LSU Sweden

Security Update & Crypto update

Nordic

Large Systems Update Seminar

October 2006

Uno Bengtsson

IBM Server Tegchnology Group (STG)
e-Mail: uno.bengtsson@se.ibm.com

© 2006 IBM Corporation

Agenda
Mainframe Security Differentiator

- **IBM mainframe security strategy**
- **Encryption Facility & Tape Security**
- **z/OS 1.8 Security update**

© 2006 IBM Corporation

LSU Sweden

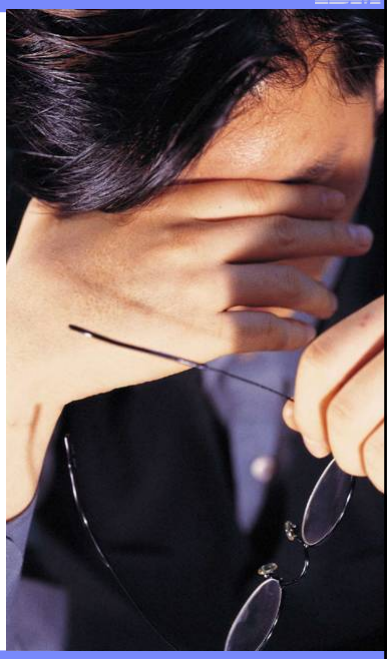
Sweden LSU November 2006
Uno Bengtsson

11/15/2006

© 2006 IBM Corporation

Potential Costs of A Security Breach

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

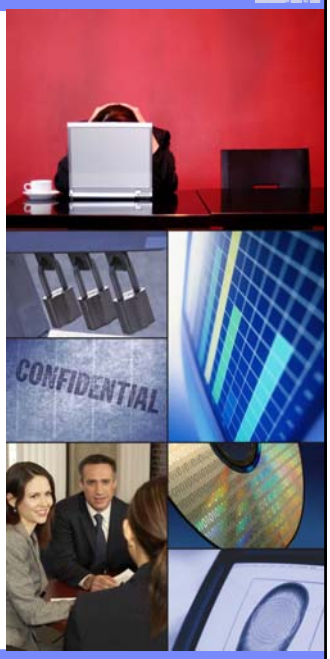


© 2006 IBM Corporation

IT security challenges

Need to maintain business innovation and growth in the face of risks, while decreasing operational costs

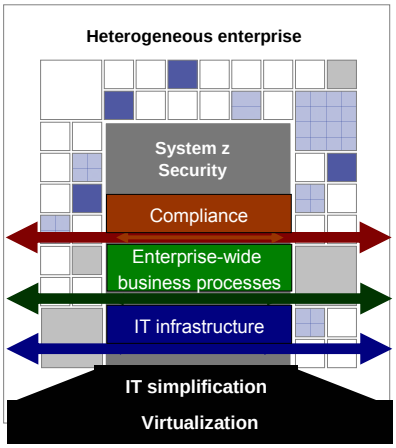
- **Increasing *complexity* of security issues in today's environment**
- ***Compliance* with regulations and audit requirements is difficult**
- ***Managing change* *by limiting* and *tracking access* to sensitive or private information and assets**
- **Establishing a *trusted relationship* with customers and partners**
- **Protecting against *security incursions* and *risks to confidential information***
- **Security issues are hurting the *bottom line!***



© 2006 IBM Corporation

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.



© 2006 IBM Corporation

Managing risk across the enterprise

The pillars of mainframe security

Compliance

- Provide policy based security processes
- Provide audit information, enable regulatory compliance
- Help detect and prevent a security breach and reduce impact

Enterprise-wide business processes

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

IT Infrastructure

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

© 2006 IBM Corporation

Mainframe security – IT infrastructure

Protect system from compromise

- System and application integrity features in architecture
- Centralized identity management and access control
- Health checking of the security configuration

Help secure access from the Internet

- Network encryption options using industry standards (SSL, TLS, IPsec)
- Integrated intrusion detection services for added protection beyond firewalls
- Highly secure perimeters (DMZ) with Linux firewalls on your mainframe

Help secure data from theft or compromise

- High performance encryption and secure key management
- Data encryption for tape with centralized key management
- Data encryption with DB2 and IMS Data Encryption tool
- XML security gateway for SOA applications with DataPower

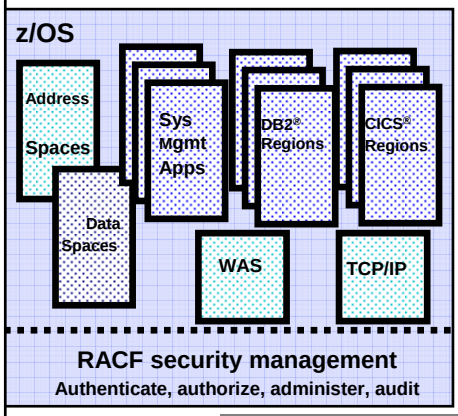
- System z architecture
- Health Checker
- RACF
- z/OS Health checker

- Communications Server
- IBM Directory Server
- Stonegate Firewall

- Encryption Services
- Tape Encryption
- DB2 & IMS Encryption tool
- DataPower

© 2006 IBM Corporation

System and application integrity by design
Protect system from compromise



- Workload Isolation
  - Unique address spaces
  - Programs must have special authority to securely access data owned by others
- Memory protection
  - Storage protect keys provide additional integrity, built into the hardware
  - Information in real memory is protected from unauthorized use
  - User programs and data are protected from other jobs
  - Invalid requests result in a program exception interrupt

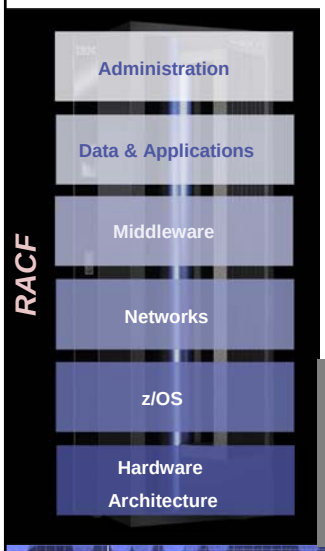
Allows placement of mixed business-critical workloads on single z/OS image

Can help prevent intrusion from malware, viruses and worms

Designed so user buffer overflows do not crash systems software code

© 2006 IBM Corporation

Resource Access Control Facility (RACF)



Centralized security management across mainframes in the enterprise

Separate security processes from applications

- Identity and Access Management

  Authentication, Authorization, Administration and Auditing
- Checking for "Best Practices" with z/OS HealthChecker
- Over 30 years experience

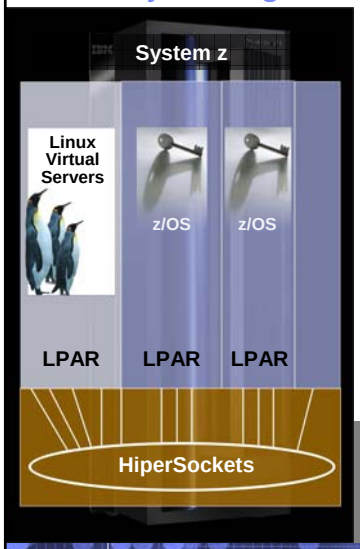
Can reduce security complexity and expense:

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

© 2006 IBM Corporation

Protect system from compromise

Security through virtualization



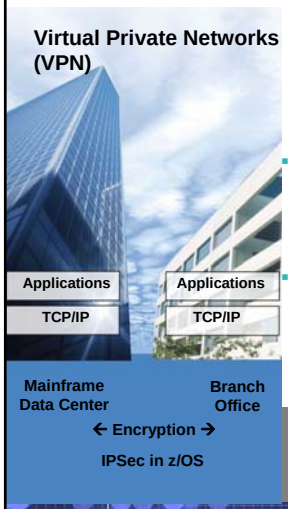
- Virtual servers on a single mainframe: Logical Partitions (LPAR)
  - LPAR provides up to 60 isolated system images
  - Flexible dynamic relocation of hardware resources
  - Common criteria certification – EAL5
- z/VM allows further virtualization of hundreds of Linux images
- Virtual network in the 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

•Integrity of separate images maintained through virtualization technology
•Reduced complexity through consolidation
•Allows data transfers between images without exposing to the network

© 2006 IBM Corporation

Help secure access from the Internet

Network security – encryption over the Internet



- **Application-layer encryption with SSL and TLS**
  - Encryption acceleration provided in each engine on System z server
    - Support for up to 6000 SSL handshakes per second*
  - Help reduce development complexity and costs with 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 locations (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*

*** In a recent test using a System z9 with four CPs and both PCI-X adapters configured as accelerators the Crypto Express2 feature**

Mainframe uses latest technologies to help protect exchanges over the Internet

© 2006 IBM Corporation

Network security – z/OS intrusion detection services

Help secure access from the Internet

Detects events such as:
- Scans Attacks Flooding

Provides Defenses on z/OS
- Packet discard
- Limited # connections

Reports:
- Logging - Console
- Packet trace
- Notifications

A component of z/OS
Integrated in the IP stack

- Compliments network based IDS
- Enables further detection of attacks and application of defensive mechanisms
- Can be extended with Netview IDS

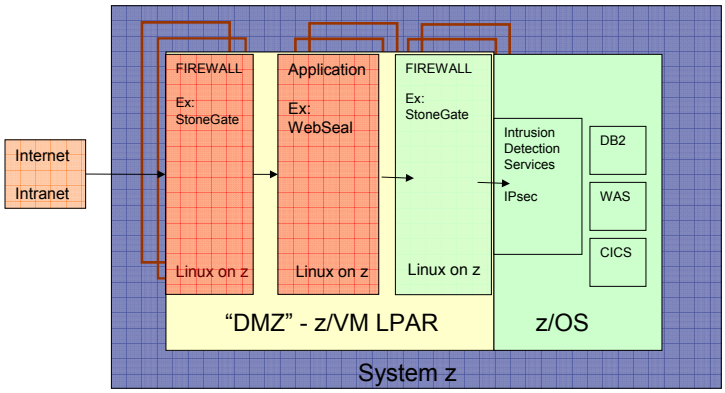
- Evaluates inbound IPsec encrypted data after decryption on the mainframe
- Evaluates many known attacks
- Can evaluate unknown attacks
- Detects problems in real-time
- Policy based
- New in z/OS 1.8:
  - **No longer requires LDAP**
  - **Configuration assistant**

Helps protect against network attacks
Can evaluate IPsec inbound data after decryption

© 2006 IBM Corporation

Network security – perimeter defense Options for a DMZ on System z

Help secure access from the Internet



- **Builds on integrity of mainframe: LPAR, HiperSockets**
- **Consolidation for ease of management**
- **Easy provisioning of additional Linux images**

© 2006 IBM Corporation

Mainframe security – business processes

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

- Federating identities across business boundaries with Federated Identity Manager for z/OS
- RACF and Tivoli security products optimize enterprise security
- Consistent directories
- Multi-level security for data access with different levels of "need to know"

Provide enterprise-wide security processes for the extended enterprise

- Enterprise-wide tape encryption key management
- Enable companies to be their own Certificate Authority
- Federated Identity Management and user lifecycle management

- Tivoli Federated Identity Manager for z/OS
- RACF and Tivoli suite
- Tivoli Directory Integrator

- Encryption Facility for z/OS
- CryptoExpress2
- Tape encryption
- z/OS PKI Services
- Tivoli Federated Identity Manager for z/OS
- Tivoli Identity Manager for z/OS

© 2006 IBM Corporation

Digital certificate hosting on System z

Provide an identity authentication process

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web.

A certificate authority (CA) is an authority in a network that issues and manages digital certificates.

CA often provided by third parties.

z/OS PKI Services to enable a Certificate Authority solution

- Ability to host Digital Certificate management for the banks, government agencies…
- TCO advantage - no need to pay a third party CA for certificates
- Relatively low mips to drive thousands of certificates
- Scalable (Sysplex exploitation)
- Secure with System z cryptography (Secure Key)

Used by large finance institution to save an estimated $16M a year

© 2006 IBM Corporation

PKI Services Milestones

- **z/OS V1R3 – Initial release**
  - Only one instance of the started task
  - Only one CA key pair
  - CRL in LDAP only
- **z/OS V1R4 – Sysplex support**
  - Multiple instances of the started task in a sysplex can share the VSAM datasets (using RLS)
- **z/OS V1R5**
  - CRL distribution points
  - Identrus compliance
  - Suspend/resume of certificates
- **z/OS V1R7**
  - Digital Signature Algorithm (DSA) Key Support
  - Enhanced CRL/ARL Distribution Point
  - Online Certificate Status Protocol (OCSP) Support
  - CRL via HTTP

© 2006 IBM Corporation

Requirements to deploy z/OS PKI Services

- **HTTP Server**

–Provides browser/CGI interface for end-users and administrators
–Web page logic defined in certificate templates file
–CGIs-Read template file, control flow

- **R_PKIServ-SAF callable service backed by RACF (or other)**

–End-user functions -Request, retrieve, verify, revoke, or renew a certificate
–Administrator functions -Query, approve, modify, or reject certificate requests, query and revoke issued certificates
–Interface to call PKI Services
–SMF auditing

- **PKI Services Daemon**

–Services threads for incoming requests
–Background threads for certificate approval/certificate revocation list (CRL) issuance
–VSAM DBsfor requests (ObjectStore) and issued certificate list (ICL)

- **Open Cryptographic Services Facility (OCSF) and Open Cryptographic Enhanced Plug-ins (OCEP)**

–OCSF -PKI Services daemon uses for posting certificates and CRL's to LDAP
–OCEP -Used by the PKI Services Trust Policy

© 2006 IBM Corporation

Mainframe security – compliance

Provide policy based security processes

- Role-based access management in RACF
- z/OS Healthchecker analyzes RACF configuration
- Vanguard Enforcer helps manage and enforce security policy in z/OS and RACF

Provide audit information, enable regulatory compliance

- Audit security-relevant events with RACF logging and reporting tools
- Tivoli Security Operations Manager includes RACF security events
- Vanguard Analyzer assists with security snapshots or full scale System security audits
- Certification of mainframe products and components

Help detect and prevent a security breach and reduce impact

- Increased network protection with Intrusion Detection Services
- Vanguard Advisor provides event detection, analysts and reporting

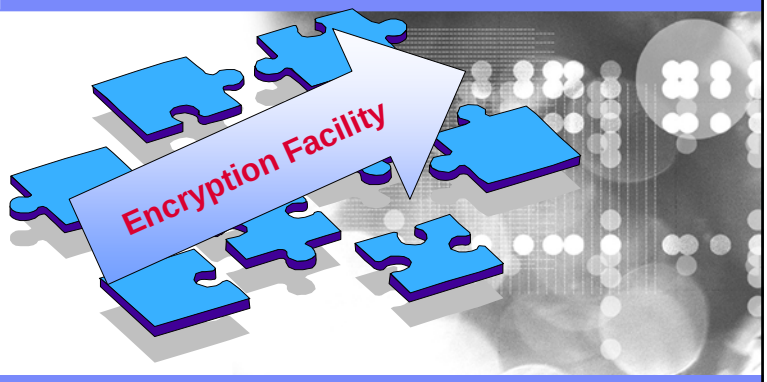
- RACF
- Health checker
- ISV tools

- RACF logging
- Tivoli Security Operations Manager support
- ISV tools
- Common Criteria Certifications

- Intrusion Detection Services
- ISV tools

© 2006 IBM Corporation

LSU Sweden



© 2006 IBM Corporation

The Mainframe –
A History of Enterprise Security

- **Hardware Cryptography: 1970**
- **RACF: controls access to resources and applications – 1976**
- **Key management built into operating system (ICSF) – 1991**
- **Security Applications: Tivoli & Leading Software Vendors**
- **Intrusion Detection Services (IDS): 2001**
- **PKI: create digital certificates & act as Certificate Authority (CA) – 2002**
- **Multilevel Security (MLS): 2004**
- **Encryption Facility for z/OS: 2005**
- **Encrypting Tape Drive TS1120: 2006**

© 2006 IBM Corporation

The Power of Mainframe Encryption
Helping to reduce risk across your value-net

Helping to protect data over the Internet

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**

Centralized Key Management

Helping to protect archived data*

- IBM Encryption Facility for z/OS planned GA dates:
  - Encryption Services – 28 Oct, 2005
  - DFSMSdss Encryption - 2 Dec, 2005

© 2006 IBM Corporation

System z Encryption Hardware

Integrated Cryptographic Server Facility (ICSF)

Crypto Express2 | CP CP CP CP CP CP CP CP | CP Assist for Cryptographic Function

Accelerating encryption and providing Secure Key services

Secure Key

- Key information never appears in server storage (never "in the clear")
- Master keys in "tamper-resistant" package
- Dual control for Master Key management
- Important for banking functions
  - ✓ ATM support, Triple-DES, Trusted Key Entry
- Designed to comply with FIPS 140-2

CP

CP Assist for Cryptographic Function (z9 EC, z9 BC, z990, z890)

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

*Requires z9 EC or z9 BC

© 2006 IBM Corporation

System z Encryption z/OS Software

Integrated Cryptographic Server Facility (ICSF)

Crypto Express2 | CP CP CP CP CP CP CP CP | CP Assist for Cryptographic Function

Providing centralized key management

- Helps to protect and manage keys
  - **Highly secure and available key data store**
  - **Provides key recovery capabilities**
  - **Long term key management**
  - **Disaster recovery capabilities**
  - **Audit compliance**
- Single point of control
- Over a decade of production use

Encryption support

- **Manage based on security policies**
- **Support for multiple encryption and hashing functions**
- **Utilizes the tamper resistant hardware for "secure keys"**

Access controls

- **z/OS RACF for authorization, authentication**

Can be complimented with z/OS Digital Certificate hosting services

- **Customer can deploy their own Certificate Authority**
- **Identrust[tm] certified (z/OS 1.5)**

© 2006 IBM Corporation

IBM Encryption Facility for z/OS, 1.1

Licensed Program Product
MSU-based pricing*

Runs on the following servers: System z9 109 (z9-109), or equivalent
zSeries z900 or z990, or equivalent
zSeries z800 or z890, or equivalent

Requires: z/OS V1.4 or higher z/OS.e V1.4 or higher

Feature: *Encryption Services*

Optional Priced Feature

- Supports encrypting and decrypting of data at rest (tapes, disk)
- Supports either Public Key/Private keys or passwords to create highly-secure exchange between partners

Encryption Facility Client

Web download

- Java technology-based code that allows client systems to decrypt and encrypts data for exchange with z/OS systems

Decryption Client for z/OS

Web download
The Decryption Client for z/OS is supported on z/OS systems only.

Feature: *DFSMSdss Encryption*

Optional Priced Feature

- Allows encryption and compression of DUMP data sets created by DFSMSdss
- Supports decryption and decompression during RESTORE

© 2006 IBM Corporation

Future Directions – Extending Encryption to IBM TotalStorage

- **Statement of Direction:**
  - To address customers' growing concern with data security, IBM is announcing a statement of direction for the development, enhancement and support of encryption capabilities within storage environments such that the capability does not require the use of host server resources.
  - This includes the intent to offer, among other things, capabilities for products within the IBM TotalStorage portfolio to support outboard encryption and to leverage the centralized key management functions planned for z/OS ICSF.

Enterprise-wide Key Management

Data
Encryption keys

Tape

Announced 2006

Data
Encryption keys

Disk

Statement of Direction

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only

© 2006 IBM Corporation

Tape encryption with System z in the enterprise

Help secure data from theft or compromise

Why z/OS centralized key management?

- Can help to protect and manage keys
  - Highly secure and available key data store
  - Long term key management
  - Disaster recovery capabilities
- Single point of control
- Over a decade of production use

Encryption Facility for z/OS, V1.1

Data Encryption in the Server

Centralized Key Management

Protected Encryption Keys

Data Encryption in TS1120*

*Plans for encryption in IBM System Storage 2H2006**

Enterprise scope

- Flexible options for business partner exchange
- Partners can encrypt and decrypt using no-charge JAVA client
- Supports public key or password based exchange

- Highly secure tape library
- High performance archive encryption
- Transparent to existing processes and applications
- Can help provide audit compliance

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
© 2006 IBM Corporation

Establishing a Trusted Exchange with Your Partners

Key Exchange –
- **Digital Certificates or passwords can be used to identify and authenticate**

Enterprise-wide Key Management

You

PKDS

Your private key
Partner's public key

Digital Certificate

"public key"

Your Partner

PKDS

Partner's private key

"I know you by your Public Key, so I can create a file that only you can read."
OR
"I know you by your password."

Options for Partners to acquire a Digital Certificate:
1. z/OS customer can generate a certificate for the partner
   - z/OS can be a Digital Certificate Authority using z/OS PKI Services
2. Partner may already have a Digital Certificate
3. Partner may use third party Digital Certificate Authority

© 2006 IBM Corporation

Encrypting with Key Management

Enterprise-wide Key Management

You

Encryption Facility feature: *Encryption Services*

Invoked via JCL
1) Generate data key for either AES128 or TDES encryption
   - random for RSA key management, or
   - derived from password via PKCS#12
2) If RSA key mgmt:
   - encrypt data key with RSA public key, and
   - store encrypted data key in the file header
3) Compress the data
4) Encrypt the data using the data key
5) Send file to partner

Your Partner

Encryption Facility Client

Partner decrypts file
1 Decrypt data key with RSA private key, or derive data key from the password
2 Decrypt the data

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

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

© 2006 IBM Corporation

Archival Encryption with DFSMSdss and Key Management

Enterprise-wide Key Management

z/OS with DFSMSdss

Encryption Facility feature: DFSMSdss *Encryption*

Three options for invoking encryption in DFSMSdss:
1. **Additional Keyword in DUMP and RESTORE commands**
2. **DFSMShsm**
3. **ISMF panels**

1) Generate data key for either AES128 or TDES encryption
   - random for RSA key management, or
   - derived from password via PKCS#12
2) If RSA key mngt, encrypt data key with RSA public key, and
   - Store encrypted data key in the file header
3) Compress the data
4) Encrypt the data using the data key
5) Send file to off-site storage facility

→ **Off-site Storage Facility**

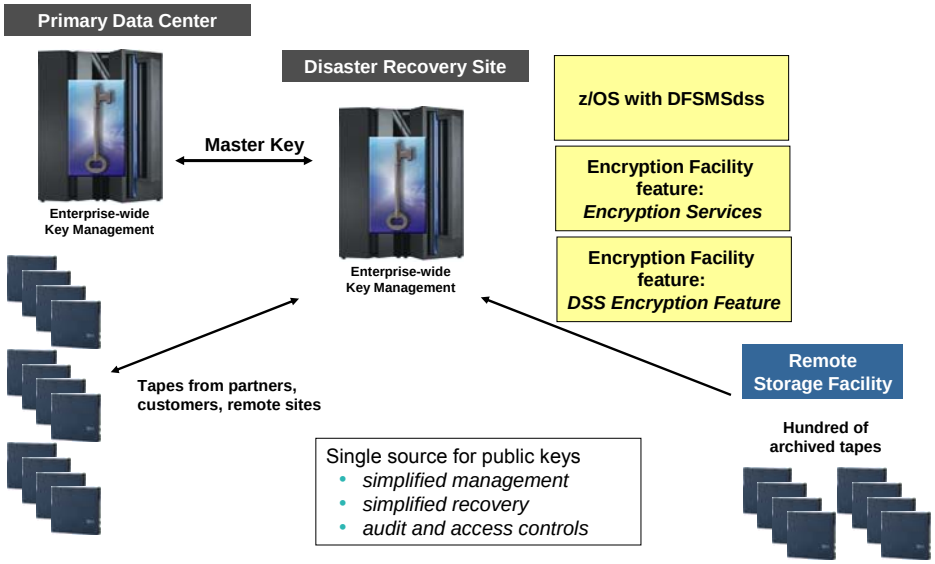
Archived tapes

	Tapes without Encryption	With Encryption No Compression	With Encryption and Hardware Compression
Estimated* resulting tape volumes:	X	2-3X	1-1.5X

* These measurements are examples of the maximum compression achieved in a lab environment with no other processing occurring and do not represent actual filed measurements. Further, the type of data will affect the hardware and software compression capabilities. Details available upon request.

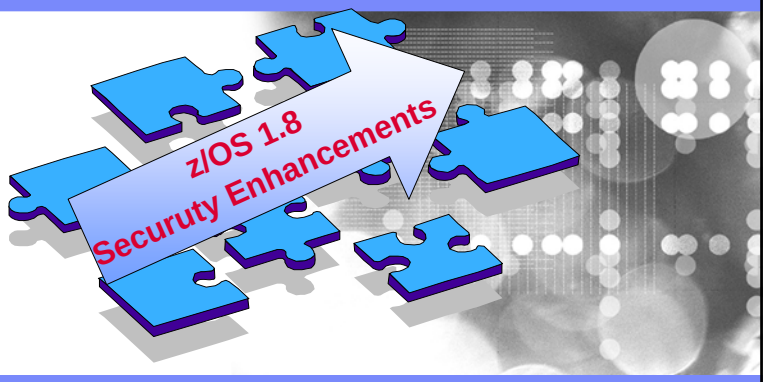
© 2006 IBM Corporation

Recovery with Centralized Key Management



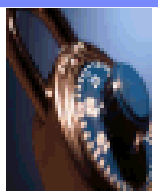
© 2006 IBM Corporation

LSU Sweden



© 2006 IBM Corporation

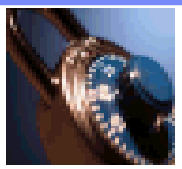
Security



- RACF DB enhancements
- IRRUT200 and IRRUT400 utility updates
- Distributed identity support
- Password phrase support
- PKI Extensions
- PKDS Key Management SPE
- Virtual key-ring support
- Support for defining IDS policy in a file
- Improved tape data set security administration
- IPSEC support for 128-bit AES

© 2006 IBM Corporation

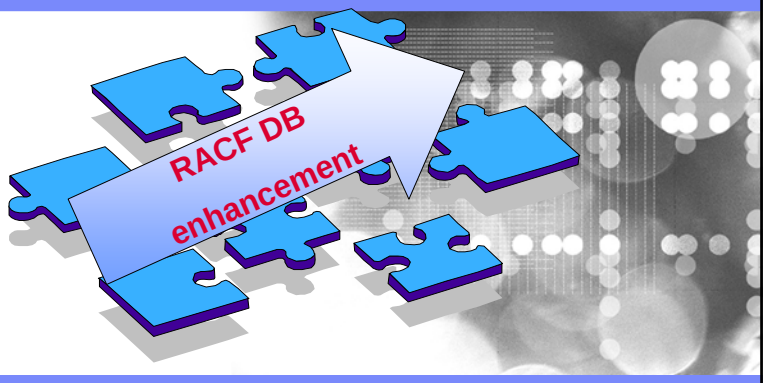
Security



- **PKI Extensions**:
  - SCEP support (programmatic certificate request support for network devices)
  - Multiple CA support (in a single image)
- **PKDS Key Management SPE**
- **Virtual key-ring support**
  - All certificates owned by the same user ID can be in a virtual key-ring
  - No need to manually create the virtual key-ring
  - Can help simplify administration for SSL applications such as FTP
- **Support for defining IDS policy in a file**
  - In addition to via LDAP
- **Improved tape data set security administration**
  - Can use DATASET class without activating TAPEVOL or TAPEDSN
  - Can specify that all data sets on the same tape should have common authorization
- **IPSEC support for 128-bit AES**

© 2006 IBM Corporation

LSU Sweden



© 2006 IBM Corporation

Security
RACF DB Enhancement

- Template expansion
- Generic Profiles enhancements
- IRRDPI00 LIST Enhancements

© 2006 IBM Corporation

Security RACF DB Enhancement
Template expansion

- **The RACF user profile template is almost full.**
  - Template for each type of profile (group, user, dataset, general resource) fits in one 4K block
  - In order to add new RACF database fields to the user profile the template must expand into another block
- **With z/OS 1.8 RACF Initialization and utility processing is updated to allow for any template to expand more than one block (4K)**
  - This means that new fields can be added to RACF DB in future
- **Any application which reads and processes the RACF database templates *directly* may be affected**
  - **Support is transparent to applications which use intended interfaces to process RACF database fields**
    - RACROUTE, ICHEINTY / ICHEACTN / ICHETEST, RACF commands(ADDUSER, RDEFINE, etc),
      RACF callable services (R_admin, ck_access, etc)
- ► The support is being rolled back to z/OS **V1R4, V1R5, V1R6**, and **V1R7** with APAR **OA12443**

© 2006 IBM Corporation

Security RACF DB Enhancement
Generic Profiles

- **No way to disallow Generic profile processing for install defined class**
  - With z/OS 1.8 a RACF class can be defined with an attribute that prevents generic profiles from being created in that class
- **New ICHERCDE keyword: GENERIC=<u>ALLOWED</u> | DISALLOWED**
  - Following IBM defined classes are updated with GENERIC=DISALLOWED
    - CDT, KERBLINK, REALM, SECLABEL, and SECLMBR
- **When shring DB with a lower level system make sure you:**
  - Always administer a dynamic class that disallows generics from a system running z/OS V1R8 or higher.
  - Always administer profiles in dynamic classes where generics are disallowed from systems running z/OS V1R8 and higher.

© 2006 IBM Corporation

Security RACF DB Enhancement
IRRDPI00 enhancements

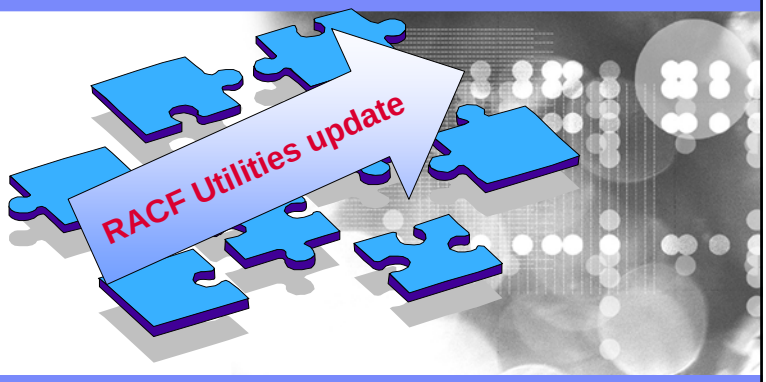
- **IRRDPI00 lists every field definition in the RACF DB.**
  - This causes thousands of lines of output
- **With this enhancement you will have a possibility to specify a more granular listing**
- IRRDPI00 LIST command has new keywords to specify profile type, segment name, and field name
  - **IRRDPI00 LIST [(*profile-type* [*segment-name* [*field-name*]])]**
    - Example: To list all fields in the OMVS segment of the USER profile, issue:

      IRRDPI00 LIST(USER OMVS)
    - Example: To list the HOME keyword in the OMVS segment of the USER profile, issue:

      IRRDPI00 LIST(USER OMVS HOME)

© 2006 IBM Corporation

LSU Sweden



© 2006 IBM Corporation

Security Utility Enhancement Problem

- **Both IRRUT200 and IRRUT400 has enhancements to prevent potential Database corruptions.**
- **Database corruption resulting from running IRRUT200**
  - IRRUT200 copies/verifies datasets on a 1-1 basis. Used to backup datasets.
    - Corruption may occur when DD SYSRACF (source) equals DD SYSUT1 (target).
    - Corruption may also occur if both DDs are specified and SYSUT1 is an in-use active RACF dataset.
- **Database corruption resulting from running IRRUT400**
  - IRRUT400 copies datasets on an X-to-Y basis. Used to shrink a database from X to X-n datasets. Used to expand a database from X to X+n datasets. Also used to copy X to X datasets across DASD types. All rebuild the index.
    - Corruption may occur when DD INDDx (source) equals DD OUTDDx (target).
    - Corruption may also occur if OUTDDx is an in-use active RACF dataset
- **Copying active primay datasets to active backups may not result in mirror images**.
  - The process is multi-step and **unserialized.**
    - Today one must use IRRUT200 to copy the active primary to a dataset with the same name as the active backup, but on a different volume. Then RVARY INACT the active backup and uncatalog it. Then catalog the new copy. Then RVARY ACTIVE the backup, picking up the new copy.
    - **If updates to the primary occur after the IRRUT200 copy function, then by the time the backup is activated, it is no longer an exact copy of the primary**

© 2006 IBM Corporation

Security Utility Enhancement Solution

- **The new safety features for both IRRUT200 and IRRUT400 are similar.**
- **Both will take volume labels into account.**
- **IRRUT200**
  - when DD SYSRACF (source) equals DD SYSUT1 (target) issue message IRR62073I, terminate utility with RC=12
  - when both DDs are specified and SYSUT1 (target) is an active RACF dataset, issue message IRR62072I, terminate utility with RC=12
- **IRRUT400**
  - when INDDx (source) = OUTDDx (target) issue message IRR65041I, terminate utility with RC=16
  - when OUTDDx (target) is an active RACF dataset, issue message IRR65040I, terminate utility with RC=16

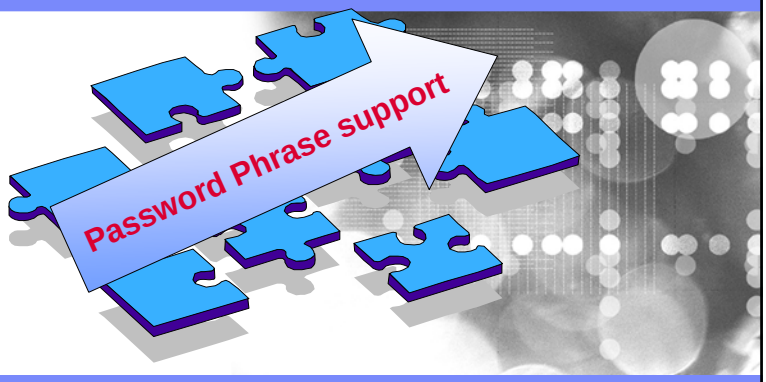
© 2006 IBM Corporation

Security Utility Enhancement Solution

- **The new IRRUT200 synchronized copy:**
  - First run IRRUT200 in the usual **verify mode** to ensure that the active primary dataset is **not damaged**.
  - Run IRRUT200 as if you were doing a copy (DDs for both SYSRACF and SYSUT1), but add new keyword **PARM=ACTIVATE**
    - no verification is performed for PARM=ACTIVATE, SYSIN and SYSPRINT are ignored
  - **SYSUT1 (target)** must be the in-use inactive backup associated with the SYSRACF (source) specified in-use active primary
    - the existing IRRUT200 rule of copying only between similar device types still applies
  - **IRRUT200** will get **exclusive serialization**. After the copy completes, an internal RVARY ACTIVATE against the SYSUT1 (target) specified backup will be done. Serialization will be released.
    - In addition to the IRRUT200 messages, RVARY messages will now be found in IRRUT200's SYSUT2 DD.
    - There will be no RVARY password prompt.

© 2006 IBM Corporation

LSU Sweden



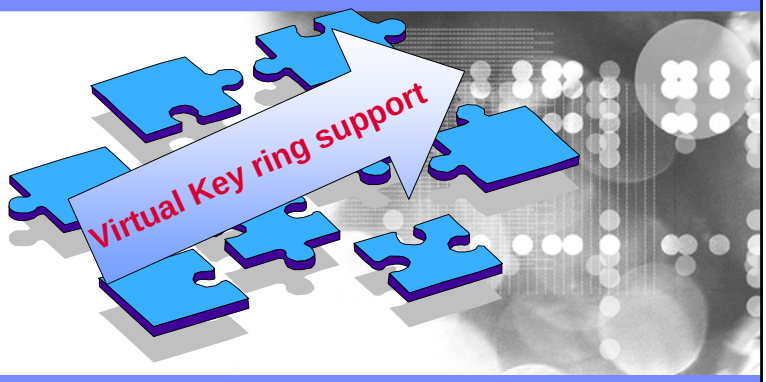
© 2006 IBM Corporation

Security
Password Phrase support

- **In z/OS V1R7, RACF introduced support for mixed-case passwords.**
  - This provided for a more favorable comparison when contrasting password security between z/OS and competitive operating systems.
- **In z/OS V1R8 RACF has implemented the infrastructure for pass phrases as an alternative to passwords greater than 8 characters.**
  - This enables applications that exploit this new infrastructure to specify an authentication value longer than 8 characters to better fit in the heterogeneous world, while traditional applications may continue to use the traditional password.
- **Passphrase can now be between 14-100 characters**
- **Support for Pass Phrases entails changes in:**
  - RACF Initzialization, Commands, Callable Services….etc.

© 2006 IBM Corporation

LSU Sweden



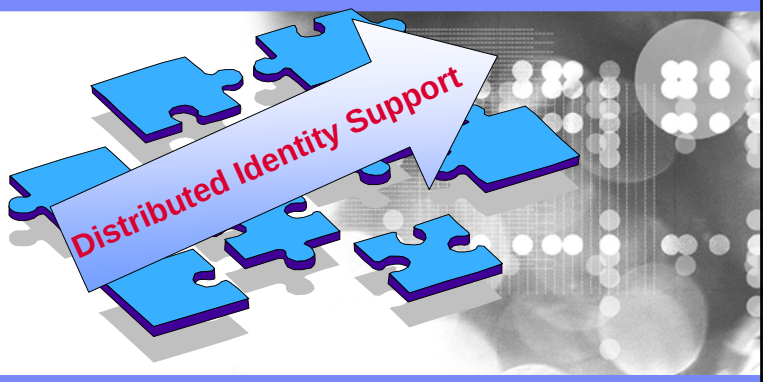
© 2006 IBM Corporation

Security
Virtual Key Ring Support

- **In the past, SSL-enabled applications required creating a key ring for each unique user ID along with any CA certificates.**
  - This situation propagated, when in most cases the same set of CA certificates would be used for each user ID. Thus these key rings would all be replicas.
- **To solve this problem, RACF now treats all the certificates installed under a given user ID as a virtual key ring.**
  - This key ring is created when the user ID is added and destroyed when the user ID is deleted.

© 2006 IBM Corporation

LSU Sweden



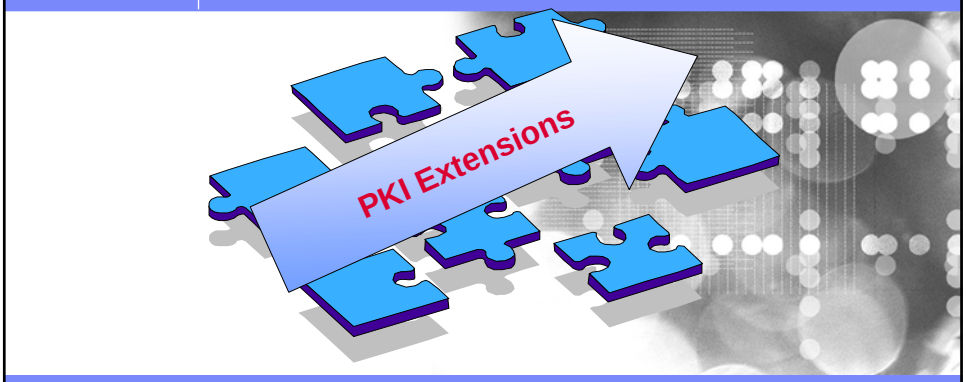
© 2006 IBM Corporation

Security
Distributed Identity Support

- SAF identity token provides increased user accountability and audit resources by providing end-to-end auditing that tracks the identity initially used for authentication as well as the identity on the current platform.
- This support is especially valuable to customers maintaining heterogeneous environments, where requests and entry points to network resources come from a variety of platforms.

© 2006 IBM Corporation

LSU Sweden

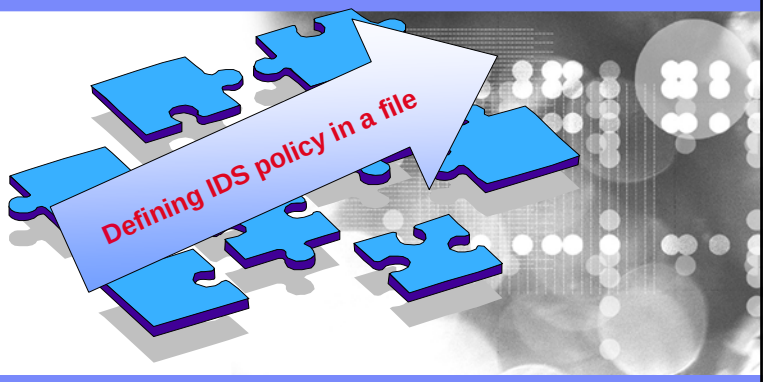


© 2006 IBM Corporation

Security
PKI Extensions

- **Enabling multiple CA support for PKI Services:**
  - This function lifts the restriction that prevented more than one instance of the PKI Services daemon from being started simultaneously on a single MVS image.
    - This allows PKI Services customers to establish **multiple certificate authorities** on a **single MVS image**.
- **Add SCEP(**Simple certificate enrollment protocol) **support to PKI Services:**
  - This allows SCEP-enabled clients to request certificates by sending messages to a certificate authority using the http protocol.
  - Adding SCEP support allows PKI Services to accept, decrypt, and respond to the various SCEP messages and supports both the manual and automatic enrollment modes as defined in the standard.
  - Manual enrollment requires the CA administrator to manually approve requests.
  - With automatic enrollment, certificate requests are auto-approved and fulfilled synchronously, based on the requestor' knowledge of a predetermined secret, the challenge password.

© 2006 IBM Corporation



© 2006 IBM Corporation

Security
Defining IDS policy

- In V1R8, Communications Server provides a flat file equivalent to the IDS policy that has been stored in LDAP in previous releases.
- The policy continues to be read and processed by the policy agent and will give z/OS Communications Server policy a consistent flat file support for all policy disciplines.

© 2006 IBM Corporation

LSU Sweden

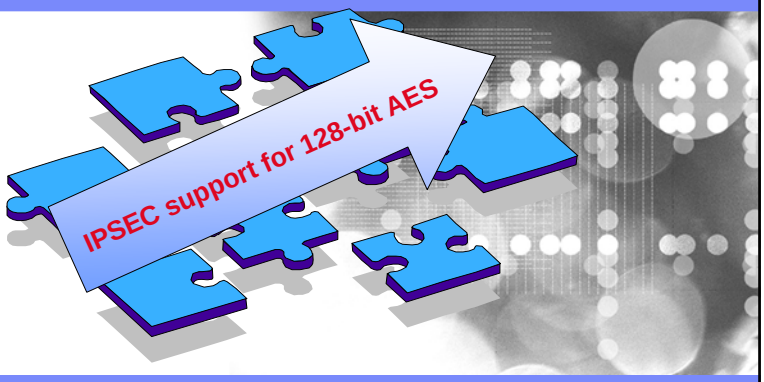
© 2006 IBM Corporation

Security
Tape Dataset Security

- **DFSMS introduces new options for securing tape data sets using SAF.**
  - The new options allows you to avoid the use of the **RACF TAPEDSN** option and the **TAPEVOL** class.
  - Instead you can use the **DATASET** class, enabling you to have common authorization for data sets regardless of the type of volume on which they are stored.
  - DFSMS also provides options for ensuring that all data sets on a tape volume have common authorization, and that a user is authorized to overwrite an existing first file on a volume.

© 2006 IBM Corporation

LSU Sweden



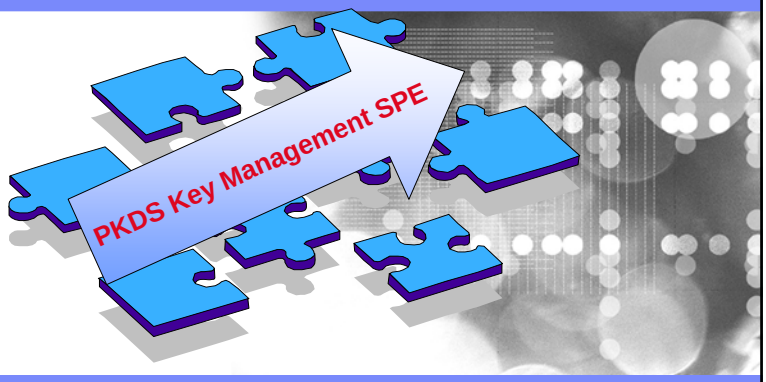
© 2006 IBM Corporation

Security
IPSEC support for 128-bit AES

- Support is provided for the **Advanced Encryption Standard (AES)** algorithm for IP Security with a 128-bit key length.
- This algorithm replaces DES as the standard encryption algorithm.
- Infoprint Server documentation has been enhanced to describe how this can be used to encrypt print output between z/OS and distributed printers.

© 2006 IBM Corporation

LSU Sweden



© 2006 IBM Corporation

Security

PKDS Key Management SPE

- **z/OS Encryption Facility (EF) became available 4Q2005**
  - Requires exchanging public keys with business partners to enable data encryption
  - No native PKDS key management functions in ICSF
    - End users need to generate key pairs and extract public keys
    - EF requires certificate/key management support in the Security Manager (RACF, ACF/2, etc) to do the above
  - Procedure to exchange keys between mixed shops difficult
  - ICSF for z/OS 1.8 updated with new panels to:
    - Generate/delete public and private key pairs in the PKDS
    - Export the public half as a self-signed x.509 certificate
    - Import a public key from a partner's certificate into the PKDS
- **Function contained in the base of HCR7731 (V1R8)**
- **Also rolled back to earlier releases as an SPE**
  - APAR Number - **OA15156**
  - Releases
    - HCR770A, HCR770B, HCR7720, and HCR7730

© 2006 IBM Corporation