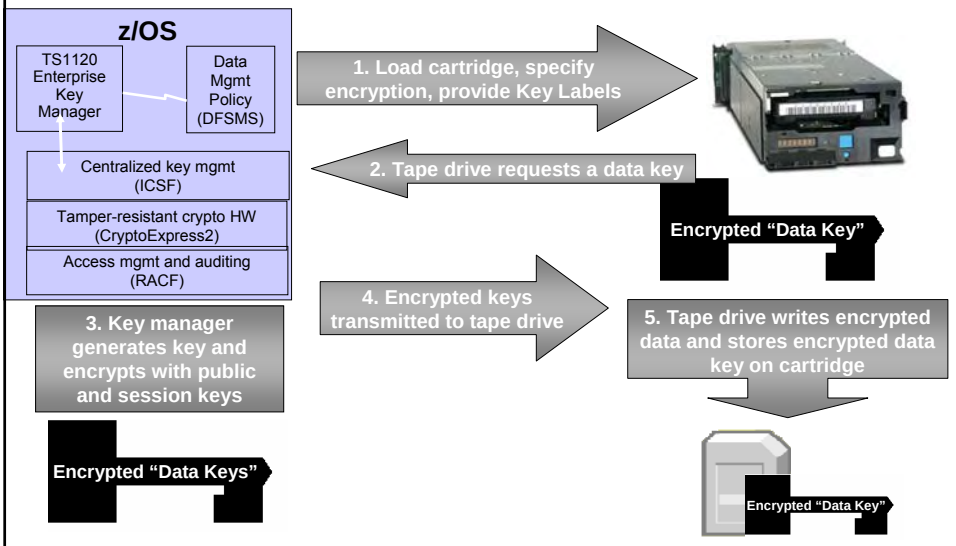
- Single point of control
- Over 15 years of production use

Announcing the industry's first comprehensive end to end tape encryption solution

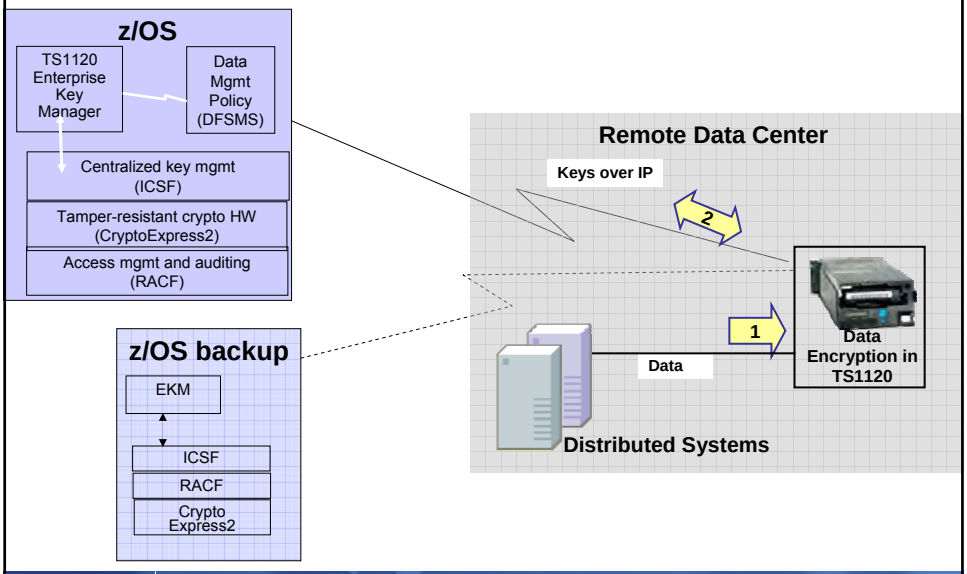
- IBM System Storage TS1120 Tape Drive
- Designed with a cross-IBM team driven by customer requirements
- New Encryption Key Manager program
- Integration with System z security and encryption capabilities
- Services and consulting

Customer Objectives
Data can only be decrypted by intended party
Keys available when and where you need them

TS1120 tape encryption leveraging PKI (Public Key Infrastructure)



IBM Mainframe Enterprise Key Management



Tape encryption to exchange with business partners

Encryption Facility for z/OS, V1.1

Centralized
Key Management

Data Encryption in the Server

- Flexible options for business partner exchange
- Partners do not need TS1120 encrypting drives
- Supports public key or password based exchange

Uses no-charge Java client to decrypt tape cartridge

Can also encrypt data to send back

Network security – encryption over the Internet

SSL

Mainframe Data Center ⟺ Web browser HTTPS

IPsec (VPN)

Mainframe Data Center ⟺ Branch Office

- **Application-layer encryption with SSL and TLS**
  - **Encryption acceleration in the System z server (CPACF)**
    - **Support for up to 6000 SSL handshakes per second**
  - **Application Transparent TLS (z/OS 1.7)**
    - **Define a TLS or SSL secured connection with no anticipated changes to existing applications**
- **Network layer encryption with IPsec**
  - **Allows secure tunnel between two IP entities (Virtual Private Network)**
  - **Improved scale and performance in z/OS 1.7**
- **Simpler and consistent configuration of the above technologies**
  - ***z/OS Network Security Configuration Assistant***

Network security – z/OS intrusion detection services

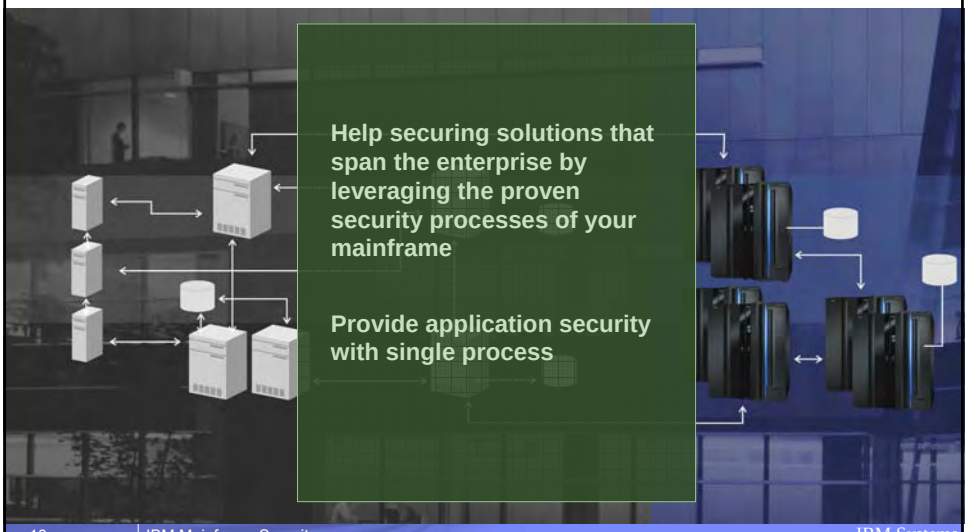
More than Intrusion Detection -

Intrusion Defense!

- **Built-in self-protection**
  - **Complements network-based IDS devices by detecting attacks that otherwise would go undetected**
- **Monitors incoming traffic, detecting both new and known attacks**
  - **Can evaluate encrypted data *after* decryption**
- **Easy administration**
  - **Policy-based controls, eliminates overhead of updating intrusion signatures**
- **Auditing and Reporting:**
  - **IDS events can be tracked by Tivoli Security Operations Manager 3.1.**
  - **TSOM can correlate and analyze events, and include in reports**
- **IDS events trigger NetView automation**

New in z/OS 1.8:
- No longer requires LDAP
- Policy administration simplified

Mainframe security – enterprise wide processes



Help securing solutions that span the enterprise by leveraging the proven security processes of your mainframe

Provide application security with single process

End-to-end identity and access management

authentication, authorization, administration, audit

Distributed Security Domain
Tivoli Security Suite

- Access Manager
- Identity Manager
- Federated Identity Manager

Mainframe Security Domain

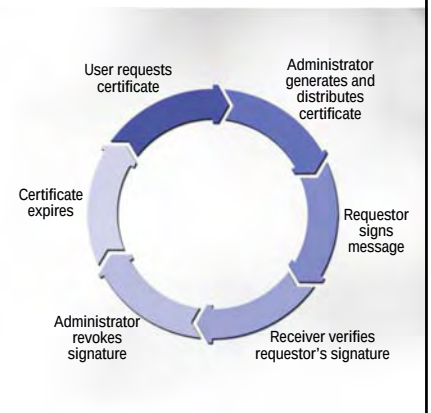
- z/OS RACF
- z/OS 1.8 Improved LDAP
- Tivoli Directory Integrator

Recent Enhancements

- TAM components in WAS on z/OS
- Federated Identity Manager on z/OS
- Integration services
- Roadmap for further integration

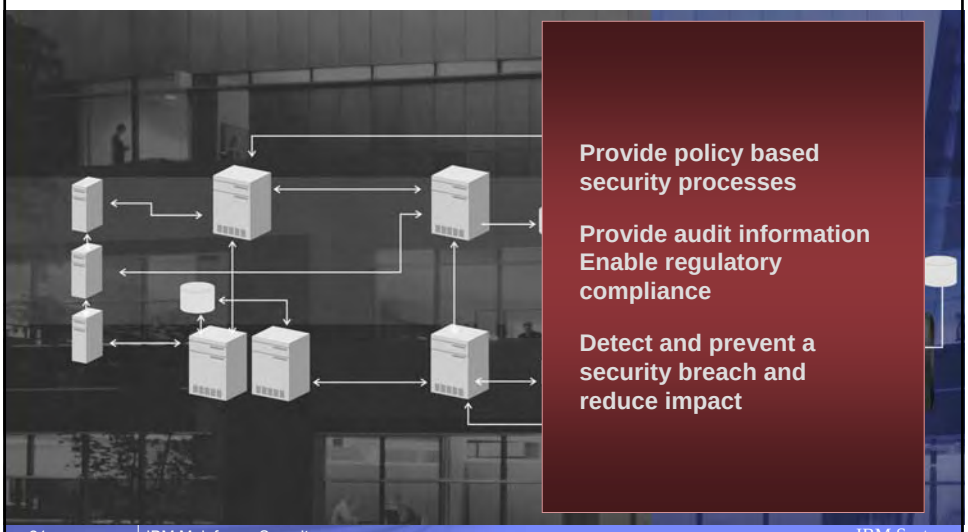
Digital certificate life cycle management
A TCO advantage with z/OS

- z/OS PKI Services is a Certification Authority solution
- Provides certificate life cycle mgmt
- IBM services available



Large bank used PKI to help secure connection with branch offices - Saved an estimated $16M a year

Mainframe security – risk compliance

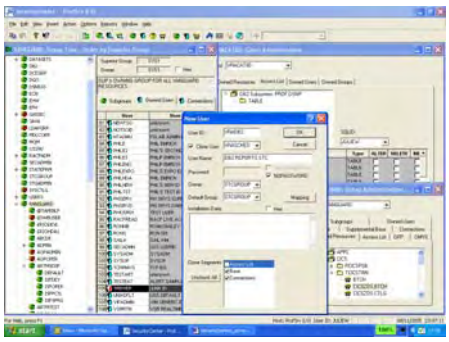


Provide policy based security processes

Provide audit information Enable regulatory compliance

Detect and prevent a security breach and reduce impact

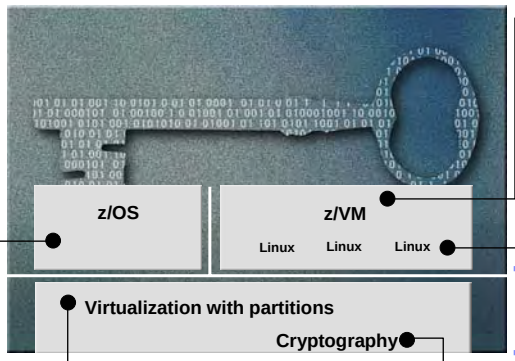
Complimenting the mainframe security portfolio
Vanguard Security Solutions



- **IBM & Vanguard Security Solutions**
  - **Vanguard Security Center** offers ease-to-use graphical user interface for RACF and DB2 security administration on z/OS
  - **Vanguard Administrator** provides advanced security server management and analysis with automation and power utilities
  - **Vanguard Analyzer** assists with security system snapshots or full-scale System z9 security audits
  - **Vanguard Enforcer** manages and enforces security policy in z/OS and RACF
  - **Vanguard Advisor** provides event detection, analysis and reporting capabilities for the z/OS and RACF

Certifications on System z

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



z/VM
- **Common Criteria** EAL3+
  - with CAPP and LSPP
  - **z/VM 5.1 + RACF**

Linux on System z
- **Common Criteria** EAL4+
  - with CAPP and LSPP
  - **SUSE LES9 certified**
- **Common Criteria** EAL3+
  - with CAPP and LSPP
  - **Red Hat EL3 certified at EAL3+**
  - **Red Hat EL4 EAL4+ in progress**

z/OS
- **Common Criteria EAL4+**
  - with CAPP and LSPP
  - z/OS 1.7 + RACF
- **IdenTrust™ certification** for z/OS as a Digital Certificate Authority (PKI Services)

System z9 EC and z9 BC and other System z servers
- **Common Criteria** EAL5 for Logical partitions
- **FIPS 140-2 level 4** for Crypto Express 2

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

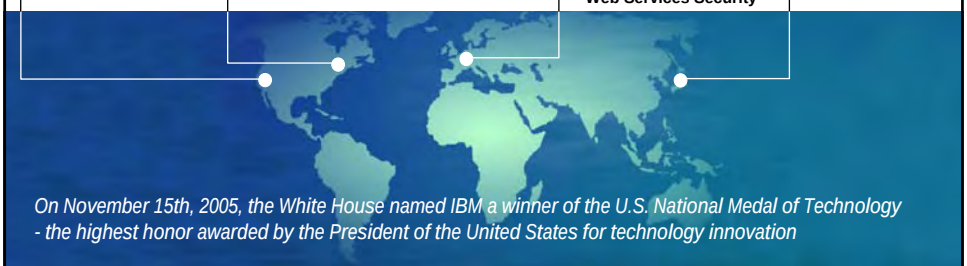
Continued innovation in security

Almaden
- **Cryptographic Foundations**
- **Digital Rights Management**
- **Privacy-Preserving Data Mining**

Watson
- **Cryptographic Foundations**
- **Network Security & "Ethical Hacking"**
- **Secure Embedded Systems**
- **Security of Autonomic Systems**
- **Secure Hardware**
- **Security Engineering**
- **Secure Hypervisors**
- **Integrity Based Computing**
- **Secure Linux systems & Applications**
- **High Assurance Systems**
- **Security Assessment Tools**
- **Privacy Technology**
- **Web Services Security**
- **Biometrics & Surveillance Systems**

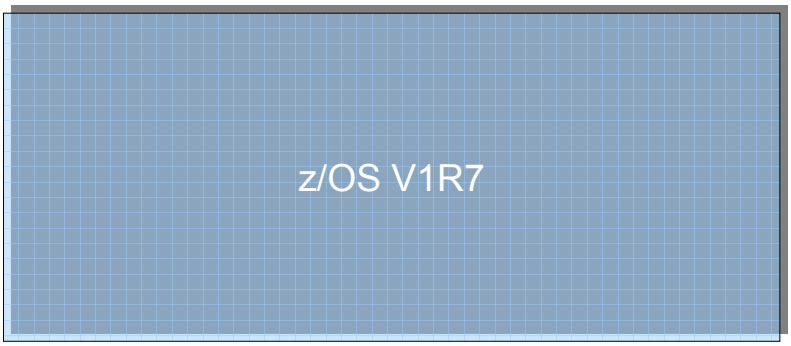
Zürich
- **Cryptographic Foundations**
- **Java Cryptography**
- **Privacy Technology**
- **Identity Management**
- **Integrity-Based Computing**
- **Grid Computing & Web Services Security**
- **Intrusion Detection & Alert Correlation**
- **Smart Card Systems and Applications**
- **Java Card**
- **Web Services Security**

Tokyo
- **Web Services Security**
- **Mobile Security**
- **XML Security**
- **VLSI for crypto**
- **Digital Watermarking**



On November 15th, 2005, the White House named IBM a winner of the U.S. National Medal of Technology - the highest honor awarded by the President of the United States for technology innovation

z/OS Security Server (RACF) Update



RACF USER-related Enhancements: Mixed-Case Passwords

- Allows RACF to distinguish between upper- and lower-case characters in passwords.
- Supported by TSO/E, CICS TS 3.1 (and 2.2 and 2.3 via PTF), Console logon, JOB statements, and z/OS UNIX functions.
- Controlled by SETR PASSWORD(MIXEDCASE | NOMIXEDCASE)
  - **Do not enable mixed-case passwords unless all local systems sharing RACF DB are at z/OS R7**
  - **For RRSF, RACF will ensure passwords are in upper-case if sent to an RRSF node at z/OS R6 or earlier.**

RACF USER-related Enhancements: Mixed-Case Passwords…

- Notes:
  - **RACF will remember whether a user has ever had a mixed-case password. If not, when comparing a password entered by the user RACF will check both the value as presented to RACF and the upper-case version of that value.**
  - **When the user is changing his password, RACF will check that the new password and current password, when converted to upper-case, are different. Example:**
    - **If current password is ABCD**
    - **Then new password aBcD will be rejected**

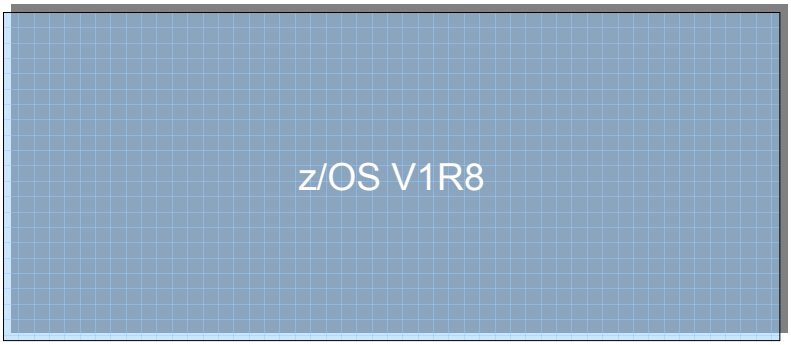
RACF Support for the IBM Health Checker for z/OS

- **What is the IBM Health Checker for z/OS?**
  - Originally a tool developed by ITSO to address component configuration and setup errors commonly made by installations
    - Web download
    - Implemented as a batch job
    - 37 checks
  - With z/OS V1R7, the IBM Health Checker for z/OS is integrated into z/OS
    - Implemented as a started task
    - 55 checks
    - Rolled back to z/OS V1R4 as a web download
    - Checks are shipped with components
    - Installations and vendors can write checks
    - Extensive SDSF support

Common Criteria

- **Common Criteria certification for z/OS R7 completed**
  - Labeled Security Protection Profile (LSPP) at Evaluation Assurance Level 4 (EAL4)
  - Controlled Access Protection Profile (CAPP) at EAL4

z/OS Security Server (RACF) Update

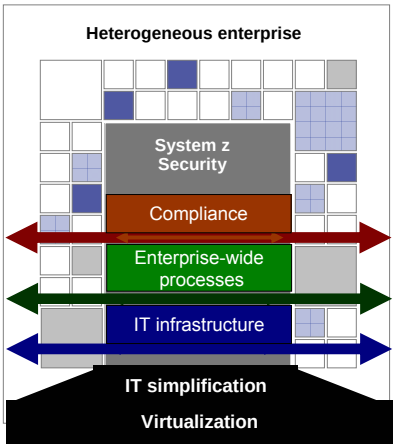


z/OS Version 1 Release 8

- Support for RACF pass phrases from 14 to 100 characters is length
- Significant improvements to Identrus-certified support for digital certificates, included SCEP and multiple certificate authority (multiple-CA) support
- Improvement for tape data set protection using RACF or another external security manager
- Support for Advanced Encryption Standard for AES for IPSec
- Support for SAF Identity Tokens
- Support for virtual key rings

IBM mainframe security

Our goal is to continually **increase value** to protect our customers' investments by **extending** premiere System z **capabilities** across **heterogeneous platforms** to become the '**Enterprise Trust Authority**' for On Demand Business.



ibm.com/systems/z/security