



IBM Systems and Technology Group

RACF z/OS V1R7 Update

Georgia RACF Users Group

November, 2005

Walt Farrell, CISSP®
z/OS Security Design
IBM Poughkeepsie
wfarrell@us.ibm.com

Trademarks

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

DB2*
e-business logo
IBM*
IBM eServer
IBM logo*
OS/390*
RACF*
z/OS*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
UNIX is a registered trademark of The Open Group in the United States and other countries.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

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

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- **RACF Enhancements in z/OS Version 1 Release 7**
 - ▶ Mixed-case passwords
 - ▶ Detect or prevent password recycling
 - ▶ Maintain revoke date when resuming users
 - ▶ Improve SETR INACTIVE processing for new users
 - ▶ Automatic RVARY SWITCH to backup for some errors
 - ▶ R_admin functions to extract USER, GROUP, and CONNECT information
 - ▶ PassTicket API & Audit Enhancements
 - ▶ XML Output for SMF Unload
 - ▶ Delegated Resources (AKA Nested ACEEs)

- **IBM Encryption Facility for z/OS, V1.1**

z/OS V1R7: 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.

z/OS V1R7: Mixed-Case Passwords ...

- **Additional SETROPTS password rules:**
 - ▶ NATIONAL
 - # (X'7B'), \$ (X'5B'), and @ (X'7C')
 - ▶ MIXEDCONSONANT
 - Upper- or lower-case consonants (A-Z, a-z)
 - ▶ MIXEDVOWEL
 - Upper- or lower-case vowels (a, e, i, o, u, A, E, I, O, U)
 - ▶ MIXEDNUM
 - Upper- or lower-case alphabetic, or numeric, or national
 - At least one upper-case alpha or national, one lower-case alpha, and one numeric
- **Old rules (ALPHA, ALPHANUM, CONSONANT, VOWEL, NOVOWEL) will not match lower-case alphabetic characters.**

z/OS V1R7: 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

z/OS V1R7: Detect or Prevent Password Recycling

- **Problem: Users can change passwords repeatedly and recycle their password history, keeping same password.**
- **Part 1 of Solution:** With SETROPTS AUDIT(USER) in effect, RACROUTE REQUEST=VERIFY (logon, etc.) processing will create a type 80 SMF record indicating a password change.
 - ▶ SMF Unload event JOBINIT, qualifier RACINITI, audit reason INIT_LOG_CLASS = YES

z/OS V1R7: Detect or Prevent Password Recycling ...

- **Part 2 of Solution:** SETROPTS PASSWORD(MINCHANGE(nnn))
- **The MINCHANGE value specifies the minimum lifetime of a user's password, from 0 (not limited) up to the SETR PASSWORD(INTERVAL(mmm)) value.**
 - ▶ Before nnn days, a user cannot change his/her own password again.
 - ▶ Helpdesk personnel authorized via IRR.PASSWORD.RESET need CONTROL authority to change a user's password before nnn days.
 - ▶ SPECIAL and group-SPECIAL users can change another user's password during that interval, but not their own password.

z/OS V1R7: Maintain Revoke Date When Resuming Users

- **Problem: Administrator specifies**
ALTUSER U1 REVOKE(mm/dd/yy)
then U1 forgets password, becomes revoked early, and administrator resumes U1.

RACF removes the REVOKE date.

- **Solution: RACF will keep the revoke date.**
- **ALTUSER has new keywords NOREVOKE, NORESUME which will clear the REVOKE or RESUME dates, if present.**
- **LISTUSER and LISTGRP will show REVOKE and RESUME dates, even if in the past.**

z/OS V1R7: Improve SETR INACTIVE Processing for New Users

- **Problem:** SETR INACTIVE(30) specified. Administrator creates new user U1, who does not logon for 45 days.

When U1 does logon, RACF does not consider him inactive, and allows the logon.

- **Solution:** RACF will put the user's creation date into the LJDATE field during ADDUSER processing. Then RACROUTE REQUEST=VERIFY (logon, etc.) processing will have a value to use for checking inactivity.
- LJTIME is not set during ADDUSER, so logon processing and LISTUSER and applications can still tell the user has never signed on.

z/OS V1R7: Automatic RVARV SWITCH to Backup for Some Errors

- **Problem: RVARV SWITCH is needed to recover from device errors on primary RACF DB, but**
 - ▶ It can take awhile to issue this command, especially if operator needs to supply the password.
 - ▶ RVARV cannot work while requests to use the DB are in process, so even after entering password, operator must VARY the device offline.
- **Improvement:**
 - ▶ If major device errors have occurred, affecting RACF and other users of the device, operator can VARY the RACF primary DB device offline (V nnn,OFFLINE,FORCE).
 - ▶ z/OS will terminate any outstanding requests with I/O error.
 - ▶ RACF will detect this I/O error, see device is offline, and automatically RVARV SWITCH to the backup
 - No password needed
 - SWITCH will happen on all systems in SYSPLEX Communication.

z/OS V1R7: Automatic RVARY SWITCH to Backup for Some Errors ...

■ **Notes:**

- ▶ RVARY is still the preferred method for many cases.
 - VARY will affect all applications using data on that volume

- ▶ However, if the device is really broken, the other applications are probably in trouble, anyway.

z/OS V1R7: R_admin Enhancement

- **Problem: Program wants to issue RACF commands, especially LISTUSER or LISTGRP. Program can use R_admin to do this, but:**
 - ▶ Command output is difficult to read, not a programming interface, and can change
 - ▶ R_admin limits command output to 4096 lines; long user or group listings are truncated

- **Solution: New Extract functions for R_admin**

z/OS V1R7: R_admin Enhancement...

- **New USER-related functions:**
 - ▶ Extract USER
 - ▶ Extract next USER
 - ▶ Extract CONNECT

- **New GROUP-related functions:**
 - ▶ Extract GROUP
 - ▶ Extract next GROUP

- **Data returned in a structured format**
 - ▶ Segment name
 - ▶ Field name
 - ▶ Data

z/OS V1R7: R_admin Enhancement...

- R_admin extract can be viewed as a combination of a RACROUTE REQUEST=EXTRACT and a 'list' command.

Like a command
(tastes great)

Like RACROUTE
(less filling)

Returned data is character (EBCDIC)

Format is architected (i.e. supported, unlike command output)

Returned data is 'symmetric'

Supervisor state caller can bypass authorization

Problem state enabled – requires same authorization as command

Unambiguous return codes

Mostly returns only data displayed by list command

Can iteratively cycle through profiles

z/OS V1R7: R_admin Enhancement...

- Authorization:
 - ▶ Problem state caller must have READ access to FACILITY class profile IRR.RADMIN.xx, where xx=LISTUSER (user & connect) or LISTGROUP (group).
 - ▶ Additionally, users must have the same access as would be required to perform a LISTUSER or LISTGROUP on the profile being extracted.
 - ▶ Field Level Access checking is performed on all non-base segments in the profile, if field level access checking is active on the system.
 - ▶ If the user is not authorized to see specific fields or segments, they are silently omitted from output.

z/OS V1R7: R_admin Enhancement...

- What data is not returned by R_admin extract?
 - ▶ Data in Reserved/unused RACF database fields
 - ▶ Encrypted data such as Password.
 - ▶ Fields described as 'reserved for installation usage'
 - ▶ Data which exists in a profile other than the one being extracted.
 - For example, CONNECT information between a USER and GROUP is split between the USER and GROUP profile. When extracting a USER, the portion of the CONNECT information contained in the GROUP profile is not displayed. Use R_admin extract CONNECT to retrieve all CONNECT information if it is needed.

z/OS R7: PassTicket API & Audit Enhancements

■ **Review:**

- ▶ **The RACF PassTicket is a one-time-only password that is generated by a requesting product or function. It is an alternative to the RACF password that removes the need to send RACF passwords across the network in clear text.**
- ▶ **A PassTicket is only valid for a few minutes before it expires.**
- ▶ **PassTicket functionality has existed in RACF for over 10 years.**

z/OS R7: PassTicket API & Audit Enhancements...

■ **More Review:**

- ▶ **In order to use PassTickets, one or more profiles are created in the PTKTDATA class using the RDEFINE command. A secret key is specified in the SSIGNON segment in this profile.**
- ▶ **Each profile corresponds to a specific application for the PassTicket. These applications include APPC, CICS, IMS, TSO, MVS batch and VM, as well as custom applications.**
- ▶ **An application generates a PassTicket using either a RACF service or implements the published PassTicket algorithm as documented in “z/OS Security Server RACF Macros and Interfaces”.**
- ▶ **Application then logs into z/OS (RACF) supplying userid and PassTicket & application and the PassTicket is evaluated.**

z/OS R7: PassTicket API & Audit Enhancements

■ **More Review:**

- ▶ **The secret key must be shared between the application which generates the PassTicket, and RACF. The PassTicket generation algorithm is documented in “z/OS Security Server RACF Macros and Interfaces”.**
- ▶ **PassTicket functionality can be disabled by deleting all PTKTDATA profiles.**
- ▶ **Supervisor state, key 0 callers have always been able to call a ‘legacy’ branch entered function to generate PassTickets.**

z/OS R7: PassTicket API & Audit Enhancements

■ **New in R7:**

- ▶ **RACF callable services in RACF allow problem state callers (who have been granted access) to generate and evaluate PassTickets.**
- ▶ **Java interfaces to allow Java applications to generate and evaluate PassTickets.**
- ▶ **PassTicket Generation and Evaluation is now audited.**
 - **Even for callers of the old PassTicket generation function**
 - **Check AUDIT options on your PTKTDATA profiles & LOGOPTIONS for PTKTDATA class**

z/OS V1R7: XML Output for SMF Unload

- XML - eXtensible Markup Language
 - ▶ Elements (<tag>...</tag>) and attributes
 - ▶ Documents - simple.xml
- Looks like HTML, however
 - ▶ Describes the data not how the data should look.
 - ▶ Stricter in enforcing syntax
- Used for
 - ▶ Document interchange
 - ▶ Rendering data into different formats
- Applications use XML components
 - ▶ Parsers
 - ▶ Processors - ex. XSL style sheet

z/OS V1R7: XML Output for SMF Unload...

A simple XML Instance Document

```
1. <?xml version='1.0' encoding='ebcdic-cp-us' ?>
2. <simpleEventLog xmlns='http://www.ibm.com/Simple'>
3.   <!-- a simple event -->
4.   <event>
5.     <eventType>JOBINIT</eventType>
6.   </event>
7. </simpleEventLog>
```

Processing Instruction
Elements
Comment
Attributes

z/OS V1R7: XML Output for SMF Unload...

The SMF Unload *securityEventLog*

- XML document created by SMF Unload
 - ▶ Unformatted
 - ▶ Formatted
- All RACF SMF Unload events are supported (30, 80, 81, and 83)
- Tag for each field in an event
 - ▶ Tag name derived from the corresponding DB2 field name (exceptions documented)
- Grammar (i.e. Schema) defined in
 - ▶ IRRSCHEM and IRREIMSC in SYS1.SAMPLIB
 - ▶ Schema documents are ASIS Code

z/OS V1R7: XML Output for SMF Unload...

SMF Unload Output - XML Document

```
<?xml version='1.0' encoding='ebcdic-cp-us' ?>
<securityEventLog xmlns='http://www.ibm.com/xmlns/zOS/IRRSchema'>
  <rdf:Description rdf:about=''
    xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax
    xmlns:dc='http://purl.org/dc/elements/1.1/'>
    <dc:creator> z/OS Security Server RACF SMF Unload (HRF7720)</dc...>
    <dc:subject>RACF Security Event Log 2005-01-17 22:12:09</dc...>
    <dc:language>en</dc:language>
  </rdf:Description>
  ...Events...
</securityEventLog>
```

z/OS V1R7: XML Output for SMF Unload...

SMF Unload - XML Document...

XML Unformatted (XMLOUT DD)

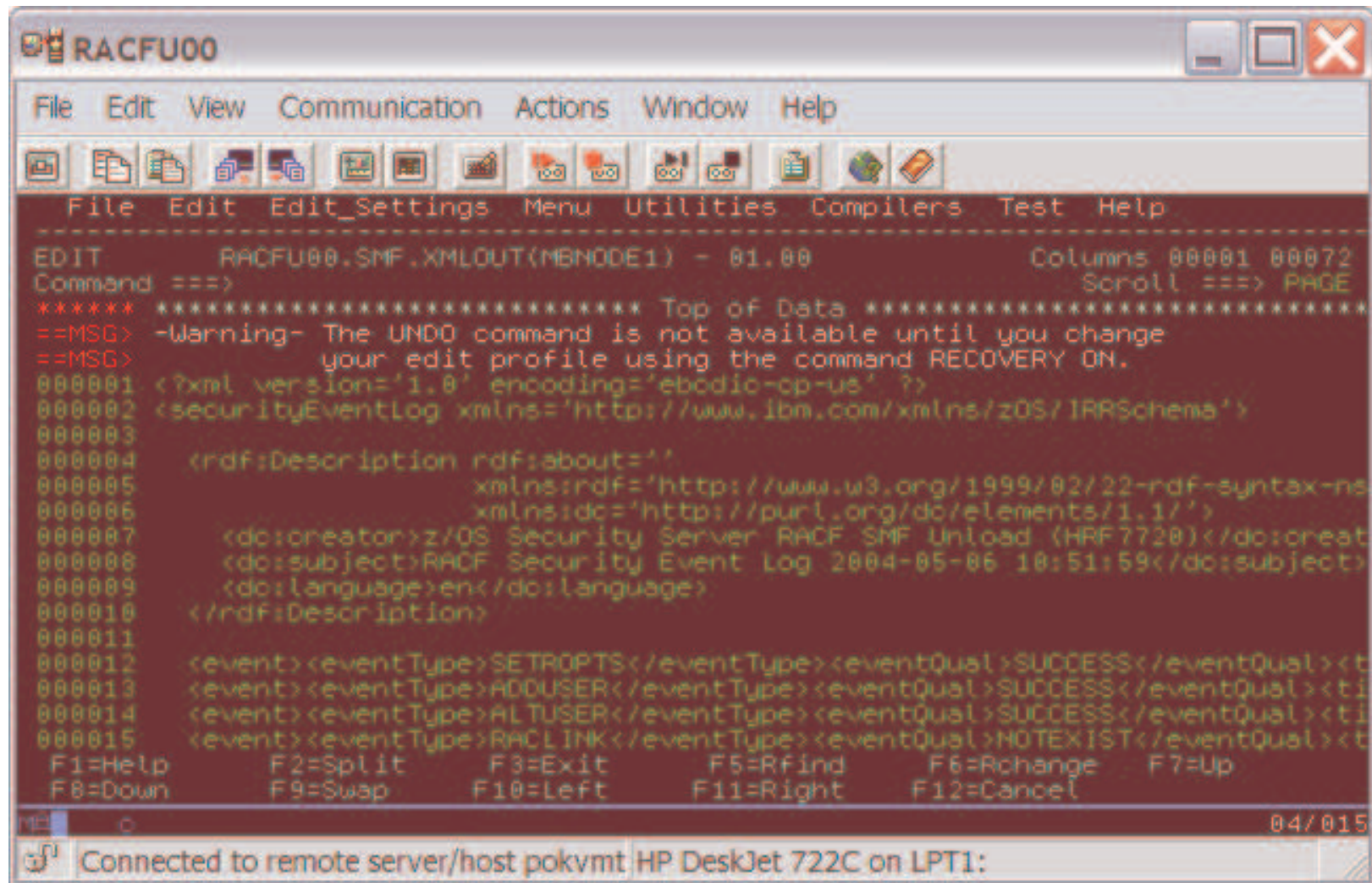
```
<event><eventType>ADDUSER</eventType><eventQual>SU...
```

XML Formatted (XMLFORM DD)

```
<event>  
  <eventType>ADDUSER</eventType>  
  <eventQual>SUCCESS</eventQual>  
  <timeWritten>21:51:55.54</timeWritten>  
  <dateWritten>2005-01-17</dateWritten>  
  <systemSmfid>IM13</systemSmfid>  
  <prodFmid>HRF7720</prodFmid>  
  <prodName>RACF</prodName>  
  <details>  
    <violation>N</violation>
```

Etc.

z/OS V1R7: XML Output for SMF Unload... ISPF - XMLOUT Format



```
RACFU00
File Edit View Communication Actions Window Help
File Edit Edit_Settings Menu Utilities Compilers Test Help
-----
EDIT          RACFU00.SMF.XMLOUT(MBNODE1) - 01.00          Columns 00001 00072
Command ===>          Scroll ===> PAGE
***** ***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG>          your edit profile using the command RECOVERY ON.
000001 <?xml version='1.0' encoding='ebodic-cp-us' ?>
000002 <securityEventLog xmlns='http://www.ibm.com/xmlns/zOS/IRRSchema'>
000003
000004   <rdf:Description rdf:about=''
000005     xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns
000006     xmlns:dc='http://purl.org/dc/elements/1.1/'>
000007     <dc:creator>z/OS Security Server RACF SMF Unload (HRF7720)</dc:creat
000008     <dc:subject>RACF Security Event Log 2004-05-06 10:51:59</dc:subject>
000009     <dc:language>en</dc:language>
000010   </rdf:Description>
000011
000012   <event><eventType>SETROPTS</eventType><eventQual>SUCCESS</eventQual><t
000013   <event><eventType>ADDUSER</eventType><eventQual>SUCCESS</eventQual><ti
000014   <event><eventType>ALTUSER</eventType><eventQual>SUCCESS</eventQual><ti
000015   <event><eventType>RACL INK</eventType><eventQual>NOTEXIST</eventQual><t
F1=Help      F2=Split    F3=Exit     F5=Rfind    F6=Rchange  F7=Up
F8=Down      F9=Swap     F10=Left    F11=Right   F12=Cancel
NE          04/015
Connected to remote server/host pokvmt HP DeskJet 722C on LPT1:
```

z/OS V1R7: XML Output for SMF Unload... ISPF - XMLFORM + ISPF Commands

```

RACFU00
File Edit View Communication Actions Window Help
File Edit Edit_Settings Menu Utilities Compilers Test Help
EDIT RACFU00.SMF.XMLFORM(X500) - 01.01 Columns 00001 00072
Command ===> Scroll ===> CSR
000258 <eventType>RDEFINE</eventType> - - - - 10 Line(s) not Displayed
000269 <evtUserId>IBMUER</evtUserId> - - - - 57 Line(s) not Displayed
000327 <specified>LEVEL(00)</specified> - - - - 242 Line(s) not Displayed
000570 <eventType>ADDUSER</eventType> - - - - 10 Line(s) not Displayed
000581 <evtUserId>IBMUER</evtUserId> - - - - 58 Line(s) not Displayed
000640 <userId>OGATA</userId>
000641 <specified>DFLTGRP(SYS1) PASSWORD NAME(&apos;TEST USER007&apos;) A - - - - 3 Line(s) not Displayed
000645 <eventType>JOBINIT</eventType> - - - - 6 Line(s) not Displayed
000652 <evtUserId>IBMUER</evtUserId> - - - - 7 Line(s) not Displayed
F1=Help F2=Split F3=Exit F5=Rfind F6=Rchange F7=Up
F8=Down F9=Swap F10=Left F11=Right F12=Cancel
05/002
Connected to remote server/host pokvmt HP DeskJet 722C on LPT1:

```

ISPF commands:

exclude all

find <eventType> all

find <evtUserId> all or

find <evtUserId>R00

find <specified> all

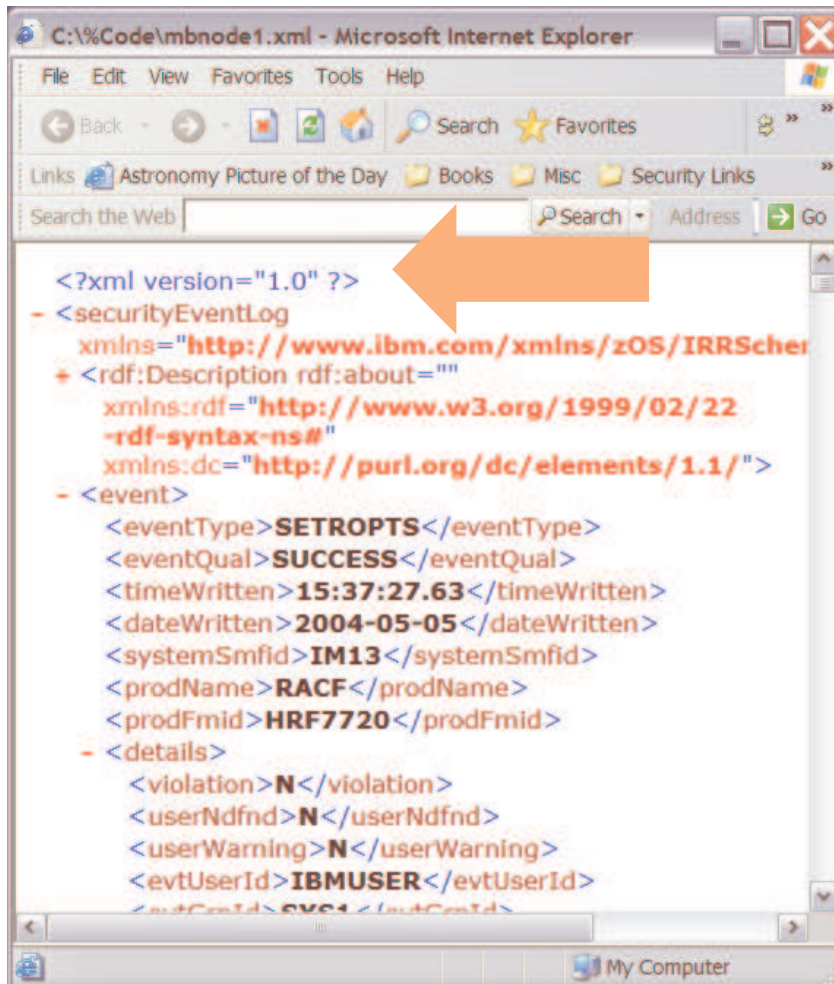
Combine in ISPF

Edit Macros or

REXX execs

z/OS V1R7: XML Output for SMF Unload...

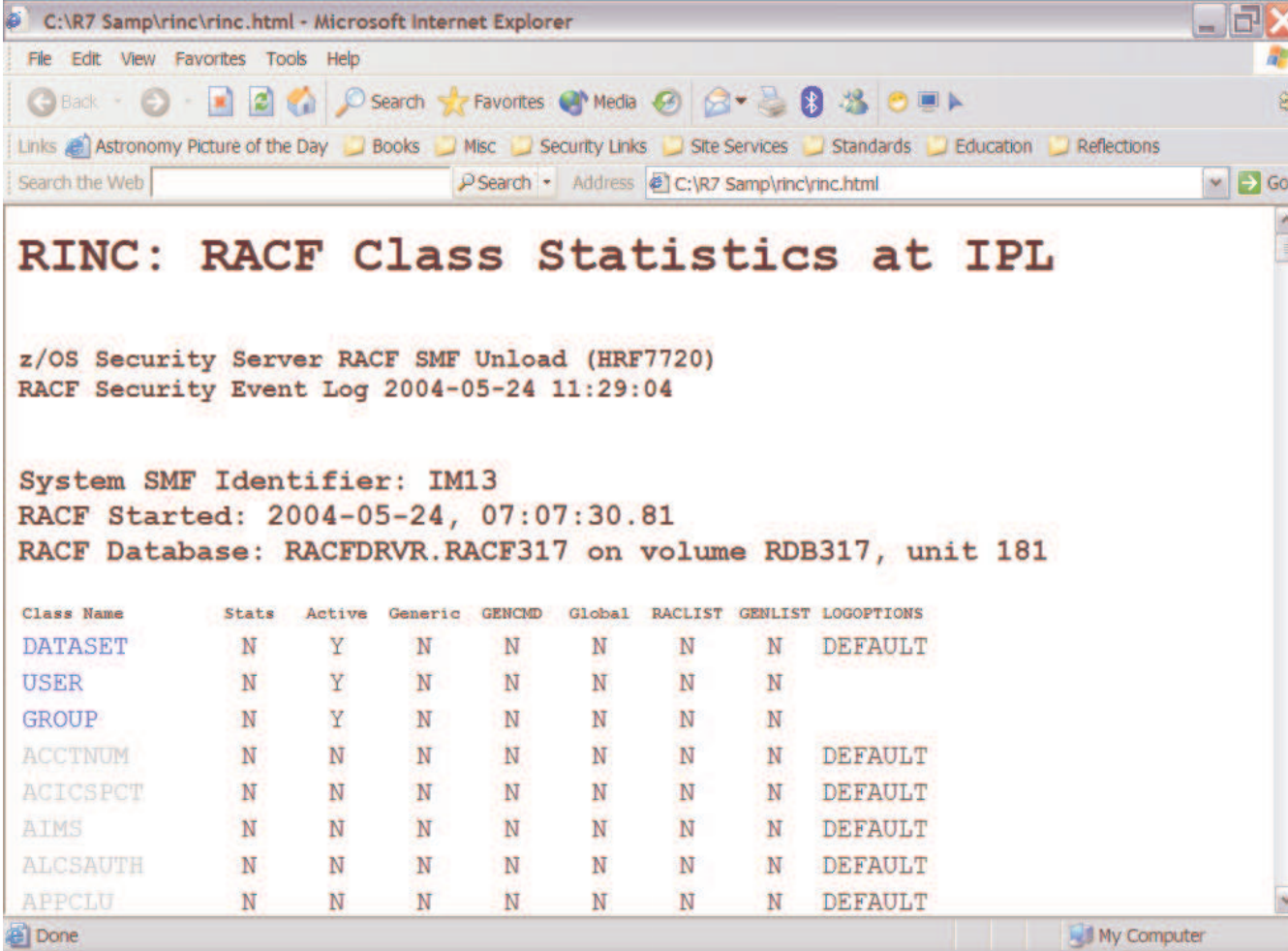
Browsing an XML document



Step 1. Download should convert to ASCII
Step 2. Remove encoding='ebcdic-cp-us'
Step 3. Open file using browser

- Compress/expand sections
- Edit -> find actions

z/OS V1R7: XML Output for SMF Unload... Using an XSLT style sheet



The screenshot shows a Microsoft Internet Explorer window displaying the output of an SMF unload operation. The title bar indicates the file path is C:\R7 Samp\rinc\rinc.html. The page content is as follows:

RINC: RACF Class Statistics at IPL

z/OS Security Server RACF SMF Unload (HRF7720)
RACF Security Event Log 2004-05-24 11:29:04

System SMF Identifier: IM13
RACF Started: 2004-05-24, 07:07:30.81
RACF Database: RACFDRVR.RACF317 on volume RDB317, unit 181

Class Name	Stats	Active	Generic	GENCMD	Global	RACLIST	GENLIST	LOGOPTIONS
DATASET	N	Y	N	N	N	N	N	DEFAULT
USER	N	Y	N	N	N	N	N	
GROUP	N	Y	N	N	N	N	N	
ACCTNUM	N	N	N	N	N	N	N	DEFAULT
ACICSPCT	N	N	N	N	N	N	N	DEFAULT
AIMS	N	N	N	N	N	N	N	DEFAULT
ALCSAUTH	N	N	N	N	N	N	N	DEFAULT
APPCLU	N	N	N	N	N	N	N	DEFAULT

z/OS V1R7: XML Output for SMF Unload...

Other Ideas

- Convert securityEventLog to
 - ▶ A different XML tag language
 - ▶ To text
 - ▶ To a new tabular format
 - ▶ Upload to DB2 using the XML Extender
 - ▶ Add graphics
 - ▶ Pie charts
- Cautions:
 - ▶ Can be processing/memory intensive

z/OS V1R7: XML Output for SMF Unload... securityEventLog XML documents are...

- **Readable!**
- **Flexible and extendable**
- **Enables data interchange**
- **Transformation between formats...XML Document + Style Sheet => web pages, filtered data, pie charts, ...**
- **Displayable on a browser**

z/OS V1R7: Delegated Resources (AKA Nested ACEEs)

- Scenario: A server authenticates a client, creates ACEE, and then does access checking.
- Problem: Sometimes a check should use the server identity, not the client identity.
 - ▶ Example: Server may use SSL or TLS for communication security, but after client authentication occurs, it may be the client (today) who needs authority to use ICSF crypto services or keys.
- This is solved for FTP today, in different ways depending on z/OS release, via PTFs
- Not solved for other servers, though, and a fix like the one in FTP is very complex
 - ▶ We need a simpler solution

z/OS V1R7: Delegated Resources (AKA Nested ACEEs) ...

■ **Solution:**

- ▶ The server tells RACF to create a client ACEE, but to also embed a copy of the server ACEE in the client ACEE, as an ENVR object
- ▶ The administrator (only if instructed by server documentation) tells RACF to use the embedded ACEE.
 - Example: `RALTER CSFSERV CSFENC
 APPLDATA('RACF-DELEGATED')`
- ▶ Server then uses `RACROUTE REQUEST=FASTAUTH` to do the authorization check
- ▶ `FASTAUTH` first checks client authority to the resource, and if that fails, checks server authority
- ▶ `ICH408I` messages and SMF records have both identities

IBM Encryption Facility for z/OS, V1.1

- **Consists of two optional z/OS features:**

- ▶ **IBM Encryption Services**

- 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
 - Can use z/OS PKI Services, or external vendor, or RACDCERT, to create certificates for public/private key
- Planned general availability: 28 October 2005
- Invoked via JCL as a utility program

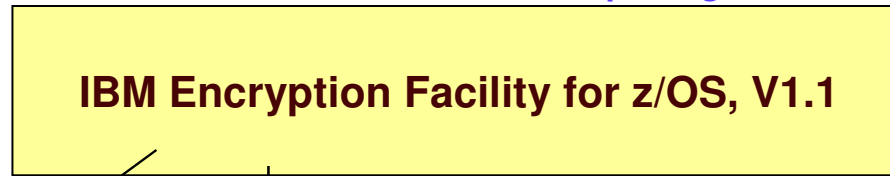
- ▶ **IBM DFSMSdss encryption feature**

- Allows encryption and compression of DUMP data sets created by DFSMSdss™
- Supports decryption and decompression during RESTORE
- Planned availability: 2 December 2005

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

EF Parts

Licensed Program Product
MSU-based pricing*

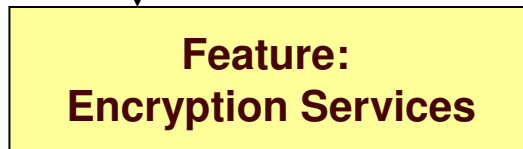


Optional Priced Feature*
Planned availability:
Dec 2, 2005



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

Optional Priced Feature
Planned availability:
Oct 28, 2005



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

Web download
Planned availability:
Oct 28, 2005

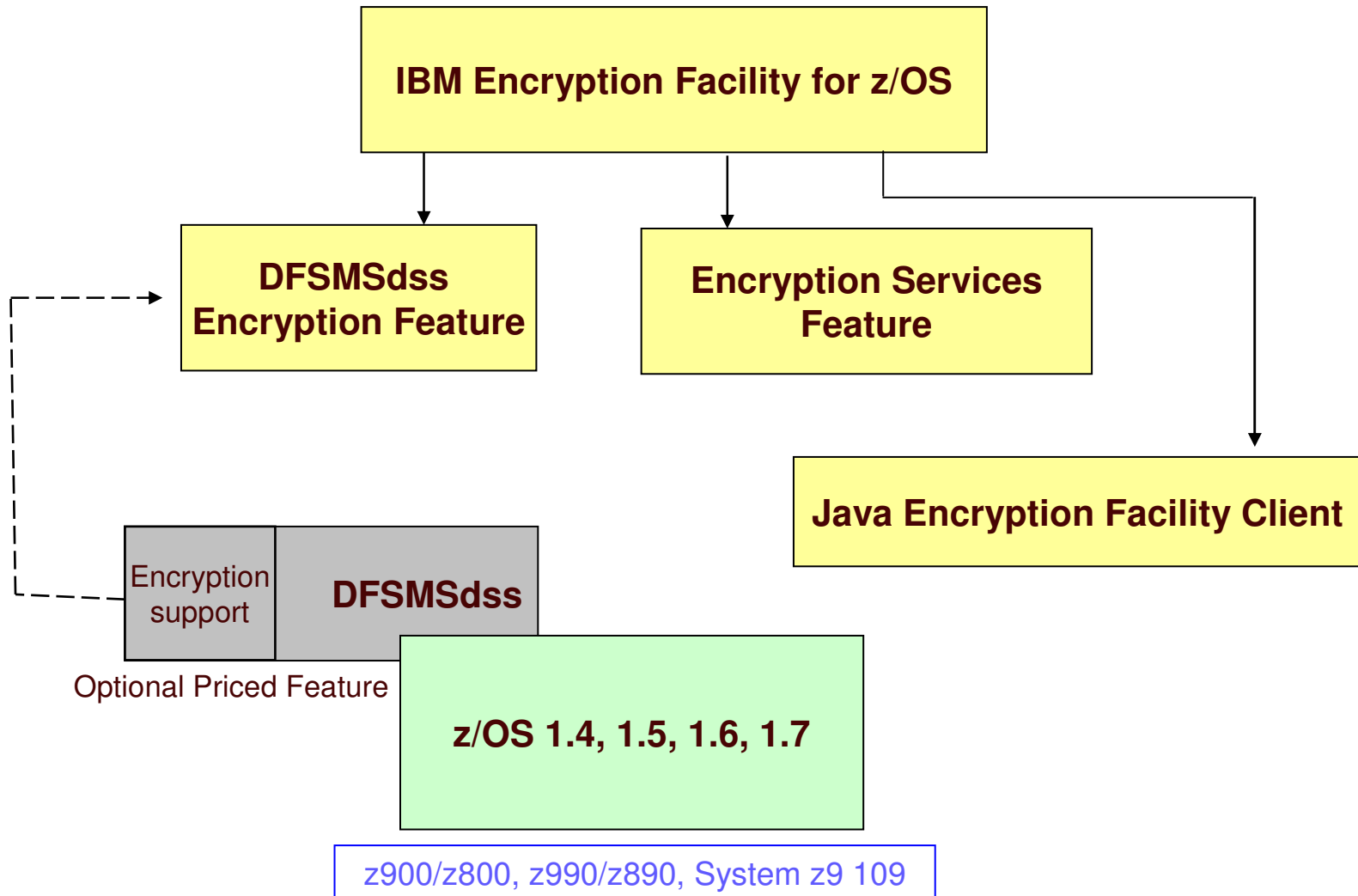


- Java-based code that allows client systems to decrypt and encrypt tapes for exchange with z/OS systems
- Must be used in conjunction with z/OS systems using the Encryption Services feature
- Can be used on any Java-enabled system

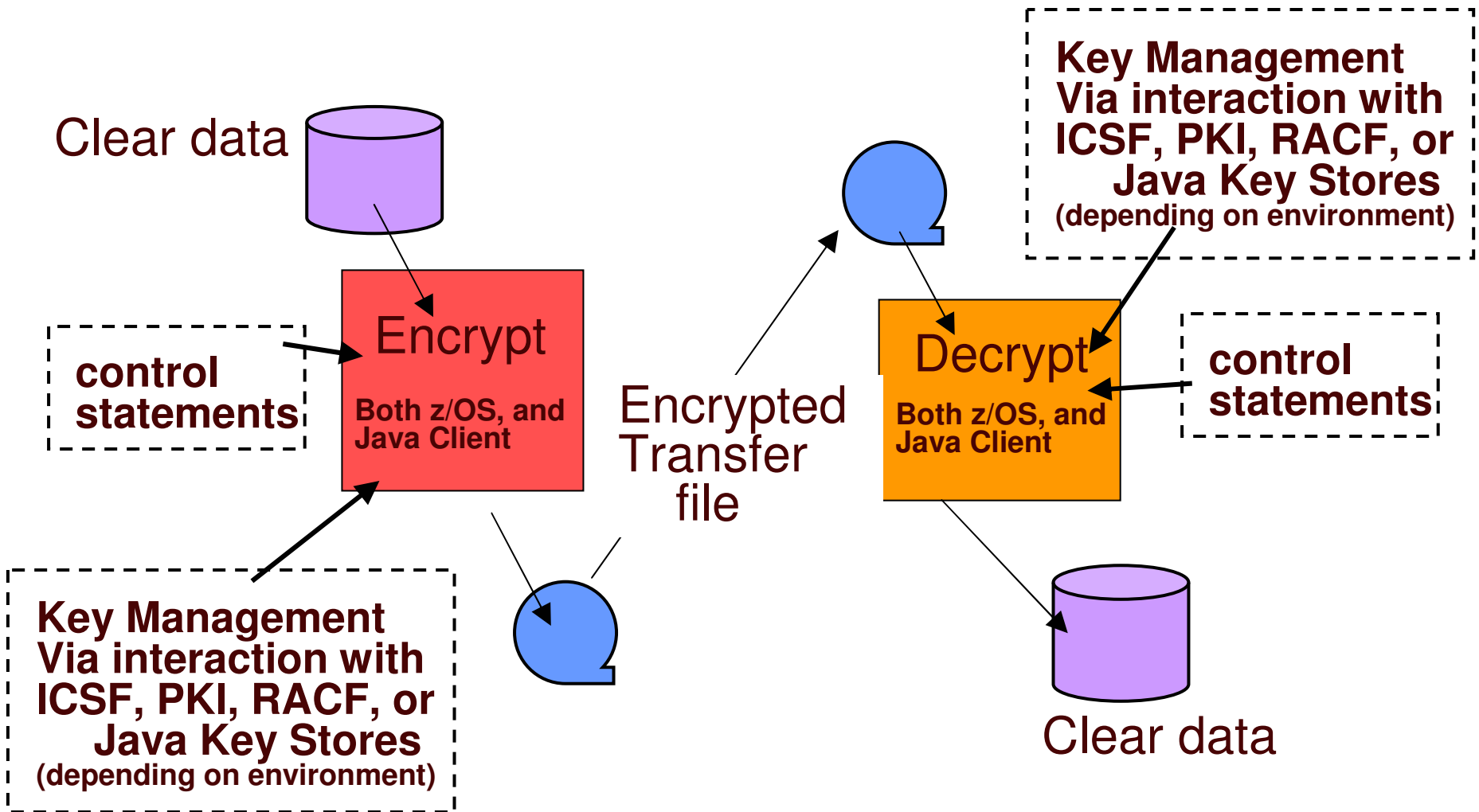
Leverages z/OS centralized key management and IBM mainframe cryptographic and compression capabilities

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

EF: relationship to DFSMSdss, platforms and hardware



Encryption Facility Logical Flow



Encrypting with Key Management



Enterprise-wide
Key Management

You

Encryption Facility for
z/OS 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 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 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

Archival Encryption with DFSMSdss™ and Key Management



Enterprise-wide Key Management



Three options for invoking encryption in DFSMSdss:

1. Additional Keyword in the dss DUMP and RESTORE commands,
2. DFSMShsm, and
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
X	2-3X	1-1.5X

Estimated* resulting tape volumes:

* 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.

References

- **z/OS V1R7**

- ▶ <http://www3.ibm.com/servers/eserver/zseries/zos/bkserv/>

- **IBM Health Checker for z/OS**

- ▶ *“An apple a day.... keeps the PMRs away! An overview of the IBM Health Checker for z/OS”*
 - z/OS Hot Topics, Issue 13, August 2005, available at http://www.ibm.com/servers/eserver/zseries/zos/bkserv/hot_topics.html
- ▶ *“RACF and the IBM Health Checker for z/OS”*
 - ibid
- ▶ IBM Health Checker for z/OS User’s Guide (SA22-7994)
 - <http://www.ibm.com/servers/eserver/zseries/zos/hchecker/>

- **IBM Encryption Services for z/OS, V1.1**

- ▶ ibm.com/servers/systems/systemz9/security

References (XML)

- **IBM Developer Works has a section on XML including “New to XML”**
 - ▶ <http://www.ibm.com/developerworks>

- **Security Server RACF Auditor's Guide - SA22-7684**
- **Security Server RACF Macros and Interfaces - SA22-7682**
- **Integrated Security Services Enterprise Identity Mapping (EIM) Guide and Reference - SA22-7875**

- **IBM Classes in XML**
 - ▶ XM301 Introduction to XML and Related Technologies (2.5 days)
 - ▶ XM321 Programming XML and Related Technologies for Java (2.5 days)