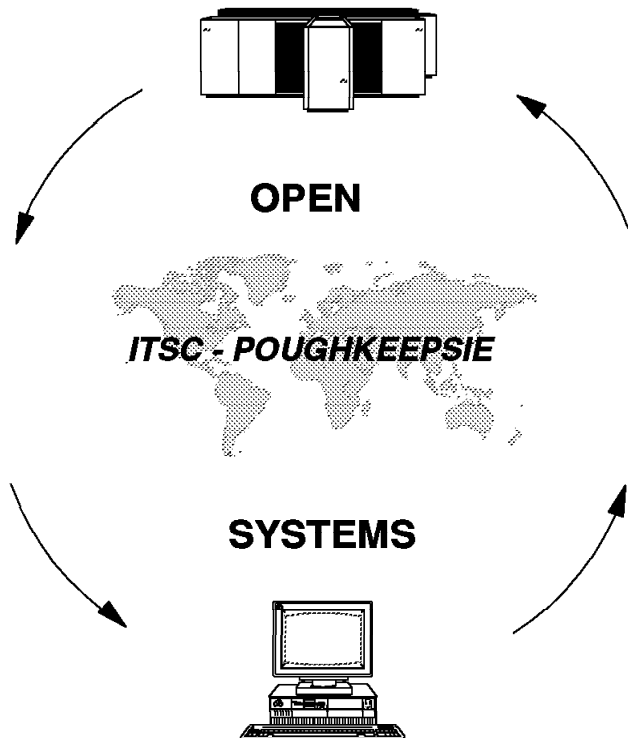


Elements of Security: RACF Installation - Student Notes

Document Number GG24-3971

December 1992

IBM International Technical Support Center
Poughkeepsie, New York, USA



Take Note!

Before using this information and the product it supports, there is some information you should be aware of. This information is in a section called Special Notices, which immediately follows the Table of Contents.

First Edition (December, 1992)

This edition applies to multiple releases of RACF. Release related items are noted in the text.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

An ITSC Evaluation Form for reader's feedback appears in the document. If the form has been removed, comments may be addressed to:

International Technical Support Center
Department H52, Building 930
PO Box 950
Poughkeepsie, New York 12603

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 1992.. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Abstract

This document is intended to provide additional information for students attending a RACF presentation or workshop. This document consists of the "foils" (overhead projections) typically used when an IBM systems engineer presents an informal RACF class. The material contained in these foils would normally be presented during a two or three day lecture period. Readers are assumed to understand common MVS terms and acronyms. (These are not the foils used for formal IBM RACF education courses.)

LS

(45 pages)

Contents

1. Introduction.	1
2. Installation	3
RACF Data Base	4
Started Tasks	7
System Authorization Facility	9
Router Exit and Table	11
General Resources and CDT	13
Other Parameter Modules	15
Complete install	16
3. Select options	19
RACF Indicator, PROTECTALL and CATDSNS	20
Always Use ICF Catalogs	21
Data Set Naming	22
Model New Profiles	25
Generic profiles	27
Automatic Data Set Protection	30
Other Data Set Options	31
Password Rules and Quality	32
Password Encryption	33
General Resource Classes	34
4. Tune the system	37
5. Activate functions	41
Erase On Scratch.	41
DASDVOL authorization	42
TAPE Protection	43
Index	45

Special Notices

This publication is intended to provide additional information for students attending a RACF presentation or workshop. The information is not intended as the specification of the programming interfaces that are provided by RACF for use by customers in writing programs that request or receive its services. See the Publications section of the IBM Programming Announcement for RACF for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM program product in this document is not intended to state or imply that only IBM's program product may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Commercial relations, IBM Corporation, Purchase, NY 10577 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "As Is" basis without any warranty, either express or implied. The use of this information, or the implementation of any of these techniques, is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

The following terms, denoted by an asterisk (*) in this publication, are trademarks of the IBM Corporation in the United States and/or other countries:

- RACF*
- MVS/ESA*
- DFSMS/MVS*
- DFSMSdfp*
- DFSMSdss*
- DFSMSHsm*
- CICS/ESA*
- IMS/ESA*

The following terms, denoted by a double asterisk (**) in this publication, are trademarks of other companies, as follows:

(none)

Preface

This document is one of a series:

- Elements of Security: RACF Overview - Student Notes (GG24-3970)
- Elements of Security: RACF Installation - Student Notes (GG24-3971)
- Elements of Security: RACF Advanced Topics - Student Notes (GG24-3972)

This series is intended for use as student "handouts" for informal RACF training presented by IBM Systems Engineers or by other qualified instructors. This document, the second of the series, covers RACF installation. It is intended for a narrow audience, since most MVS systems, as provided by IBM, already have RACF installed.

This document is the result of a project at the International Technical Support Center, in Poughkeepsie, New York. The project participants were:

- A. H. J. (Guus) Bonnes, IBM Netherlands (Primary author)
- William R. Ogden, ITSC Poughkeepsie (Project coordinator)

During the preparation of the material in this document, many people in IBM were of help. Of these, Walt Farrell of RACF Development should be mentioned for his assistance in getting all the details right.

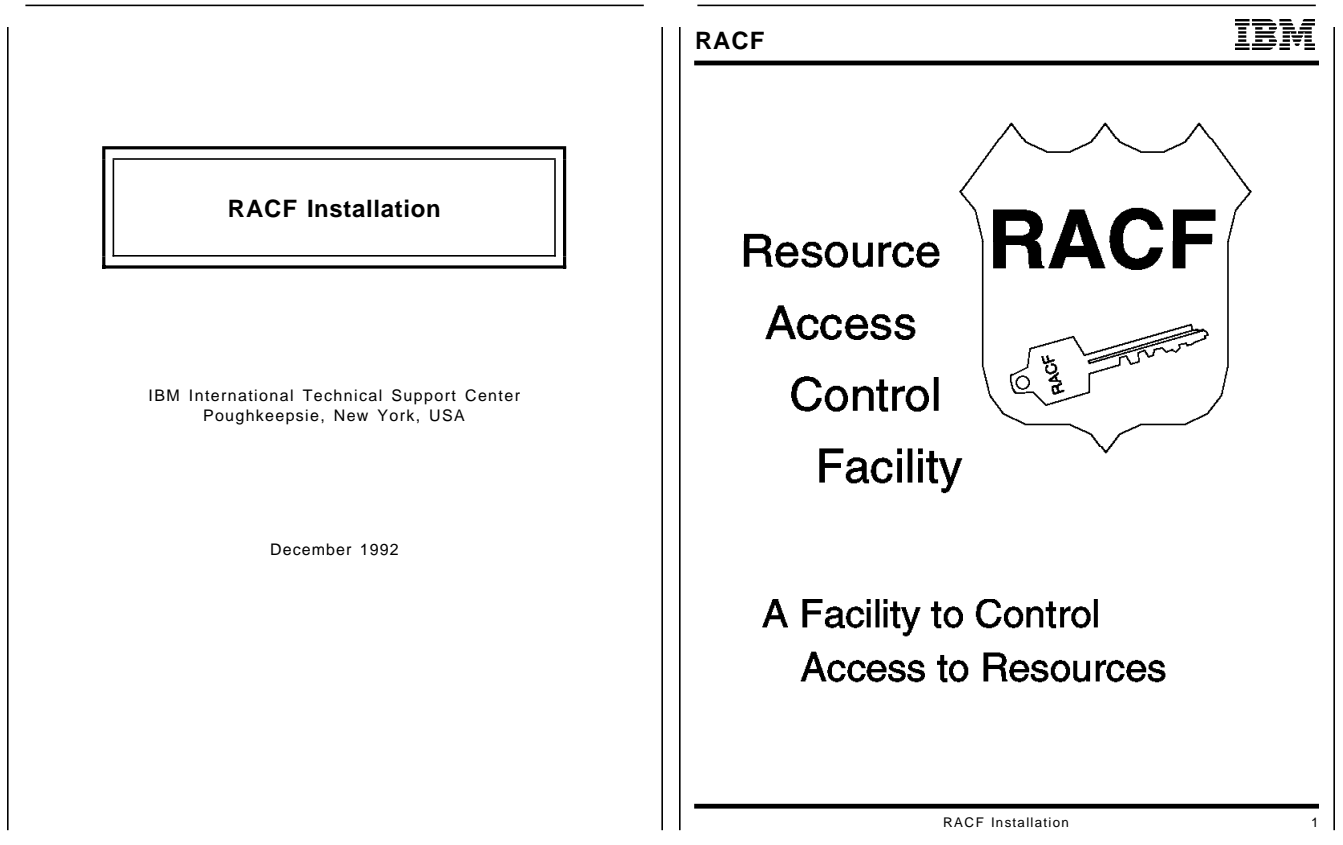
In his position of Staff MVS Systems Programmer, Mr. Bonnes has been responsible for the implementation of RACF at various IBM internal computing centers. He also assisted several customers with this process. Aside from this, he has written and presented RACF courses to customers in Western Europe during the past years. The material in this document is derived from his experience in both these areas.

Mr. Bonnes can be reached at:

Internet: Guus@VNET.IBM.COM
IBMMAIL: NLIBMBBL at IBMMAIL
IBM Internal: NL10255 at EAMSVM1

Very little text, outside the contents of the individual foil slides, is presented in this document. This material is intended for use during a hands-on or installation-specific class, and the instructor is expected to tailor his presentation to match the class environment.

1. Introduction.



Purpose of this foil

- Introduction.
- Intended for systems programmers.

Most MVS systems using RACF are supplied by IBM with RACF already installed. The CBIPO and various Express offerings provide this option. The material in this document helps a skilled instructor explain the base RACF installation process, which is needed only if your MVS system does not have RACF already installed.

2. Installation

Installation	IBM
Installation	
<ul style="list-style-type: none">• Install RACF using SMP/E,• Allocate RACF Data Base,• Initialize RACF Data Base,• RE-IPL the system• Set RACF Options,• Define Users and Groups,• Define Resources.	
RACF Installation	2

Parameter modules	IBM
ICHRDSNT RACF Data Set Name Table	
ICRRNG Profile Range table	
ICHRIN03 Started Procedures Table.	
ICHRRCDE Class Descriptor Table.	
ICHRFR01 RACF-router table.	
ICHRSMFI RACFRW defaults and parameters.	
ICHSECOP RACF Security Options.	
ICHAUTAB Authorized Callers Table.	
RACF Installation	3

Purpose of this foil

- Overview of the items that need to be done.
- Overview of modules that need be assembled before starting RACF.

RACF Data Base

RACF Data Base	IBM
<ul style="list-style-type: none">• Dynamic backup copy,• RVAR Y command,• Data Base utilities,• Failsoft processing,• Splitting of Data Base,• Shared DASD.	
RACF Installation	4

RACF Data Base ...	IBM
<p>Dynamic backup copy</p> <ul style="list-style-type: none">• Automatic,• Indicated via ICHRDSNT.	
<p>RVAR Y command</p> <ul style="list-style-type: none">• RVAR Y SWITCH<ul style="list-style-type: none">– Primary Data Base inactive,– Backup Data Base becomes Primary,• RVAR Y ACTIVE/INACTIVE<ul style="list-style-type: none">– Enables maintenance to RACF Data Base.– Only Alternate inactive, or– Primary and Backup both inactive.• Password via Console Operator.	
RACF Installation	5

Purpose of these foils

- RACF Data Base related parameter modules,
- Choices to be made,
- Possibilities to recover,
- Utilities to maintain.

Database Utilities

- Initialize Data Base
 - IRRMIN00 to initialize,
 - IRRDSC00 to fill with data from old Data Base.
- Backup of Data Base,
 - IRRUT200 for verify and copy,
 - IRRUT400 for reorganize.

Failsoft

- RACF inactive,
- In-storage tables still used,
- Other access via Console Operator.

Split

- Impact of I/O error reduced,
- Some users not impacted by errors.

Shared DB

- ICHRDSNT identical,
- Password encryption identical,
- SYSGEN shared,
- Problems for non-shared data sets.

Resident Data Blocks

- Specify in ICHRDSNT,
- Maximum is 255 (1M ECSA),
- Buffer for data and index of RACF Data Base.

Updates to backup

- Specify in ICHRDSNT,
- Enable updates,
- Disable statistics updates.

Multiple databases

- Range table
- Point to Data Base.

ICHRDSNT

#DB	Primary-DB-name	Backup-DB-name
	# data-buffers	update flags
	Secondary-DB	Backup-DB-name
	# data-buffers	update flags

ICHRRNG

#ranges	Range-start value	DB#
	Range-start value	DB#
	Range-start value	DB#

- RACF 1.9 is only supported release for non-RDS,
 - Blocksize increased to 4K,
 - 16 DB-segments per block,
 - Profile Segments in own DB-segment,
- Less I/O required for access,
- Profile name now maximum 256 bytes,
 - Default values not recorded,
 - Don't use old utilities:
 - ICHUT...

IRRDSC00

- Only available in RACF 1.9.0
- Takes about as long as IxxUT400
- Primary and Backup independent
- Detailed description in SPL.

Notes

- Preferably during off-line hours,
- IRRDSC00 can prevent updates to RACF Data Base,
- IRRUT400 required after conversion,
- Combination of IRRDSC00 jobs, RENAME and RVARY commands will allow conversion without IPL.

Purpose of these foils

- Only use Restructured Data Base,
- Convert while still possible.

Instructor suggestion: the conversion process typically has about six steps. Draw it on the blackboard. In the process make sure that:

- There's always one RACF Data Base active,
- All Data Bases are reorganized,
- No updates to the RACF Data Base are lost.

Started Tasks

Started Tasks



- System created JOBCARD.
- Table for relation:
 - Procedure name,
 - Userid,
 - Group,
 - Special authorizations.
- ICHRIN03 in SYS1.LPALIB
- If not present, STC will be RACF 'undefined'

Started Tasks ...



Privileged

- Via flag in SPT,
- All RACHECKs return 'OKE',
- No exits,
- No SMF records,
- No Statistics,
- Other RACF functions still performed.

Trusted

- Via flag in SPT,
- All RACHECKs return 'OKE',
- No exits,
- SMF records according to audit options,
- No Statistics,
- Other RACF functions still performed.

ICHRIN03

Count	Procname	Userid	Group	Flags
X'8005'	JES2	JES2	SYST	X'80'
	CICSPROD	T9OPROD	CICSGRP	X'00'
	TSO	TSOPROD		X'00'
	RACF	STCPROD	STCGRP	X'00'
	*	STCPROD	=	X'00'

Generics

- Last entry,
- Procname is '**'
- Userid is '='
- Group is '='
- **One** '=' allowed.

Purpose of these foils

- Why ICHRIN03 at all,
- Describe flags,
- Sample table with generics.
- Remember about 'splat-is-blank-priv'.

System Authorization Facility

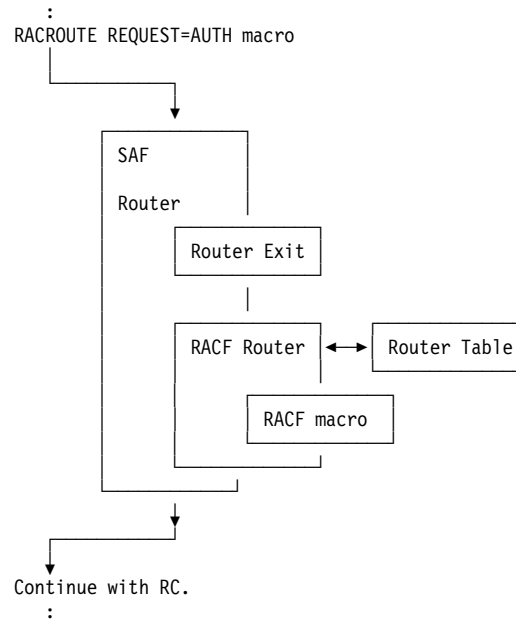
System Authorization Facility



Primary interface to security software.

- Part of MVS,
- Always present,
- Called by all resource managers,
- RACROUTE macro,
- SAF router ICHSFR00,
- Builds Security TOKEN,
- Invokes Router Exit ICHRTX00,
- May pass through to RACF router ICHRFR00,
 - Refers to Router Table ICHRFR01
 - May issue RACF macro.

System Authorization Facility ...



```

RACROUTE REQUEST=request type
      ,WORKA=work area address
      [,REQSTOR=requestor name]
      [,SUBSYS=subsystem name]
      [,DECOUPL=YESNO]
      [,MSGIRN=YESNO]
      [,MSGSUPP=YESNO]
      [,MSGSP=subpool number]
      [,RELATED=value]
      [,RELEASE=number]
      :
      :
      :

```

Request-types

AUTH	Check RACF authorization
DEFINE	Define, Modify, Rename or Delete a Resource to RACF
VERIFY	Identify and Verify a RACF defined user
VERIFYX	Identify, Verify and Build UTOKEN for a RACF defined user
LIST	Build in-storage profiles
FASTAUTH	Verify access to Resource via in-storage profiles
AUDIT	Security Audit request (SMF)
DIRAUTH	Check authorization to a sent message
EXTRACT	Replace or Retrieve field in RACF profile
STAT	Determine RACF status
SIGNON	Manage Persistent-Verification Signed-on lists
TOKENBLD	Copy or Modify User TOKEN
TOKENMAP	Convert TOKEN information
TOKENXTR	Build User Token from existing security environment

Purpose of these foils

- Introduce SAF,
- Introduce ICHSFR00,
- Introduce ICHRFR00,
- Introduce ICHRFR01,
- Point to RACROUTE macro,
- Point to REQSTOR and SUBSYS and DECOUPL.

Router Exit and Table

Router Exit	IBM	RACF Router Table	IBM
ICHRTX00		ICHRFR01	
<ul style="list-style-type: none">• If present, always called,• Runs in same environment as caller,• Can determine if Router should pass through to RACF,• Before JES 3.1.3 used for JES(EARLYVERIFY), Never pass through to RACF,		<ul style="list-style-type: none">• RACF router (ICHRFR00) uses router table,• Determines if RACF macro should be issued,• Two modules:<ul style="list-style-type: none">– ICHRFR0X, IBM supplied, not for installation modification.– ICHRFR01. Installation dependent. Created via ICHRFR01 macro and LKED'ed into SYS1.LINKLIB.• Loaded during system IPL.	
RACF Installation	19	RACF Installation	20

Purpose of these foils

- Tell something about RTX00 and RFR01
- Point to example in RACINSTL in SAMPLIB.

```
[label] ICHRFRTB [CLASS=class name]
           [,REQSTOR=requestor name]
           [,SUBSYS=subsystem name]
           [,ACTION=NONE RACF]
           [,TYPE=END]
```

Purpose of this foils

- Tell something about the macro.
- Point to REQSTOR and SUBSYS keywords.
- Refer to DB2 for SUBSYS.
- Refer to CDT for your own stuff.

General Resources and CDT

General Resources	IBM	CDT	IBM
Everything that is defined in CDT.		ICHRRCDE	
Examples of IBM-supplied:		• Definition of General Resource Classes.	
<ul style="list-style-type: none">• DASD-volumes,• Tape-volumes,• Programs• Terminals,• CICS-transactions,• Facility.		• Two modules:	
Or your own resources classes		– ICHRRCDX, IBM supplied, not for installation modification.	
<ul style="list-style-type: none">• \$DASD• \$SUBMIT• \$ASDATA		– ICHRRCDE, Installation dependent. Created via ICHERCDE macro and LKED'ed into SYS1.LINKLIB.	
		• Loaded during system IPL.	
RACF Installation	22	RACF Installation	23

Purpose of these foils

- Introduction to General Resources
- Introduce ICHRRCDX and ICHRRCDE.
- Point to example in RACINSTL in SAMPLIB.

```
[label] ICHERCDE [CLASS=class name]
[ ,ID=class number]
[ ,GROUP=grp class MEMBER=mem class]
[ ,MAXLNTH=number]
[ ,FIRST=ALPHA NUMERIC ALPHANUM
  ANY NONATABC NONNUM]
[ ,OTHER=ALPHA NUMERIC ALPHANUM
  ANY NONATABC NONNUM]
[ ,POSIT=number]
[ ,OPER=YES NO]
[ ,DFTUACC=ALTER CONTROL UPDATE
  READ NONE]
[ ,RACLIST=ALLOWED DISALLOWED]
[ ,GENLIST=ALLOWED DISALLOWED]
[ ,RACLREQ=YES NO]
[ ,PROFDEF=YES NO]
[ ,DFTRETC=0 4 8]
[ ,KEYQUAL=0 nm]
[ ,SLBLREQ=YES NO]
[ ,RVRSMAC=YES NO]
```


Notes

- Class name
 - When RDS, first 8 characters unique,
 - When NON-RDS, first 4 characters unique,
 - National character (@ # \$) advised.
- POSIT value
 - Used for CLASSACT,
 - Used for AUDIT, STATISTICS, RACLIST,
 - Used for CLAUTH,
 - Used for resource class LOGOPTIONS.

Purpose of these foils

- Restriction in name to avoid conflicts with IBM,
- POSIT value for grouping together.
- Really should use example. LKED statements are important.

Other Parameter Modules

ICHSECOP 


ICHSECOP

No RACF No Duplicate names reserved
.....
(Number of Resident data blocks
if ICHRDSNT is not used)

Only use for:

- Disable RACF initialization,
- Prevent duplicate data set names.

RACF Installation 26

ICHAUTAB 

ICHAUTAB

Program name flags
Program name flags
blanks

Don't use anymore:

- Integrity exposure,
- Not needed for any current product.

RACF Installation 27

Purpose of these foils

- For completeness only.

Complete install

PARMLIB



APF commands

- RACF commands need APF authorization,
- Specified in IKJTSOxx, or
- Specified in IKJEFTE2/E8.
- Sample in RACINSTL in SAMPLIB,

RACF as Subsystem

- RACF entry in IEFSSNxx
RACF,IRRSSI00,#
- RACF entry in SCHEDxx
PPT PGMNAME(IRRSSM00),.....
- RACF entry in STC-table

IRRDP100



Dynamic parse initialization

- IRRDP100 TSO command,
- Required at every IPL,
- Authorized via
 - IRRDP100 in Facility class, or
 - IRRDP100 is RACF controlled program, or
 - User has SPECIAL.
- Can be automated via
 - IRRDPTAB Started Task, and
 - START command in PARMLIB.

IRRGTS

Group Tree in Storage

- Only part of tree required for access verification,
- Use of VLF for data storage,
- Use only if:
 - All RACF systems at 1.9 or higher,
 - MVS/ESA 3.1.0

IRRACEE

Save ACEE for reuse

- ACEE saved and reused for:
 - Same userid,
 - Same group,
 - Same Port of Entry,
 - Same APPLication,
 - Same Terminal.
- Use of VLF for data storage,
- Information invalidated:
 - SETROPTS REFRESH RACLIST(.....)
 - Add, delete, change group connections,
 - Updates from another system.

3. Select options

SETROPTS	IBM
Command options	
ADSP	Allow automatic creation of discrete data set profiles,
CATDSNS	Access to uncataloged data sets not allowed,
CLASSACT	Activate RACF processing for a resource class,
CMDVIOL	Audit command violations,
EGN	Activate Enhanced Generic Naming for data sets
ERASE	Activate Erase On Scratch,
GENCMD	Allow definition of generic profiles,
GENERIC	Specify that RACF should use generic profiles,
GENERICOWNER	Control definition of general resource profiles,
GENLIST	Load generic profiles in common-storage,
RACLIST	Load profiles in common-storage,
GLOBAL	Activate Global Access Checking,

RACF Installation 31

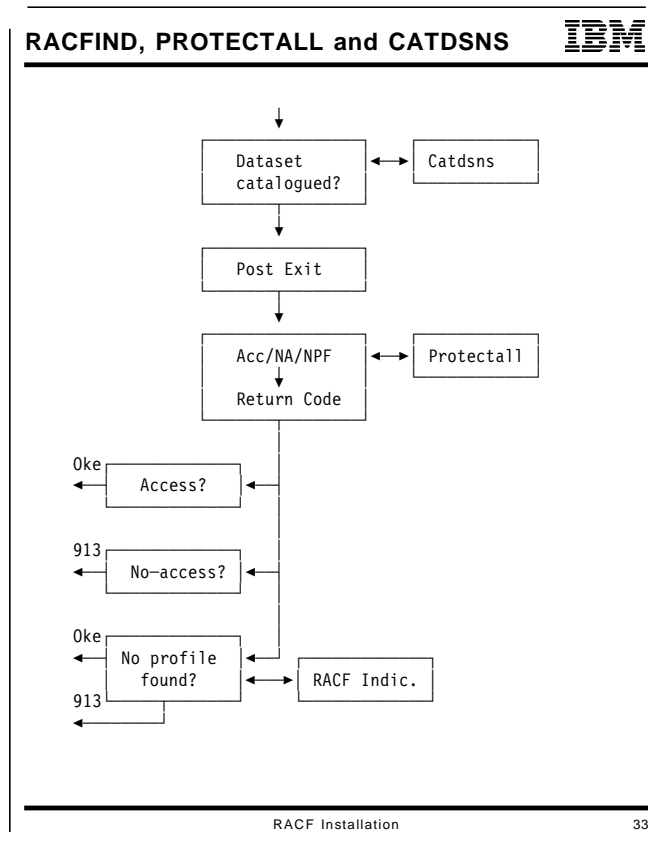
SETROPTS ...	IBM
GRPLIST	Use all connect-groups for access control,
INACTIVE	Revoke inactive users,
INITSTATS	Record logon statistics in RACF Data Base
MODEL	Allow modelling for data set profiles,
PREFIX	Set prefix for one qualifier data sets,
PROTECTALL	Specify that all data sets should be RACF protected,
RETPD	Specify retention period for tape data sets,
RVARYPW	Password for RVARY commando,
STATISTICS	Maintain usage statistics in RACF Data Base,
TAPEDSN	Specify that data sets on tape should be protected,
TERMINAL	Specify access to undefined terminals
WHEN	Activate program control.


RACF Installation 32

Purpose of these foils

- Overview of RACF options,
- Introduce settings to come.

RACF Indicator, PROTECTALL and CATDSNS



- Data Set Features** 
- Protectall**
- RACF facility,
 - Only for data sets,
 - New data sets,
 - Existing data sets,
 - Profile required,
 - 'WARNING' or 'FAILURE'.
- RACF Installation 34

Purpose of these foils

- Explain place of PROTECTALL,
- Explain activation.

Always Use ICF Catalogs

RACF-bit and Always-Call



RACF-indicator

- DFP facility
- Located in VTOC for NVSAM data sets,
- Located in Catalog for VSAM data sets,
- Causes different options on RACHECK.

Always-Call

- DFP facility
- RACF-indicator less important,
- Requires use of ICF-catalogs.

OS and VSAM Passwords



Password protection

- DFP facility,
- RACF replaces OS and VSAM passwords,
- If RACF unprotected, password possible,
- Not for SMS-managed data sets.

Purpose of these foils

- Explain why people should use ICF catalogs.
- Warn that OS and VSAM password will no longer work.
- Passwords still kept in PASSWORD or the catalog.

Data Set Naming

Naming Conventions



Single level DSN

- RACF installation problem,
- RACF: HLQ oriented,
- One (1) qualifier is not a HLQ,
- Prefix with HLQ (Prefix),
- SETROPTS PREFIX(xxxxx),
- Prefix must be unique,
- If not specified, ABENDs may occur,

RACF Installation

37

Naming Conventions ...



SYSCTLG

- Looks like single level data set,
- Vvolser is always added to data set name,
- RACF commands use extended name.

RACF Installation

38

Purpose of these foils

- Two simple examples of data set name problems.
- More to follow on the following foils.

- RACF is HLQ oriented,
- Installation may not be,
- Translate table:
 - ICHNCV00
- Messages with REAL name or INTERNAL name,
 - SETROPTS REALDSN.

ICHNCV00

Example of usage:

- DASD.ABC.XYZ
- DASD.PAYROLL.HMOFF.MASTER
- DASD.ACCTREC.REGION.NUM007
- DASD.PRSNNL.MASTER.BRANCH

Reverse first two qualifiers:

- ABC.DASD.XYZ
- PAYROLL.DASD.HMOFF.MASTER
- ACCTREC.DASD.REGION.NUM007
- PRSNNL.DASD.MASTER.BRANCH

Purpose of these foils

- Introduction of RACF Naming convention table.
- May also be used for discrete profiles in DFHSM 'setsys profilebackup' environment.

ICHNCONV macro

- DEFINE the name of the convention,
- SELECT the data sets this convention applies to,
- ACTION describes what should be done,
- END terminates this convention,
- FINAL concludes the entire table.

Example

```
ICHNCONV DEFINE,NAME=CHECK1
ICHNCONV SELECT,COND=((GQ,1),EQ,RACUID,OR)
ICHNCONV SELECT,COND=((GQ,1),EQ,RACGPID)
ICHNCONV END,NEXT='SUCCESS'
ICHNCONV DEFINE,NAME=CHECK2
ICHNCONV SELECT,COND=(GQT,GE,3,AND)
ICHNCONV SELECT,COND=(GQ,,EQ,RACUID)
ICHNCONV ACTION,SET=(NAMETYPE,USER)
ICHNCONV ACTION,SET=((UQ,0),(GQ,G))
ICHNCONV ACTION,SET=((UQ,G),' ')
ICHNCONV END,NEXT='SUCCESS'
ICHNCONV FINAL
END
```

Purpose of these foils

- Describe the ICHNCONV macro,
- Give an example. Explain example to the students.

Model New Profiles

Modelling



Four types of modelling

- Via commands,
- Per user,
- Per group,
- GDG modelling.

May be used for

- Data sets,
- General resources.

Modelling ...



Per user

- MODEL profile indicated in USER profile,
- Existing discrete profile or MODEL profile,
- Profile always prefixed with USERID,
- System-wide enabled via
SETROPTS MODEL(USER),

Per group

- Similar to USER.
- System-wide enabled via
SETROPTS MODEL(GROUP).

GDG-modelling

- Not truly modelling,
- Shared usage of discrete profile,
- GDG-base on catalog volume,
- RACF-indicated generations,
- Replaced by generics profiles.

Purpose of these foils

- Describe modelling process,
- Indicate that USER and GROUP must be enabled,
- Discredit GDG-Modelling.

Generic profiles

Activate Generics	IBM	Generic Profiles	IBM
Activate		Several Types of Generics	
• Only for commands:		• Standard generics,	
SETROPTS GENCMD(class-name)		These contain a generic character,	
• Also for access verification:		• Enhanced generics,	
SETROPTS GENERIC(class-name)		This is an extended form of generics,	
• Some resource classes always enabled for generics:		• Fully qualified generics,	
– PROGRAM may always contain '**'.		Generic profiles without a generic character	
		• Generics via RACF variables.	
		A variable defined in the RACFVARS class with its possible values.	
RACF Installation	46	RACF Installation	47

Purpose of these foils

- Explain that Generics must be enabled.
- Introduction to generic profiles in general.

Recognizable by:

- (G) in list output,
- % in profile name,
- * in profile name.

Form:

- SYS1.* (G)
- SYS2.*.ISPLLIB (G)
- SYS1.LOCAL.* (G)
- ABCD.E%%.H* (G)
- ABCD.E* (G)

Usage:

- All resources that fit the generic profile are covered.
- Must be activated via SETROPTS GENERIC(class-name).

Generic Characters

- % represents one (1) character,
- * represents zero (0) or more characters to complete one qualifier,
- * represents one (1) or more qualifiers to complete the profile name,
- * represents one (1) qualifier in the middle of a profile name.

Recognizable by:

- (G) in list output,
- % in profile name,
- * in profile name,
- .** in profile name.

Form:

- SYS1.** (G)
- SYS2.**.ISPLLIB (G)
- SYS1.LOCAL.** (G)
- ABCD.E%%.H.** (G)
- ABCD.E.** (G)

Usage:

- All resources that fit the generic profile are covered.
- For general resources always active.
- For data sets activated via SETROPTS EGN.

Generic Characters

- % represents one (1) character,
- * represents zero (0) or more characters to complete one qualifier,
- * represents one (1) entire qualifier,
- .** represents zero (0) or more qualifiers.

Purpose of these foils

- Explain difference between NON-EGN and EGN,
- Make sure that people will *want* to activate EGN.

IBM

(De-)Activate EGN


- SETROPTS EGN
- NON-EGN profiles protect exactly the same resources as before,
- New profiles interpreted as EGN profiles,
- Reversal possible via:
 - SETROPTS NOEGN
 - EGN profiles maybe unused if using new (now unsupported) features.

RACF Installation 52

Purpose of these foils

- Explain that activate/de-activate EGN is simple,
- Nothing that can go wrong,
- Fully automatic and reversible,
- No conversion needed,
- Communication to users is important.

Automatic Data Set Protection

ADSP 

ADSP

- Automatic creation of Discrete Data Set Profiles,
- System wide enabled,
- Activate per user,
- Activate per group for a user,
- Replaced by generic profiles.

RACF Installation 53

Purpose of these foils

- Explain advantage of SETROPTS NOADSP.

Other Data Set Options

Temporary Data Sets



Temporary data sets

- Data sets created without DSNAME,
- System name:
SYS92264.Ttttttt.RA000.jobname.ddname
- Always DELETED at end of JOB, unless:
 - System failure,
 - Initiator failure or FORCE command,
 - Automatic restart after ABEND.
- Inaccessible during running of JOB (ENQ),
- Not protected via RACF.

TEMPDSN

- **Only** user with OPERATIONS can scratch,
- **Only** restart-job can read/write.
- Activate via SETROPTS CLASSACT(TEMPDSN),
- No profiles, auditing via LOGOPTIONS.

Purpose of this foil

- Explain need for initial activation during quiesced time.

Password Rules and Quality

Password rules



Rules

- Eight (8) different rules possible,
- Minimum and maximum length,
- Type character:
 - ALPHA** Letters and 'national' (@,#,\$)
 - NUMERIC** Digits
 - ALPHANUM** Letters, digits and 'national'
 - VOWEL** Vowels (a,e,i,o,u)
 - CONSONANT** Consonants
 - NOVOWEL** Consonants, digits and 'national'
- SETROPTS PASSWORD(RULE1(LENGTH(6:8)
ALPHANUM(1:8)

RACF Installation

55

Password rules ...



Installation exit

- ICHPWX01
- Called from:
 - ALTUSER command,
 - PASSWORD command,
 - RACINIT.
- May evaluate new password,
May evaluate password interval,
 - Reject,
 - Accept,
 - Modify.
- Usually has OLD and NEW password available.

RACF Installation

56

Purpose of this foil

- Explain why password exit may be needed for comparison.

Password Encryption

IBM

Password rules ...

Encryption


- Password always encrypted in RACF Data Base,
- Two methods,
 - Masking,
 - DES
- System-wide choice via exit ICHDEX01:
 - Exit absent:
 - Encryption via DES,
 - Comparison via DES and Masking.
 - Exit present:
 - Exit chooses,
 - Exit may encrypt/compare.

RACF Installation 57

Purpose of this foil

- CBIPO and RACF **used to** ship masking exit.
- RACF 1.9.2 no more.

General Resource Classes


General Resources 

Create Authorization

Authorization to create General Resource Profiles is:

- SPECIAL,
 - Use for one-time only definitions,
 - Use for system-related definitions.
- CLAUTH,
 - Use for decentralization,
 - Use for daily activities,
 - Restrict via GENERICOWNER.

RACF Installation 58

General Resources ... 

GENERICOWNER

Prevent creation of more specific profiles.

- Activate via SETROPTS GENERICOWNER
- Required authorization now:
 - SPECIAL, or
 - CLAUTH plus,
 - Owner of best-fitting generic, of
 - Group-SPECIAL over owner of best-fitting generic.

If no fitting profile, only CLAUTH required.

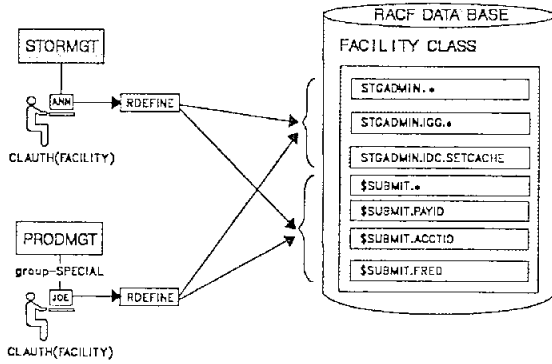
RACF Installation 59

Purpose of these foils

- Activate genericowner,
- Define 'top-generic' for all classes you intend to delegate.
- Next foils illustrate function of Genericowner.

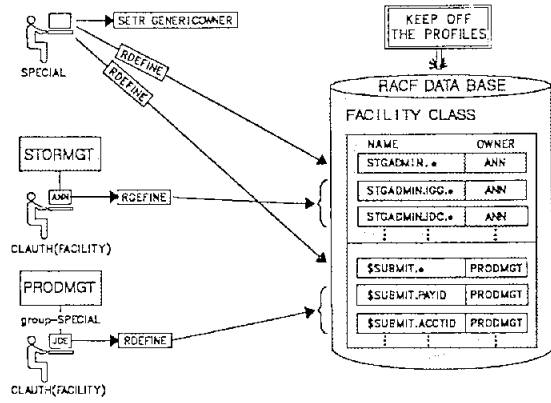
CLAUTH

PROBLEM-DELEGATION OF CLASS AUTHORITY



Generic Owner

SOLUTION - GENERICOWNER



4. Tune the system

In-storage profiles	IBM	Global Access Checking	IBM
Performance and Storage usage		GAC	
<ul style="list-style-type: none">• Global Access Checking,• Private-storage profiles,• Private-storage generic profiles,• Common-storage profiles,• Common-storage generic profiles.		<ul style="list-style-type: none">• Only for allowing access,• Very start of access verification,• Not used if all profiles RACLISTed,• If no access, refer to RACF Data Base,• If access, no further processing at all,• Generics possible,<ul style="list-style-type: none">• Special generics<ul style="list-style-type: none">– &RACUID,– &RACGPID.– * as High Level Qualifier (HLQ).• Updates active after IPL or REFRESH.	
RACF Installation	62	RACF Installation	63

Purpose of these foils

- Overview of in-storage profiles,
- Put GAC in place,
- Point at options an installation can set,
- Private RACLIST nothing to say about.

Data set

- Activate GAC
 - SETROPTS CLASSACT(GLOBAL)
 - RDEFINE GLOBAL DATASET
 - RALTER GLOBAL DATASET
ADDMEM('DSname'/access)
 - SETROPTS GLOBAL(DATASET)
- Update GAC-table
 - RALTER GLOBAL DATASET
ADDMEM('DSname'/access)
 - RALTER GLOBAL DATASET
DELMEM('DSname'/access)
 - SETROPTS GLOBAL(DATASET) REFRESH
- Copy GAC-table to 'real' profiles.

Example GAC-table

- &RACUID.*.**/ALTER
- &RACGPID.*.**/ALTER
- SYS1.BROADCAST/UPDATE
- SYS1.DUMP*/NONE
- SYS1.HASP*/NONE
- SYS1.MAN*/NONE
- SYS1.RACF*/NONE
- ...
- SYS1.*.**/READ

Note: By including SYS1.*.**/READ, RACF is using 'OLD-Style' control:

Access allowed, unless explicitly denied.

Purpose of these foils

- Overview of commands needed,
- Example table,
- Explain jump-out of table,
- Explain sort-order and incore process.

Private-storage generic profiles

- Automatic,
- In (E)LSQA,
- Table per
 - HLQ for data sets,
 - n qualifiers for general resources.
- Maximum of 4 tables,
- Modifications active after:
 - 4 references to other HLQ,
 - LOGOFF/LOGON,
 - SETROPTS REFRESH GENERIC(class-name)
 - LD DA('dsname') GEN

Purpose of this foil

- Introduce automatic feature,
- Point at thrashing of tables,
- Stress Naming Conventions,
- Explain refresh possibilities.

Common-storage profiles**RACLIST**

- All profiles in (E)CSA or dataspace,
- Used by all users of the system,
- Only for general resource classes,
- Activate via:
 - SETROPTS RACLIST(class-name)
- Updates active after:
 - IPL,
 - SETROPTS REFRESH RACLIST(class-name).
- Used for activation of grouping resource class.

Common-storage generic profiles**GENLIST**



- Originally intended for VM,
- Generic profiles in (E)CSA or dataspace,
- Used by all users of the system,
- Only for general resource classes,
- Activate via:
 - SETROPTS GENLIST(class-name)
- Updates active after::
 - IPL,
 - SETROPTS REFRESH GENERIC(class-name).

Purpose of this foil

- Some classes need it,
- Performance gain,
- Not for data sets.

5. Activate functions


Erase On Scratch.

Erase On Scratch 	Erase On Scratch ... 
<p>Erase On Scratch</p> <ul style="list-style-type: none">• Physical overwriting of data set during delete,• Hardware activity activated by DFP• Specifiable in three ways:<ul style="list-style-type: none">– SETROPTS ERASE(ALL), All data sets (including temporary),– SETROPTS ERASE(SECLEVEL(levelname)), All Data sets with the specified SECLEVEL or higher,– SETROPTS ERASE Allow per data set specification. ALTDSD dsname ERASE	<p>Notes</p> <ul style="list-style-type: none">• Entire allocated part overwritten,• One track per I/O,• Uses ERASE CCW with Inhibit Cache,• NON-VSAM data sets:<ul style="list-style-type: none">– RACF options,• VSAM in ICF catalog:<ul style="list-style-type: none">– IDCAMS option,– RACF options (overrule IDCAMS option).• Device does all the work,• ENQ on data set during erase,• Reserve on volume per 'I/O Burst'.
RACF Installation 69	RACF Installation 70

Purpose of these foils

- Explain EOS, and temporary data sets,
- How to switch it on, and performance impact.

DASDVOL authorization

DASDVOL Authorization

Which products?

- DFDSS
(Data Facility Data Set Services)
- DFDSF
(Data Facility Device Support Facility)
- DADSM Scratch
(Direct Access Device Space Management)
- DFP for VTOC

ALTER access provides

- All DFDSS functions for non-sms
- All DFDSF functions
- VTOC Update (e.g. AMASPZAP)

RACF Installation71

Purpose of this foil

- Explain DASDVOL,
- Explain how it helps against VTOCUPD.

TAPE Protection

TAPE Protection



TAPEVOL

- General Resource class,
- If active, every tape verified,
 - Best fitting profile will be used,
 - If not protected, everyone may access,
 - For NL-tapes, label from JCL is used.
- Profile can be Multi-Volume (Tape-volume-set).

HSMHSM tape set for DFHSM

TAPEDSN

- RACF System-wide option,
- Enables discrete tape data set profiles,
- Existing generic data set profiles will be used,
- Watch out for naming conventions!

RACF Installation

72

TAPE Protection ...



Tape VTOC

- Part of TAPEVOL profile,
- Maintained by RACF,
- Relation between
 - Physical files on tape,
 - TAPEVOL profile,
 - Possible discrete data set profiles.
- Contains:
 - Full 44 character data set name,
 - Tape File sequence number,
 - Data set creation date,
 - Volume serial within Tape volume set.

RACF Installation

73

Purpose of this foil

- Explain TAPEVOL,
- Explain TAPEDSN,
- Next foil explains RETPD,
- Specify system-wide default for discrete
- Specify on generic for all the rest.

Retention Period

- Protection against overwrite,
- Specify via:
 - RETPD keyword on ADDSD en ALTDSD,
 - For discrete data set profiles system-wide via SETROPTS RETPD.
- Kept in RACF Data Base,
- Used at overwrite of every tape data set.

Labels**Bypass Label Processing**

- BLP not supported in JES
 - Specify in converter parameters,
 - BLP is translated into NL,
 - RACF checking on volume,
 - DFP will check NL/SL mismatch.
- BLP supported in JES
 - ICHBLP resource in FACILITY class,
 - READ, only use BLP when reading a tape,
 - UPDATE, BLP mode allowed during writing.
 - If ICHBLP authorized, RACF check on JCL VOLSER
- Now dependent on LABEL verification by operator.

Index

A

ACEE reuse 16
ADSP 19, 30
always-call 21
AMASPZAP 42
APF 16
automatic data set protection 30

B

blocksize, 4K 6
BLP 43
bypass label processing 43

C

CATDSNS 19, 20
CDT 13
CLASSACT 19
CLAUTH 34
CMDVIOL 19

D

DADASM Scratch 42
DASDVOL 42
data set naming 22
DES 32
DFDSF 42
DFDSS 42

E

EGN 19, 29
encryption, password 32
enhanced generic names 27
ERASE 19, 41
erase on scratch 41
erase, VSAM 41
exit, router 11

F

failsoft, RACF 6
fully qualified generic names 27

G

GAC 37
GDG models 25
GENCMD 19, 27
general resource classes 34
general resources 13

GENERIC 19
generic profiles 27, 39
GENERICOWNER 19, 34
GENLIST 19, 40
GLOBAL 19
global table 37
GRPLIST 19

H

HLQ 22, 23, 39

I

ICF catalogs 21
ICHAUTAB 3, 15
ICHDEX01 32
ICHNCV00 23
ICHPWX01 32
ICHRDR01 11
ICHRDSNT 3, 4, 6
ICHRFR01 3
ICHRIN03 3, 7
ICHRRCDE 3, 13
ICHRRNG 3, 6
ICHRSMFI 3
ICHRTX00 9, 11
ICHSECOP 3, 15
ICHSF00 9
IEFXXNxx 16
IKJEFTE2/8 16
IKJTSoxx 16
INACTIVE 19
INITSTATS 19
IRRACEE 16
IRRDPI00 16
IRRDPTAB 16
IRRDSC00 6
IRRGTS 16
IRRRMIN00 6
IRRUT200 6
IRRUT400 6

L

LSQA 39

M

masking 32
MODEL 19
models 25

N

naming conventions 22

O

operator, password 4
OS passwords 21

P

password 4
password encryption 32
password rules 32
passwords 32
passwords, OS 21
passwords, VSAM 21
POSIT value 13
PPT 16
PREFIX 19
PROTECTALL 19, 20

R

RACF indicator 20, 21
RACFVARS 27
RACLIST 19, 37, 40
RACROUTE 9
range table 6
refresh 16, 37
resident data blocks 6
restructured database 6
RETPD 19, 43
router exit 11
RVARY 4
RVARYPW 19

S

SAF 9
SCHEDxx 16
security token 9
SMF 7
SMP/E 3
SPECIAL 34
split data base 6
SPT 7
START command 16
started tasks 7
statistics 6, 19
STC table 16
superzap 42
SYS1.LPALIB 7

T

tape labels 43
tape protection 43

tape VTOC 43
TAPEDSN 19, 43
TAPEVOL 43
TEMPDSN 31
temporary data set names 31
TERMINAL 19
token, security 9
translate table 23
TVTOC 43

V

VLf usage 16
VSAM passwords 21
VTOC update 42

W

WARNING 20
WHEN 19

