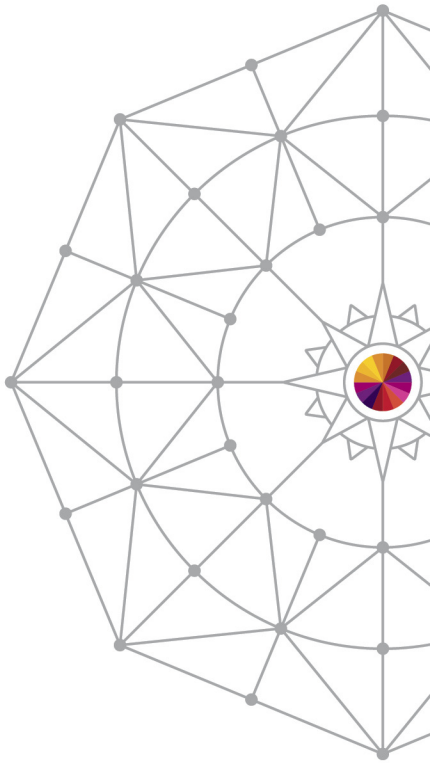
# RACF/PKI V2R1 updates

**Wai Choi, CISSP®**
**IBM Corporation**

**August 4th, 2014**
**Session:** 15666



#SHAREorg

Copyright (c) 2014 by SHARE Inc. Except where otherwise noted, this work is licensed under http://creativecommons.org/licenses/by-nc-sa/3.0/

SHARE in Pittsburgh 2014

# Trademarks

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

| | | | | |
|---|---|---|---|---|
| AIX* | Domino* | Language Environment* | SYSREXX | z10 |
| BladeCenter* | DS6000 | MVS | System Storage | z10 BC |
| BookManager* | DS8000* | ParallelSysplex* | System x* | z10 EC |
| CICS* | FICON* | ProductPac* | System z | zEnterprise* |
| DataPower* | IBM* | RACF* | System z9 | zSeries* |
| DB2* | IBM eServer | Redbooks* | System z10 | |
| DFSMS | IBM logo* | REXX | System z10 Business Class | |
| DFSMSdss | IMS | RMF | Tivoli* | |
| DFSMShsm | InfinBand | ServerPac* | WebSphere* | |
| DFSMSrmm | | | | |
| DFSORT | | | | |

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Windows Server and the Windows logo are trademarks of the Microsoft group of countries.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

* Other product and service names might be trademarks of IBM or other 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.

This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the "Authorized Use Table for IBM Machines" provided at www.ibm.com/systems/support/machine_warranties/machine_code/authtml ("AUT"). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

# Agenda

- **Common Criteria Evaluation Update**
- **RRSF**
  - Support for TCP/IP V6
  - Comments in the RACF parameter library
  - TLS 1.2 cipher suite support
- **New and improved RACF Health Checks**
  - RACF_AIM_STAGE
  - RACF_AUTOUID
  - RACF_CERTIFICATE_EXPIRATION
  - RACF_SENSITIVE_RESOURCES
  - RACF_CSFKEYS_ACTIVE
  - RACF_CSFSERV_ACTIVE
- **&RACUID in home directory path name**
- **DBUnload enhancement**
- **RACDCERT Enhancements:**
  - RACDCERT ADD update for certificate chains
  - RACDCERT LISTCHAIN new command
  - RACDCERT CHECKCERT update
  - RACDCERT GENREQ help
- **PKI Enhancements:**
  - Extended Validation Certificates
  - Granular Access Control
  - TKDS Support
  - CA Path length
  - CRL Notification
  - DB2 Custom Columns
- **Statement of direction**


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Common Criteria Update

## Common Criteria Update

# Recent Common Criteria Evaluations of Interest:

*z/OS V1.13, EAL4+, 12 September, 2012*

*z/OS V1.13/RACF, EAL5+, 27 February, 2013*

*z/VM Version 6 Release 1, EAL4+, 20 February, 2013*

*PR/SM on IBM Systems z196 GA2 z114 GA1, 1 March, 2012*

*PR/SM for IBM zEnterprise EC12 GA1 EAL5+, 19 February, 2013*

*PR/SM for IBM zEnterprise EC12 GA2/BC12 GA1 EAL5+, 19 February, 2014*

http://www.ibm.com/security/standards/security_evaluations.html **has the details**


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# RRSF

# RRSF
# Quick TCP/IP Review

- **Starting with z/OS V1.13, you can link RRSF nodes using TCP/IP instead of APPC! This means that you can now:**
  - Manage your RRSF network using the same skills as the rest of your TCP/IP network.
  - Ensure that the same network security policy (IDS, IPS, etc.) is in place for your RRSF network as in place for the rest of your z/OS TCP/IP network.
  - Utilize the encryption and peer-node authentication of AT-TLS
  - Convert a node from using APPC to TCP/IP without stopping communication
  - **Keep up with improvements in z/OS Communications Server Security.**


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# RRSF
# IPv6 Support

- **Starting with z/OS V2.1, RRSF supports the use of TCP/IP V6 for communications between/among your RRSF nodes**
  - Once the z/OS Communications Server on your local note is configured for Ipv6:
    - IPv6-format addresses will be displayed
  - You do not have to migrate to IPv6 all at once: Some “remote” nodes can be IPv4 and some IPv6.


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# RRSF
# IPv6 Addresses

| Description | IPv4 | IPv6 |
|---|---|---|
| Address length | 32 bits long (4 bytes) | 128 bits long (16 bytes).<br>64 bits for network number, 64 bits for host number |
| Total addresses | 4,294,967,296<br>(about 4.3 billion) | About 3.4 x $10^{38}$ |
| Address format in text | nnn.nnn.nnn.nnn<br>Where 0<=nnn<=255 | xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (8 hex blocks)<br>Where x is hex number.<br>Double colon (::) designates any number of 0 bits |
| Example | 9.127.42.144 | `2001:0db8:85a3:0000:0000:8a2e:0370:7334` |
| Equivalent addresses | 10.120.78.40 | `::ffff:10.120.78.40`<br>IPv4-mapped IPv6 address |
| Unspecified address | 0.0.0.0 | `::` (128 0 bits) |


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# RRSF
# TARGET LIST (V2.1)

```
NODE1  <target list node(node1)
NODE1  IRRM010I (<) RSWJ SUBSYSTEM PROPERTIES OF LOCAL RRSF NODE NODE1:
   STATE       - OPERATIVE ACTIVE
   DESCRIPTION - <NOT SPECIFIED>
   PROTOCOL    - APPC
                 LU NAME           - MF1AP001
                 TP PROFILE NAME   - IRRRACF
                 MODENAME          - <NOT SPECIFIED>
                 LISTENER STATUS   - ACTIVE
   PROTOCOL    - TCP
                 HOST ADDRESS      - ::                    <<< IPv6 default
                 IP ADDRESS        - ::FFFF:9.57.1.243     <<< IPv6 address
                 LISTENER PORT     - 18136
                 LISTENER STATUS   - ACTIVE
   TIME OF LAST TRANSMISSION TO    - <NONE>
   TIME OF LAST TRANSMISSION FROM  - <NONE>
   WORKSPACE FILE SPECIFICATION
         PREFIX                    - "NODE1.WORK"
         WDSQUAL                   - <NOT SPECIFIED>
         FILESIZE                  - 500
         VOLUME                    - TEMP01
         FILE USAGE
                 "NODE1.WORK.NODE1.INMSG"
                                   - CONTAINS 0 RECORD(S)
                                   - OCCUPIES 1 EXTENT(S)
                 "NODE1.WORK.NODE1.OUTMSG"
                                   - CONTAINS 0 RECORD(S)
                                   - OCCUPIES 1 EXTENT(S)
```

If IPv6 is enabled, addresses
Are displayed in IPv6 format

# RRSF
# TLS 1.2 Cipher Suite Support

- **RRSF uses Application Transparent Transport Layer Security (AT-TLS) to encrypt data between RRSF nodes**
  - AT-TLS supports more cryptography suites in z/OS V2.1
  - Certificates are used in AT-TLS to provide secure connections between RRSF systems using TCP/IP
  - In z/OS V2R1, ECC certificates with stronger encryption may be used
  - All cryptography suites in Transport Layer Security (TLS) Protocol Version 1.2 are supported

- **When a connection is established between 2 RRSF systems, here is an example of the informational message issued by RACF:**
  - `IRRI027I (>) RACF COMMUNICATION WITH TCP NODE NODE1 HAS BEEN SUCCESSFULLY ESTABLISHED USING CIPHER ALGORITHM C026 TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384.`


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Health Check Updates

# Health Checks: New and Updated Checks

- Automatic start for the Health Checker address space at IPL time
- New RACF Health Checks

  RACF_AIM_STAGE
  RACF_UNIX_ID

  } Help migrating from BPX.DEFAULT.USER

  RACF_CERTIFICATE_EXPIRATION

  RACF_CSFKEYS_ACTIVE

  RACF_CSFSERV_ACTIVE

  Note: BPX.DEFAULT.USER is withdrawn from V2.1 and rolled back to z/OS V1.12 and z/OS V1.13 with OA37164

- Updated RACF Check

  RACF_SENSITIVE_RESOURCES

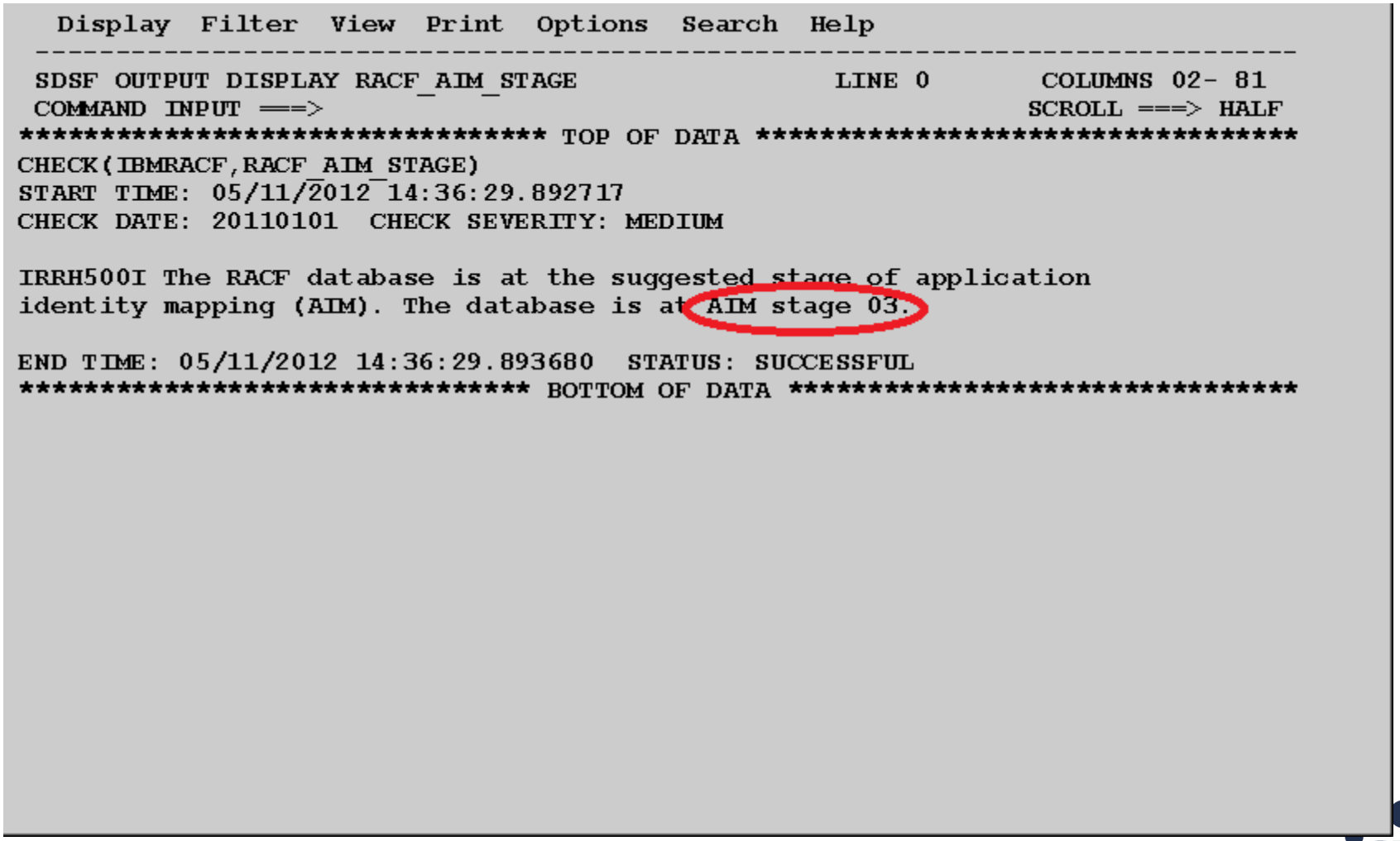
  - General resources
  - ICSF CKDS, PKDS, and TKDS data sets


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

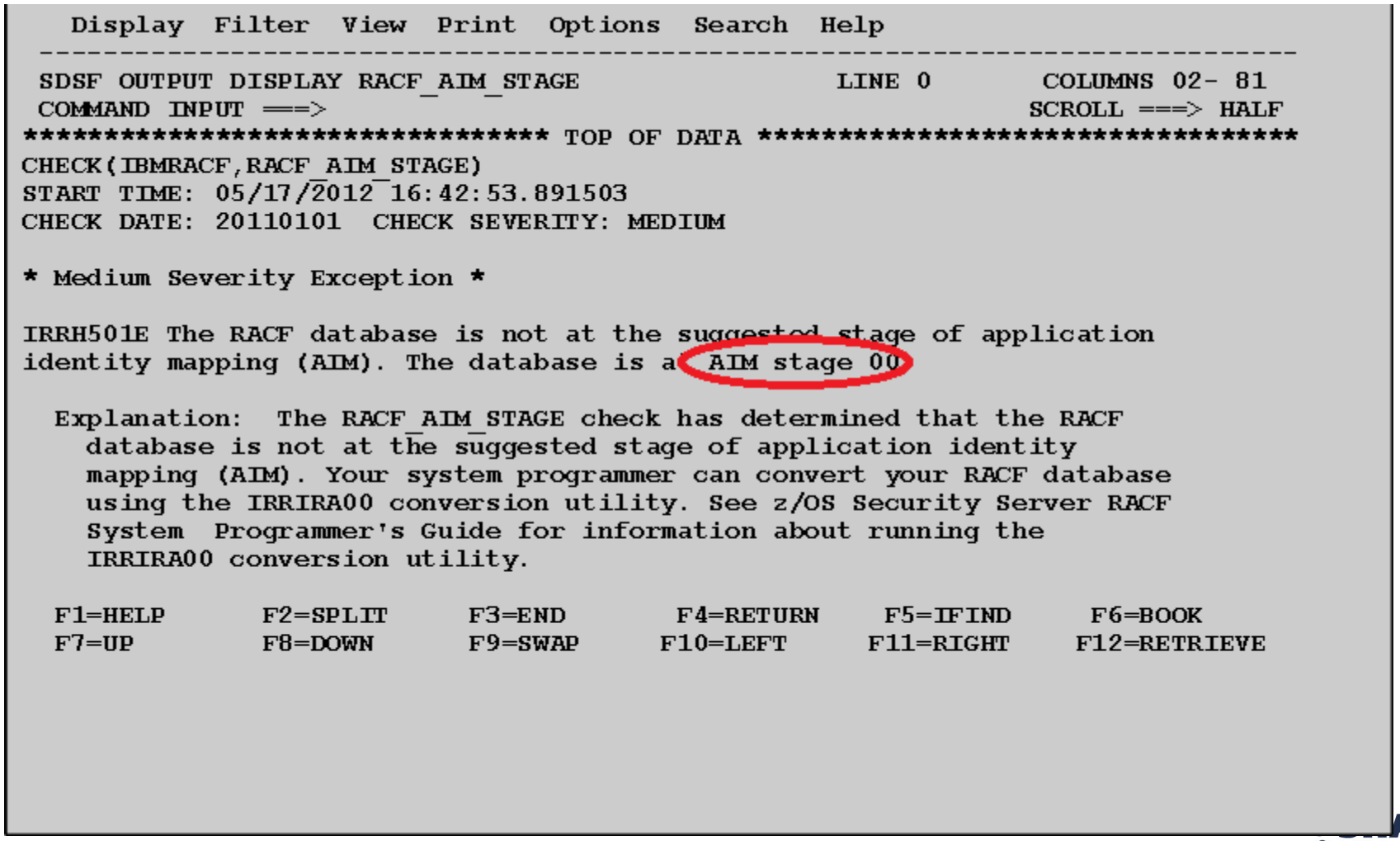
# Health Checks
# RACF_AIM_STAGE - new

- **The RACF_AIM_STAGE Health Check examines your application identity mapping (AIM) setting and flags as an exception if you are at a stage less than stage 3.**
  - Stage 0: No AIM support; only mapping profiles are used
  - Stage 1: Mapping profiles are used; alternate index created and managed, but not used
  - Stage 2: Alternate index create, managed, and used; mapping profiles maintained.
  - Stage 3: Only alternate index maintained and used. Mapping profiles deleted.
- **Moving from each stage requires the execution of the IRRIRA00 utility.**
- **AIM stage 2 or stage 3 is needed for certain RACF functions**

# Health Checks
# RACF_AIM_STAGE (OK)



# Health Checks
# RACF_AIM_STAGE (Exception)



# Health Checks
# RACF_UNIX_ID - new

- **The RACF_UNIX_ID Health Check determines whether RACF will automatically assign unique z/OS UNIX System Services identities when users without OMVS segments use certain UNIX services**
  - If you are not relying on RACF to assign UIDs and GIDs, the check informs you that you must continue to assign z/OS UNIX identities
  - If you are relying on the BPX.UNIQUE.USER support, the check will verify the following requirements and indicate if any exceptions are found
    - FACILITY class profile BPX.UNIQUE.USER must exist
    - RACF database must be at Application Identity Mapping (AIM) stage 3
    - UNIXPRIV class profile SHARED.IDS must be defined
    - UNIXPRIV class must be active and RACLISTed
    - FACILITY class profile BPX.NEXT.USER must be defined and its APPLDATA field must contain valid ID values or ranges
      - *Note: The check only lists the APPLDATA content, it does not validate it.*

# Health Checks
# RACF_UNIX_ID (OK)

```
********************************** TOP OF DATA
**********************************
CHECK(IBMRACF,RACF_UNIX_ID)
START TIME: 05/18/2012 14:12:18.914396
CHECK DATE: 20110101  CHECK SEVERITY: MEDIUM

IRRH502I RACF attempts to assign unique UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services.

Requirements for this support:

S Requirement
- ------------------------------------------------------------------------
  FACILITY class profile BPX.UNIQUE.USER is defined
  RACF database is at the required AIM stage:
    AIM stage = 03
  UNIXPRIV class profile SHARED.IDS is defined
  UNIXPRIV class is active
  UNIXPRIV class is RACLISTed
  FACILITY class profile BPX.NEXT.USER is defined
  BPX.NEXT.USER profile APPLDATA is specified (not verified):
    APPLDATA = 1000/100

IRRH506I The RACF UNIX identity check has detected no exceptions.

END TIME: 05/18/2012 14:12:18.921241  STATUS: SUCCESSFUL
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Health Checks
# RACF_UNIX_ID (Exception)

```
   Display  Filter  View  Print  Options  Search  Help
 -------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_UNIX_ID                  LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                            SCROLL ===> HALF
********************************* TOP OF DATA ***********************************
CHECK(IBMRACF,RACF_UNIX_ID)
START TIME: 05/17/2012 16:45:01.400010
CHECK DATE: 20110101  CHECK SEVERITY: MEDIUM

IRRH502I RACF attempts to assign unique UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services.

Requirements for this support:

S Requirement
- ------------------------------------------------------------------------
  FACILITY class profile BPX.UNIQUE.USER is defined
E RACF database is not at the required AIM stage:
    AIM stage = 00
E UNIXPRIV class profile SHARED.IDS is not defined
E UNIXPRIV class is not active
E UNIXPRIV class is not RACLISTed
E FACILITY class profile BPX.NEXT.USER is not defined

* Medium Severity Exception *

IRRH503E RACF cannot assign unique UNIX IDs when users or groups that
do not have OMVS segments use certain z/OS UNIX services. One or more
requirements are not satisfied.

  Explanation:  The RACF UNIX identity check has determined that you
    want RACF to assign unique UNIX IDs when users or groups without
    OMVS segments use certain z/OS UNIX services. However, RACF is not
    able to assign unique UNIX identities for z/OS UNIX services because
    one or more of the following requirements are not satisfied:
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Health Checks
# RACF_CERTIFICATE_EXPIRATION - new

- **The RACF_CERTIFICATE_EXPIRATION health check finds the certificates in the RACF database expired or about to expire**
  - Expiration window is an installation-defined value with a default of 60 days.
  - Valid expiration window values are 0-366 days
- **For each certificate, the check displays:**
  - The certificate “owner” ('SITE', 'CERTAUTH', or 'ID(*user_id*)')
  - The certificate label
  - The end date
  - The trust status
  - The number of rings to which the certificate is connected
- **The check only flags as exceptions those certificates which are TRUSTED.**

# Health Checks
# RACF_CERTIFICATE_EXPIRATION (OK)

```
CHECK(IBMRACF,RACF_CERTIFICATE_EXPIRATION)
START TIME: 01/23/2012 08:10:01.603497
CHECK DATE: 20111010  CHECK SEVERITY: MEDIUM



                    Certificates Expiring in 60 Days



S Cert Owner   Certificate Label                 End Date   Trust Rings
- ------------ -------------------------------- ---------- ----- -----



IRRH277I No exceptions are detected. Expired certificates that are not
trusted or are associated with only a virtual key ring are not
exceptions.



END TIME: 01/23/2012 08:10:01.643285  STATUS: SUCCESSFUL
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Health Checks
# RACF_CERTIFICATE_EXPIRATION (Exception)

```
CHECK(IBMRACF,RACF_CERTIFICATE_EXPIRATION)
START TIME: 02/28/2013 09:23:37.747549
CHECK DATE: 20111010  CHECK SEVERITY: MEDIUM

                  Certificates Expiring within 60 Days

S Cert Owner    Certificate Label                 End Date   Trust Rings
- ------------ -------------------------------- ---------- ----- -----
E CERTAUTH      VERISIGN CLASS 1 INDIVIDUAL       2008-05-12 Yes     0
E ID(MARKN)     MARK-001                          2012-11-11 Yes     0
E ID(MARKN)     MARK0001                          2012-11-05 Yes     0
  ID(CERTAUTH)  START_OFF_M001__END_OFF_M001       2012-01-25 No      0
  ID(MARKN)     START_OFF_M001__END_OFF_M001       2012-01-25 No      0
  ID(SITE)      START_OFF_M001__END_OFF_M001       2012-01-25 No      0
  CERTAUTH      START_OFF_M365__END_OFF_M001       2012-01-25 No      0
  ID(CERTAUTH)  START_OFF_M365__END_OFF_M001       2012-01-25 No      0
  CERTAUTH      ICP-Brasil CA                     2011-11-30 No      0
  CERTAUTH      MICROSOFT ROOT AUTHORITY - 01     2002-12-31 No      0
  CERTAUTH      VERISIGN CLASS 3 PUBLIC           2004-01-07 No      0
  CERTAUTH      VERISIGN CLASS 2 PUBLIC           2004-01-06 No      0

* Medium Severity Exception *

IRRH276E One or more certificates expired or are expiring within
the warning period.

  Explanation:  The RACF_CERTIFICATE_EXPIRATION check found one or more
    certificates that expired or are expiring within the warning period.
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Health Checks
# RACF_CSFKEYS_ACTIVE - new
# RACF_CSFSERV_ACTIVE - new

```
********************************** TOP OF DATA **********
CHECK(IBMRACF,RACF_CSFKEYS_ACTIVE)
SYSPLEX:     CFCIMGUK  SYSTEM: DCEIMGUK
START TIME: 07/17/2014 09:30:00.741474
CHECK DATE: 20140106  CHECK SEVERITY: MEDIUM
CHECK PARM: CSFKEYS

IRRH228I The class CSFKEYS is active.

END TIME: 07/17/2014 09:30:00.742052  STATUS: SUCCESSFUL
********************************** BOTTOM OF DATA *********
```

Class not active ->
No protection!!!

```
********************************** TOP OF DATA **********
CHECK(IBMRACF,RACF_CSFSERV_ACTIVE)
SYSPLEX:     CFCIMGUK  SYSTEM: DCEIMGUK
START TIME: 07/31/2014 08:46:38.218119
CHECK DATE: 20140106  CHECK SEVERITY: MEDIUM
CHECK PARM: CSFSERV

* Medium Severity Exception *

IRRH229E The class CSFSERV is not active.

  Explanation:  The class is not active. IBM recommends that the
    security administrator evaluate the need for this class, define
    profiles in it as appropriate, and activate the class.
```

# Health Checks
# RACF_SENSITIVE_RESOURCES - updated

- **The RACF_SENSITIVE_RESOURCES check has been updated to check these new "static" resources names:**
  - BPX.DEBUG/FACILITY
  - BPX.WLMSERVER/FACILITY
  - IEAABD.DMPAKEY/FACILITY
  - MVS.SLIP/OPERCMDS
  - SUPERUSER.PROCESS.GETPSENT/UNIXPRIV
  - SUPERUSER.PROCESS.KILL/UNIXPRIV
  - SUPERUSER.PROCESS.PTRACE/UNIXPRIV

# Health Checks
# RACF_SENSITIVE_RESOURCES - updated

- **The RACF_SENSITIVE_RESOURCES check has been updated check these new "dynamic" resources names:**
  - CSVAPF.*data_set_name*/FACILITY, excluding
    - CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC
  - CSVDYLPA.ADD.*module_name*/FACILITY
  - CSVDYNEX.*exit_name.function.modname*/FACILITY, *excluding*
    - *CSVDYNEX.LIST*
    - *CSVDYNEX.exit_name.*RECOVER
    - CSVDYNEX.exit_name.CALL
  - CSVDYNL.*lnklstname. Function*/FACILITY*excluding*
    - CSVDYNL.*lnklstname*.DEFINE CSVDYNL.*lnklstname.*UNDEFINE)
- **No validation is performed on the dynamic portion of these resource names (for example *data_set_ name, module_name,lnklstname*)**


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Health Checks
# RACF_SENSITIVE_RESOURCES - updated

Sensitive General Resources Report

| S | Resource Name | Class | UACC | Warn | ID* | User |
|---|---|---|---|---|---|---|
| | <existing resources> | | | | | |
| | BPX.WLMSERVER | FACILITY | Updt | No | **** | |
| | CSVAPF.RACFDEV.DISCRETE.NONE.LOAD | FACILITY | None | No | **** | |
| | CSVAPF.RACFDEV.DISCRETE.READ.LOAD | FACILITY | Read | No | **** | |
| E | CSVAPF.RACFDEV.DISCRETE.UPDATE.LOAD | FACILITY | Updt | No | **** | |
| | CSVAPF.RACFDEV.**.NONE.LOAD | FACILITY | None | No | **** | |
| | CSVAPF.RACFDEV.**.READ.LOAD | FACILITY | Read | No | **** | |
| E | CSVAPF.RACFDEV.**.UPDATE.LOAD | FACILITY | Updt | No | **** | |
| E | CSVDYLPA.ADD.MODULE001 | FACILITY | Updt | No | **** | |
| E | CSVDYLPA.DELETE.MODULE01 | FACILITY | Updt | No | **** | |
| E | CSVDYLPA.ADD.* | FACILITY | Updt | No | **** | |
| E | CSVDYLPA.DELETE.* | FACILITY | Updt | No | **** | |
| | CSVDYNEX.EXITNAME_READ.MODNAME01 | FACILITY | Read | No | **** | |
| E | CSVDYNEX.EXITNAME_UPDATE.DEFINE | FACILITY | Updt | No | **** | |
| E | CSVDYNEX.EXITNAME_UPDATE.MODNAME01 | FACILITY | Updt | No | **** | |
| E | CSVDYNEX.*.DEFINE | FACILITY | Updt | No | **** | |
| E | CSVDYNEX.*.MODNAME01 | FACILITY | Updt | No | **** | |
| E | CSVDYNEX.* | FACILITY | Updt | No | **** | |
| E | IEAABD.DMPAKEY | FACILITY | Read | No | **** | |
| E | IEAABD.DMPAUTH | FACILITY | Read | No | **** | |

# Health Checks
# RACF_SENSITIVE_RESOURCES - updated

- **The RACF_SENSITIVE_RESOURCES check has been updated check these ICSF datasets:**
  - CKDS
  - PKDS
  - TKDS
- **If ICSF has not been started, informational message "IRRH242I: ICSF has not been started on this system" is issued and the check continues processing.**
- **Any access to these datasets raises an exception.**


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# &RACUID and BPX.UNIQUE.USER

# &RACUID in BPX.UNIQUE.USER

- **Clients who are using BPX.UNIQUE.USER to assign z/OS UNIX information to user IDs will be able to specify specification of &racuid in the home directory field of the model user's OMVS segment.**
  - `RDEF FACILITY BPX.UNIQUE.USER APPLDATA('BPXMODEL')`
  - `ADDUSER BPXMODEL OMVS(HOME(/u/&racuid))`
- **The appropriate user ID will be substituted for &racuid in the home directory when a new OMVS segment is created for a user using BPX.UNIQUE.USER, the substituted string will be**
  - in upper case if "&RACUID" is specified in upper case
  - in lower case if "&Racuid" is specified with any lower case characters
- **Notes**
  - Roll back to z/OS V1.12 – OA42554
  - Only the first occurrence of &racuid is substituted
  - If the substitution would result in a path name exceeding the 1023 character maximum then substitution is not performed.
  - If sharing the RACF database with a downlevel system, substitution will not be performed on the downlevel system

# Certificate Distinguished Names in IRRDBU00 Output

# IRRDBU00: Additional Certificate Information

- **The RACF Database Unload Utility (IRRDBU00) unloads basic information about digital certificates into the 0560 (“General Resource Certificate Data Record”).**
- **A new record type (“1560”) is added to contain:**
  - The issuer's distinguished name
  - The subject's distinguished name
  - The hashing algorithm used for the signing the certificate
- **The “1560” record links to the “0560” record using the profile name**
  - DFSORT's JOINKEY operator can be used when processing IRRDBU00 output
- **The Mapping of the1560 Record is:**

| | | Position | | |
|---|---|---|---|---|
| **Field Name** | **Type** | **Start** | **End** | **Comments** |
| CERTN_RECORD_TYPE | Int | 1 | 4 | Record type of the certificate information record (1560). |
| CERTN_NAME | Char | 6 | 251 | General resource name as taken from the profile name. |
| CERTN_CLASS_NAME | Char | 253 | 260 | Name of the class to which the general resource profile belongs. |
| CERTN_ISSUER_DN | Char | 262 | 1285 | Issuer’s distinguished name. (1024 characters) |
| CERTN_SUBJECT_DN | Char | 1287 | 2310 | Subject’s distinguished name. (1024 characters) |
| CERTN_SIG_ALG | Char | 2312 | 2327 | Certificate signature algorithm. Valid values are md2RSA, md5RSA, sha1RSA, sha1DSA, sha256RSA, sha224RSA, sha384RSA, sha512RSA, sha1ECDSA, sha256ECDSA, sha224ECDSA, sha384ECDSA, sha512ECDSA, and UNKNOWN. |

# RACDCERT Enhancements

# RACDCERT ADD enhancement

- When importing a **PKCS#12** or **PKCS#7** certificate chain using the RACDCERT ADD command, only the end entity certificate can be named using a specified label.
  - RACDCERT generates labels for the rest of the certificates in the chain, but previously **did not display what labels** had been added.
  - Starting in V2R1, RACDCERT will **display the generated labels** of any certificates in the chain that were added.

```
RACDCERT ID(CHOI) ADD('CHOI.CERTS.MYPKCS12') WITHLABEL('MyCert')
Certificate with label 'MyCert' is added under ID CHOI
Certificate with label 'LABEL00000002' is added under CERTAUTH
Certificate with label 'LABEL00000003' is added under CERTAUTH
```


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# RACDCERT LISTCHAIN - New

- **RACDCERT LISTCHAIN Syntax:**

  RACDCERT [ ID(certificate-owner)| SITE | CERTAUTH]
  LISTCHAIN (LABEL('label-name'))

- Information provided:
  - Certificate details for the specified certificate
  - Details for each issuing certificate which is in RACF
  - Summary of the Chain:
    - Number of certificates in the chain
    - Whether RACF contains the complete chain
      - *– chain is complete*
      - *– chain is incomplete*
    - Indication of expired certificate(s), if any
      - *– chain contains expired certificate(s)*
    - List of rings that all certificates in chain share

# RACDCERT LISTCHAIN Example

```
RACDCERT LISTCHAIN(LABEL('samplecert'))

Certificate 1:
  Digital certificate information for user CHOI:
  Label: samplecert
  ...
  Ring Associations:
    Ring Owner: COOPER
    Ring:
      >testring<

Certificate 2:
  Digital certificate information for CERTAUTH:
  Label: sampleCA
  ...
  Ring Associations:
  Ring Owner: COOPER
  Ring:
  >testring<
```

```
Certificate 3:
  Digital certificate information for CERTAUTH:
  Label: MasterCA
  ...
  Ring Associations:
  Ring Owner: COOPER
  Ring:
    >testring<

Chain information:
  Chain contains 3 certificate(s), chain is complete
  Chain contains ring in common: COOPER/testring
```

# RACDCERT CHECKCERT

- RACDCERT CHECKCERT enhancement:
  - LISTCHAIN is used to list certificates in RACF, while CHECKCERT is to list certificates in a dataset (which is going to be an input to the RACDCERT ADD)
  - Enhancements similar to LISTCHAIN were added to the display text of RACDCERT CHECKCERT, when displaying information on a certificate in a dataset.

# RACDCERT GENREQ

- Generating a Certificate Request (CSR) from RACDCERT GENREQ requires an existing certificate in RACF with a private key (usually a self signed certificate created with GENCERT).
- Don't delete that cert!
  - A common issue encountered by RACDCERT users, is deleting the original certificate from RACF after the CSR has been generated... erroneously concluding that the certificate had no use.
  - If the original certificate is deleted from RACF after the CSR is created, the private key is also deleted, rendering any signed certificate based on this CSR useless (oops!).
- We can help!
  - Starting in V2R1 RACDCERT will prevent the deletion of a certificate that has been used for generating a request with GENREQ.
  - Force override mechanism is provided to delete this certificate when needed

# Secure TKDS Support

- Unlike the keys stored in the Public Key Data Set (PKDS), the keys stored in the Token Key Data Set (TKDS) are clear keys, not secure keys.
- "**Secure Key**" means that sensitive key material is always wrapped under a master key.
- In Web Deliverable #12, ICSF supports secure key on TKDS.
- To enable the applications to use the secure key in TKDS, RACF, PKI Services and System SSL need to be updated accordingly.

# RACF
# Secure TKDS Support

- RACDCERT can create a secure key on a specified PKCS#11 token on TKDS during certificate creation
- New sub keyword TOKEN is added to GENCERT and REKEY to indicate the generation of secure TKDS key. For example: to generate a certificate with RSA key stored in a token called MY.PKCS11.TOKEN1 in TKDS

  RACDCERT GENCERT SUB(CN('Company A')) WITHLABEL('New RSA cert')
  RSA(TOKEN(MY.PKCS11.TOKEN1))

  **Note:** RACDCERT EXPORT can not export any secure key neither from PKDS or TKDS
- The R_datalib callable service can return this label from RACF


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Secure TKDS Support
# Clear Key Restriction

- ICSF can now restrict use of TKDS clear keys:
  - With WD#12, ICSF checks a new RACF resource profile in the CRYPTOZ class to restrict the use of clear keys in the PKCS#11 services
    - CLEARKEY.<token-label>

- Insufficient access to CLEARKEY.SYSTOK-SESSION-ONLY will cause the failure on the generation of clear TKDS key from RACDCERT

  Note: SYSTOK-SESSION-ONLY is an ICSF predefined temporary token name


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# PKI Services Enhancements

# PKI Services
# Secure TKDS Support

- PKI Services can issue certificates with key pairs created in ICSF and with the private key stored in the TKDS.
- Starting in V2R1, PKI Services can create **secure** keys in the TKDS during certificate creation and return a PKCS#12 package containing the secure key to the requestor
- Provides better security on the key generation capability in PKI Services
- PKI Service configuration (pkiserv.conf):
  - Specify T for the **SecureKey** entry in the PKI Services configuration file to enable secure key generation:

    [SAF]

    ...

    TokenName=PKISRVD.PKIToken

    **SecureKey=T**
- Insufficient access to CLEARKEY.<token specified in pkiserv.conf> will cause unexpected result on key generation from PKI Services even if no configuration update is made to have the new secure key support


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# PKI Services
# Extended Validation Certificates

- An Extended Validation Certificate (EV) is an X.509 certificate issued according to a specific set of identity verification criteria.
- These criteria require extensive verification of the requesting entity's identity by the certificate authority (CA).
- In V2R1 PKI Services is adding support for the relative distinguished names (RDN) that are required by Extended Validation certificates:
  - **businessCategory** (2.5.4.15) - Required
  - **jurisdictionOfIncorporationCountryName** (1.3.6.1.4.1.311.60.2.1.3) - Required
  - **jurisdictionOfIncorporationStateOrProvinceName** (1.3.6.1.4.1.311.60.2.1.2) - Optional
  - **jurisdictionOfIncorporationLocalityName** (1.3.6.1.4.1.311.60.2.1.1) - Optional

# PKI Services
# Granular Administrative Access Control

- Prior to V2R1, all PKI Administrators have full control over a single PKI CA domain.
- Starting in V2R1, PKI Services adds granular administration authorization control:
  - Enables multiple PKI Services administrators to perform different actions on different types of certificates within a domain.
  - An administrator can be authorized to approve a server digital certificate, but not be authorized to approve a SCEP digital certificate.
- Authorization is based on the domain, action and the template:
  - A switch is provided to turn on this granular check
  - A new class PKISERV is created for resources used by different types of administration functions
  - If granular checking is on, these resources will be checked, in addition to the existing authority check on the administrative functions
  - Example:
    - READ access to
      - *MYDOMAIN.QUERYREQS.1YBSSL and MYDOMAIN.QUERYCERTS.1YBSSL*
    - Allow the administrator to perform QUERYREQS and QUERYCERTS on the requests and certificates respectively, created with the '1-Year PKI SSL Browser Certificate' template in domain named MYDOMAIN.

# PKI Services
# Granular Administrative Access Control

- Enabling Granular Administrative Access Control:
- Set up new protection profiles in the new PKISERV class
- If setting up a new instance of PKI Services, update the IKYSETUP set up script:
  - PKI Services IKYSETUP (A REXX script to set up authorization for PKI)
    - Specify **AdminGranularControl** equals 1 to set up granular control
    - Provide the template nick names you want to act on and assign the corresponding administration groups for setting up new profiles in the **PKISERV** class
- PKI Services configuration (pkiserv.conf):
  - Specify T for the **AdminGranularControl** entry in the PKI Services configuration file, to enable granular control:

**AdminGranularControl = T**


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# PKI Services
# DB2 Custom Columns

- PKI Services certificate requests and issued certificates are stored in either VSAM or optionally DB2.
- Prior to V2R1, PKI Services installations are unable to add custom columns to the PKI DB2 tables.
- In V2R1 PKI Services is enhanced to allow installations to add custom columns to the PKI DB2 tables.
  - This capability was restricted by the SQL processing in the PKI Services daemon
  - Enhance the SQL processing on the backend tables to facilitate DB2 customization

- Enables customers who uses DB2 as the PKI backend stores to add their own customized columns in the tables which are used by PKI internal processing


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# PKI Services
# CA Path Length Enforcement

- PKI Services can issue intermediate Certificate Authority certificates. All CA Certificates must contain the Basic Constraints extension, which identifies:
  - Whether the certificate is a CA (required)
  - The maximum depth of the certification path (optional)
- PKI Services only create the CA indication field, but not the path length value. Although it is optional, many customers would like to have that value set to control the number of CAs that can follow
- Starting in V2R1 PKI Services can optionally create the path length value in the Basic Constraints extension.
- This allows a CA to restrict a subordinate CA from signing another subordinate CA through the path length constraint value.


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# PKI Services
# CRL Notification

- PKI Services can create Certificate Revocations Lists (CRLs) on regular intervals and post them to LDAP or an HTTP server.
- Starting in V2R1 PKI Services can be configured to optionally issue console message when CRL processing ends:
  - **IKYP044I** CRL number *crl-serial-number* processing for CA domain ca-domain completed successfully
  - **IKYP045I** CRL number *crl-serial-number* processing for CA domain ca-domain failed
  - CRL Notification console messages are optional

- A console message for CRL completion can act as a trigger for some automation processing, eg. CRLs can be saved for either legal reasons or a matter of policy


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# RACF Statement of Direction

# z/OS V2.1 RACF Statement of General Direction

## Enhanced RACF password encryption algorithm:

In the future, an enhanced RACF password encryption algorithm is planned. This support will be designed to provide improved cryptographic strength in RACF password algorithm processing. This will be intended to help protect RACF password data in the event that a copy of a RACF database becomes inadvertently accessible.


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Helpful Publications

- SA22-7691 - z/OS Security Server RACF Callable Services
- SA22-7687 - z/OS Security Server RACF Command Language Reference
- GA22-7680 - z/OS Security Server RACF Data Areas
- SA22-7682 - z/OS Security Server RACF Macros and Interfaces
- SA22-7686 - z/OS Security Server RACF Messages and Codes
- SA22-7683 - z/OS Security Server RACF Security Administrator's Guide
- SA22-7681 - z/OS Security Server RACF System Programmer's Guide
- SA22-7692 - z/OS Security Server RACROUTE Macro Reference
- GA22-7689 - z/OS Security Server RACF Diagnosis Guide
- SA22-7693 - z/OS Cryptographic Services PKI Services Guide and Reference
- SC24-5901 - z/OS Cryptographic Services System Secure Sockets Layer Programming
- SA23-2231 - z/OS ICSF Writing PKCS #11 Applications
- SA22-7807 - z/OS UNIX System Services: Messages and Codes
- SA22-7803 - z/OS UNIX System Services Programming: Assembler Callable Services Reference
- SC31-8775 - z/OS Communication Server: IP Configuration Guide
- GC31-8782 - z/OS Communication Server: IP Diagnosis Guide
- SC31-8781 - z/OS Communication Server: IP System Administrator's Commands
- SA22-7994 - IBM Health Checker for z/OS User's Guide


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# Background: z/OS V1.13 Statement of Direction BPX.DEFAULT.USER

# Statement of Direction

**z/OS V1.13 is planned to be the last release to support BPX.DEFAULT.USER. IBM recommends that you either use the BPX.UNIQUE.USER support that was introduced in z/OS V1.11, or assign unique UIDs to users who need them and assign GIDs for their groups.**

From *Preview: z/OS Version 1 Release 13 and z/OS Management Facility Version 1 Release 13 are planned to offer new availability, batch programming, and usability functions (*IBM United States Software Announcement 211-007, February 15, 2011)

# z/OS V1.13 Statement of Direction…

- **Background: Assigning UID and GIDs**
  - **RACF 2.1 (1994):** Introduced OMVS segments for USERs and GROUPs.
    - Users with an OMVS segment could now use “Open MVS” (now z/OS UNIX System Services)
  - **OS/390 R2.4 (1997**): Introduced BPX.DEFAULT.USER FACILITY class profile
    - Allows assigning UIDs and GIDs to users and groups who do not have OMVS segments;

***One UID and one GID shared by all default users***


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval

# z/OS V1.13 Statement of Direction…

- ***Background: Assigning UID and GIDs…***
  - **z/OS V1.4 (2002):** Introduced AUTOUID/AUTOGID keyword on ADDUSER, ALTUSER, ADDGROUP, ALTGROUP
    - RACF could now find the next available UID or GID using the BPX.NEXT.USER profile in the FACILITY class
    - Required enabling RACF Alternate Index Mapping ("AIM") to stage 2
      - *Limitation of 129 eight-character users sharing one UID*
      - *Required running migration utility ("IRRIRA00")*
  - **z/OS V1.11 (2009):** Automatic generation of OMVS segment for USERs and groups
    - Built upon AUTOUID/AUTOGID
    - Requires AIM stage 3
    - Uses the BPX.UNIQUE.USER profile in the FACILITY class

# z/OS V1.13 Statement of Direction (RACF)…

***What this means to you:***

- If you are using BPX.UNIQUE.USER then:
  - You are not using BPX.DEFAULT.USER (even if it is defined)
  - This SoD has no impact to you.

- If you are already assigning UIDs and GIDs to all users using z/OS UNIX System Services by assigning OMVS segments to all necessary users and groups, then:
  - You must continue to assign all new users and groups OMVS segments

- If you are already assigning UIDs and GIDS to all users using z/OS UNIX System Services by defining OMVS segments using AUTOUID/AUTOGID (which uses BPX.NEXT.USER) then:
  - You are already using AIM at a minimum of stage 2
  - You must continue to assign all new users and groups OMVS segments

- If you are using only BPX.DEFAULT.USER
  - You must either move to the automatic generation of OMVS user and group segments or assign OMVS user and group segments to all necessary users and groups

# z/OS V1.13: Health Check – Default UNIX ID

```
    Display  Filter  View  Print  Options  Search  Help
 -------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY ZOSMIGV2R1_DEFAULT_UNIX_ID    LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                           SCROLL ===> HALF
********************************* TOP OF DATA ***********************************
CHECK(IBMRACF,ZOSMIGV2R1_DEFAULT_UNIX_ID)
START TIME: 05/11/2012 14:38:04.920543
CHECK DATE: 20110101  CHECK SEVERITY: LOW

IRRH504I RACF is not enabled to assign UNIX IDs when users or groups
that do not have OMVS segments use certain z/OS UNIX services. If you
choose not to define UNIX IDs for each user of UNIX functions, you can
enable RACF to automatically generate unique UNIX UIDs and GIDs for you.

END TIME: 05/11/2012 14:38:04.921996  STATUS: SUCCESSFUL
******************************** BOTTOM OF DATA *********************************
```

- ***This is a migration check!***
  - Note the name: ZOSMIGV2R1.....This check is to prepare you to identify issues when you migrate to z/OS V2.1
  - Shipped INACTIVE;  you activate when you start your V2.1 migration planning


Complete your session evaluations online at www.SHARE.org/Pittsburgh-Eval