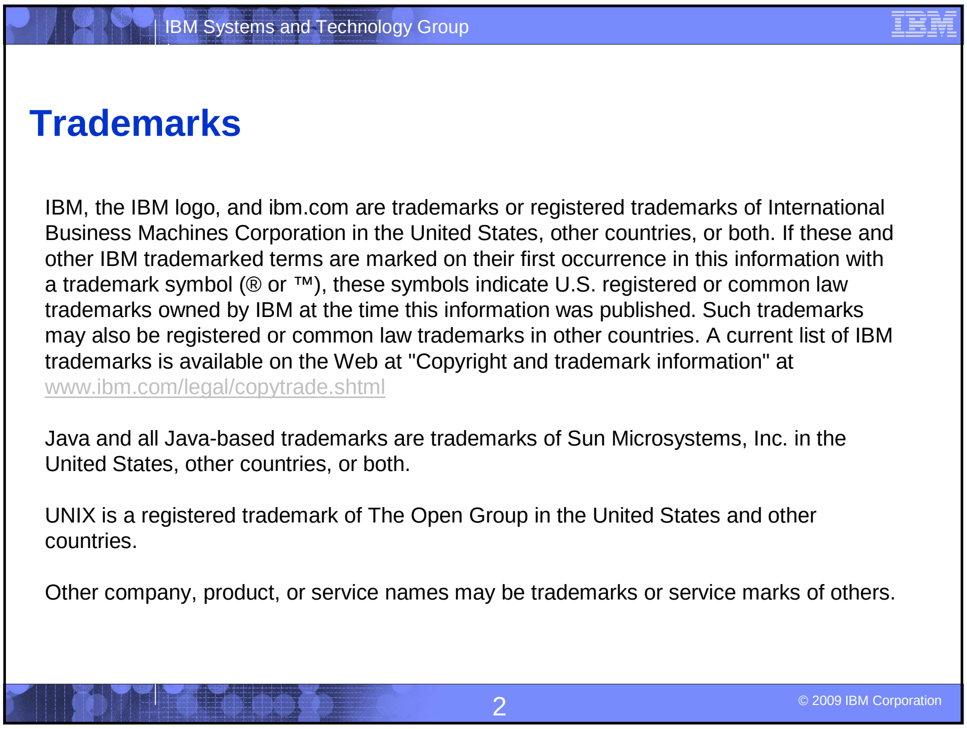
RACF® Update

Baltimore/Washington RACF Users Group

Mark Nelson, CISSP®, CSSLP
z/OS® Security Server (RACF) Design and Development
IBM Poughkeepsie
markan@us.ibm.com



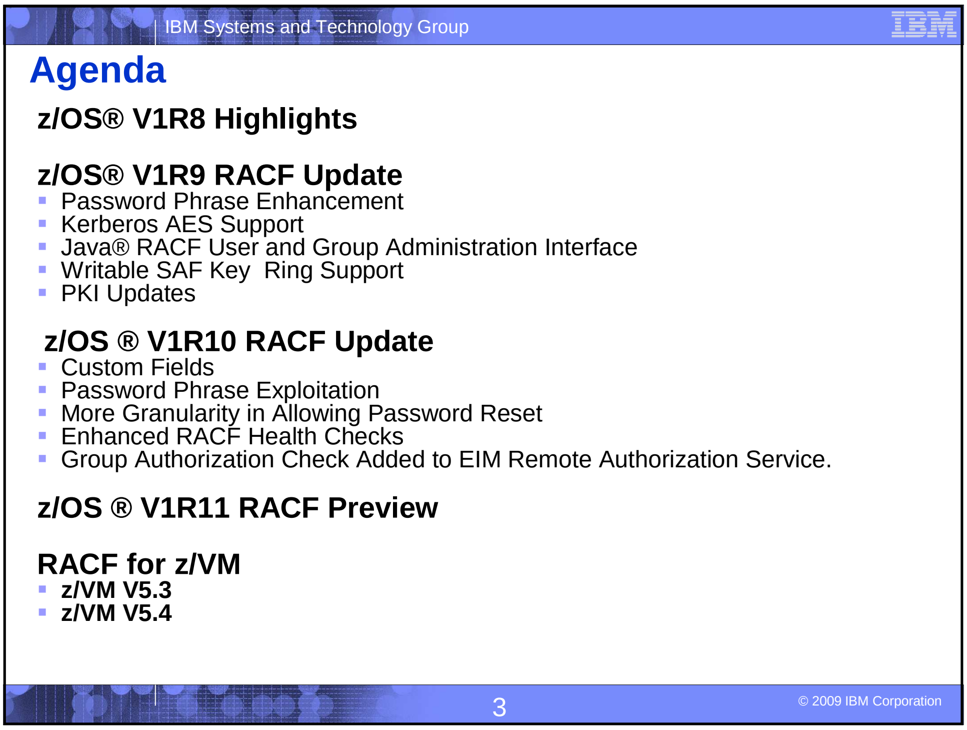
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.



Agenda

z/OS® V1R8 Highlights

z/OS® V1R9 RACF Update

- Password Phrase Enhancement
- Kerberos AES Support
- Java® RACF User and Group Administration Interface
- Writable SAF Key Ring Support
- PKI Updates

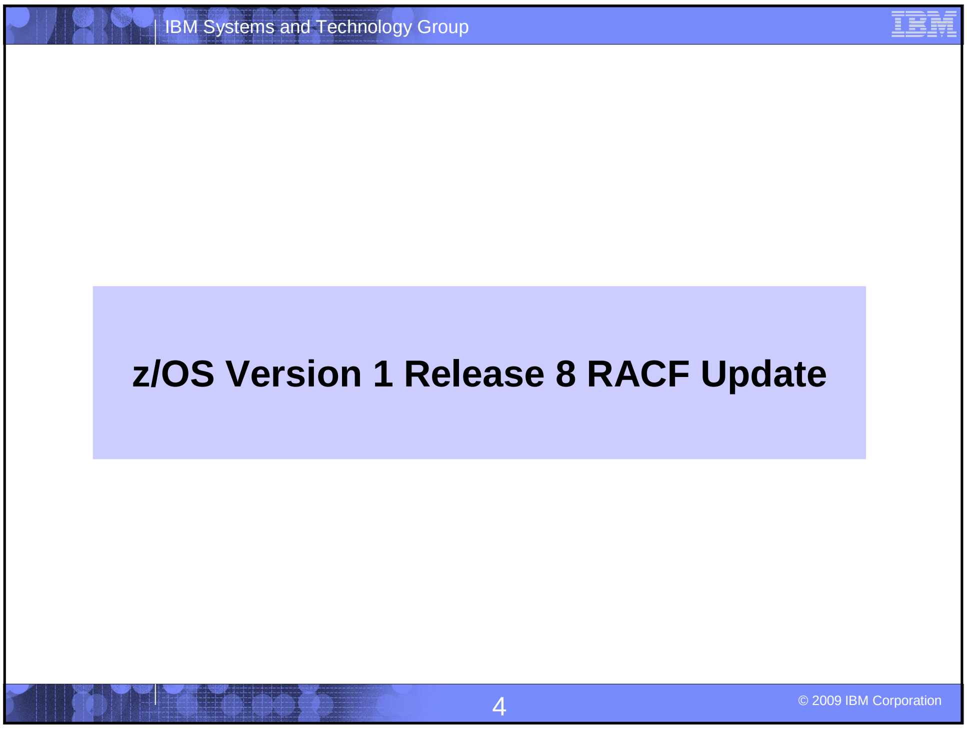
z/OS ® V1R10 RACF Update

- Custom Fields
- Password Phrase Exploitation
- More Granularity in Allowing Password Reset
- Enhanced RACF Health Checks
- Group Authorization Check Added to EIM Remote Authorization Service.

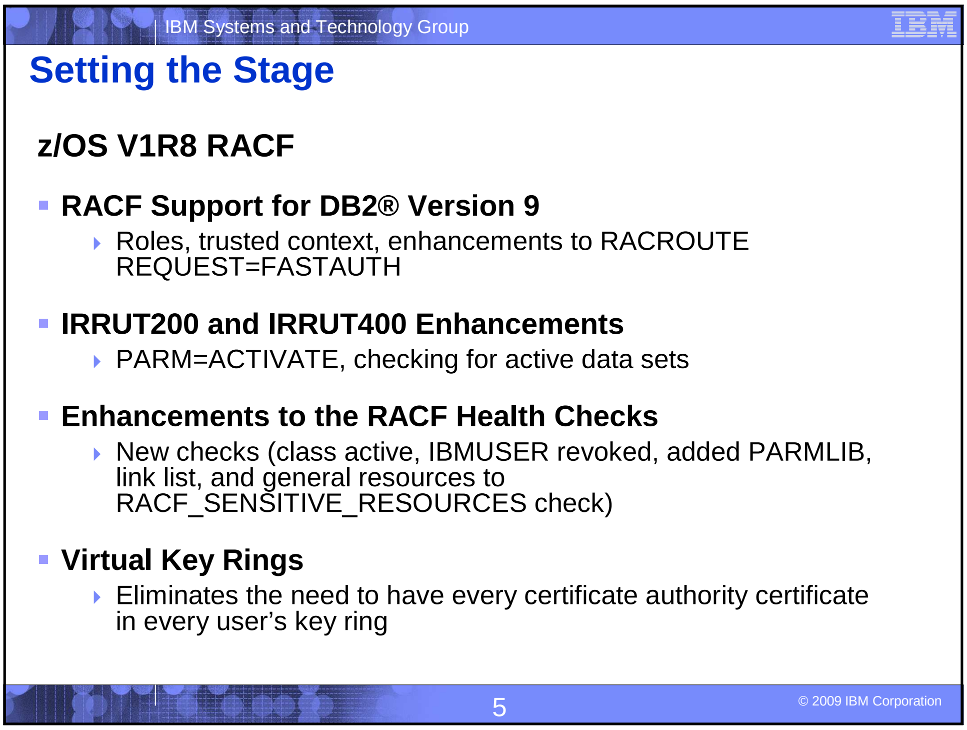
z/OS ® V1R11 RACF Preview

RACF for z/VM

- **z/VM V5.3**
- **z/VM V5.4**



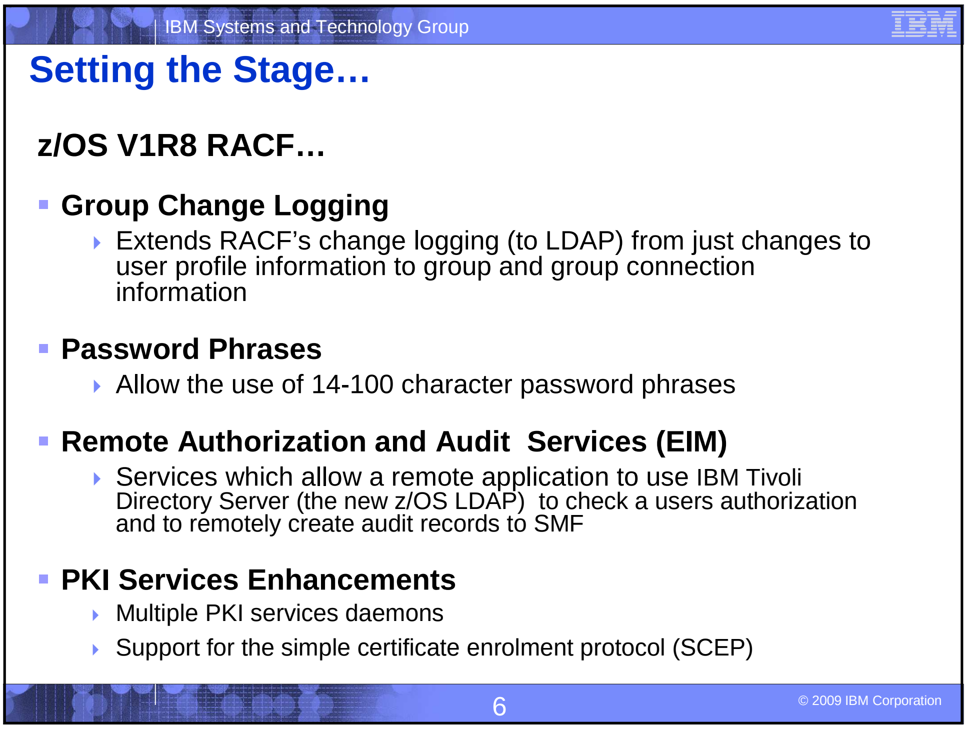
z/OS Version 1 Release 8 RACF Update



Setting the Stage

z/OS V1R8 RACF

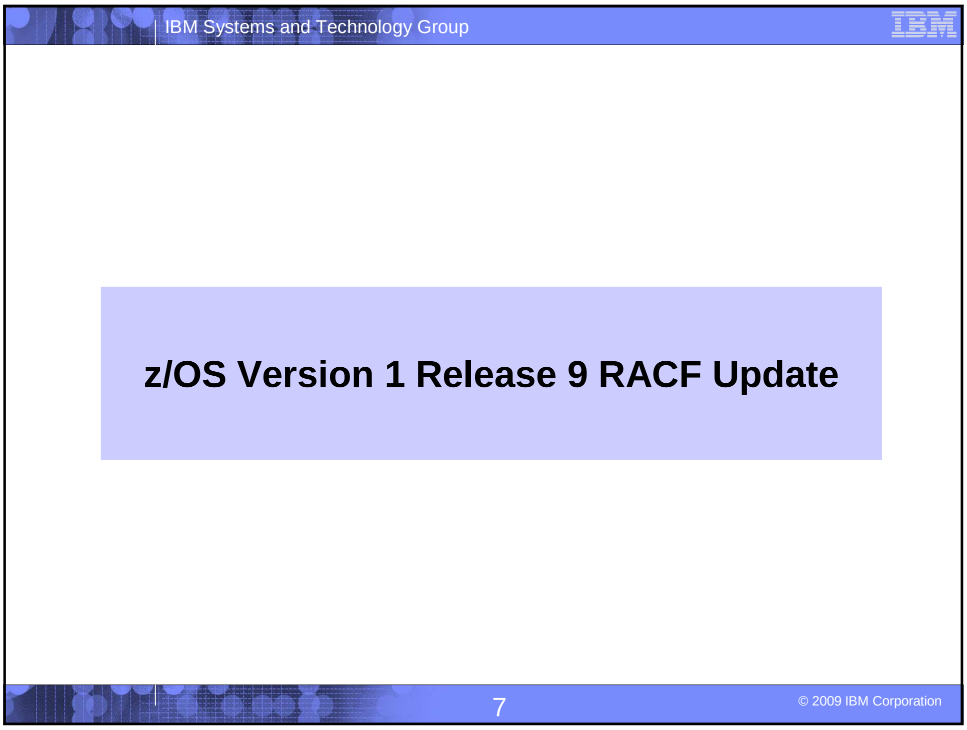
- **RACF Support for DB2® Version 9**
  - Roles, trusted context, enhancements to RACROUTE REQUEST=FASTAUTH
- **IRRUT200 and IRRUT400 Enhancements**
  - PARM=ACTIVATE, checking for active data sets
- **Enhancements to the RACF Health Checks**
  - New checks (class active, IBMUSER revoked, added PARMLIB, link list, and general resources to RACF_SENSITIVE_RESOURCES check)
- **Virtual Key Rings**
  - Eliminates the need to have every certificate authority certificate in every user's key ring



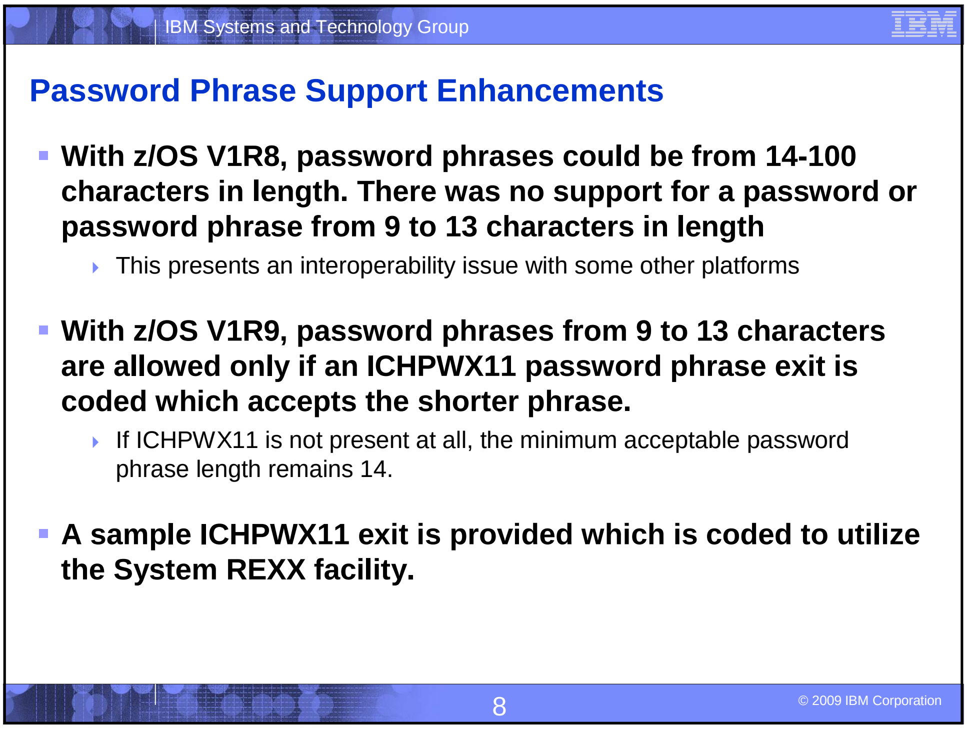
Setting the Stage…

z/OS V1R8 RACF…

- **Group Change Logging**
  - Extends RACF's change logging (to LDAP) from just changes to user profile information to group and group connection information
- **Password Phrases**
  - Allow the use of 14-100 character password phrases
- **Remote Authorization and Audit Services (EIM)**
  - Services which allow a remote application to use IBM Tivoli Directory Server (the new z/OS LDAP) to check a users authorization and to remotely create audit records to SMF
- **PKI Services Enhancements**
  - Multiple PKI services daemons
  - Support for the simple certificate enrolment protocol (SCEP)



z/OS Version 1 Release 9 RACF Update



Password Phrase Support Enhancements

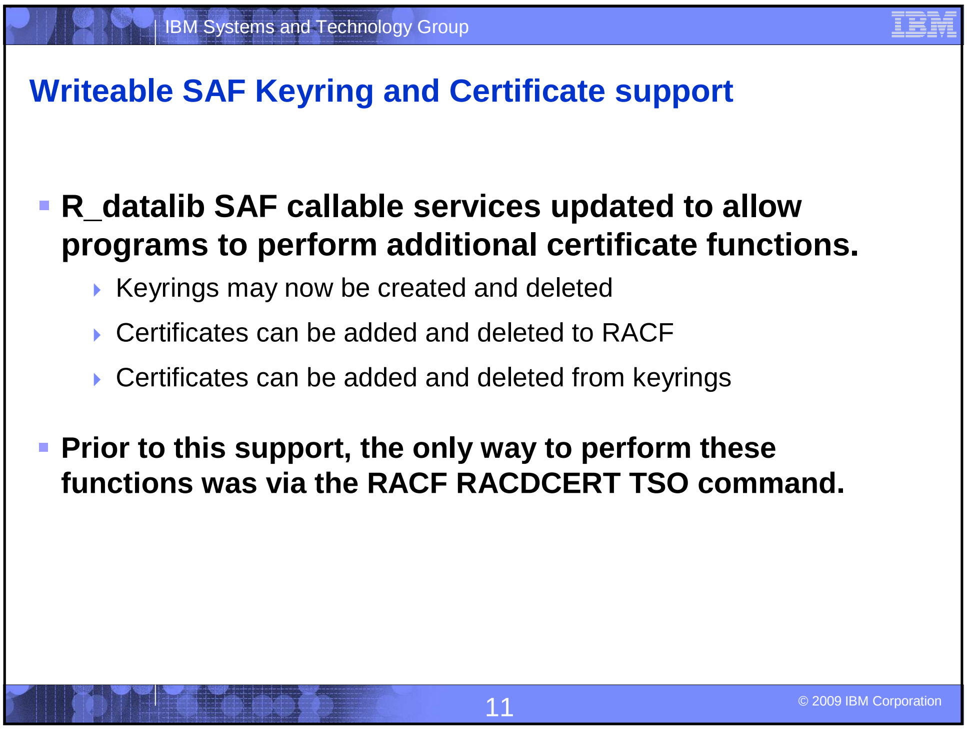
- **With z/OS V1R8, password phrases could be from 14-100 characters in length. There was no support for a password or password phrase from 9 to 13 characters in length**
  - This presents an interoperability issue with some other platforms
- **With z/OS V1R9, password phrases from 9 to 13 characters are allowed only if an ICHPWX11 password phrase exit is coded which accepts the shorter phrase.**
  - If ICHPWX11 is not present at all, the minimum acceptable password phrase length remains 14.
- **A sample ICHPWX11 exit is provided which is coded to utilize the System REXX facility.**

Kerberos AES support

- **z/OS’s Kerberos has been extended to support the AES encryption algorithm.**
  - This increases compatibility between z/OS Kerberos and implementations of Kerberos on other systems for improved interoperability in support of RFC3962.
- **In addition, functionality has been incorporated to implement SPKM/LIPKEY RFCs:**
  - RFC2025 — The Simple Public-Key GSS-API Mechanism (SPKM)
  - RFC2253 — UTF-8 String Representation of Distinguished Names
  - RFC2459 — X.509 Public Key Infrastructure
  - RFC2847 — LIPKEY — A Low Infrastructure Public Key Mechanism Using SPKM

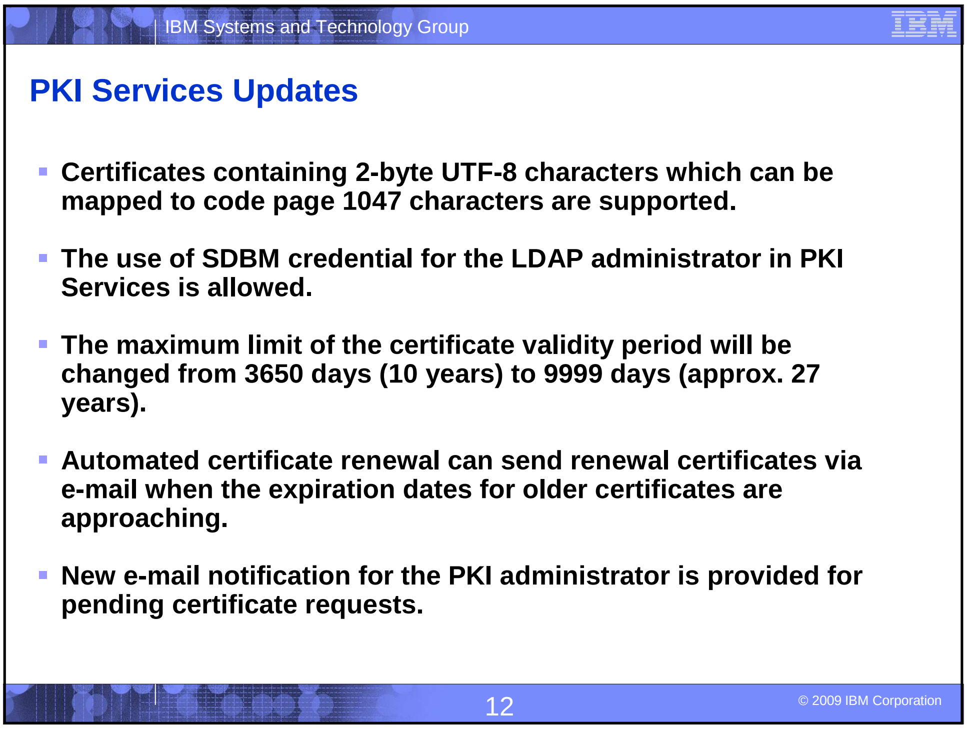
Java RACF User and Group administration interface

- **New Java interfaces**
  - Allow administration and querying of users, groups and user-group connection information via JAVA API calls.
  - These APIs internally call the z/OS LDAP (ISS or ITDS) server to perform the functions.
  - This makes these APIs callable from applications running on or off the z/OS platform.



Writeable SAF Keyring and Certificate support

- **R_datalib SAF callable services updated to allow programs to perform additional certificate functions.**
  - Keyrings may now be created and deleted
  - Certificates can be added and deleted to RACF
  - Certificates can be added and deleted from keyrings
- **Prior to this support, the only way to perform these functions was via the RACF RACDCERT TSO command.**



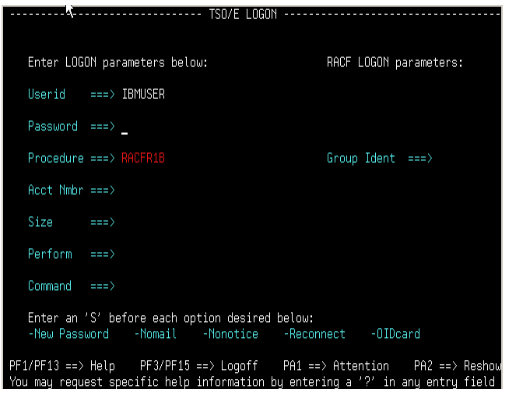
PKI Services Updates

- **Certificates containing 2-byte UTF-8 characters which can be mapped to code page 1047 characters are supported.**
- **The use of SDBM credential for the LDAP administrator in PKI Services is allowed.**
- **The maximum limit of the certificate validity period will be changed from 3650 days (10 years) to 9999 days (approx. 27 years).**
- **Automated certificate renewal can send renewal certificates via e-mail when the expiration dates for older certificates are approaching.**
- **New e-mail notification for the PKI administrator is provided for pending certificate requests.**

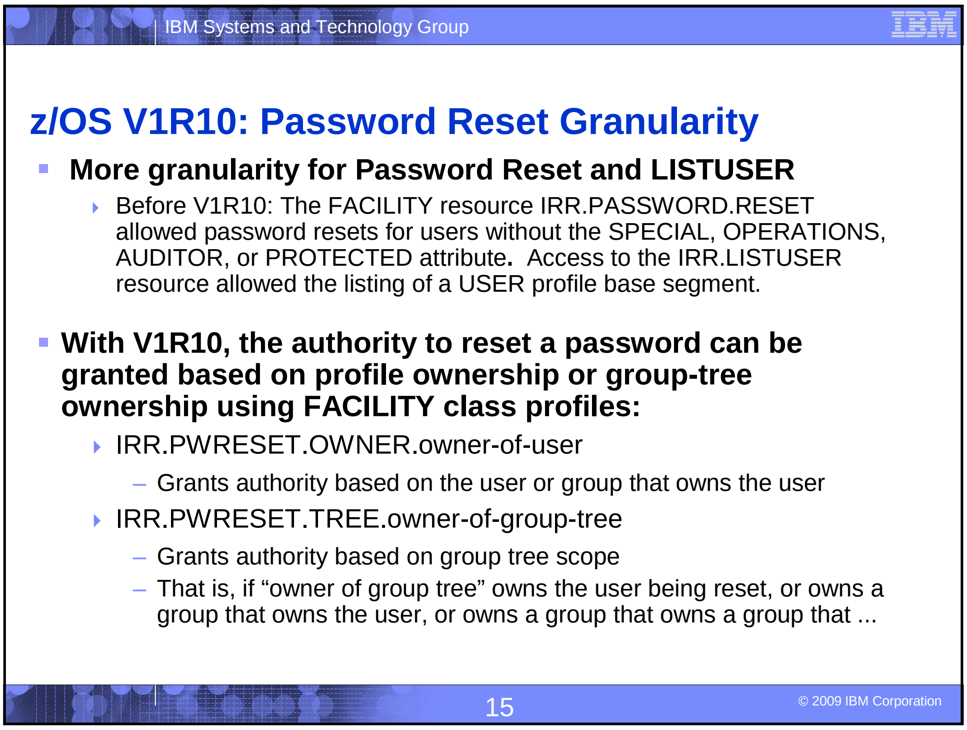
z/OS Version 1 Release 10 RACF Update

z/OS V1R10: Password Phrase Exploitation

- **Password phrase exploitation**
  - TSO/E
  - z/OS UNIX® rlogin, BPX1PWD, BPX1SEC, BPX1TLS
  - z/OS UNIX su and passwd commands
  - z/OS Kerberos
  - z/OS LDAP for z/OS SDBM backend
  - OpenSSH (IBM Ported Tools for z/OS)

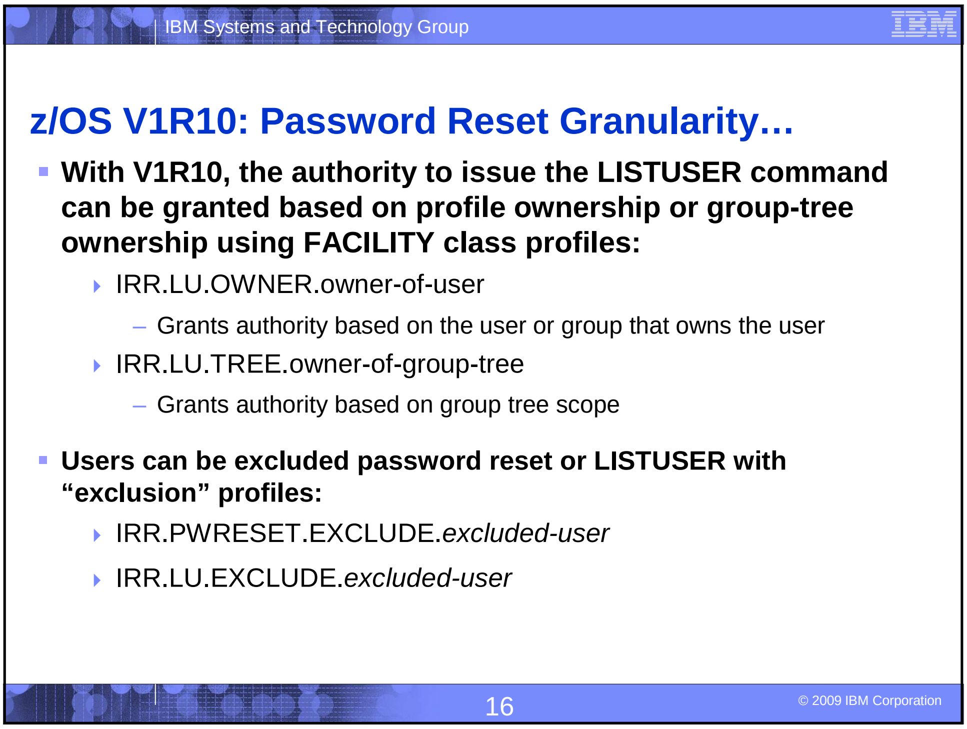


```
----------------------------- TSO/E LOGON -----------------------------------


   Enter LOGON parameters below:                   RACF LOGON parameters:

   Userid    ===> IBMUSER

   Password  ===> _

   Procedure ===> RACFR1B                          Group Ident  ===>

   Acct Nmbr ===>

   Size      ===>

   Perform   ===>

   Command   ===>

   Enter an 'S' before each option desired below:
   -New Password    -Nomail    -Nonotice    -Reconnect    -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
```



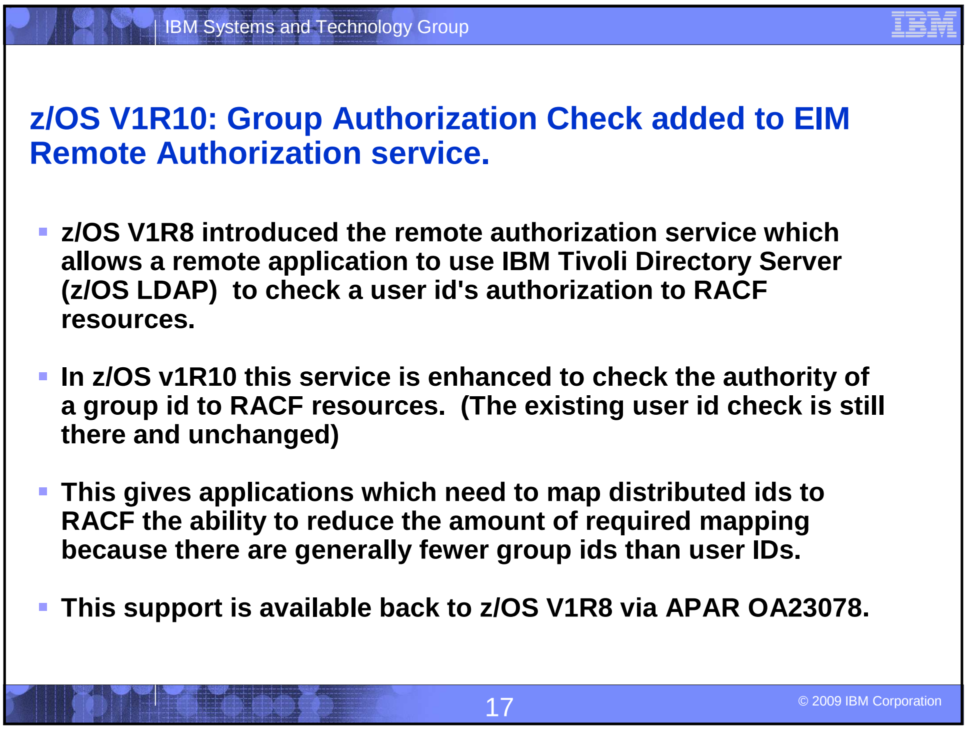
z/OS V1R10: Password Reset Granularity

- **More granularity for Password Reset and LISTUSER**
  - Before V1R10: The FACILITY resource IRR.PASSWORD.RESET allowed password resets for users without the SPECIAL, OPERATIONS, AUDITOR, or PROTECTED attribute**.** Access to the IRR.LISTUSER resource allowed the listing of a USER profile base segment.
- **With V1R10, the authority to reset a password can be granted based on profile ownership or group-tree ownership using FACILITY class profiles:**
  - IRR.PWRESET.OWNER.owner-of-user
    - Grants authority based on the user or group that owns the user
  - IRR.PWRESET.TREE.owner-of-group-tree
    - Grants authority based on group tree scope
    - That is, if “owner of group tree” owns the user being reset, or owns a group that owns the user, or owns a group that owns a group that ...



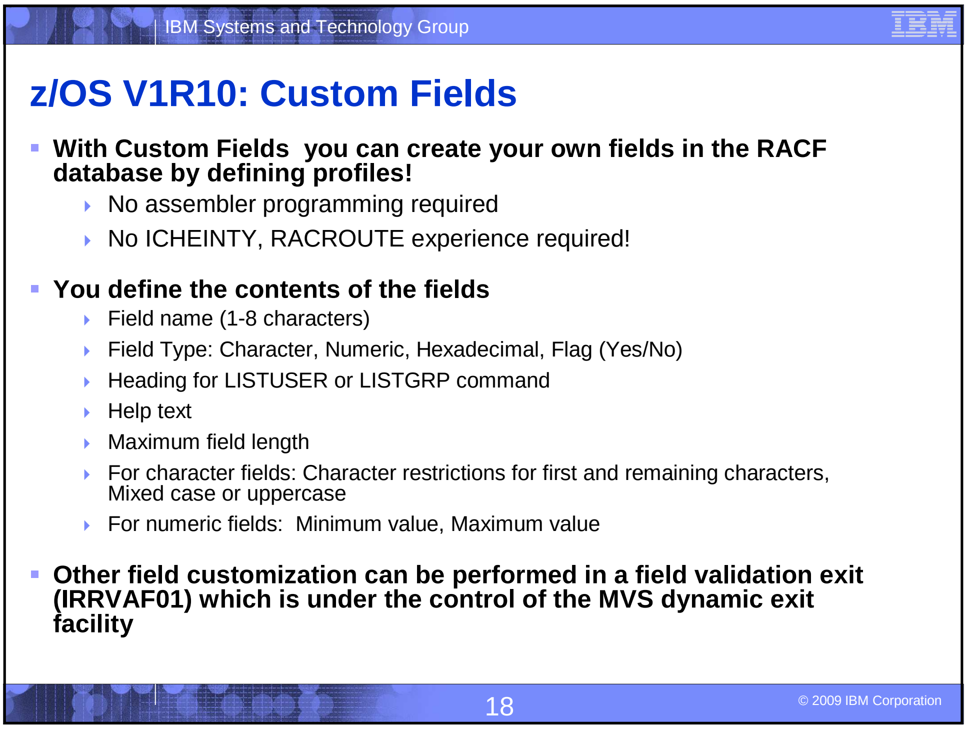
z/OS V1R10: Password Reset Granularity…

- **With V1R10, the authority to issue the LISTUSER command can be granted based on profile ownership or group-tree ownership using FACILITY class profiles:**
  - IRR.LU.OWNER.owner-of-user
    - Grants authority based on the user or group that owns the user
  - IRR.LU.TREE.owner-of-group-tree
    - Grants authority based on group tree scope
- **Users can be excluded password reset or LISTUSER with “exclusion” profiles:**
  - IRR.PWRESET.EXCLUDE.*excluded-user*
  - IRR.LU.EXCLUDE.*excluded-user*



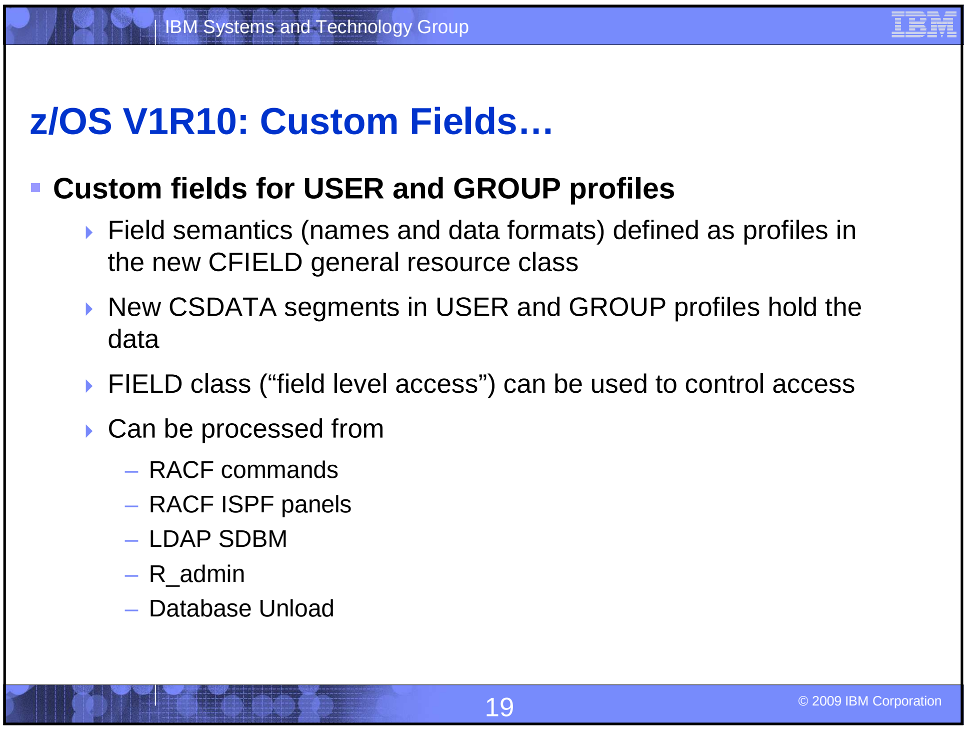
z/OS V1R10: Group Authorization Check added to EIM Remote Authorization service.

- **z/OS V1R8 introduced the remote authorization service which allows a remote application to use IBM Tivoli Directory Server (z/OS LDAP) to check a user id's authorization to RACF resources.**
- **In z/OS v1R10 this service is enhanced to check the authority of a group id to RACF resources. (The existing user id check is still there and unchanged)**
- **This gives applications which need to map distributed ids to RACF the ability to reduce the amount of required mapping because there are generally fewer group ids than user IDs.**
- **This support is available back to z/OS V1R8 via APAR OA23078.**



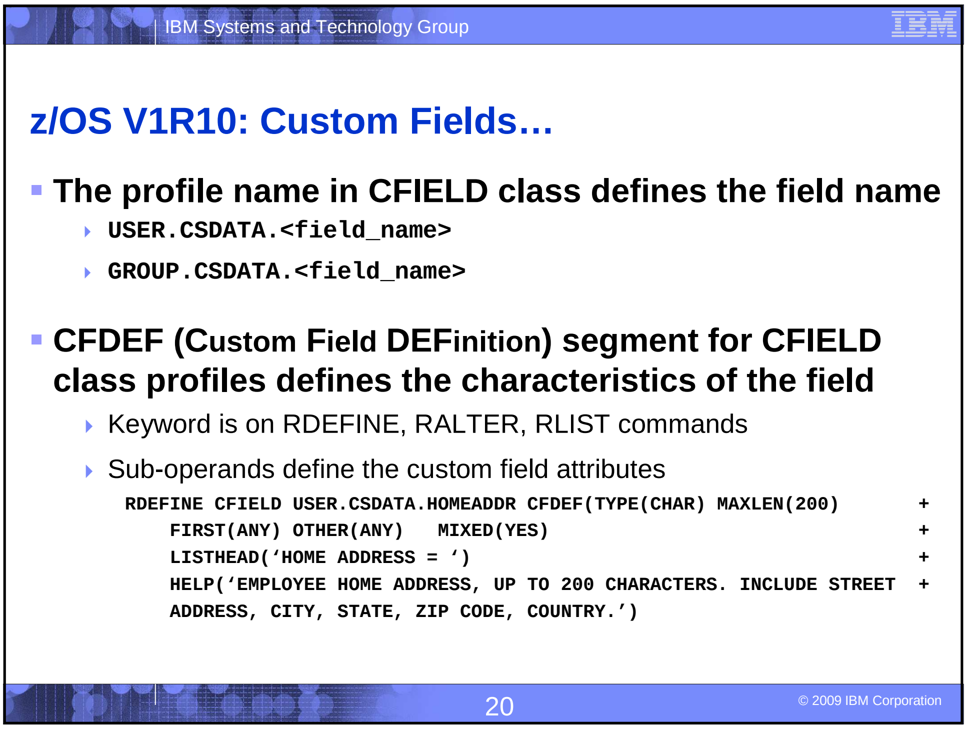
z/OS V1R10: Custom Fields

- **With Custom Fields you can create your own fields in the RACF database by defining profiles!**
  - No assembler programming required
  - No ICHEINTY, RACROUTE experience required!
- **You define the contents of the fields**
  - Field name (1-8 characters)
  - Field Type: Character, Numeric, Hexadecimal, Flag (Yes/No)
  - Heading for LISTUSER or LISTGRP command
  - Help text
  - Maximum field length
  - For character fields: Character restrictions for first and remaining characters, Mixed case or uppercase
  - For numeric fields: Minimum value, Maximum value
- **Other field customization can be performed in a field validation exit (IRRVAF01) which is under the control of the MVS dynamic exit facility**



z/OS V1R10: Custom Fields…

- **Custom fields for USER and GROUP profiles**
  - Field semantics (names and data formats) defined as profiles in the new CFIELD general resource class
  - New CSDATA segments in USER and GROUP profiles hold the data
  - FIELD class (“field level access”) can be used to control access
  - Can be processed from
    - RACF commands
    - RACF ISPF panels
    - LDAP SDBM
    - R_admin
    - Database Unload



z/OS V1R10: Custom Fields…

- **The profile name in CFIELD class defines the field name**
  - **`USER.CSDATA.<field_name>`**
  - **`GROUP.CSDATA.<field_name>`**
- **CFDEF (Custom Field DEFinition) segment for CFIELD class profiles defines the characteristics of the field**
  - Keyword is on RDEFINE, RALTER, RLIST commands
  - Sub-operands define the custom field attributes

```
RDEFINE CFIELD USER.CSDATA.HOMEADDR CFDEF(TYPE(CHAR) MAXLEN(200)       +
    FIRST(ANY) OTHER(ANY)   MIXED(YES)                                 +
    LISTHEAD(‘HOME ADDRESS = ‘)                                        +
    HELP(‘EMPLOYEE HOME ADDRESS, UP TO 200 CHARACTERS. INCLUDE STREET  +
    ADDRESS, CITY, STATE, ZIP CODE, COUNTRY.’)
```

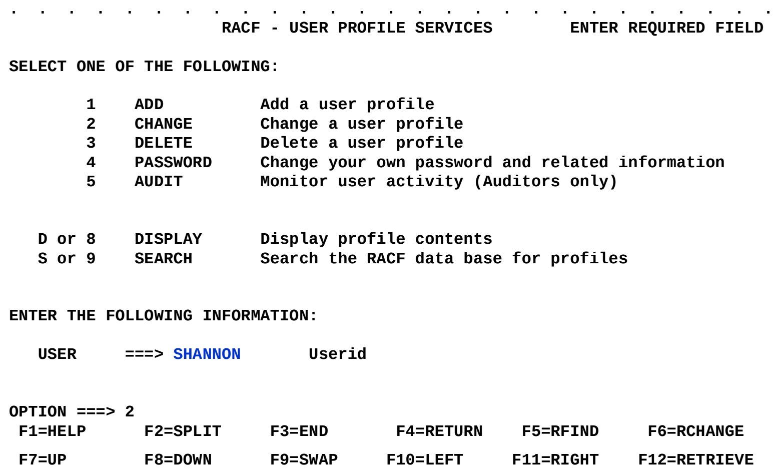
z/OS V1R10: Custom Fields…

- **CSDATA (CuStom DATA) segment for USER and GROUP profiles**
  - Keyword is on ADDUSER, ALTUSER, LISTUSER, ADDGROUP ALTGROUP, LISTGRP commands
  - Sub-operands are YOUR custom fields!
    - `ALTUSER SHANNON CSDATA(HOMEADDR('14 Main Street, Anywhere, NY 12345, USA'))`
- **The `LISTUSER` command shows**

```
LU SHANNON NORACF CSDATA
 USER=SHANNON

 CSDATA INFORMATION
 ------------------
 HOME ADDRESS = 14 Main Street, Anywhere, NY 12345, USA

 READY
```

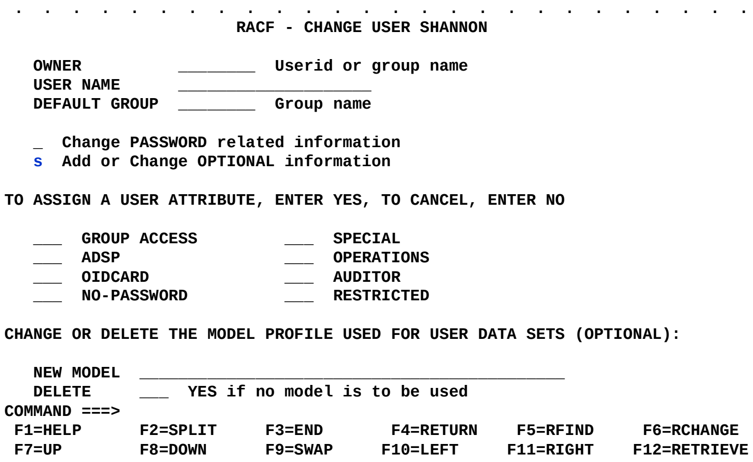
- **RACF panels can be used with Custom Fields**

z/OS V1R10: Custom Fields…



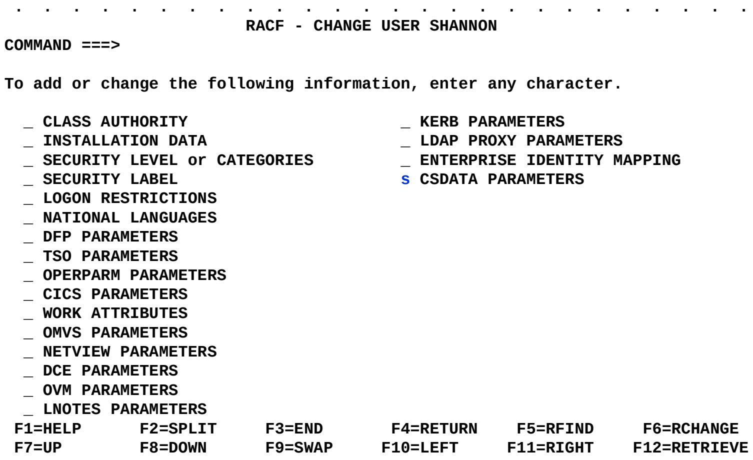
```
.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                     RACF - USER PROFILE SERVICES       ENTER REQUIRED FIELD

SELECT ONE OF THE FOLLOWING:

        1    ADD          Add a user profile
        2    CHANGE       Change a user profile
        3    DELETE       Delete a user profile
        4    PASSWORD     Change your own password and related information
        5    AUDIT        Monitor user activity (Auditors only)


   D or 8    DISPLAY      Display profile contents
   S or 9    SEARCH       Search the RACF data base for profiles


ENTER THE FOLLOWING INFORMATION:

   USER     ===> SHANNON      Userid


OPTION ===> 2
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE

 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

z/OS V1R10: Custom Fields…

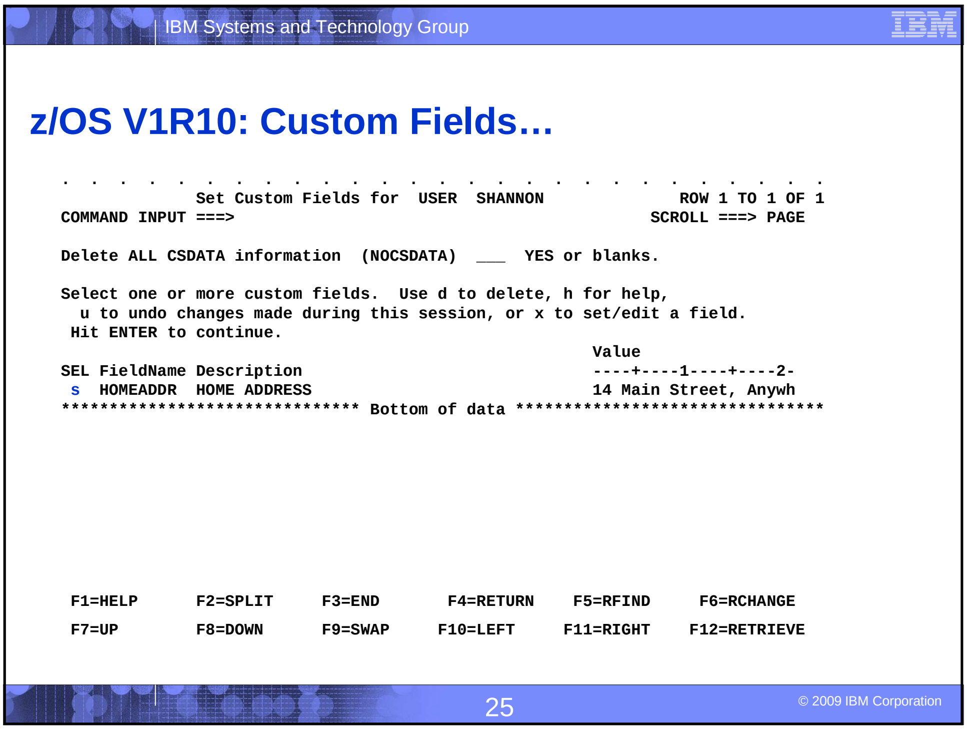


```
 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                        RACF - CHANGE USER SHANNON

   OWNER          ________  Userid or group name
   USER NAME      ____________________
   DEFAULT GROUP  ________  Group name

   _  Change PASSWORD related information
   s  Add or Change OPTIONAL information

TO ASSIGN A USER ATTRIBUTE, ENTER YES, TO CANCEL, ENTER NO

   ___  GROUP ACCESS          ___  SPECIAL
   ___  ADSP                  ___  OPERATIONS
   ___  OIDCARD               ___  AUDITOR
   ___  NO-PASSWORD           ___  RESTRICTED

CHANGE OR DELETE THE MODEL PROFILE USED FOR USER DATA SETS (OPTIONAL):

   NEW MODEL  ____________________________________________
   DELETE     ___  YES if no model is to be used
COMMAND ===>
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

z/OS V1R10: Custom Fields…

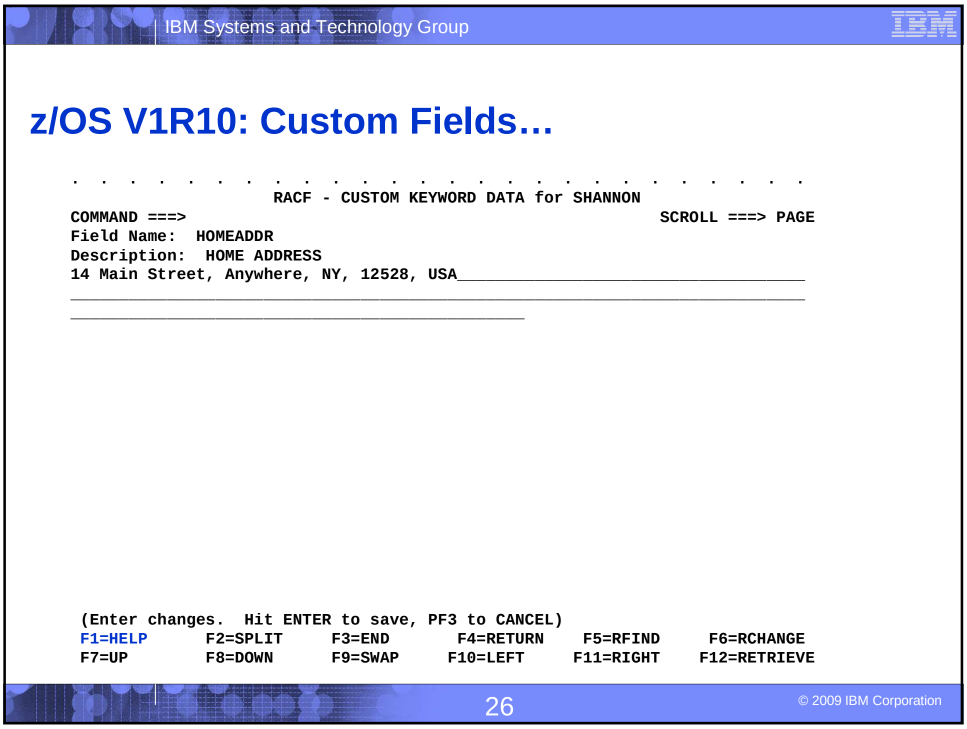


```
 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                         RACF - CHANGE USER SHANNON
COMMAND ===>

To add or change the following information, enter any character.

  _ CLASS AUTHORITY                       _ KERB PARAMETERS
  _ INSTALLATION DATA                     _ LDAP PROXY PARAMETERS
  _ SECURITY LEVEL or CATEGORIES          _ ENTERPRISE IDENTITY MAPPING
  _ SECURITY LABEL                        s CSDATA PARAMETERS
  _ LOGON RESTRICTIONS
  _ NATIONAL LANGUAGES
  _ DFP PARAMETERS
  _ TSO PARAMETERS
  _ OPERPARM PARAMETERS
  _ CICS PARAMETERS
  _ WORK ATTRIBUTES
  _ OMVS PARAMETERS
  _ NETVIEW PARAMETERS
  _ DCE PARAMETERS
  _ OVM PARAMETERS
  _ LNOTES PARAMETERS
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```



z/OS V1R10: Custom Fields…

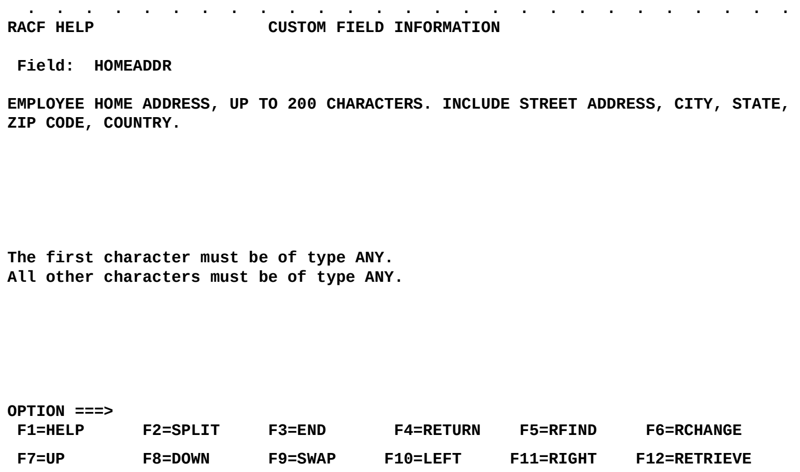
```
 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
              Set Custom Fields for  USER  SHANNON              ROW 1 TO 1 OF 1
COMMAND INPUT ===>                                           SCROLL ===> PAGE

Delete ALL CSDATA information  (NOCSDATA)  ___  YES or blanks.

Select one or more custom fields.  Use d to delete, h for help,
  u to undo changes made during this session, or x to set/edit a field.
 Hit ENTER to continue.
                                                       Value
SEL FieldName Description                              ----+----1----+----2-
 s  HOMEADDR  HOME ADDRESS                             14 Main Street, Anywh
******************************* Bottom of data ********************************




 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE

 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```



z/OS V1R10: Custom Fields…

```
 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
                     RACF - CUSTOM KEYWORD DATA for SHANNON
COMMAND ===>                                                 SCROLL ===> PAGE
Field Name:  HOMEADDR
Description:  HOME ADDRESS
14 Main Street, Anywhere, NY, 12528, USA______________________________________
____________________________________________________________________________
_______________________________________________




 (Enter changes.  Hit ENTER to save, PF3 to CANCEL)
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

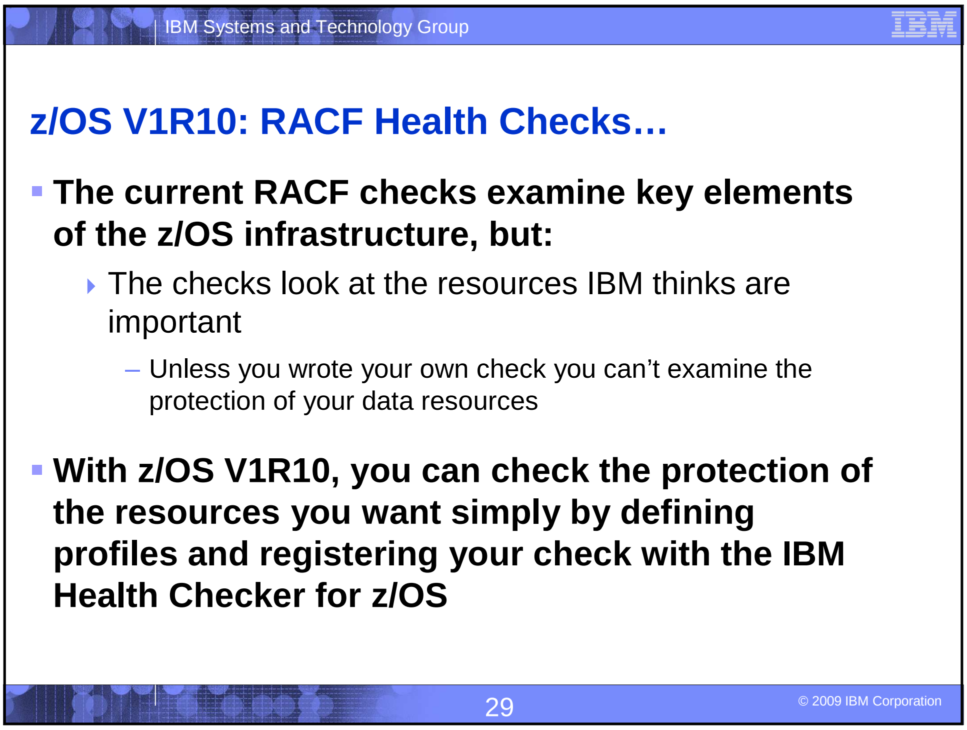
z/OS V1R10: Custom Fields…



```
  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
RACF HELP                  CUSTOM FIELD INFORMATION

 Field:  HOMEADDR

EMPLOYEE HOME ADDRESS, UP TO 200 CHARACTERS. INCLUDE STREET ADDRESS, CITY, STATE,
ZIP CODE, COUNTRY.





The first character must be of type ANY.
All other characters must be of type ANY.





OPTION ===>
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE

 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

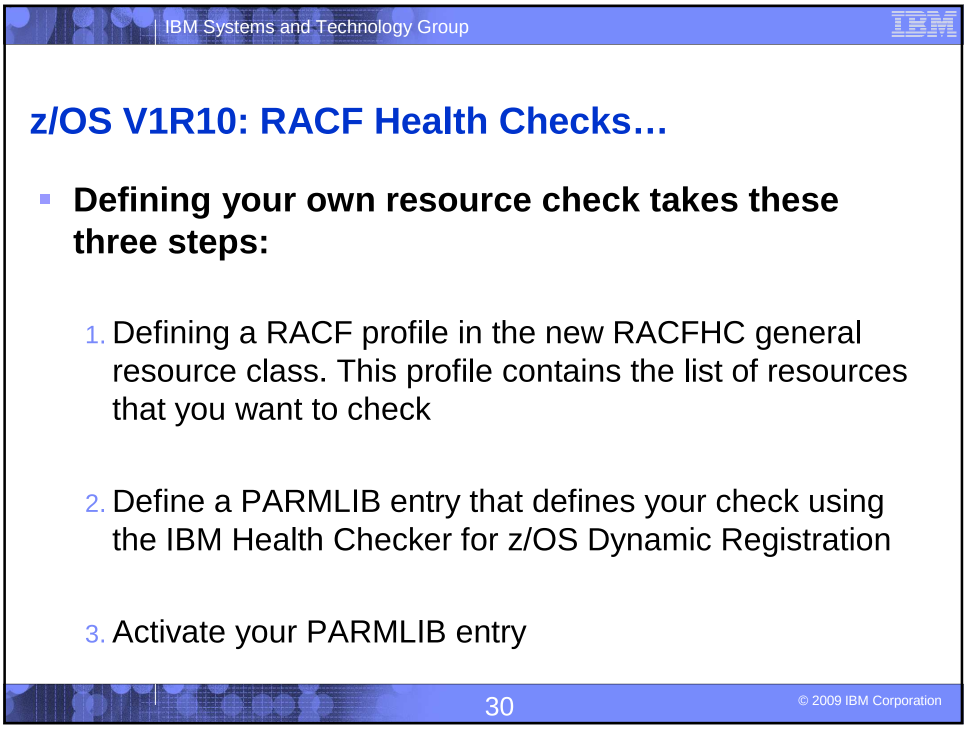
z/OS V1R10: RACF Health Checks

- **RACF Health Check Enhancements:**
  - **ICHAUTAB checks:**
    - For over 20 years, IBM has recommended not using the RACF Authorized Caller Table (ICHAUTAB)
    - RACF introduces a new check to verify that ICHAUTAB is not being used
      - RACF_ICHAUTAB_NONLPA raises a SEV(MED) exception if a non-LPA resident ICHAUTAB is found
    - The existing RACF_SENSITIVE_RESOURCES raises a SEV(HIGH) exception if an LPA-resident ICHAUTAB is found



z/OS V1R10: RACF Health Checks…

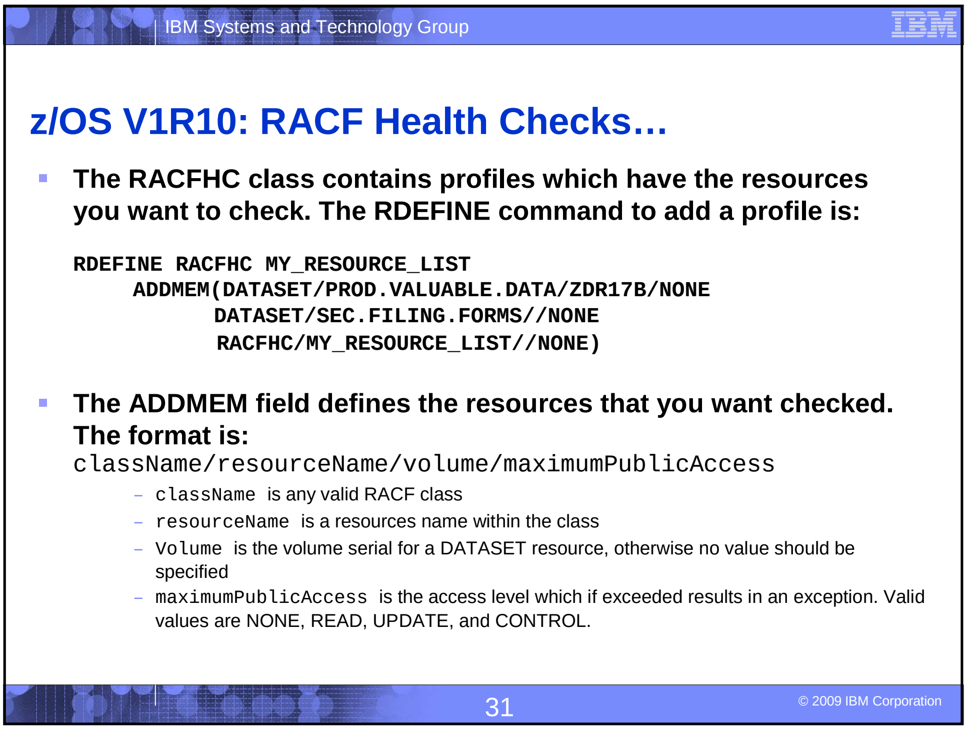
- **The current RACF checks examine key elements of the z/OS infrastructure, but:**
  - The checks look at the resources IBM thinks are important
    - Unless you wrote your own check you can't examine the protection of your data resources
- **With z/OS V1R10, you can check the protection of the resources you want simply by defining profiles and registering your check with the IBM Health Checker for z/OS**



z/OS V1R10: RACF Health Checks…

- **Defining your own resource check takes these three steps:**

  1. Defining a RACF profile in the new RACFHC general resource class. This profile contains the list of resources that you want to check
  2. Define a PARMLIB entry that defines your check using the IBM Health Checker for z/OS Dynamic Registration
  3. Activate your PARMLIB entry

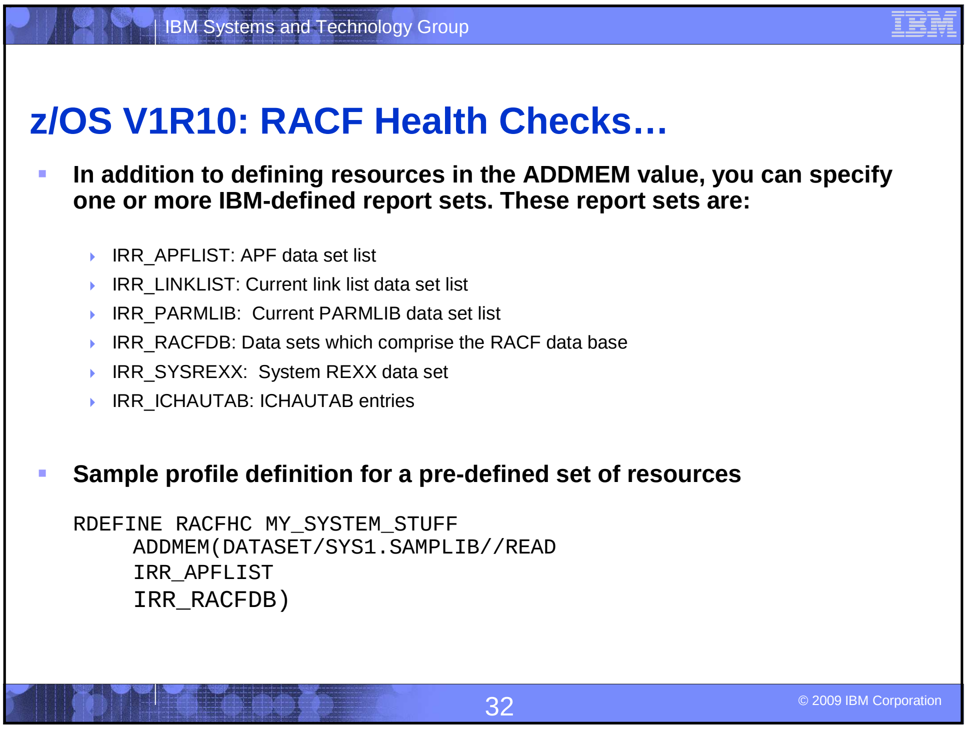


z/OS V1R10: RACF Health Checks…

- **The RACFHC class contains profiles which have the resources you want to check. The RDEFINE command to add a profile is:**

```
RDEFINE RACFHC MY_RESOURCE_LIST
     ADDMEM(DATASET/PROD.VALUABLE.DATA/ZDR17B/NONE
            DATASET/SEC.FILING.FORMS//NONE
            RACFHC/MY_RESOURCE_LIST//NONE)
```

- **The ADDMEM field defines the resources that you want checked. The format is:**
  `classNameresourceName/volume/maximumPublicAccess`
  - `className` is any valid RACF class
  - `resourceName` is a resources name within the class
  - `Volume` is the volume serial for a DATASET resource, otherwise no value should be specified
  - `maximumPublicAccess` is the access level which if exceeded results in an exception. Valid values are NONE, READ, UPDATE, and CONTROL.



z/OS V1R10: RACF Health Checks…

- **In addition to defining resources in the ADDMEM value, you can specify one or more IBM-defined report sets. These report sets are:**
  - IRR_APFLIST: APF data set list
  - IRR_LINKLIST: Current link list data set list
  - IRR_PARMLIB: Current PARMLIB data set list
  - IRR_RACFDB: Data sets which comprise the RACF data base
  - IRR_SYSREXX: System REXX data set
  - IRR_ICHAUTAB: ICHAUTAB entries

- **Sample profile definition for a pre-defined set of resources**

```
RDEFINE RACFHC MY_SYSTEM_STUFF
     ADDMEM(DATASET/SYS1.SAMPLIB//READ
     IRR_APFLIST
     IRR_RACFDB)
```

z/OS V1R10: RACF Health Checks…

- A Health Checker PARMLIB statement is used to define your check, set its characteristics (such as the interval, severity), and associate the check with the RACFHC profile which contains the resources you want checked

```
ADD CHECK(USER01,MY_INSTALLATION_HEALTH_CHECK)
     CHECKROUTINE(IRRHCR00)
     MESSAGETABLE(IRRHCM00)
     ENTRYCODE(100)
     PARM('USER(USER01)  RESOURCELIST(MY_RESOURCE_LIST)')
     DATE(yyyymmdd)
     REASON('My sensitive resources')
     GLOBAL
     ACTIVE
     SEVERITY(HIGH)
     INTERVAL(08:00)
```

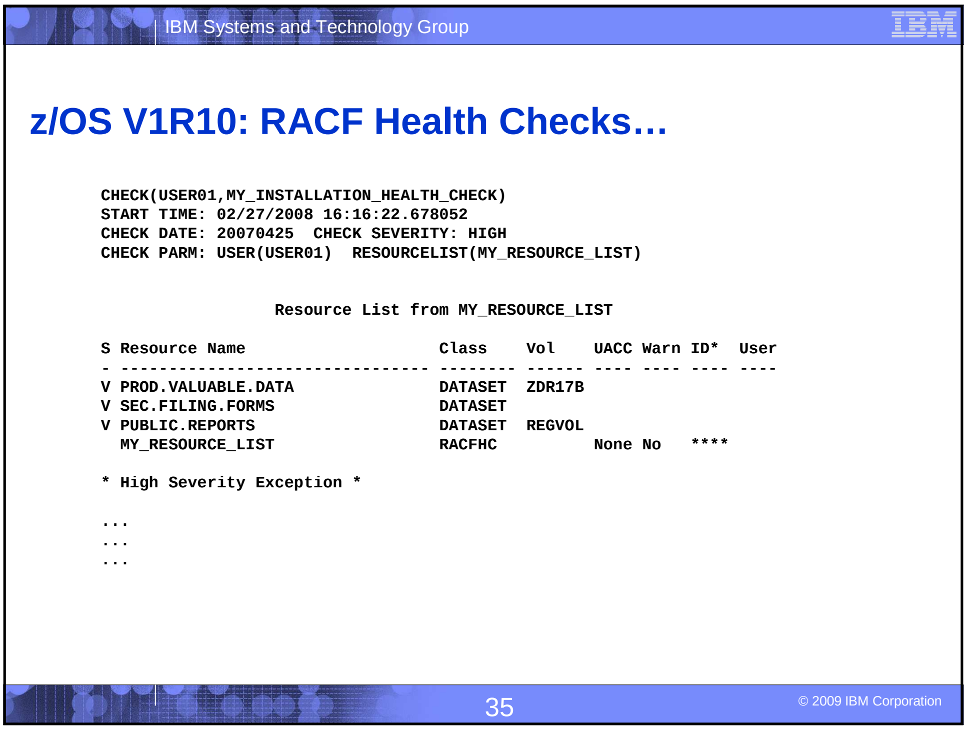
z/OS V1R10: RACF Health Checks…

- The final step is to activate your check. After adding it to a member (HZSPRMMN in this example) activate the PARMLIB entry using the MVS modify command for the Health Checker address space:

```
F HC,ADD,PARMLIB=MN
```

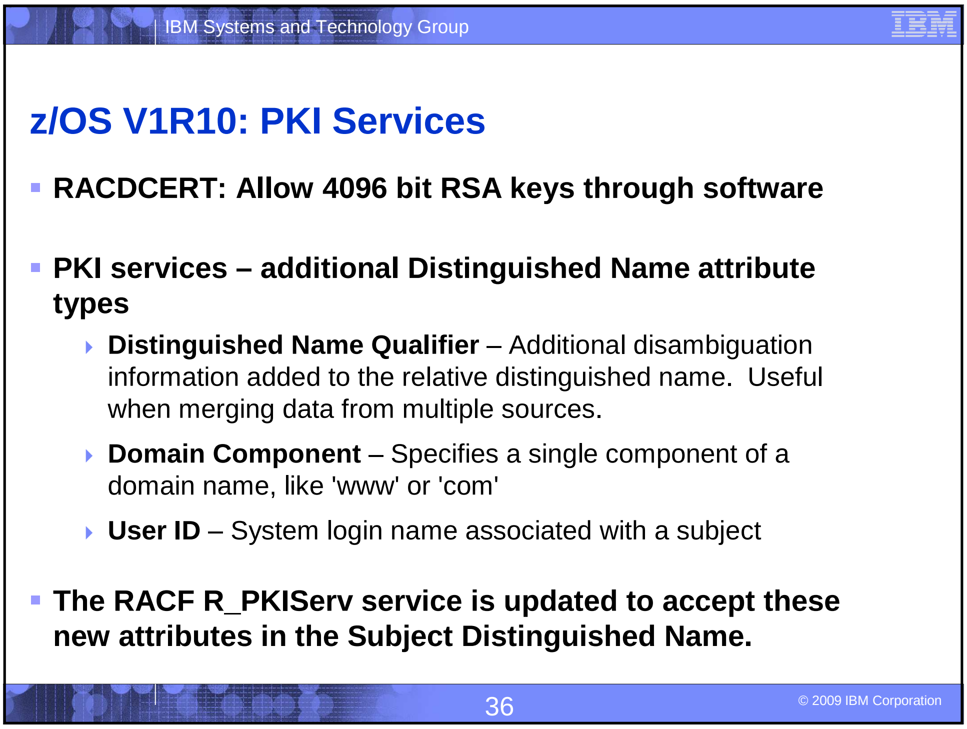
- Your check is now registered with the IBM Health Checker for z/OS!

```
Display  Filter  View  Print  Options  Help
-------------------------------------------------------------------------------
SDSF HEALTH CHECKER DISPLAY  RACFR1B                  LINE 38-53 (92)
NP   NAME                           CheckOwner       State              Status
     MY_INSTALLATION_HEALTH_CHECK   USER01           ACTIVE(ENABLED)    EXCEPT
     PDSE_SMSPDSE1                  IBMPDSE          ACTIVE(ENABLED)    EXCEPT
     RACF_FACILITY_ACTIVE           IBMRACF          ACTIVE(ENABLED)    SUCCES
     RACF_GRS_RNL                   IBMRACF          ACTIVE(DISABLED)   ENV N/
```



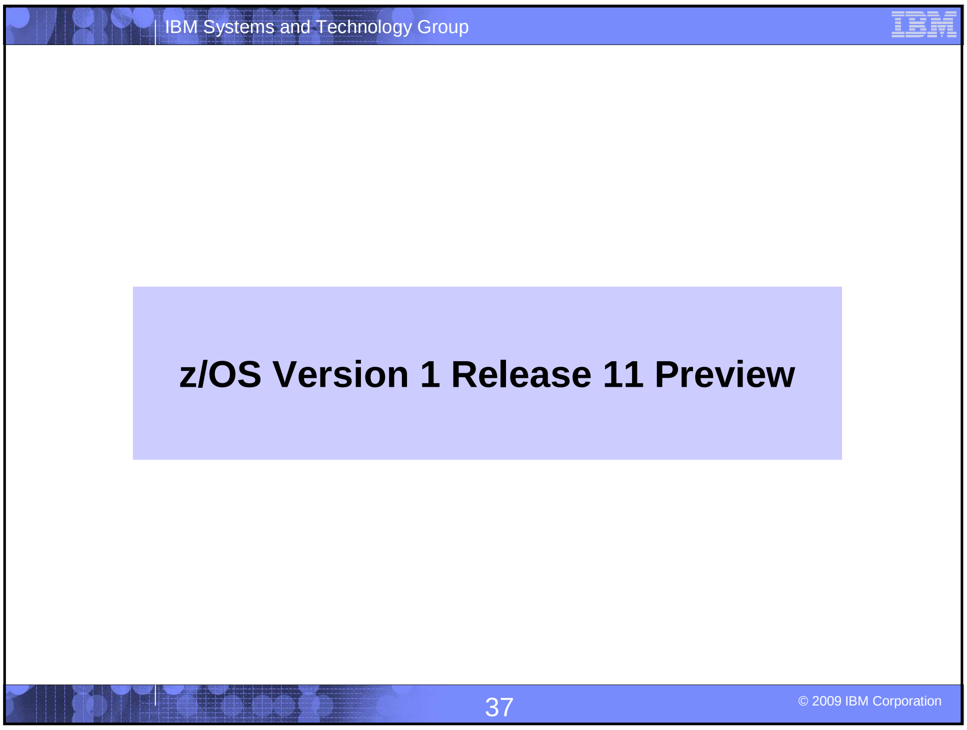
z/OS V1R10: RACF Health Checks…

```
CHECK(USER01,MY_INSTALLATION_HEALTH_CHECK)
START TIME: 02/27/2008 16:16:22.678052
CHECK DATE: 20070425  CHECK SEVERITY: HIGH
CHECK PARM: USER(USER01)  RESOURCELIST(MY_RESOURCE_LIST)


                  Resource List from MY_RESOURCE_LIST

S Resource Name                    Class    Vol    UACC Warn ID*  User
- -------------------------------- -------- ------ ---- ---- ---- ----
V PROD.VALUABLE.DATA               DATASET  ZDR17B
V SEC.FILING.FORMS                 DATASET
V PUBLIC.REPORTS                   DATASET  REGVOL
  MY_RESOURCE_LIST                 RACFHC          None No   ****

* High Severity Exception *

...
...
...
```

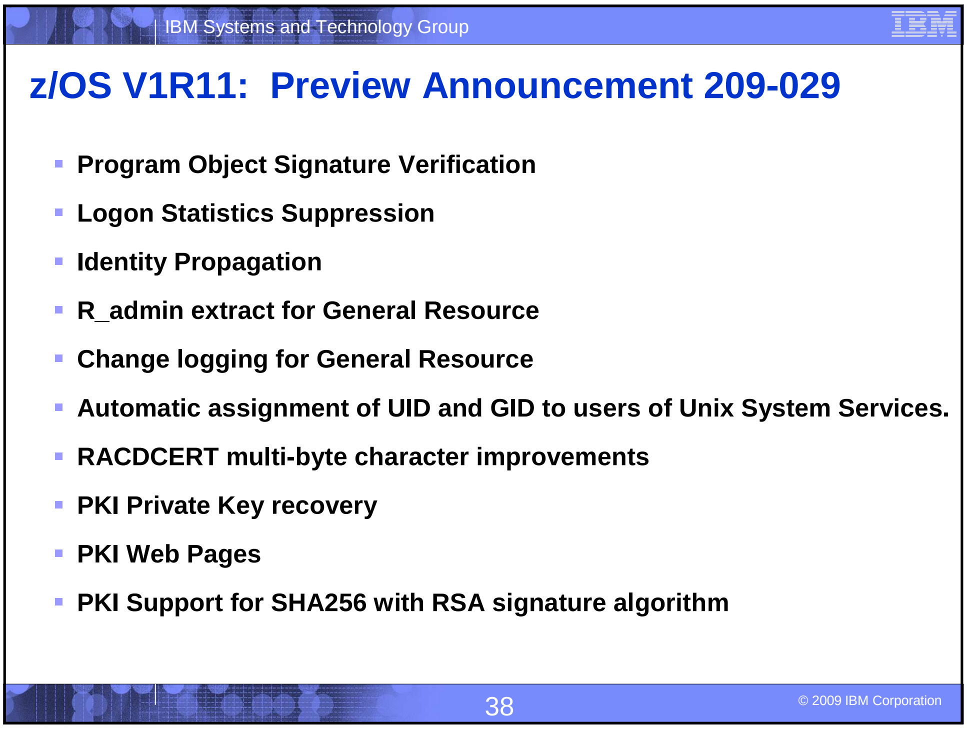


z/OS V1R10: PKI Services

- **RACDCERT: Allow 4096 bit RSA keys through software**
- **PKI services – additional Distinguished Name attribute types**
  - **Distinguished Name Qualifier** – Additional disambiguation information added to the relative distinguished name. Useful when merging data from multiple sources.
  - **Domain Component** – Specifies a single component of a domain name, like 'www' or 'com'
  - **User ID** – System login name associated with a subject
- **The RACF R_PKIServ service is updated to accept these new attributes in the Subject Distinguished Name.**

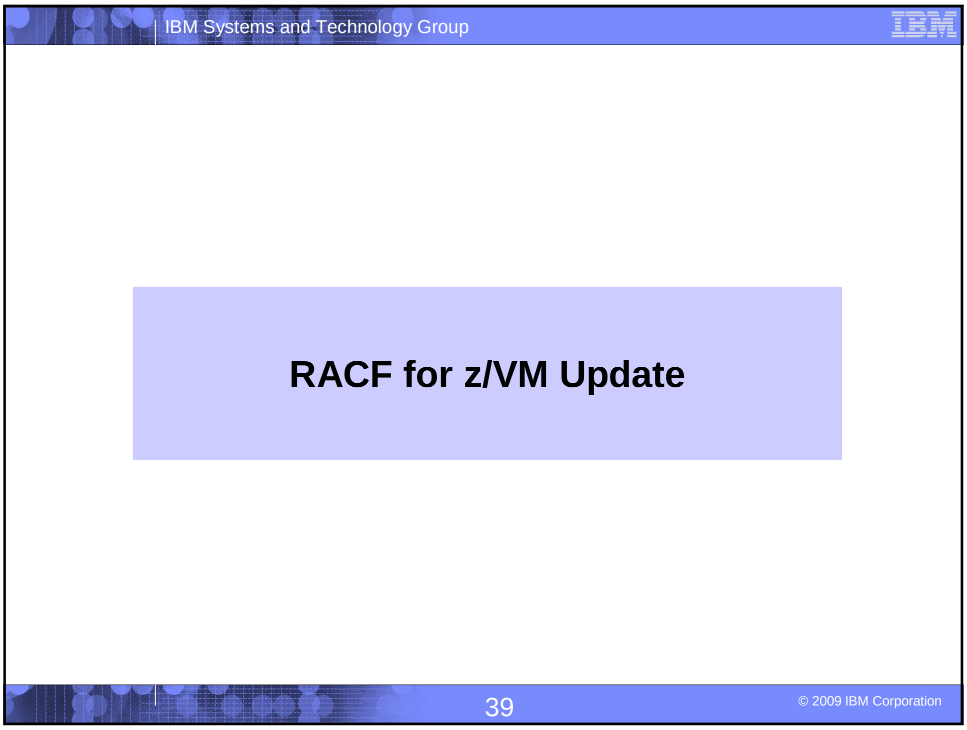


z/OS Version 1 Release 11 Preview

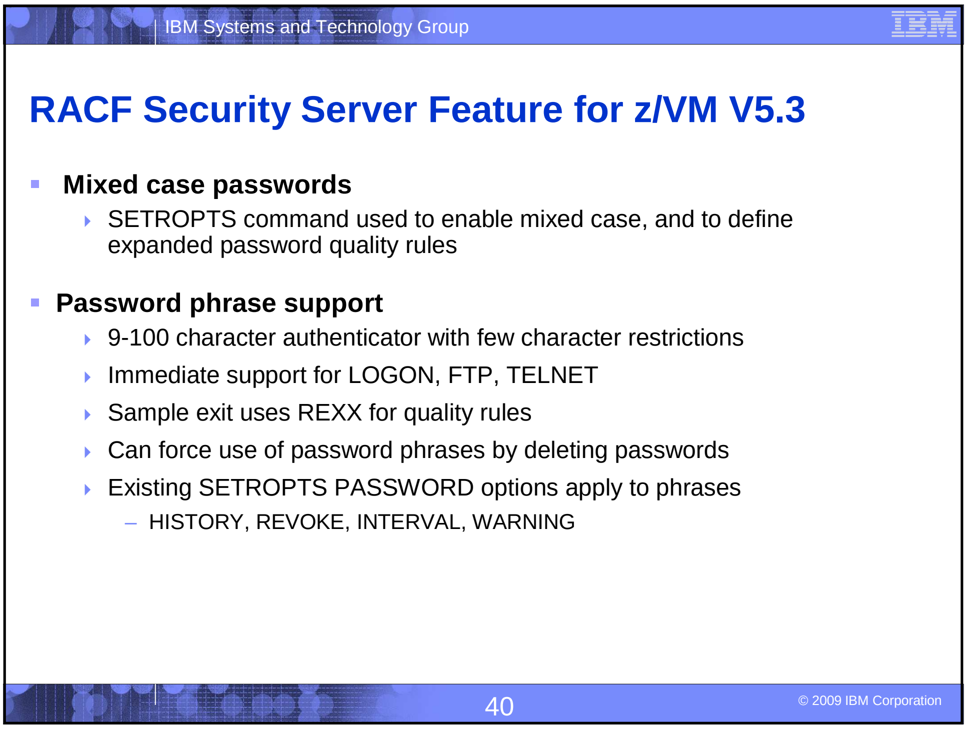


z/OS V1R11: Preview Announcement 209-029

- **Program Object Signature Verification**
- **Logon Statistics Suppression**
- **Identity Propagation**
- **R_admin extract for General Resource**
- **Change logging for General Resource**
- **Automatic assignment of UID and GID to users of Unix System Services.**
- **RACDCERT multi-byte character improvements**
- **PKI Private Key recovery**
- **PKI Web Pages**
- **PKI Support for SHA256 with RSA signature algorithm**

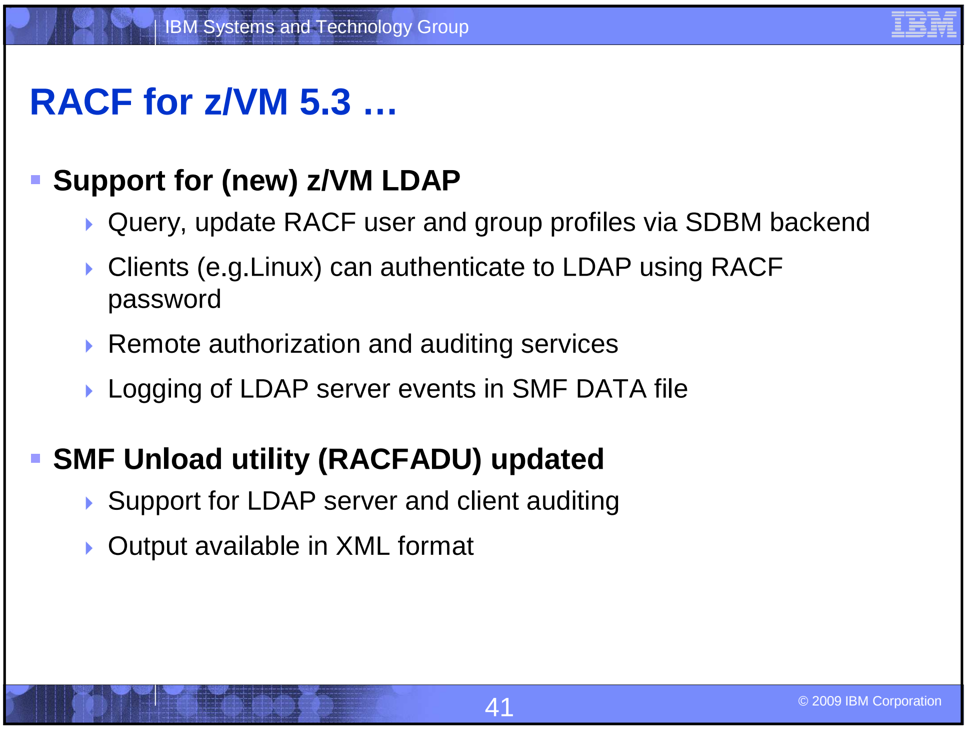


RACF for z/VM Update



RACF Security Server Feature for z/VM V5.3

- **Mixed case passwords**
  - SETROPTS command used to enable mixed case, and to define expanded password quality rules
- **Password phrase support**
  - 9-100 character authenticator with few character restrictions
  - Immediate support for LOGON, FTP, TELNET
  - Sample exit uses REXX for quality rules
  - Can force use of password phrases by deleting passwords
  - Existing SETROPTS PASSWORD options apply to phrases
    - HISTORY, REVOKE, INTERVAL, WARNING



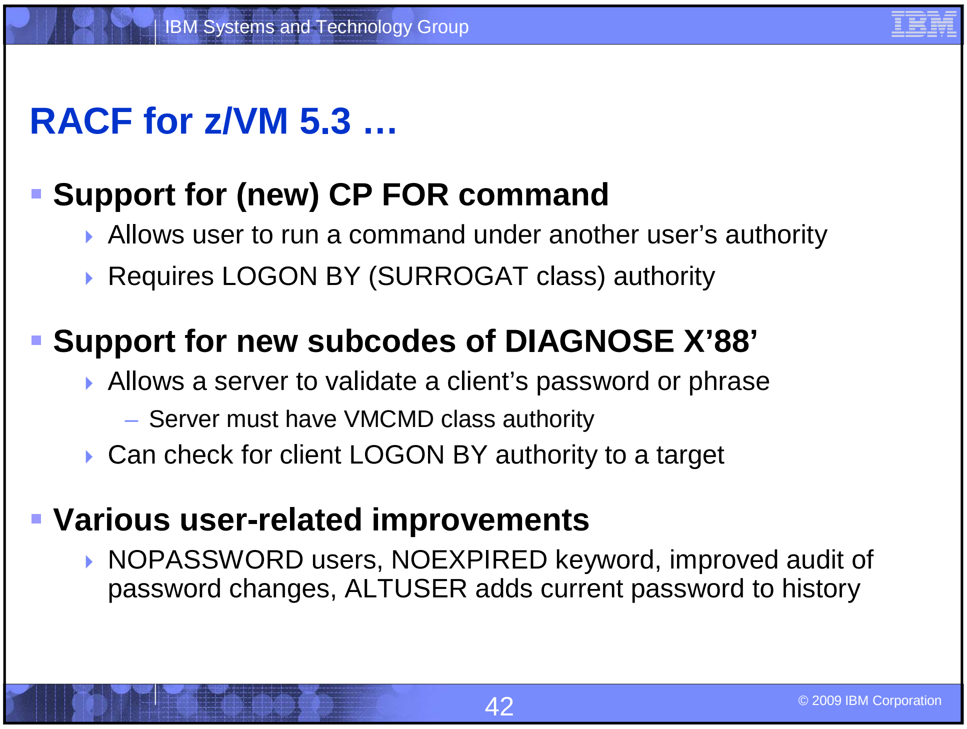
IBM Systems and Technology Group

RACF for z/VM 5.3 …

- **Support for (new) z/VM LDAP**
  - Query, update RACF user and group profiles via SDBM backend
  - Clients (e.g.Linux) can authenticate to LDAP using RACF password
  - Remote authorization and auditing services
  - Logging of LDAP server events in SMF DATA file
- **SMF Unload utility (RACFADU) updated**
  - Support for LDAP server and client auditing
  - Output available in XML format

41

© 2009 IBM Corporation



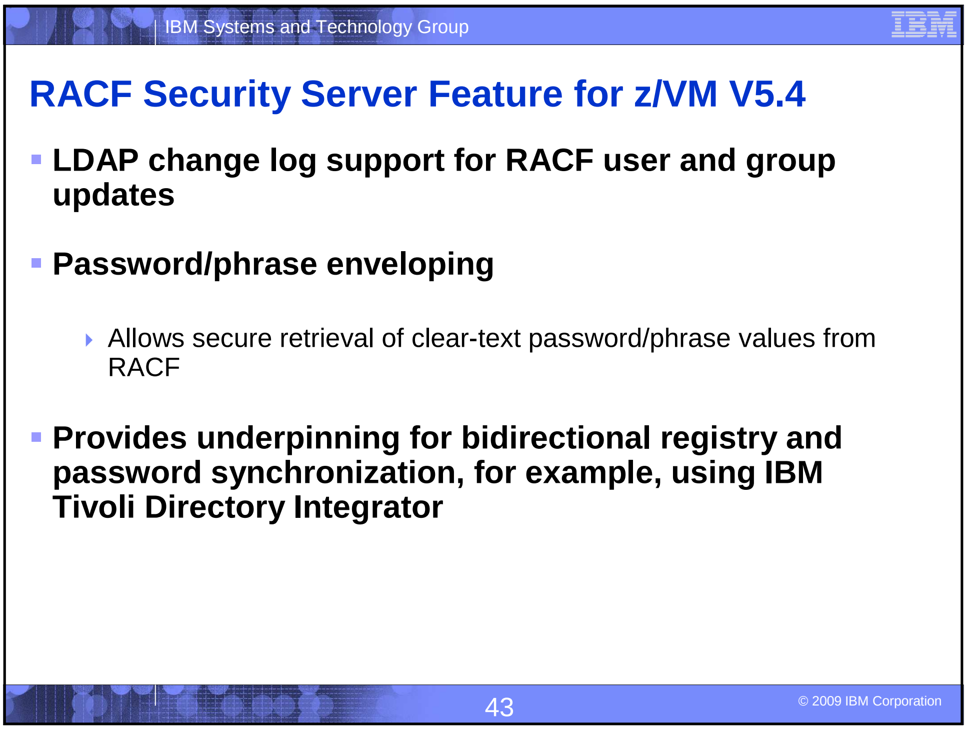
IBM Systems and Technology Group

RACF for z/VM 5.3 …

- **Support for (new) CP FOR command**
  - Allows user to run a command under another user’s authority
  - Requires LOGON BY (SURROGAT class) authority
- **Support for new subcodes of DIAGNOSE X’88’**
  - Allows a server to validate a client’s password or phrase
    - Server must have VMCMD class authority
  - Can check for client LOGON BY authority to a target
- **Various user-related improvements**
  - NOPASSWORD users, NOEXPIRED keyword, improved audit of password changes, ALTUSER adds current password to history

42

© 2009 IBM Corporation



IBM Systems and Technology Group

RACF Security Server Feature for z/VM V5.4

- **LDAP change log support for RACF user and group updates**
- **Password/phrase enveloping**
  - Allows secure retrieval of clear-text password/phrase values from RACF
- **Provides underpinning for bidirectional registry and password synchronization, for example, using IBM Tivoli Directory Integrator**

43