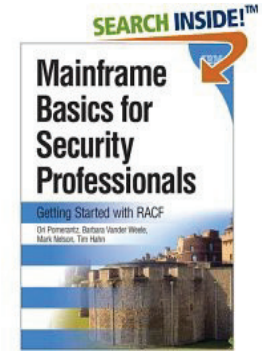
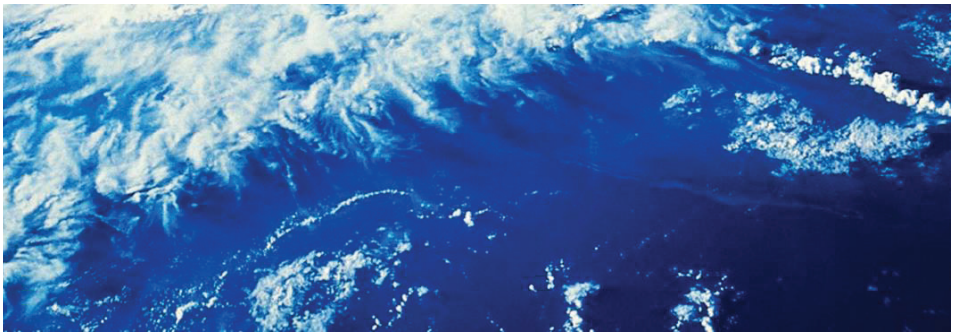
The Joy of JOINKEYS

NY RACF® Users Group
12 March 2013

Mark Nelson, CISSP®, CSSLP®
markan@us.ibm.com





Trademarks

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

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

* 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/aut.html ("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.

New Certificate Distinguished Information in IRRDBU00

- **Since OS/390® R4, RACF has stored digital certificates in the RACF data base**
  - Stored as profiles in the DIGTCERT class
  - Profile name is a “munged” version of the certificate issuer and serial #
- **The issuer's distinguished name (IDN) and subject's distinguished name (SDN) are stored as opaque data within the DIGTCERT profile**
  - To get the IDN and SDN, the certificate has to be extracted and decoded
- **With z/OS® V2.1, the RACF Database Unload Utility now unloads the issuers distinguished name and the subjects distinguished**
  - Unloaded into the new 1560 record
  - “Additional information” for the 0560 record
  - The profile name and class link the 1560 record to the other 05xx records
- **How can these records be joined using DFSORT™? JOINKEYS!**

JOINKEYS

- **JOINKEYS was introduced to DFSORT in November, 2009:**
  - UK51706 for z/OS DFSORT V1R5 PTF
  - UK51707 for z/OS DFSORT V1R10
- **JOINKEYS allows you easily to create joined records in a variety of ways including inner join, full outer join, left outer join, right outer join, and unpaired combinations.**
- **The data for the JOINKEYS is in two input DD names**
  - The two input DD names can be of different types (fixed, variable, VSAM, and so on)
  - The keys (common fields) can be in different locations in the record
  - The two DD names can point to the same data set
- **There are three control statements for a JOINKEYS operation:**
  - **JOINKEYS**: You must specify **two** JOINKEYS statements, one for each input file, specifying:
    - The DD name of the file
    - The length and sequence of the keys in the file
    - Indicate whether the file is already sorted by those keys,
  - **JOIN** (optional): Defines the type of join. Defaults to “inner”
  - **REFORMAT** (optional for JOIN ONLY) **:** Defines the fields that you want in the joined records. You can also request an indicator of where the key was found ('B' for both files, '1' for file 1 only or '2' for file 2 only).and a fill character for missing bytes.

The Types of Joins

- **Consider two tables**
  - One which contains baseball players names and a team ID
  - One which contains the team ID and the name of the team

Player	Team ID
Kranepool, Ed	NYM
Berra, Yogi	NYY
Gaedel, Eddie	SLB

Team ID	Name
NYM	NY Mets
NYY	NY Yankees
SFG	SF Giants

- **JOINKEYS allows you to create these JOINs**
  - **Inner join:** (Default) Only the paired records from (Kranepool, Berra)
  - **Left outer join:** The player records (Kranepool, Berra, Gaedel)
    - NAME will be blank for Gaedel
  - **Right outer join**: The team ID records
    - Player will be blank for SF Giants
  - **Full outer join:** All records
    - Player will be blank for SF Giants
    - NAME will be blank for Gaedel
  - **Unpaired players** (Gaedel)
  - **Unpaired teams** (SFG)
  - **All unpaired** (Gaedel, SFG)

Sample JOINKEYS Job

```
//STEP0100 EXEC PGM=SORT
//SYSOUT   DD SYSOUT=*
//INA      DD *
----+----1----+----2----+----3----+----4
KRANEPOOL, ED                 NYM
BERRA, YOGI                   NYY
GAEDEL, EDDIE                 SLB
//INB      DD *
NYM NY METS
NYY NY YANKEES
SFG SF GIANTS
//SORTOUT  DD SYSOUT=*
//SYSIN    DD *
  OPTION COPY
  JOINKEYS F1=INA,FIELDS=(31,3,A)
  JOINKEYS F2=INB,FIELDS=(01,3,A)
  REFORMAT FIELDS=(F1:1,35,F2:5,15)
//*

The output would be:


----+----1----+----2----+----3----+----4----+----5
KRANEPOOL, ED                 NYM  NY METS
BERRA, YOGI                   NYY  NY YANKEES
```

The New 1560 Record

- **A new record type (“1560”) is planned 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 the 1560 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.

The Existing 0560 Record

- **The Mapping of the existing 0560 Record is:**

		Position		
Field Name	**Type**	**Start**	**End**	**Comments**
GRCERT_RECORD_TYPE	Int	1	4	Record type of the Certificate Data Record (0560)
GRCERT_NAME	Char	6	251	General resource name as taken from the profile name.
GRCERT_CLASS_NAME	Char	253	260	Name of the class to which the profile belongs.
GRCERT_START_DATE	Date	262	271	The date from which this certificate is valid.
GRCERT_START_TIME	Time	273	280	The time from which this certificate is valid.
GRCERT_END_DATE	Date	282	291	The date from which this certificate is no longer valid
GRCERT_END_TIME	Time	293	300	The time from which this certificate is no longer valid.
GRCERT_KEY_TYPE	Char	302	309	The type of key associated with the certificate.
GRCERT_KEY_SIZE	Int	311	320	The size of private key associated with the certificate.
GRCERT_LAST_SERIAL	Char	322	337	The hexadecimal representation of the low-order eight-bytes of the serial number last signed with this key.
GRCERT_RING_SEQN	Int	339	348	A sequence number for certificates within the ring.

JOINKEYS to Join 1560 and 0560 Records

```
//MARKNSRT  JOB CLASS=A,MSGCLASS=H,NOTIFY=&SYSUID,MSGLEVEL=1
//DS$STAND  EXEC PGM=SORT
//SYSOUT    DD SYSOUT=*
//SORTJNF1  DD DISP=SHR,DSN=MARKN.TEST.IRRDBU00
//SORTJNF2  DD DISP=SHR,DSN=MARKN.TEST.IRRDBU00
//SORTOUT   DD SYSOUT=*
//*--------------------------------------------------------------------
//* Remember: The IRRDBU00 Output is VB! Add +4 to all of the starting
//* positions documented in RACF Macros and Interfaces (SA22-7682)
//*--------------------------------------------------------------------
//SYSIN     DD *
 JOINKEYS FILE=F1,FIELDS=(10,246,A,257,8,A)
 JOINKEYS FILE=F2,FIELDS=(10,246,A,257,8,A)

 REFORMAT FIELDS=(F1:266,20,286,20,
                  F2:2316,16,266,1025,1291,1025)
 OPTION COPY
```


JOINKEYS to Join 1560 and 0560 Records....

```
 OUTFILE HEADER2=(50:'Certificates in the RACF Data Base',
         /,
         58:'Prepared on ',DATE,//,
         63:'at ',TIME,//,
        105:'Page:',PAGE=(EDIT=(TTT)),3/,

         01:'Subject DN',
         76:'Start',
         96:'End',/,
         01:'Issuer  DN',
         76:'Date',
         87:'Time',
         96:'Date',
        107:'Time',
        116:'Key Type',/,
         01:74'-',
         76:10'-',
         87:08'-',
         96:10'-',
        107:08'-',
        116:15'-'),
  BUILD=(01:57,74,/01:1082,74,76:1,20,21,20,41,16,/)
/*
```

JOINKEYS to Join 1560 and 0560 Records...

```
//JNF1CNTL   DD *
    OPTION   VLSHRT
       INCLUDE COND=(5,4,CH,EQ,C'0560')
/*
//JNF2CNTL   DD *
  OPTION   VLSHRT
     INCLUDE COND=(5,4,CH,EQ,C'1560')
/*
```


JOINKEYS to Join 1560 and 0560 Records....

```
                                          Certificates in the RACF Data Base
                                                 Prepared on 12/24/12
                                                    at 14:14:46
                                                                                                Page:001
Subject DN                                                            Start               End
Issuer  DN                                                            Date       Time     Date       Time     Key Type
--------------------------------------------------------------------- ---------- -------- ---------- -------- ---------------
OU=Class 1 Public Primary Certification Authority.O=VeriSign, Inc..C=US
CN=VeriSign Class 1 CA Individual Subscriber-Persona Not Validated.OU=www. 1998-05-12 00:00:00 2008-05-12 23:59:59 md2RSA

personal-basic@thawte.com.CN=Thawte Personal Basic CA.OU=Certification Ser
personal-basic@thawte.com.CN=Thawte Personal Basic CA.OU=Certification Ser 1996-01-01 00:00:00 2020-12-31 23:59:59 md5RSA

personal-freemail@thawte.com.CN=Thawte Personal Freemail CA.OU=Certificati
personal-freemail@thawte.com.CN=Thawte Personal Freemail CA.OU=Certificati 1996-01-01 00:00:00 2020-12-31 23:59:59 md5RSA

personal-premium@thawte.com.CN=Thawte Personal Premium CA.OU=Certification
personal-premium@thawte.com.CN=Thawte Personal Premium CA.OU=Certification 1996-01-01 00:00:00 2020-12-31 23:59:59 md5RSA

CN=BAD LABEL.T=UNIT TESTING.OU=RACF_CERTIFICATE_EXPIRATION.O=IBM.L=POUGHKE
CN=BAD LABEL.T=UNIT TESTING.OU=RACF_CERTIFICATE_EXPIRATION.O=IBM.L=POUGHKE 2009-01-01 04:00:00 2010-01-02 03:59:59 sha1RSA

CN=DAVE FRISHBERG.T=SENIOR SOFTWARE ENGINEER.OU=SYSTEMS AND TECHNOLOGY GRO
CN=DAVE FRISHBERG.T=SENIOR SOFTWARE ENGINEER.OU=SYSTEMS AND TECHNOLOGY GRO 2011-11-10 04:00:00 2012-11-11 03:59:59 sha1RSA

CN=MARK NELSON.T=SENIOR SOFTWARE ENGINEER.OU=SYSTEMS AND TECHNOLOGY GROUP.
CN=MARK NELSON.T=SENIOR SOFTWARE ENGINEER.OU=SYSTEMS AND TECHNOLOGY GROUP. 2011-11-04 04:00:00 2012-11-05 03:59:59 sha1RSA

CN=STG Code Signing CA.OU=IBM Code Signing.O=IBM Corporation.C=US
CN=STG Code Signing CA.OU=IBM Code Signing.O=IBM Corporation.C=US          2008-07-01 04:00:00 2028-07-01 03:59:59 sha1RSA

CN=Test Certificate.T=RACF_CERTIFICATE_EXPIRATION.OU=Unit Test.OU=CertLabe
CN=Test Certificate.T=RACF_CERTIFICATE_EXPIRATION.OU=Unit Test.OU=CertLabe 2012-01-24 05:00:00 2012-01-25 04:59:59 sha1RSA

CN=Test Certificate.T=RACF_CERTIFICATE_EXPIRATION.OU=Unit Test.OU=CertLabe
CN=Test Certificate.T=RACF_CERTIFICATE_EXPIRATION.OU=Unit Test.OU=CertLabe 2012-01-24 05:00:00 2012-01-25 04:59:59 sha1RSA

CN=Test Certificate.T=RACF_CERTIFICATE_EXPIRATION.OU=Unit Test.OU=CertLabe
CN=Test Certificate.T=RACF_CERTIFICATE_EXPIRATION.OU=Unit Test.OU=CertLabe 2012-01-24 05:00:00 2012-01-25 04:59:59 sha1RSA
```

Background

- **Imagine a RACF database with a group (we'll call it "BIGGRP") into which almost every user is placed**
- **Imagine how easy it would be to merely put BIGGRP on access lists to "get things to work"**
- **Imagine an auditor finding that profiles which had BIGGRP on the access list were flagged as violating the installations "need to know" policy**
- **What would you do?**

Background...

- **What this installation decided to do was to segment BIGGRP into a set of organizational groups (we'll call them SMLGRP01, SMLGRP02, SMLGRP03.... etc.)**
- **Considerations: The client had:**
  - Only three months to get this done
  - A major application and an unmovable project deadline that depended on the BIGGROUP entries
- **Question: How would the client:**
  - Find all of the references to BIGGRP
  - Notify the profile owners that they needed to move from BIGGRP to one or more SMLGRPxx access list entries?
  - Provide a backout plan in to ensure that there were application outages caused by this migration?

Approach

1.Create a list/report which identified every BIGGRP access list entry, showing the:

- Profile name and class
- Access level
- Profile owner

2.Survey all of the application owners and users and create and populate the SMLGRPs

3.Work with the application owners and profile owners to add the SMLGRPs to the access list

- BIGGRP would remain on the access list

4.De-populate BIGGRP

- In the event of a production problem, users could be re-connected to BIGGRP on an emergency basis.

How to Analyze the RACF Data Base?

- **We used an IRRDBU00-unload of the RACF Data Base to create the reports and data needed to:**
  - **Find all of the BIGGRP references and the associated profile owners**
  - **Map the contents of the BIGGRP and the SMLGRPs to identify:**
    - All of the users in BIGGRP who were not in any SMLGRP
      - These were the users who would no longer have access once BIGGRP was “drained”
    - The set of SMLGRP members who were not in BIGGRP
      - These were the users who may have gotten more authority than they had before

JOINKEYS Joining Access List Entry to Profile Owner

```
//GROUPREF  EXEC PGM=ICETOOL
//TOOLMSG   DD SYSOUT=*
//PRINT     DD SYSOUT=*
//DFSMSG    DD SYSOUT=*
//DBU1      DD DISP=SHR,DSN=USER01.IRRDBU00
//DBU2      DD DISP=SHR,DSN=USER01.IRRDBU00
//TEMP0001  DD UNIT=SYSALLDA,SPACE=(TRK,(10,10,0))
//TOOLIN    DD *
COPY JKFROM          TO(TEMP0001) USING(JOIN)

DISPLAY  FROM(TEMP0001) LIST(PRINT) -
         PAGE -
         TITLE('Data Set Profiles with References to BIGGROUP') -
         DATE(YMD/) -
         TIME(12:)  -
         BLANK -
         ON(01,44,CH)                HEADER('Data Set Name')    -
         ON(46,06,CH)                HEADER('VOLSER')           -
         ON(53,08,CH)                HEADER('Owner')


//JOINCNTL  DD *
 OPTION VLSCMP
 JOINKEYS F1=DBU1,FIELDS=(10,44,A,55,6,A),
    INCLUDE=(5,4,CH,EQ,C'0400')
 JOINKEYS F2=DBU2,FIELDS=(10,44,A,55,6,A),
    INCLUDE=(5,4,CH,EQ,C'0404',AND,62,8,CH,EQ,C'BIGGROUP')
 REFORMAT FIELDS=(F1:10,45,55,7,78,9,
                  F2:71,9)
/*
```


JOINKEYS Joining Access List Entry to Profile Owner

```
- 89 -        Data Set Profiles with References to BIGGROUP        13/03/10        11:03:37 pm

 Data Set Name                                 VOLSER   Owner
 -------------------------------------------   ------   --------
 SYS1.MACS                                              PPP
 SYS1.TOOL*                                             PPP
 SYS1.TOOL.TSCENV                                       MVSSPT
 SYS1.TOOL.TSCUSER                                      MVSSPT
```