OS/390

SecureWay Security Server RACF General User's Guide

SC28-1917-07

OS/390

SecureWay Security Server RACF General User’s Guide

SC28-1917-07

Note

Before using this information and the product it supports, be sure to read the general information under "Appendix B. Notices" on page 93.

Eighth Edition, September 2000

This is a major revision of SC28-1917-06.

This edition applies to Version 2 Release 10 of OS/390 (5647-A01) and to all subsequent releases and modifications until otherwise indicated in new editions.

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

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication, or you may address your comments to the following address:

IBM Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States and Canada): 1+845+432-9405
FAX (Other Countries): Your International Access Code +1+845+432-9405

IBMLink (United States only): IBMUSM10(MHVRCFS)
Internet e-mail: mhvrcfs@us.ibm.com
World Wide Web: http://www.ibm.com/s390/os390/webreqs.html

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:
- Title and order number of this book
- Page number or topic related to your comment

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

Contents

Tables

Figures

About This Book

This book contains information about the OS/390 Security Server, which consists of these components:

- Resource Access Control Facility (RACF)
- DCE Security Server
- OS/390 Firewall Technologies
- Lightweight Directory Access Protocol (LDAP) Server
- Open Cryptographic Enhanced Plug-ins
- SecureWay Security Server Network Authentication and Privacy Service

This book teaches the general user how to use the RACF component of the SecureWay Security Server for OS/390 (Security Server) to perform security functions. It contains an introduction to RACF, as well as sections that guide the user through basic security tasks.

For information about the other components of the Security Server, see the publications related to those components.

Who Should Use This Book

This book is for general users who need to use RACF to protect their own data sets or general resources, and for users responsible for the security of group data sets. You can use either panels or commands to perform these tasks. This book also explains how to authorize another user to submit jobs for you.

What You Should Know Before Reading This Book

This book assumes you know how to conduct a terminal session on your system. For more information about a TSO/E terminal session, see the *OS/390 TSO/E Primer*.

To use RACF, you must:

- Know how to conduct a TSO/E terminal session
- Know how to enter commands or use ISPF panels
- Be defined to RACF

How to Use This Book

To use this book:

- Read “Chapter 1. What Is RACF?” on page 1. It tells you how RACF provides security on the operating system and protects your resources.
- Choose whether to use the RACF panels or commands to perform the security tasks.
  - If you want to use panels, read “Chapter 2. Using RACF Panels” on page 3. This chapter explains how to get help while using the RACF panels.
  - If you want to use commands, “Chapter 3. Using RACF Commands” on page 5 contains a table of commands to help you perform your security tasks.
- Read “Chapter 4. How Am I Defined to RACF?” on page 13 through “Chapter 9. Protecting General Resources” on page 73. These chapters contain step-by-step procedures for you to follow; they do not require that you have had any previous experience with RACF.

- Use “Appendix A. Reference Summary” on page 79 as a reference for information such as access authority, naming conventions, and RACF-defined classes.

Where to Find More Information

Where necessary, this book references information in other books. For complete titles and order numbers for all elements of OS/390, see *OS/390 Information Roadmap*.

Softcopy Publications

The Security Server library is available on the following CD-ROMs. The CD-ROM online library collections include the IBM Library Reader, which is a program that enables you to view the softcopy books.

SK2T-6718 *OS/390 PDF Library Collection*

This collection contains the set of unlicensed books for the current release of OS/390 in Portable Document Format (PDF) files. You can view or print these files with the Adobe Acrobat reader.

SK2T-6700 *Online Library Omnibus Edition OS/390 Collection*

This softcopy collection contains a set of unlicensed books for OS/390 and related products. The collection contains the publications for multiple releases of these products.

SK2T-2180 *Online Library OS/390 SecureWay Security Server RACF Information Package*

This softcopy collection kit contains the Security Server library. It also contains the RACF/MVS Version 2 product libraries, the RACF/VM 1.10 product library, product books from the OS/390 and VM collections, International Technical Support Organization (ITSO) books (redbooks), and Washington System Center (WSC) books (orange books) that contain information related to RACF. The kit does not contain any licensed publications. By using this CD-ROM, you have access to RACF-related information from IBM products such as OS/390, VM/ESA, CICS, and NetView. For more information, see the advertisement at the back of the book.

SK2T-2177 *IBM System/390 Redbooks Collection*

This softcopy collection contains a set of S/390 redbooks.

SK2T-0710 *Online Library Omnibus Edition MVS Collection Kit*

This softcopy collection contains a set of key MVS and MVS-related product books. It also includes the RACF Version 2 product libraries.

RACF Courses

The following RACF classroom courses are available:

ES840	*Implementing RACF Security for CICS/ESA and CICS/TS*
H3917	*Basics of OS/390 SecureWay Security Server RACF Administration*
H3927	*Effective RACF Administration*
H4020	*Exploiting the Features of OS/390 SecureWay Security Server RACF*

IBM provides a variety of educational offerings for RACF. For more information about classroom courses and other offerings, do any of the following:

- See your IBM representative
- Call 1-800-IBM-TEACH (1-800-426-8322)

IBM Systems Center Publications

IBM systems centers produce red and orange books that can be helpful in setting up and using RACF. These books have not been subjected to any formal review nor have they been checked for technical accuracy, but they represent current product understanding (at the time of their publication) and provide valuable information on a wide range of RACF topics. They are not shipped with RACF; you must order them separately. A selected list of these books follows. Other books are available, but they are not included in this list, either because the information they present has been incorporated into IBM product manuals, or because their technical content is outdated.

G320-9279	*Systems Security Publications Bibliography*
GG22-9396	*Tutorial: Options for Tuning RACF*
GG24-2539	*RACF Version 2 Release 2 Technical Presentation Guide*
GG24-3378	*DFSMS and RACF Usage Considerations*
GG24-3451	*Introduction to System and Network Security: Considerations, Options, and Techniques*
GG24-3524	*Network Security Involving the NetView Family of Products*
GG24-3585	*MVS/ESA and RACF Version 1 Release 9 Security Implementation Guide*
GG24-3970	*Elements of Security: RACF Overview - Student Notes*
GG24-3971	*Elements of Security: RACF Installation - Student Notes*
GG24-3972	*Elements of Security: RACF Advanced Topics - Student Notes*
GG24-3984	*RACF Macros and Exit Coding*
GG24-4282	*Secured Single Signon in a Client/Server Environment*
GG24-4453	*Enhanced Auditing Using the RACF SMF Data Unload Utility*
GG26-2005	*RACF Support for Open Systems Technical Presentation Guide*
GC28-1210	*System/390 MVS Sysplex Hardware and Software Migration*
SG24-4580	*RACF Version 2 Release 2 Installation and Implementation Guide*
SG24-4704	*OS/390 Security Services and RACF-DCE Interoperation*
SG24-4820	*OS/390 Security Server Audit Tool and Report Application*
SG24-5158	*Ready for e-business: OS/390 Security Server Enhancements*
SG24-5339	*The OS/390 Security Server Meets Tivoli: Managing RACF with Tivoli Security Products*

Other Sources of Information

IBM provides customer-accessible discussion areas where RACF may be discussed by customer and IBM participants. Other information is also available through the Internet.

IBM Discussion Areas

IBM provides the following discussion areas for RACF and security-related topics.

- **MVSRACF**

  MVSRACF is available to customers through IBM’s TalkLink offering. To access MVSRACF from TalkLink:

  1. Select S390 (the S/390 Developers’ Association).
  2. Use the fastpath keyword: MVSRACF.

- **SECURITY**

  SECURITY is available to customers through IBM's DialIBM offering, which may be known by other names in various countries. To access SECURITY:

  1. Use the CONFER fastpath option.
  2. Select the SECURITY CFORUM.

Contact your IBM representative for information on TalkLink, DialIBM, or equivalent offerings for your country and for more information on the availability of the MVSRACF and SECURITY discussions.

Internet Sources

The following resources are available through the Internet to provide additional information about the OS/390 library and other security-related topics:

- **OS/390 Online Library**

  To view and print online versions of the OS/390 publications, use this address:

  `http://www.ibm.com/s390/os390/bkserv/`

- **System/390 Redbooks**

  The redbooks that are produced by the International Technical Support Organization (ITSO) are available at the following address:

  `http://www.ibm.com/redbooks/`

- **S/390 and OS/390 Security**

  For more information about security on the S/390 platform and OS/390, including the elements that comprise the SecureWay Security Server for OS/390, use this address:

  `http://www.ibm.com/s390/security/`

- **RACF Home Page**

  You can visit the RACF home page on the World Wide Web using this address:

  `http://www.ibm.com/s390/racf/`

- **RACF-L Discussion List**

  Customers and IBM participants may also discuss RACF on the RACF-L discussion list. RACF-L is not operated or sponsored by IBM; it is run by the University of Georgia.

  To subscribe to the RACF-L discussion and receive postings, send a note to:

  `listserv@listserv.uga.edu`

  Include the following line in the body of the note, substituting your first name and last name as indicated:

  subscribe racf-l *first_name last_name*

  To post a question or response to RACF-L, send a note, including an appropriate `Subject:` line, to:

  `racf-l@listserv.uga.edu`

- **Sample Code**

  You can get sample code, internally-developed tools, and exits to help you use RACF. This code works in our environment, at the time we make it available, but is not officially supported. Each tool or sample has a README file that describes the tool or sample and any restrictions on its use.

  To access this code from a Web browser, go to the RACF home page and select the “Downloads” topic from the navigation bar. From the IBM RACF Downloads page, you can view and download the available samples.

The code is also available from `ftp.s390.ibm.com` through anonymous FTP. To get access:

1. Log in as user **anonymous**.
2. Change the directory, as follows, to find the subdirectories that contain the sample code:

   ```
   cd os390\racf
   ```

An announcement will be posted on RACF-L, MVSRACF, and SECURITY CFORUM whenever something is added.

Note: Some Web browsers and some FTP clients (especially those using a graphical interface) might have problems using `ftp.s390.ibm.com` because of inconsistencies in the way they implement the FTP protocols. If you have problems, you can try the following:

- Try to get access by using a Web browser and the links from the RACF home page.
- Use a different FTP client. If necessary, use a client that is based on command line interfaces instead of graphical interfaces.
- If your FTP client has configuration parameters for the type of remote system, configure it as UNIX instead of MVS.

Restrictions

Because the sample code and tools are not officially supported,

- There are no guaranteed enhancements.
- No APARs can be accepted.

To Request Copies of IBM Publications

Direct your request for copies of any IBM publication to your IBM representative or to the IBM branch office serving your locality.

There is also a toll-free customer support number (1-800-879-2755) available Monday through Friday from 6:30 a.m. through 5:00 p.m. Mountain Time. You can use this number to:

- Order or inquire about IBM publications
- Resolve any software manufacturing or delivery concerns
- Activate the program reorder form to provide faster and more convenient ordering of software updates

Summary of Changes

Summary of Changes
for SC28-1917-07
OS/390 Version 2 Release 10

This book contains information previously presented in the *OS/390 Security Server (RACF) General User's Guide*, SC28-1917-06, which supports OS/390 Version 2 Release 8 and OS/390 Version 2 Release 9. The following changes appear only in the online version of this publication.

New Information

"Description of RACF Classes" on page 85 includes new classes.

This book includes terminology, maintenance, and editorial changes, including the following:

> The OS/390 Security Server, of which RACF is a component, has joined the IBM SecureWay family of products. As such, occurrences of OS/390 Security Server have been changed to SecureWay Security Server for OS/390, or its abbreviated name, Security Server. OS/390 Security Server may continue to appear in messages, panel text, and other code with SecureWay Security Server for OS/390.

Technical changes or additions to the text and illustrations are indicated by a vertical line to the left of the change.

Summary of Changes
for SC28-1917-06
OS/390 Version 2 Release 8

This book contains information previously presented in the *OS/390 Security Server (RACF) General User's Guide*, SC28-1917-05, which supports OS/390 Version 2 Release 6 and OS/390 Version 2 Release 7.

New Information

"Chapter 4. How Am I Defined to RACF?" on page 13 describes how to find out what information related to Lotus Notes for OS/390 and Novell Directory Services for OS/390 RACF has about you.

"Chapter 4. How Am I Defined to RACF?" on page 13 describes additional information in the OMVS segment of the user profile that RACF might have about you.

"Chapter 4. How Am I Defined to RACF?" on page 13 describes how to list information about your digital key rings.

"Description of RACF Classes" on page 85 includes new classes.

Summary of Changes
for SC28-1917-05
OS/390 Version 2 Release 6

This book contains information previously presented in *OS/390 Security Server (RACF) General User's Guide*, SC28-1917-04, which supports OS/390 Version 2 Release 5.

New Information

"Description of RACF Classes" on page 85 includes new classes.

Changed Information

This book includes editorial, maintenance, and terminology changes, including the following:

> As part of the name change of OpenEdition to OS/390 UNIX System Services, occurrences of OS/390 OpenEdition have been changed to OS/390 UNIX System Services or its abbreviated name, OS/390 UNIX. OpenEdition may continue to appear in messages, panel text, and other code with OS/390 UNIX System Services.

Chapter 1. What Is RACF?

Resource Access Control Facility (RACF) is a security program. It is a component of the SecureWay Security Server for OS/390 (Security Server). RACF controls what you can do on the OS/390 operating system. You can use RACF to protect your resources. RACF protects information and other resources by controlling the access to those resources. RACF provides security on OS/390 by:

- Identifying and verifying users
- Authorizing users to access protected resources
- Recording and reporting access attempts

Identifying and Verifying Users

RACF identifies you when you log on to the operating system you want to use. It does so by requiring a user identification, the user ID—a unique identification string. RACF then verifies that you are the user you say you are by requesting and checking a password. Each RACF user ID has a unique password. You should be the only one who knows your password. That way, RACF can ensure personal accountability.

When you are first defined to RACF, your group or security administrator assigns you a user ID and a temporary password. This temporary password enables you to log on to the system the first time. As soon as you log on, RACF requires you to supply a new password of your choice. Your password may expire after a certain time interval, so you may have to change it periodically. See "Changing Your Password" on page 39 for information on how to do this.

Note: Your password may have to satisfy certain installation-defined rules. For example, your password may have to be longer than five characters, and be made up of a mixture of alphabetic and numeric characters. Check with your system administrator or security administrator for the rules you should follow when you create a password.

Authorizing Users to Access Protected Resources

RACF enables your organization to define individuals and groups who use the system RACF protects. For example, for a secretary in your organization, a security administrator uses RACF to define a user profile that defines the secretary's user ID, initial password, and other information.

A *group* is a collection of individuals who have common needs and requirements. For example, the secretaries for a whole department may be defined as one group.

RACF also enables an installation to define what authorities you have, or what authorities a group to which you belong has. RACF controls what you can do on the system. Some individuals have a great degree of authority, while others have little authority. The degree of authority you are given is based on what you need to do your job.

Besides defining user and group authorities, RACF protects resources. A *resource* is your organization's information stored in its computer system, such as data sets. For example, a secretary might have a data set as a resource. RACF provides a way to control who has authority to access a resource.

RACF stores all this information about users, groups, and resources in profiles. A *profile* is a record of RACF information that has been defined by the security administrator. There are user, group, and resource profiles.

Using information in its profiles, RACF authorizes access to certain resources. RACF applies user attributes, group authorities, and resource authorities to control use of the system.

- Your user profile provides your user attributes. User attributes describe what system-wide and group-wide access privileges you have to protected resources.
- Your group profile describes the kind of authority you as a group member have to access resources that belong to your group.
- The resources themselves have profiles describing the type of authority needed to use them.

The security administrator or someone in authority in your organization controls the information in your user profile, in group profiles, and in resource profiles. You, as the end user, control the information in profiles describing your own resources, such as your own data sets. You can protect your data by setting up resource profiles.

A *resource profile* can contain an access list as well as a default level of access authority for the resources it protects. An *access list* identifies the access authorities of specific users and groups, while the default level of access authority applies to anyone not specifically in the access list. You can specify the users you want on the access list and what authority they have to use your data. You can change your resource profiles, but you cannot change the user or group profiles, since they are established by the system administrator.

RACF enables you to perform security tasks. You can use RACF to see the authorities you have, to protect your resources with profiles you create, or to give other users the authority to access your resources. For example, you may want to let someone look at a data set that contains a program you are developing, but not be able to change that data set. In the data set’s profile, you can add that person to the access list with the authority to view, but not change, your data. In this way, RACF helps you protect your work.

Recording and Reporting Access Attempts

Besides uniquely identifying and authorizing you, RACF can record what you do on the system. It keeps track of what happens on the system so that your organization can monitor who is logged on the system at any time. RACF reports if persons have attempted to perform unauthorized actions. For example, RACF can record when someone who does not have the proper authority tries to use or change your data.

Chapter 2. Using RACF Panels

If your installation has installed the RACF panels, you can use them to perform security tasks. To get to the RACF panels, enter the command:

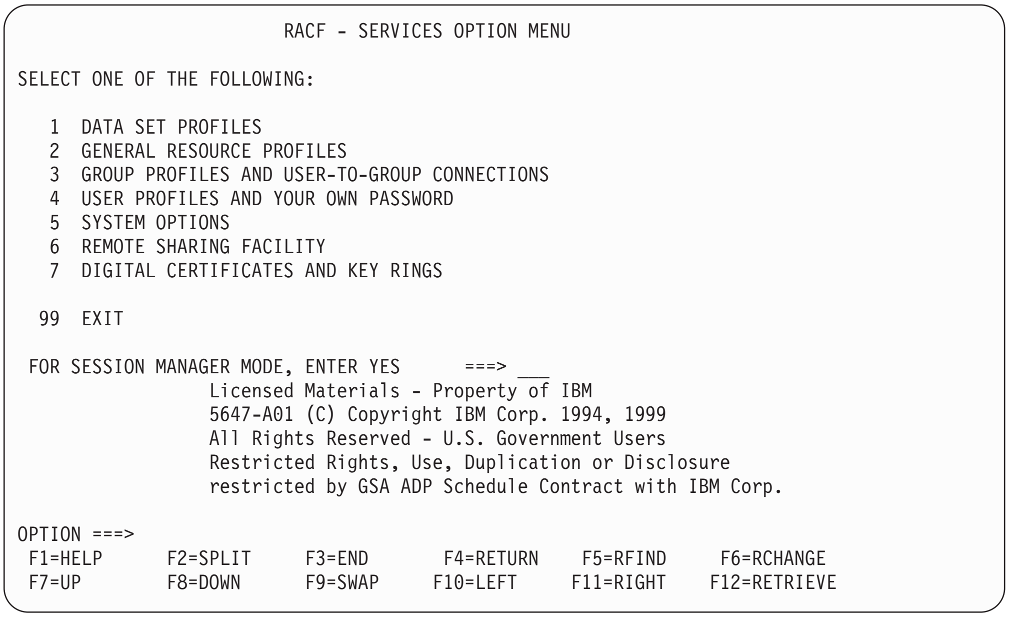
```
ISPF
```

The Interactive System Productivity Facility (ISPF) primary menu appears. Choose option **R** for RACF.

Notes:

1. Although this is the usual way to access RACF panels, your installation may have implemented a different path. Check with your security administrator for more information.
2. From any panel, pressing PF1 leads you to a help screen.

When you choose option **R**, you will see a screen that looks something like this:



```
                          RACF - SERVICES OPTION MENU

SELECT ONE OF THE FOLLOWING:

   1  DATA SET PROFILES
   2  GENERAL RESOURCE PROFILES
   3  GROUP PROFILES AND USER-TO-GROUP CONNECTIONS
   4  USER PROFILES AND YOUR OWN PASSWORD
   5  SYSTEM OPTIONS
   6  REMOTE SHARING FACILITY
   7  DIGITAL CERTIFICATES AND KEY RINGS

  99  EXIT

 FOR SESSION MANAGER MODE, ENTER YES      ===> ___
                  Licensed Materials - Property of IBM
                  5647-A01 (C) Copyright IBM Corp. 1994, 1999
                  All Rights Reserved - U.S. Government Users
                  Restricted Rights, Use, Duplication or Disclosure
                  restricted by GSA ADP Schedule Contract with IBM Corp.

OPTION ===>
 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=RCHANGE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

Figure 1. The ISPF Primary Menu Panel

The session manager mode prompt appears on this panel only if the session manager has been installed on your system.

You may need to know the panel ID for diagnosis purposes. To display the panel ID in the upper left part of the screen, enter the following ISPF command on the option line:

```
PANELID
```

You can access help information for the RACF panels. Help panels exist for each individual panel. If you have a question about the information you should provide on the panel, type **HELP** on the command line. The help panels give more information about the terms on the panel and the information you should enter.

Chapter 3. Using RACF Commands

You can use RACF commands to perform security tasks. RACF commands enable you to find out how you are defined to RACF, how to protect your resources, how to change another user's access to your resources, and how to change the way RACF defines you. You can enter RACF commands directly in the foreground during a TSO command terminal session.

This book shows examples of RACF commands in uppercase letters. When you enter these commands from a terminal or workstation, you can use uppercase letters, lowercase letters, or both.

Note: You might not be able to do all of these tasks, depending on how your security administrator sets up RACF on your system.

RACF Commands for General User Tasks

Table 1 shows which command to use for each task and where it is described.

Table 1. RACF Command Table for General User Tasks

Task	Command	Topic
Find out how you are defined to RACF	`LISTUSER`	14
Find out what CICS information RACF has about you	`LISTUSER` *your-userid* `CICS NORACF`	22
Find out what DCE information RACF has about you	`LISTUSER` *your-userid* `DCE NORACF`	23
Find out what DFP information RACF has about you	`LISTUSER` *your-userid* `DFP NORACF`	23
Find out what language information RACF has about you	`LISTUSER` *your-userid* `LANGUAGE NORACF`	24
Find out what information related to Lotus Notes for OS/390 RACF has about you	`LISTUSER` *your-userid* `LNOTES NORACF`	25
Find out what NetView information RACF has about you	`LISTUSER` *your-userid* `NETVIEW NORACF`	26
Find out what information related to Novell Directory Services for OS/390 RACF has about you	`LISTUSER` *your-userid* `NDS NORACF`	27
Find out what OS/390 UNIX System Services (OS/390 UNIX) information RACF has about you	`LISTUSER` *your-userid* `OMVS NORACF`	30
Find out what OPERPARM information RACF has about you	`LISTUSER` *your-userid* `OPERPARM NORACF`	28
Find out what OpenEdition for VM/ESA (OpenEdition VM) information RACF has about you	`LISTUSER` *your-userid* `OVM NORACF`	28
Find out what TSO/E information RACF has about you	`LISTUSER` *your-userid* `TSO NORACF`	32
Find out what WORKATTR information RACF has about you	`LISTUSER` *your-userid* `WORKATTR NORACF`	33
List all of your user ID associations	`RACLINK LIST`	34

Table 1. RACF Command Table for General User Tasks (continued)

Task	Command	Topic
List all of your user ID associations with a specific node, user ID, or both	RACLINK LIST(*node.userid*)	35
List all of your digital certificates	RACDCERT LIST	36
List all of your digital certificate key rings	RACDCERT LISTRING(*)	36
Change your password (*pw*)	PASSWORD PASSWORD(*current-pw new-pw*)	39
Change your password interval	PASSWORD INTERVAL(*interval-you-want*)	39
Log on to a group other than your default group	LOGON *userid* GROUP(*groupname*) **Note:** The LOGON command is a TSO command, not a RACF command.	42
Log on with a security label other than your default security label	LOGON *userid* SECLABEL(*security-label*) **Note:** The LOGON command is a TSO command, not a RACF command.	43

Allow another user to submit your jobs	PERMIT CLASS(SURROGAT) *userid*.SUBMIT
	ID(*surrogate-userid*)
	ACCESS(READ)
		44

Enable your user IDs to have their passwords become synchronized as they are changed	RACLINK DEFINE(*target-node.target-userid*) PEER(PWSYNC) RACLINK APPROVE(*node.userid*) **Note:** These commands need to be entered only once. All passwords are automatically changed after the password is changed for any one of the associated user IDs.	46

Define a peer user ID association with password synchronization	RACLINK
	DEFINE(*target-node.target-userid*)
	PEER(PWSYNC)
		46

Define a peer user ID association without password synchronization	RACLINK
	DEFINE(*target-node.target-userid*)
	PEER(NOPWSYNC)
		46

Define a managed user ID association	RACLINK DEFINE(*target-node.target-userid*) MANAGED	47
Approve a user ID association	RACLINK APPROVE(*node.userid*)	48
Delete a pending or existing user ID association	RACLINK UNDEFINE(*node.userid*)	48
Create a discrete profile to protect a cataloged data set	ADDSD '*dataset-name*' UACC(*access-authority*)	51

Create a discrete profile to protect an uncataloged data set	ADDSD '*dataset-name*' UNIT(*type*)
	VOLUME(*volume-serial*)
	UACC(*access-authority*)
		51

Table 1. RACF Command Table for General User Tasks (continued)

Task	Command	Topic
Create a generic profile to protect a data set	ADDSD '*dataset-name-with-generic-char.*' UACC(*access-authority*) **or** ADDSD '*dataset-name*' UACC(*access-authority*) GENERIC	53
Find out how a data set is protected	LISTDSD DATASET('*dataset-name*') ALL **or** LISTDSD DATASET('*dataset-name*') ALL GENERIC	58
Check what data set profiles you have	SEARCH	64
Delete a data set profile	DELDSD '*profile-name*'	64
Create a profile to protect a cataloged tape data set	ADDSD '*dataset-name*' TAPE UACC(*access-authority*)	67

Create a profile to protect an uncataloged tape data set	ADDSD '*dataset-name*' TAPE UNIT(*type*)
	VOLUME(*volume-serial*)
	FILESEQ(*number*)
	UACC(*access-authority*)
		67

Change a data set's universal access authority	ALTDSD '*profile-name*' UACC(*access-authority*)	69

Permit an individual or a group to use a data set	PERMIT '*profile-name*'
	ID(*userid*|*groupname*)
	ACCESS(*level*)
		70

Deny an individual or a group use of a data set	PERMIT '*profile-name*' ID(*userid*|*groupname*) ACCESS(NONE) **or** PERMIT '*profile-name*' ID(*userid*|*groupname*) DELETE	71
Search for general resource profile names	SEARCH CLASS(*classname*)	73
List the contents of general resource profiles	RLIST *classname profile-name*	74

Permit an individual or a group to use a general resource	PERMIT *profile-name*
	CLASS(*classname*)
	ID(*userid*|*groupname*)
	ACCESS(*access-authority*)
		75

Deny an individual or a group the use of a general resource	PERMIT *profile-name* CLASS(*classname*) ID(*userid*|*groupname*) ACCESS(NONE) **or** PERMIT *profile-name* CLASS(*classname*) ID(*userid*|*groupname*) DELETE	76

Getting Online Help for RACF Commands

You can get online help for RACF commands; to so, issue the following command:

```
HELP command-name
```

For example, to see online help for the PERMIT command, enter:

```
HELP PERMIT
```

To limit the information displayed, use the SYNTAX operand on the HELP command:

```
HELP command-name SYNTAX
```

For example, to see only the syntax of the PERMIT command, enter:

```
HELP PERMIT SYNTAX
```

For more information about the HELP command and other useful operands, see *OS/390 SecureWay Security Server RACF Command Language Reference*.

Escaping from a Command Prompt Sequence

If you make a mistake while entering a RACF command during a TSO terminal session, you might receive IKJ messages such as `INVALID KEYWORD` and `REENTER THIS OPERAND`. These messages describe the syntax error and will prompt you to reenter the input. To end the prompting sequence, enter the requested information or press the attention interrupt key (PA1) to cancel the command.

Using Command Abbreviations

You can abbreviate an operand on a TSO command to the least number of characters that uniquely identify the operand. To avoid conflicts in abbreviations, it is a good practice to fully spell out all operands on commands that are hardcoded (for example, in programs and CLISTs).

Directing Commands

The RACF remote sharing facility (RRSF) lets you direct most RACF commands to be processed on a node and user ID other than the one you are currently logged on to. You can also direct a command to the user ID you are currently logged on to. Directed commands run asynchronously; that is, the command issuer does not wait until the command completes processing, and results and output from the commands are returned to the command issuer in a data set. *OS/390 SecureWay Security Server RACF Command Language Reference* lists the commands that can be directed. See “User ID Associations” on page 46 for information on creating the user ID associations necessary to direct commands. Also, you must have authorization to direct commands. If you are not sure whether you are authorized, contact your security administrator or see *OS/390 SecureWay Security Server RACF Security Administrator’s Guide* for more information.

You can use the AT keyword to direct allowed RACF commands to be processed under the authority of an associated user ID without actually logging on to that ID. Add the AT keyword to the end of any allowed RACF command and specify the node and user ID (*node.userid*) at which the command should be processed. A user ID association is required for all commands directed to another node or user ID, but it is not required if you are directing the command to the user ID you are currently logged on to.

When you direct a command, the results are returned to you and are appended to the bottom of your RRSFLIST user data set. You receive a TSO SEND message telling you whether the directed command completed successfully or unsuccessfully. If you do not have an RRSFLIST user data set, RACF allocates one and adds the results. The RRSFLIST data set name is '*prefix.userid*.RRSFLIST', where *prefix* is your TSO prefix at the time you issued the command. If *prefix* matches *userid* or if you specified PROFILE NOPREFIX on the TSO PROFILE command, the data set name used is '*userid*.RRSFLIST'.

You are responsible for maintaining this data set. If your data set becomes full, the output is transmitted to your user ID. In order for RACF to append to your RRSFLIST user data set again, you must edit and delete some of the returned output in this data set. If your RRSFLIST user data set is in use when the RACF remote sharing facility tries to append the results, RACF waits for a brief time and tries again. This could cause the results of directed commands to be appended out of sequence with the output that was returned.

Format of Output

The following examples illustrate the format of the output produced by directed commands. The format of the output is the same for both your RRSFLIST data set and for the output transmitted when your data set is full. Figure 2 shows the format of output for this directed LISTGRP command:

```
LISTGRP (SYS1) AT(MVS03.SMITHJ)
```

Figure 3 shows the format of output for this directed ADDSD command:

```
ADDSD 'JWS.DEV*' AT(MVS02.JWS)
```

```
=========================================================================
LG issued at 09:14:32 on 02/02/98 was processed at MVS03.SMITHJ on
02/02/98 at 09:16:24

 COMMAND ISSUED: LISTGRP   (SYS1)

 COMMAND OUTPUT:
 INFORMATION FOR GROUP SYS1
     SUPERIOR GROUP=NONE         OWNER=SMITHJ
     NO INSTALLATION DATA
     NO MODEL DATA SET
     TERMUACC ..................

=========================================================================
```

Figure 2. A Directed LISTGRP Command: Sample Output

```
=========================================================================
ADDSD issued at 09:47:32 on 02/02/98 was processed at MVS02.JWS on
02/02/98 at 09:48:51

 COMMAND ISSUED: ADDSD        'JWS.DEV*'

 COMMAND OUTPUT:
 IRRR008I Command succeeded.  There are no messages.
=========================================================================
```

Figure 3. A Directed ADDSD Command: Sample Output

Automatic Command Direction

Automatic command direction, which is an extension of command direction, is useful primarily for keeping already-synchronized RACF profiles synchronized between two or more remote nodes. Every automatically directed command is processed on the node that originates the command; profiles in the RRSFDATA class identify the other nodes where the command should also be processed. Your RACF security administrator sets up these profiles. No user ID associations are required for automatic command direction. If user ID associations are defined, they are ignored during processing for automatic command direction.

Also, an installation decides who should be notified of results and output from automatically directed commands, so you may or may not see output or TSO SEND messages from automatically-directed commands.

If you get output or notification that an automatically directed command failed, notify your RACF security administrator. This is an indication that the RACF profiles are no longer synchronized.

Format of Output

The format of the output for automatic command direction is similar to the output from directed commands, with one additional line for automatic command direction. Figure 4 shows the format of output for an automatically directed ADDUSER command. Figure 5 shows the format of output for an automatically directed RDEFINE command.

```
=========================================================================
ADDUSER issued at 10:42:33 on 04/03/98 was processed at NODEA.LAURIE
on 04/03/98 at 10:43:45
Command was propagated by automatic direction from NODEB.LAURIE

 COMMAND ISSUED:  ADDUSER (ANDREW) PASSWORD() NAME('####################')
 AUTHORITY(USE) NOSPECIAL UACC(NONE) NOOPERATIONS NOADSP NOGRPACC NOAUDITOR

 COMMAND OUTPUT:
 IRRR008I Command succeeded.  There are no messages.
=========================================================================
```

Figure 4. An Automatically-Directed ADDUSER Command: Sample Output

```
=========================================================================
RDEFINE issued at 12:33:41 on 04/03/98 was processed at NODEA.LAURIE
on 04/03/98 at 12:35:02
Command was propagated by automatic direction from NODEB.LAURIE

 COMMAND ISSUED:  RDEFINE AUTODIRECT.**  UACC(NONE)

 COMMAND OUTPUT:
 ICH10102I AUTODIRECT.** ALREADY DEFINED TO CLASS RRSFDATA.
=========================================================================
```

Figure 5. An Automatically-Directed RDEFINE Command: Sample Output

Getting Help for RACF Messages

If a RACF command fails, you receive a message. If you do not get a message ID, enter:

```
PROFILE MSGID
```

Then, reenter the RACF command that failed. The message appears with the message ID. Refer to *OS/390 SecureWay Security Server RACF Messages and Codes* for help if the message ID starts with ICH or IRR.

Viewing Notification Messages

To see notification messages from command direction and password synchronization, enter:

```
PROFILE INTERCOM
```

To suppress notification messages from command direction and password synchronization, enter:

```
PROFILE NOINTERCOM
```

Notes:

1. RACF uses the INTERCOM setting at the time the directed command or password synchronization change occurred and if the setting was NOINTERCOM at that time, RACF does not issue a message after that command has processed.
2. If automatic command direction is active and your RACF security administrator has enabled notification for command issuers, the INTERCOM setting also controls notification messages from automatically directed commands.

Chapter 4. How Am I Defined to RACF?

To log on to a system, you must be defined to RACF. RACF records security information about you in a user profile. The profile contains information about when you last updated your password, what group you belong to, and what individual and group authority you have on the system. This chapter shows you how to find out how RACF has defined you to the system.

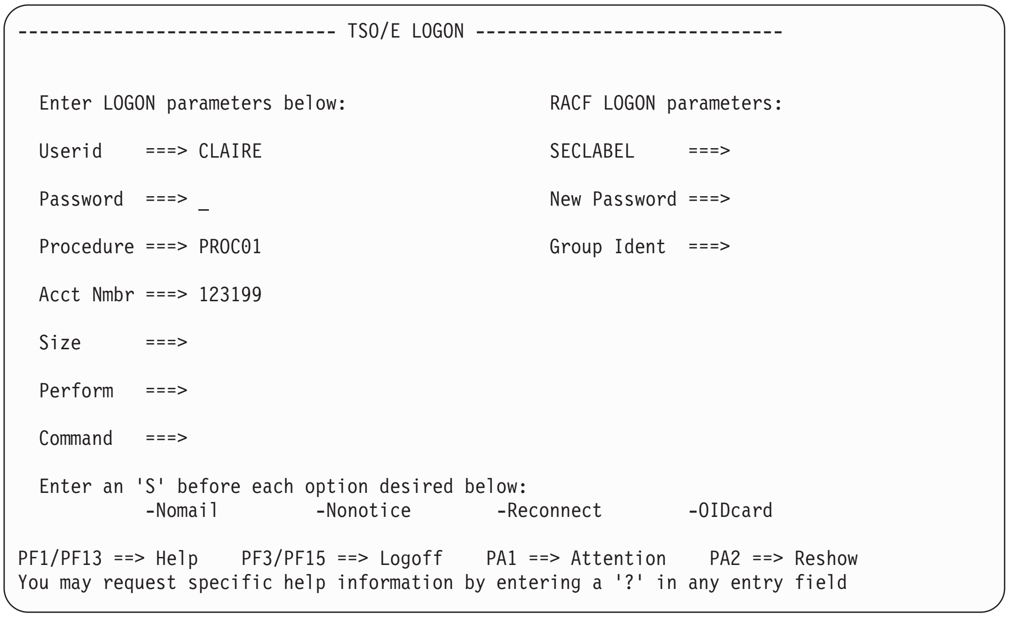
Finding Out If You Are Defined to RACF

The RACF security administrator defines new RACF users and permits them to use the system and certain protected resources. When you are defined to RACF, your ability to use the system is defined at the same time. Being RACF-defined makes your identity known to RACF and describes your authority: what you may do and what resources you may use to do your job.

If you do not know your user ID, see your RACF security administrator or someone in authority at your installation, for example, a supervisor. Without a user ID you cannot use the system.

Note: If you are RACF-defined and this is the first time you have ever logged on to the system, you must change your password. After you have entered your assigned temporary password, you will receive a message saying that it has expired. Enter a new password of your choice, following the password rules set by your installation. See “Changing Your Password” on page 39 for information about changing your password periodically.

Log on to the system. Figure 6 shows a sample logon panel:



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


  Enter LOGON parameters below:                   RACF LOGON parameters:

  Userid    ===> CLAIRE                           SECLABEL     ===>

  Password  ===> _                                New Password ===>

  Procedure ===> PROC01                           Group Ident  ===>

  Acct Nmbr ===> 123199

  Size      ===>

  Perform   ===>

  Command   ===>

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

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

Figure 6. A Sample Logon Panel

Look at the right side of your logon panel. If the **New Password**, **Group Ident**, and optionally, the **SECLABEL** fields appear, you are defined to RACF.

Finding Out How You Are Defined to RACF

As discussed in “Chapter 1. What Is RACF?” on page 1, RACF builds a description of you and your authority in a user profile. Each RACF-defined user has a user profile containing information about his or her identity, user attributes, group, and password. You belong to at least one group. This group is a default group to which your security administrator has assigned you. RACF has a profile defined for this group. This profile contains information about the group, its members, and the authority its members have to use the group’s resources.

To see a list of the information that RACF has about you and the group to which you belong, enter the command:

```
LISTUSER your-userid
```

Figure 7 shows the fields that appear in the LISTUSER command output. “Understanding the Information RACF Has about You as a User” on page 15 and “Finding Out What Authority You Have as a Member of a Group” on page 17 describe what this RACF information means. Figure 8 on page 20 and Figure 9 on page 21 show examples of LISTUSER command output.

Note: If you issue the LISTUSER command and do not specify a user ID, the current user ID information is displayed, which is the default.

```
USER=userid  NAME=your-user-name       OWNER=owner     CREATED=yy.nnn

 DEFAULT-GROUP=group     PASSDATE=yy.nnn  PASS-INTERVAL=nnn

 ATTRIBUTES=your operating privileges and restrictions

REVOKE DATE=date   RESUME DATE=date

LAST-ACCESS=yy.nnn/hh:mm:ss

CLASS AUTHORIZATIONS=installation-defined classes where you can define
profiles

INSTALLATION-DATA=information your installation maintains about you

MODEL-NAME=profile used as a model for new data set profiles

LOGON ALLOWED   (DAYS)          (TIME)
---------------------------------------------
days you have access            times you have access

 GROUP=group    AUTH=auth   CONNECT-OWNER=owner   CONNECT-DATE=yy.ddd

    CONNECTS=nn  UACC=uacc     LAST-CONNECT=connect time

    CONNECT ATTRIBUTES=your operating privileges as a group member

    REVOKE DATE=date   RESUME DATE=date

SECURITY-LEVEL=your installation-assigned security level

CATEGORY-AUTHORIZATION
 your installation-assigned security categories

SECURITY-LABEL=your installation-assigned security label
```

Figure 7. LISTUSER Output: Description

Understanding the Information RACF Has about You as a User

As Figure 7 on page 14 shows, RACF displays the following information you issue the LISTUSER command.

USER
Your *userid* is the name by which the system knows you. It is frequently a combination of such identifying information as your name, initials, personnel number, or department.

NAME
Your name as recorded in your user profile.

OWNER
The user ID or group name of the owner of your user profile. The owner of your profile can modify your profile.

CREATED
The date you were defined to RACF.

DEFAULT-GROUP
RACF connects each user to at least one group. If you are a member of only one group, that group is your default group and that group name appears in this field.

If you belong to more than one group, and have no trouble accessing information belonging to the various groups to which you belong, you can ignore this field. If you have difficulty using group resources of a group to which you belong, log on again and specify the group to which you want to be connected at the logon panel. (If you do not specify the group, RACF assumes the group named in this field.)

PASSDATE
The date you last updated your password.

PASS-INTERVAL
The number of days your current password is valid. You must change your password before this interval expires.

ATTRIBUTES
The system operating privileges and restrictions assigned to you. This field describes your system-wide attributes.

NONE Gives you no *special* operating privileges or restrictions; most users have this attribute. However, users with the NONE attribute can still use RACF. In fact, most other attributes allow extraordinary privileges, and generally only a few users or groups have these attributes.

SPECIAL
Gives you full authorization to modify all profiles in the RACF database and lets you perform all RACF functions except those requiring the AUDITOR attribute.

AUDITOR
Lets you audit the use of system resources, control the logging of detected accesses to resources, and create security reports.

OPERATIONS
Allows you to have full authorization to all RACF-protected data sets and to general resources that meet certain conditions (described in *OS/390 SecureWay Security Server RACF Security Administrator's*

Guide). OPERATIONS allows you to perform any maintenance operations, such as copying and reorganizing a RACF-protected resource.

GRPACC
Allows you to have the group data sets you allocate automatically accessible to other users in the specified group.

CLAUTH
Allows you to define profiles for any class specified in the class name.

ADSP Is the automatic data set protection attribute. If you have the ADSP attribute, RACF creates a discrete profile for every permanent DASD or tape data set you create. If your installation is using automatic direction of application updates and you have the ADSP attribute, you may be notified of the results and output from these application updates. See "Automatic Direction of Application Updates" on page 84 for more information.

REVOKE
Prohibits a user from entering the system. (You should never be able to see this attribute when you list your own profile.)

REVOKE DATE
This is the date on which RACF prevents you from using the system.

RESUME DATE
This is the date on which RACF allows you to use the system again.

LAST-ACCESS
This date is the last time you were on the system. RACF keeps records of all persons who have used the system, and what they have done, as well as recording unauthorized attempts to use the system.

CLASS AUTHORIZATIONS
Your installation assigns resources to various classes. The class appearing in this field is the class in which the user is authorized to assign RACF protection.

INSTALLATION-DATA
Additional information your installation maintains about you and your authority. If you need help understanding anything in this field, see your RACF security administrator or the owner of your user profile. If NO-INSTALLATION-DATA appears in this field, your installation is not maintaining additional information.

MODEL-NAME
If a profile name appears in this field, the profile is used as a model when you create data set profiles that have your user ID as the high-level qualifier. If NO-MODEL-NAME appears in this field, no profile is being used as a model.

LOGON ALLOWED
The days of the week and/or hours in the day that RACF allows you to access the system from a terminal. These restrictions only limit the periods during which you can log on to the system. If you are working on the system and an end-time occurs, RACF does not force you off the system. Also, these logon restrictions do not apply to batch jobs; you can still submit a batch job at any time.

SECURITY-LEVEL
Your installation can define various security levels. The name appearing in this field is the security level assigned to you.

CATEGORY-AUTHORIZATION
Your installation can define various security categories. The names appearing in this field are the security categories assigned to you.

SECURITY-LABEL
Your installation can define various security labels. A security label is a name used to represent the association between a particular security level and certain security categories. The name appearing in this field is your default security label.

Note: When you specify the user ID on the LISTUSER command, the default security label from the user profile is displayed in the output. When you do not specify the user ID on the LISTUSER command, the security label you are currently logged on with is displayed in the output.

Finding Out What Authority You Have as a Member of a Group

A group is a number of users defined together because of their common needs. For example, a group may be all the secretaries in a particular department. A group shares common access requirements to resources or has similar attributes within the system.

When you log on, RACF connects you to your default group. If you wish to log on to a group other than your default group, you can specify the group name when you log on. The group that you specify becomes your current connect group. When you are connected to a group, RACF allows you the privileges of the group.

You can receive this information about the groups to which you belong by using the following command.

```
LISTUSER your-userid
```

The information in the second part of the screen shown in Figure 7 on page 14 describes the RACF group or groups to which you belong and what you can do as a member of that group.

This section is repeated once for each RACF group of which you are a member. RACF uses the following terms to describe the group to which you belong and your authorities as a member of the group.

GROUP
The name of a group of which you are a member.

AUTH
The group authorities you have because you are a member of this group.

USE Allows you to enter the system under the control of the specified group. You may use any of the data sets the group may use.

CREATE
Allows you to RACF-protect group data sets and control who can access them. It includes the privileges of the USE authority.

CONNECT
Allows you to connect RACF-defined users to the specified group and assign these users the USE, CREATE, or CONNECT authority. It includes the privileges of the CREATE authority.

JOIN Allows you to define new users or groups to RACF and to assign group authorities. To define new users, you must also have the user attribute, CLAUTH(USER). JOIN authority includes all the privileges of the CONNECT authority.

CONNECT-OWNER
The owner of this group.

CONNECT-DATE
The date you were first connected to this group.

CONNECTS
The number of times you have been connected to this group.

UACC
The universal access authority for resources you create while connected to this group. If a user is not specifically listed in the access list describing a resource owned by the connect group, RACF looks at UACC and allows the user to use the resource in the manner specified in the UACC.

The UACC can be one of the following:

NONE Does not allow users to access the data set.

> **Attention**
> Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you may want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See “Permitting an Individual or a Group to Use a Data Set” on page 70 for information on how to permit selected users or groups to access a data set.)

READ Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

UPDATE
Allows users to read from, copy from, or write to the data set. UPDATE does not, however, authorize a user to delete, rename, move, or scratch the data set.

CONTROL
For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform control-interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER
ALTER allows users to read, update, delete, rename, move, or scratch the data set.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list*. However, ALTER does not allow users to change the owner of the profile.

When specified in a generic profile, ALTER gives users *no* authority over the profile itself, but allows users to create new data sets that are covered by that profile.

EXECUTE
For a private load library, EXECUTE allows users to load and execute, but not read or copy, programs (load modules) in the library.

Note: In order to specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

LAST-CONNECT
The last time you logged on or submitted a batch job with either the group as your default group or with the group explicitly specified. If you were never previously connected to the group, UNKNOWN is displayed.

CONNECT-ATTRIBUTES
The operating privileges and restrictions assigned to you when you are connected to this group. Connect attributes are also called group-level attributes. The connect (group-level) attributes are:

NONE Allows no *special* operating privileges or restrictions. Users with the NONE attribute can still use RACF. In fact, most other attributes allow extraordinary privileges, and generally only a few users or groups have these attributes.

SPECIAL
Gives you full authorization to all profiles in the RACF database and lets you perform all RACF functions except those requiring the AUDITOR attribute.

AUDITOR
Lets you audit the use of system resources, control the logging of detected accesses to resources, and create security reports.

OPERATIONS
Gives you full authorization to all RACF-protected data sets and to general resources that meet certain conditions (described in *OS/390 SecureWay Security Server RACF Security Administrator’s Guide*). OPERATIONS lets you perform any maintenance operations, such as copying and reorganizing a RACF-protected resource.

GRPACC
Lets you have the group data sets that you allocate automatically accessible to other users in the specified group.

CLAUTH
Lets you define profiles for any class specified in the class name.

ADSP Is the automatic data set protection attribute. If you have the ADSP attribute, RACF creates a discrete profile for every permanent DASD or tape data set you create. If your installation is using automatic direction of application updates and you have the ADSP attribute, you may be notified of the results and output from these application updates. See “Automatic Direction of Application Updates” on page 84 for more information.

REVOKE
Prohibits a user from entering the system. (You should never be able to see this attribute when you list your own profile.)

REVOKE DATE
This is the date on which RACF prevents you from using the system when you try to connect to the group.

RESUME DATE
This is the date on which RACF allows you to use the system again when you are connected to the group.

Examples of Output of the LISTUSER Command

This section contains examples of the output that is produced by the LISTUSER command for two typical RACF users.

Example 1:

G.L. Kline is an employee in the payroll department. G.L. Kline has a user ID of KLINE. If he entered the LISTUSER command, he would see output similar to that shown in Figure 8.

```
USER=KLINE    NAME=G.L.KLINE  OWNER=JONES    CREATED=96.091

 DEFAULT-GROUP=PAYROLL   PASSDATE=98.124  PASS-INTERVAL= 30

 ATTRIBUTES=NONE

 REVOKE DATE=NONE   RESUME DATE=NONE

 LAST-ACCESS=98.130/13:47:18

 CLASS AUTHORIZATIONS=NONE

 NO-INSTALLATION-DATA

 NO-MODEL-NAME

 LOGON ALLOWED   (DAYS)           (TIME)

-----------------------------------------------------------------

ANYDAY                           ANYTIME

 GROUP=PAYROLL  AUTH=USE  CONNECT-OWNER=JONES  CONNECT-DATE=96.091

   CONNECTS= 05   UACC=NONE       LAST-CONNECT=98.130/13:47:18

     CONNECT ATTRIBUTES=NONE

     REVOKE DATE=NONE   RESUME DATE=NONE

SECURITY-LEVEL=NONE SPECIFIED

CATEGORY-AUTHORIZATION
 NONE SPECIFIED

SECURITY-LABEL=NONE SPECIFIED
```

Figure 8. LISTUSER Output: Example 1

In this example, user G.L. Kline is connected to only one group, PAYROLL. He has none of the possible user attributes, but can still use RACF. For example, Kline can create, change, and delete RACF profiles to protect his data sets.

Example 2:

D. Jones is an employee in the auditing department. D. Jones has a user ID of DJONES. If she enters the LISTUSER command, she sees output similar to that shown in Figure 9.

```
USER=DJONES  NAME=D. JONES  OWNER=RYAN      CREATED=96.091

 DEFAULT-GROUP=SEARCH    PASSDATE=98.103   PASS-INTERVAL= 30

 ATTRIBUTES=AUDITOR

 REVOKE DATE=NONE   RESUME DATE=NONE

 LAST-ACCESS=98.114/13:47:18

 CLASS AUTHORIZATIONS=NONE

 NO-INSTALLATION-DATA

 NO-MODEL-NAME

 LOGON ALLOWED   (DAYS)           (TIME)

-----------------------------------------------------------------

ANYDAY                           ANYTIME

 GROUP=SEARCH AUTH=JOIN CONNECT-OWNER=WILL CONNECT-DATE=96.091

   CONNECTS= 01   UACC=NONE   LAST-CONNECT=98.114/13:50:18

   CONNECT ATTRIBUTES=NONE

   REVOKE DATE=NONE   RESUME DATE=NONE

 GROUP=PAYROLL AUTH=CREATE CONNECT-OWNER=MILL CONNECT-DATE=96.091

   CONNECTS= 00  UACC=READ  LAST-CONNECT=98.114/13:55:18

   CONNECT ATTRIBUTES=NONE

   REVOKE DATE=NONE   RESUME DATE=NONE

SECURITY-LEVEL=NONE SPECIFIED

CATEGORY-AUTHORIZATION
 NONE SPECIFIED

SECURITY-LABEL=NONE SPECIFIED
```

Figure 9. LISTUSER Output: Example 2

In this example, Jones is connected to two groups, SEARCH and PAYROLL. She has the AUDITOR system-wide attribute. Jones control access to her data sets and, as system AUDITOR, she can audit security controls and create security reports.

In the SEARCH group, Jones has JOIN group authority and can assign group authorities to members of the group. In the PAYROLL group, Jones has CREATE group authority and can create data set profiles to protect group data sets.

In the PAYROLL group, Jones also has assigned a UACC (universal access authority) of READ. If Jones logs on using PAYROLL as the current connect group, any data set profiles she creates have a UACC of READ (unless she specifies otherwise). For information on how to log on using a different connect group, see “Logging On to a Group Other Than Your Default Group” on page 42.

Finding Out What CICS Information RACF Has about You

Your user profile may contain CICS information about you. RACF lists the following details from the CICS segment of the user profile:

- The classes assigned to this operator to which BMS messages are sent (OPCLASS)
- Whether or not the operator is forced off when an XRFSOFF takeover occurs (XRFSOFF)
- The operator identification (OPIDENT)
- The priority of the operator (OPPRTY)
- The time (in minutes or hours:minutes) that the operator is allowed to be idle before being signed off (TIMEOUT)

Note: The RACF security administrator controls whether you can view all or some of the details of your CICS information.

The CICS information in the LISTUSER output has the following format:

```
USER=your user ID

CICS INFORMATION
----------------
 OPCLASS= operator classes
 OPIDENT= operator class
 OPPRTY=  operator identification
 TIMEOUT= idle time allowed
 XRFSOFF= whether or not force-off will occur
```

Figure 10. LISTUSER Output: Description of the CICS Information

Note: The ability to view and update CICS information can be controlled on a field by field basis; therefore, individual fields may not appear on your output.

To see the CICS information, issue the LISTUSER command as follows:

```
LISTUSER your-userid CICS NORACF
```

If there is CICS information in your profile, you see output similar to this:

```
 USER=DJONES

CICS INFORMATION
----------------
 OPCLASS= 001
 OPIDENT= ID2
 OPPRTY= 00010
 TIMEOUT= 12:34
 XRFSOFF= NOFORCE
```

Figure 11. LISTUSER Output: Sample CICS Information

Finding Out What DCE Information RACF Has about You

Your user profile may contain DCE information about you. RACF lists the following details from the DCE segment of the user profile:
- Your DCE principal name (DCENAME)
- Your DCE universal unique identifier (UUID)
- Your DCE home cell (HOMECELL)
- The home cell's universal unique identifier (HOMEUUID)
- Whether you have single signon processing (AUTOLOGIN)

Note: The RACF security administrator controls whether you can view all or some of the details of your DCE information.

The DCE information in the LISTUSER output has the following format:

```
USER=your user ID

DCE INFORMATION
---------------
 DCENAME= principal name
 UUID= universal unique identifier
 HOMECELL= home cell
 HOMEUUID= home cell UUID
 AUTOLOGIN= YES|NO
```

Figure 12. LISTUSER Output: Description of the DCE Information

To see the DCE information, issue the LISTUSER command as follows:

```
LISTUSER your-userid DCE NORACF
```

If your profile contains a DCE segment, you see output similar to this:

```
USER=MARTIN

DCE INFORMATION
---------------
 DCENAME= ELNINO
 UUID= 0000000035
 HOMECELL= 0000012401
 HOMEUUID= 0000000212
 AUTOLOGIN= YES
```

Figure 13. LISTUSER Output: Sample DCE Information

Finding Out What DFP Information RACF Has about You

Your user profile may contain DFP information about you. The details RACF lists from the DFP segment of the user's profile are:
- The user's default data class (DATACLAS)
- The user's default management class (MGMTCLAS)
- The user's default storage class (STORCLAS)
- The identifier for a data set application (DATAAPPL)

Note: The RACF security administrator controls whether you can view all or some of the details of your DFP information.

The DFP information in LISTUSER output has the following format:

Your RACF Definition

```
 USER=DJONES

   DFP INFORMATION
   ---------------
      MGMTCLAS= your default for management class
      STORCLAS= your default for storage class
      DATACLAS= your default for data class
      DATAAPPL= your default for data application identifier
```

Figure 14. LISTUSER Output: Description of the DFP Information

Notes:

1. DFP information can also appear at the group level. If you do not find the information needed in your user profile, check it at your default group level.
2. The ability to view and update DFP information can be controlled on a field by field basis; therefore, any individual field might not appear on your output.

To see the DFP information contained in your user profile, issue the LISTUSER command as follows:

```
LISTUSER your-userid DFP NORACF
```

If there is DFP information in your profile, you see output similar to this:

```
USER=DJONES

   DFP INFORMATION
   ---------------
      MGMTCLAS= DFPMG01
      STORCLAS= DFPST01
      DATACLAS= DFPDT01
      DATAAPPL= DFPID01
```

Figure 15. LISTUSER Output: Sample DFP Information

Finding Out What Language Information RACF Has about You

Your user profile might contain information about your language. RACF lists the following information from the LANGUAGE segment of the user profile:

- The user's primary language, if one has been specified (PRIMARY LANGUAGE)
- The user's secondary language, if one has been specified (SECONDARY LANGUAGE)

Note: The RACF security administrator controls whether you can view all or some of the details of your language information.

The language information in the LISTUSER output has the following format:

```
USER=your user ID

LANGUAGE INFORMATION
--------------------
 PRIMARY LANGUAGE:   specified primary language
 SECONDARY LANGUAGE: specified secondary language
```

Figure 16. LISTUSER Output: Description of the Language Information

Notes:

1. The ability to view and update language information can be controlled on a field by field basis; therefore, any individual field might not appear on your output.
2. The 3-character language code, and if defined, the 24-character language name is displayed. `NOT SPECIFIED` indicates that no language has been specified.

To see the language information, issue the LISTUSER command as follows:

```
LISTUSER your-userid LANGUAGE NORACF
```

If there is language information in your user profile, you see output similar to this:

```
 USER=DJONES

LANGUAGE INFORMATION
--------------------
 PRIMARY LANGUAGE: ENU
 SECONDARY LANGUAGE: DEU
```

Figure 17. LISTUSER Output: Sample Language Information

Finding Out What Lotus Notes Information RACF Has about You

Your user profile might contain information about you related to Lotus Notes for OS/390. RACF lists the following information from the LNOTES segment of the user profile:

- Your Lotus Notes short name (SNAME)

Note: The RACF security administrator controls whether you can view your information related to Lotus Notes for OS/390.

The information related to Lotus Notes for OS/390 in the LISTUSER output has the following format:

```
USER=your user ID

LNOTES INFORMATION
---------------
 SNAME= Lotus Notes for OS/390 short name
```

Figure 18. LISTUSER Output: Description of the Information Related to Lotus Notes for OS/390

To see the Lotus Notes for OS/390 information, issue the LISTUSER command as follows:

```
LISTUSER your-userid LNOTES NORACF
```

If your profile contains an LNOTES segment, you see output similar to this:

Your RACF Definition

```
USER=MARTIN

LNOTES INFORMATION
---------------
 SNAME= JMARTIN
```

Figure 19. LISTUSER Output: Sample Lotus Notes for OS/390 Information

Finding Out What NetView Information RACF Has about You

Your user profile may contain NetView information about you. The details RACF lists from the NetView segment of the user profile are:

- Command or command list to be processed at logon (IC)
- MCS extended console name (CONSNAME)
- Type of security check (CTL)
- Whether unsolicited messages will be received (MSGRECVR)
- Scope classes (OPCLASS)
- Domains (DOMAINS)
- Whether administrator authority is present for the NetView Graphic Monitor Facility (NGMFADMN)

Note: The RACF security administrator controls whether you can view all or some of the details of your NetView information.

The NetView information in the LISTUSER output has the following format:

```
USER=your user ID

NETVIEW INFORMATION
--------------------
IC= command or command list information
CONSNAME= MCS extended console name
CTL= type of security check
MSGRECVR= whether unsolicited messages will be received
OPCLASS= scope classes
DOMAINS= domains
NGMFADMN= whether administrator authority is present
```

Figure 20. LISTUSER Output: Description of the NetView Information

Note: The ability to view and update NetView information can be controlled on a field by field basis; therefore, any individual field may not appear on your output.

To see the NetView information, issue the LISTUSER command as follows:

```
LISTUSER your-userid NETVIEW NORACF
```

If there is NetView information in your user profile, you see output similar to this:

```
 USER=DJONES

NETVIEW INFORMATION
--------------------
IC= START
CONSNAME= DJONES1
CTL= GLOBAL
MSGRECVR= YES
OPCLASS= 1,2
DOMAINS= D1,D2
NGMFADMN= YES
```

Figure 21. LISTUSER Output: Sample NetView Information

Finding Out What Information Related to Novell Directory Services for OS/390 RACF Has about You

Your user profile might contain information about you related to Novell Directory Services for OS/390. RACF lists the following information from the NDS segment of the user profile:

- Your user name for Novell Directory Services for OS/390 (UNAME)

Note: The RACF security administrator controls whether you can view your information related to Novell Directory Services for OS/390.

The information related to Novell Directory Services for OS/390 in the LISTUSER output has the following format:

```
USER=your user ID

NDS INFORMATION
---------------
 UNAME= user name for Novell Directory Services for OS/390
```

Figure 22. LISTUSER Output: Description of the Novell Directory Services for OS/390 Information

To see the information related to Novell Directory Services for OS/390, issue the LISTUSER command as follows:

```
LISTUSER your-userid NDS NORACF
```

If your profile contains an NDS segment, you see output similar to this:

```
USER=MAXWELL

NDS INFORMATION
---------------
 UNAME= GeorgeMaxwell
```

Figure 23. LISTUSER Output: Sample Novell Directory Services for OS/390 Information

Finding Out What OpenEdition VM Information RACF Has about You

Your user profile may contain OpenEdition VM information about you. The details RACF lists from the OVM segment of the user profile are:

- The user identifier (UID)
- The initial directory path name (HOME)
- The program path name (PROGRAM)
- The file system root directory (FSROOT)

Note: The RACF security administrator controls whether you can view all or some of the details of your OpenEdition VM information.

The OpenEdition VM information in the LISTUSER output has the following format:

```
USER=your user ID

OVM INFORMATION
---------------
 UID= user identifier
 HOME= initial directory path name
 PROGRAM= program path name
 FSROOT= file system root directory
```

Figure 24. LISTUSER Output: Description of the OpenEdition VM Information

To see the OVM information, issue the LISTUSER command as follows:

```
LISTUSER your-userid OVM NORACF
```

If your profile contains an OVM segment, you see output similar to this:

```
USER=MARTIN

OVM INFORMATION
---------------
 UID= 0000000035
 HOME= /u/martin
 PROGRAM= /u/martin/bin/myshell
 FSROOT= /../VMBFS:SERVER7:MARTIN/
```

Figure 25. LISTUSER Output: OpenEdition VM Information (Example 1)

If the OVM segment does not exist, you see output similar to this:

```
USER=MARTIN

NO OVM INFORMATION
```

Figure 26. LISTUSER Output: OpenEdition VM Information (Example 2)

Finding Out What OPERPARM Information RACF Has about You

Your user profile may contain OPERPARM information about you. The details RACF lists from the OPERPARM segment of the user profile are:

- Console recovery group (ALTGRP)
- Operator authority (AUTH)
- System name for commands from this console (CMDSYS)
- Whether and what kind of delete operator messages are received (DOM)

- Searching key (KEY)
- Message level information (LEVEL)
- Whether system command responses are logged (LOGCMDRESP)
- Message format (MFORM)
- Whether this console is assigned a migration ID (MIGID)
- Event information (MONITOR)
- The system from which this console can receive undirected messages from (MSCOPE)
- Routing code information (ROUTCODE)
- Storage information (STORAGE)
- Whether this console can receive undeliverable messages (UD)
- Whether the extended console can receive messages that have been automated by the NetView Message Processing Facility (MPF) in the sysplex (AUTO)

Note: The RACF security administrator controls whether you can view all or some of the details of your OPERPARM information.

The OPERPARM information in the LISTUSER output has the following format:

```
USER=your user ID

OPERPARM INFORMATION
--------------------
STORAGE= storage information
AUTH= operator authority
AUTO= automated messages
ROUTCODE= routing code information
LEVEL= message level information
MFORM= message format
MONITOR= event information
LOGCMDRESP= whether system command responses are logged
MIGID= if a migration ID is assigned
DOM= whether and what kind of delete operator messages are received
KEY= searching key
CMDSYS= system name for this console's commands
MSCOPE= the system this console can receive undirected messages from
UD= whether this console can receive undeliverable messages
ALTGRP= console recovery group
```

Figure 27. LISTUSER Output: Description of the OPERPARM Information

Notes:

1. The ability to view and update OPERPARM information can be controlled on a field by field basis; therefore, any individual field may not appear on your output.
2. If there is no information in a field in the user profile for this segment then the field name is not displayed. However, if no value was specified for STORAGE when the OPERPARM segment was added to the user profile, “STORAGE=0” will appear in the listing.

To see the OPERPARM information, issue the LISTUSER command as follows:

```
LISTUSER your-userid OPERPARM NORACF
```

If there is OPERPARM information in your user profile, you see output similar to this:

```
USER=DJONES

OPERPARM INFORMATION
--------------------
STORAGE= 00002
AUTH= IO
AUTO= YES
ROUTCODE= ALL
LEVEL= ALL
MFORM= T J M
MONITOR= JOBNAMEST SESST
LOGCMDRESP= NO
MIGID= YES
DOM= NORMAL
KEY= MSC2
CMDSYS= SYS1
MSCOPE= *ALL
UD= YES
ALTGRP= BACKUP
```

Figure 28. LISTUSER Output: Sample OPERPARM Information

Finding Out What OS/390 UNIX Information RACF Has about You

Your user profile might contain OS/390 UNIX information about you. The details RACF lists from the OMVS segment of the user profile are:

- The OS/390 UNIX user identifier (UID)
- The initial directory path name (HOME)
- The program path name (PROGRAM)
- The CPU time, in seconds, the user's processes can use (CPUTIMEMAX)
- The address space region size, in bytes, the user's processes can use (ASSIZEMAX)
- The maximum number of active or open files the user can have (FILEPROCMAX)
- The maximum number of active processes the user can have (PROCUSERMAX)
- The maximum number of threads the user can have (THREADSMAX)
- The maximum amount of space, in pages, the user can map in storage (MMAPAREAMAX)

Note: The RACF security administrator controls whether you can view all or some of the details of your OS/390 UNIX information.

The OS/390 UNIX information in the LISTUSER output has the following format:

```
USER=your user ID

OMVS INFORMATION
----------------
 UID= your OS/390 UNIX user identifier
 HOME= initial directory path name
 PROGRAM= program path name
 CPUTIMEMAX= CPU time, in seconds, your processes can use
 ASSIZEMAX= address space region size, in bytes, your processes can use
 FILEPROCMAX= maximum number of active or open files you can have
 PROCUSERMAX= maximum number of active processes you can have
 THREADSMAX= maximum number of threads you can have
 MMAPAREAMAX= maximum number of pages you can map in storage
```

Figure 29. LISTUSER Output: Description of the OS/390 UNIX Information

Notes:

1. If there is no information in the HOME or PROGRAM field in the user’s profile for this segment, the field name is not displayed.
2. If UID was not specified when the OMVS segment was added to the user profile, the word NONE appears in the listing.
3. If there is no information in the CPUTIMEMAX, ASSIZEMAX, FILEPROCMAX, PROCUSERMAX, THREADSMAX, or MMAPAREAMAX field for this segment in the user’s profile, the word NONE appears in the listing, and OS/390 uses its system-level value for the field.
4. The ability to view and update OS/390 UNIX information can be controlled on a field-by-field basis; therefore, any individual field might not appear on your output.

To see the OS/390 UNIX information, issue the LISTUSER command as follows:

```
LISTUSER your-userid OMVS NORACF
```

If your profile contains an OMVS segment, you see output similar to this:

```
USER=CSMITH

OMVS INFORMATION
----------------
 UID= 0000000024
 HOME= /u/CSMITH
 PROGRAM= /u/CSMITH/bin/myshell
 CPUTIMEMAX= 0010000000
 ASSIZEMAX= NONE
 FILEPROCMAX= 0000050000
 PROCUSERMAX= NONE
 THREADSMAX= NONE
 MMAPAREAMAX= 0016777216
```

Figure 30. LISTUSER Output: OS/390 UNIX Information (Example 1)

If only the UID field has a value in the OMVS segment of your profile, you see output similar to this:

Your RACF Definition

```
USER=CSMITH

OMVS INFORMATION
----------------
 UID= 0000000024
 CPUTIMEMAX= NONE
 ASSIZEMAX= NONE
 FILEPROCMAX= NONE
 PROCUSERMAX= NONE
 THREADSMAX= NONE
 MMAPAREAMAX= NONE
```

Figure 31. LISTUSER Output: OS/390 UNIX Information (Example 2)

Finding Out What TSO/E Information RACF Has about You

Your user profile may contain TSO/E information about you. The details RACF lists from the TSO segment of the user profile are:

- The user’s default job class (JOBCLASS)
- The user’s default message class (MSGCLASS)
- The user’s default hold class (HOLDCLASS)
- The user’s default system output (SYSOUTCLASS)
- The user’s default account number (ACCTNUM)
- The user’s logon procedure name (PROC)
- The user’s default region size (SIZE)
- The user’s maximum region size (MAXSIZE)
- The unit name (UNIT)
- The destination ID for SYSOUT data sets (DEST)
- Optional user data (USERDATA)
- The user’s security label (SECLABEL)
- The TSO command to be processed at logon time (COMMAND)

Note: The RACF security administrator controls whether you can view all or some of the details of your TSO information.

The TSO/E information in LISTUSER output has the following format:

```
USER=your user ID

 TSO INFORMATION
 ---------------
  ACCTNUM= default account number
  DEST= default SYSOUT destination
  HOLDCLASS= default hold class
  JOBCLASS= default job class
  MSGCLASS= default message class
  PROC= default LOGON procedure
  SIZE= default region size
  MAXSIZE= default maximum region size
  SYSOUTCLASS= default SYSOUT class
  UNIT= default unit
  USERDATA= user data
  SECLABEL= TSO security label
  COMMAND= TSO command processed at logon time
```

Figure 32. LISTUSER Output: Description of the TSO/E Information

Notes:

1. The ability to view and update TSO information can be controlled on a field by field basis; therefore, any individual field may not appear on your output.
2. If there is no information in the fields of the TSO segment, the field name is not displayed (with the exception of SIZE, MAXSIZE, and USERDATA).

To see the TSO/E information contained in your user profile, issue the LISTUSER command as follows:

```
LISTUSER your-userid TSO NORACF
```

If there is TSO/E information in your profile, you see output similar to this:

```
USER=DJONES

TSO INFORMATION
---------------
  ACCTNUM= D5888P
  DEST= LOCAL
  HOLDCLASS= H
  JOBCLASS= C
  MSGCLASS= R
  PROC= PROC01
  SIZE= 0001024
  MAXSIZE= 0004096
  SYSOUTCLASS= J
  UNIT= SYSDA
  USERDATA= 1F09
  SECLABEL= SYSLOW
```

Figure 33. LISTUSER Output: Sample TSO/E Information

Finding Out What WORKATTR Information RACF Has about You

Your user profile may contain work attribute information about you. The details RACF lists from the WORKATTR segment of the user profile are:

- The user name on SYSOUT (WANAME)
- The building on SYSOUT (WABLDG)
- The department on SYSOUT (WADEPT)
- The room on SYSOUT (WAROOM)
- Address lines 1, 2, 3 and 4 on SYSOUT (WAADDR1, WAADDR2, WAADDR3, WAADDR4)
- The account number (WAACCNT)

Note: The RACF security administrator controls whether you can view all or some of the details of your work attribute information.

The WORKATTR information in the LISTUSER output has the following format:

Your RACF Definition

```
USER=your user ID

WORKATTR INFORMATION
--------------------
 WANAME= user name
 WABLDG= building
 WADEPT= department
 WAROOM= room
 WAADDR1= address line 1
 WAADDR2= address line 2
 WAADDR3= address line 3
 WAADDR4= address line 4
 WAACCNT= account number
```

Figure 34. LISTUSER Output: Description of the WORKATTR Information

To see the WORKATTR information, issue the LISTUSER command as follows:

```
LISTUSER your-userid WORKATTR NORACF
```

If your profile contains an WORKATTR segment, you see output similar to this:

```
USER=MARTIN

WORKATTR INFORMATION
--------------------
 WANAME= Martin W. Gilfeather
 WABLDG= 025
 WADEPT= 58HA
 WAROOM= 6W11
 WAADDR1= Boices Dairy Farms
 WAADDR2= 1 Neighborhood Road
 WAADDR3= Kingston, New York
 WAADDR4= 12401
 WAACCNT= 040362
```

Figure 35. LISTUSER Output: Sample WORKATTR Information

Finding Out If Your Password Is Synchronized with Other IDs

Your user profile may indicate if your password is being synchronized with other user IDs through user ID associations; see “Finding Out What User ID Associations Are Defined for You” for more information. Or, automatic password direction may be synchronizing your password changes without user ID associations; for more information, see “Automatic Password Direction” on page 40.

Finding Out What User ID Associations Are Defined for You

Your user profile may contain information about user ID associations defined for your user ID. The details RACF lists from the user profile are:

- Type of user ID association
- Node and user ID that are associated with you
- Whether password synchronization is in effect
- Status of the association

Note: User IDs do not need the same password to request an association. Passwords are synchronized automatically when either of the associated user IDs changes a password after the peer association with password synchronization has been established.

To see the information about your user ID associations, issue the RACLINK command as follows:

```
RACLINK LIST
```

If there are associations defined for your user ID, you see output similar to this:

```
ASSOCIATION information for user ID JUAN on node MVS01
at 09:27:12 on 07/16/98:

Association   Node.userid         Password  Association
  Type                             Sync      Status
------------  -----------------  --------  --------------

PEER OF       MVS03.JDOE          YES      ESTABLISHED

PEER OF       MVS04.JUAN          YES      ESTABLISHED

PEER OF       MVS01.SMITH         NO       PENDING APPROVAL BY SMITH

MANAGED BY    MVS04.SECADM        N/A      ESTABLISHED

MANAGER OF    MVS03.OPER2         N/A      ESTABLISHED

MANAGER OF    MVS03.MIKE          N/A      PENDING APPROVAL BY MIKE
```

Figure 36. RACLINK LIST Output: User ID Association Information (Example 1)

To see all your user ID associations defined with user IDs on node MVS03, enter the following command:

```
RACLINK LIST(MVS03.*)
```

The requesting user ID JUAN receives the following output:

```
ASSOCIATION information for user ID JUAN on node MVS01
at 10:02:54 on 07/16/98:

Association   Node.userid         Password  Association
  Type                             Sync      Status
------------  -----------------  --------  --------------

PEER OF       MVS03.JDOE          YES      ESTABLISHED

MANAGER OF    MVS03.OPER2         N/A      ESTABLISHED

MANAGER OF    MVS03.MIKE          N/A      PENDING APPROVAL BY MIKE
```

Figure 37. RACLINK LIST Output: User ID Association Information (Example 2)

To see all the user ID associations defined with your user ID JUAN on all nodes, enter the following command:

```
RACLINK LIST(*.JUAN)
```

The requesting user ID, JUAN, receives the following output:

Your RACF Definition

```
ASSOCIATION information for user ID JUAN on node MVS01
at 10:22:34 on 07/16/98:

Association   Node.userid         Password  Association
  Type                             Sync      Status
------------  -----------------  --------  --------------

PEER OF       MVS04.JUAN          YES      ESTABLISHED
```

Figure 38. RACLINK LIST Output: User ID Association Information (Example 3)

Automatic Registration of Digital Certificates

You may be able to use automatic registration of digital certificates, if this function has been enabled and you have been authorized to use it. To find out, check with your RACF security administrator or your Web administrator.

With automatic registration of digital certificates, your RACF user ID can be associated with a digital certificate through the WebSphere Application Server. Your installation may provide a registration page on the Web. This Web page prompts for the registration of the certificate for your RACF user ID. When you click on the registration box on this Web page, a secure session is set up using the Secure Sockets Layer (SSL) and your digital certificate. You are then prompted for your RACF user ID and password. At this point, the registration process is ready to begin.

Listing Your Digital Certificate Information

You might be able to list the digital certificates and key rings associated with your user ID, as shown in the following examples.

User NETB0Y requests the listing of his Savings Account digital certificate to ensure it has been defined, and that it is marked trusted. He has READ authority to the FACILITY class profile IRR.DIGTCERT.LIST. He issues the RACDCERT command with the LIST operand, specifying the label to identify his certificate:

```
RACDCERT LIST(LABEL('Savings Account'))
```

and receives the following output:

```
Digital certificate information for user NETB0Y:

 Label: Savings Account
 Status: TRUST
 Serial Number:
  >5D666C20207A6638727A413872D8413B<
 Issuer's Name:
  >OU=BobsBank Savers.O=BobsBank.L=Internet<
 Subject's Name:
  >CN=S.S.Smith.OU=Digital ID Class 1 - NetScape.OU=BobsBank Class 1 - S<
  >avingsAcct.O=BobsBank.L=Internet<
```

Figure 39. Example: Listing Your Digital Certificate Information

User GEORGEM requests a listing of his key rings. He has three key rings with certificates and one key ring that has no certificates. He has READ authority to the

FACILITY class profile IRR.DIGTCERT.LIST. He issues the RACDCERT command with the LISTRING operand, specifying * to list all of his key rings:

```
RACDCERT LISTRING(*)
```

and receives the following output:

```
Digital ring information for user GEORGEM:

   Ring:
        >GEORGEMsNewRing01<
   Certificate Label Name             Cert Owner     USAGE      DEFAULT
   --------------------------------   ------------   --------   -------
   New Cert Type - Ser # 00           ID(GEORGEM)    PERSONAL     YES
   New Type Cert - VsignC1            ID(GEORGEM)    CERTAUTH     NO
   New Type Cert - VsignC2            ID(GEORGEM)    SITE         NO
   65                                 ID(JOHNP)      PERSONAL     NO

   Ring:
        >GEORGEMsRing<
   Certificate Label Name             Cert Owner     USAGE      DEFAULT
   --------------------------------   ------------   --------   -------
   GEORGEM's Cert # 48                ID(GEORGEM)    PERSONAL     NO
   GEORGEM's Cert # 84                ID(GEORGEM)    PERSONAL     NO
   New Cert Type - Ser # 00           ID(GEORGEM)    PERSONAL     YES

   Ring:
        >GEORGEMsRing#2<
   Certificate Label Name             Cert Owner     USAGE      DEFAULT
   --------------------------------   ------------   --------   -------
   GEORGEM's Cert # 84                ID(GEORGEM)    PERSONAL     NO
   GEORGEM's Cert # 48                ID(GEORGEM)    PERSONAL     NO

   Ring:
        >GEORGEMsRing#3<
   *** No certificates connected ***
```

Figure 40. Listing Your Digital Key Ring Information

If you are unable to issue the RACDCERT command, check with your RACF security administrator to get authorization.

Chapter 5. Changing How You are Defined to RACF

You can change some of the ways you have been defined on the system by doing any or all of the tasks described in this chapter.

Changing Your Password

Your user ID identifies you to RACF and your password verifies your identity. You have to change your password after a certain interval of time to help ensure that it is known only to you. You can make the time interval between changing your password shorter at the time you change your password.

Note: You can also change your password while logging on to the system. This is the most common way of changing your password. See “Finding Out If You Are Defined to RACF” on page 13.

If you have multiple user IDs, you can keep your passwords automatically synchronized on the same system or across multiple systems by defining peer user ID associations with password synchronization enabled between your user IDs. See “Synchronizing Your Passwords” on page 40 for additional information. An installation can also maintain the synchronization of user passwords between the same user IDs on different nodes by using automatic password direction. See “Automatic Password Direction” on page 40 for additional information.

In choosing a new password, be aware that your installation has password rules. If you do not know the rules, choose a password following the format of your current password. RACF may not allow you to reuse a previous password. Ask your RACF security administrator for an explanation of your installation’s rules for passwords.

To change your password, enter the PASSWORD command with the PASSWORD keyword as follows:

```
PASSWORD PASSWORD(current-password new-password)
```

For example, to change your password from “subject” to “testers”, type:

```
PASSWORD PASSWORD(SUBJECT TESTERS)
```

To change your password interval (that is, the time allowed before you are required to change your password again), enter the PASSWORD command with the INTERVAL keyword as follows:

```
PASSWORD INTERVAL(interval-you-want)
```

For example, to change your password interval to 15 days, enter the following command:

```
PASSWORD INTERVAL(15)
```

At the end of 15 days, RACF requires you to change your current password to a new valid one.

RACF allows the interval to be in the range of 1 to 254 days. Your installation chooses its own interval in this range. You can change your password interval to a shorter length of time than your installation requires but you cannot specify a longer interval. For example, if your installation has a password interval of 30 days, you may change the interval to any number from 1 to 30 but you cannot change your password interval to 45 days.

To change your password and password interval, enter the PASSWORD command with the PASSWORD and INTERVAL keywords as follows:

```
PASSWORD PASSWORD(current-password new-password) INTERVAL(interval)
```

For example, to change the password from “subject” to “testers”, and the interval to 15 days, enter the following command:

```
PASSWORD PASSWORD(subject testers) INTERVAL(15)
```

If you do not know your current password interval, enter the LISTUSER command and check the PASS-INTERVAL field. If you need more information, see “Understanding the Information RACF Has about You as a User” on page 15.

Synchronizing Your Passwords

To synchronize your passwords (that is, keep your passwords automatically synchronized for two or more user IDs on the same system or on different systems), first you must establish a peer user ID association with password synchronization among the user IDs. Then, whenever you change the password on one of the associated user IDs, RACF automatically communicates the new password to the RACF databases of the other user IDs. For more information about defining associations for your user ID, see “User ID Associations” on page 46.

An installation can also maintain the synchronization of user passwords between the same user IDs on different nodes by using automatic password direction. See “Automatic Password Direction” on page 40 for additional information.

Notes:

1. User IDs do not have to have the same password to request an association. Passwords are synchronized automatically when either of the associated user IDs changes a password after the peer association with password synchronization has been established.
2. Password changes are not repropagated. For example:

   ```
   User1 has an established peer user ID association with password
      synchronization enabled with User2, but not with User3.

   User2 has an established peer user ID association with password
      synchronization enabled with User1 and an established peer user
      ID association with password synchronization enabled with User3.
   ```

   If User1 changes his or her password, the new password is propagated to User2. Even though User2 has an established peer user ID association with password synchronization enabled with User3, the new password from User1 is not propagated to User3.

   But, if User2 changes his or her password, the new password is propagated to both User1 and User3. This occurs because User2 has an established peer ID association with password synchronization enabled with User1 and with User3.

Automatic Password Direction

Installations using automatic command direction can optionally use automatic password direction to maintain the synchronization of user passwords between the same user IDs on different nodes. Automatic password direction does not require user ID associations. Instead, automatic password direction assumes that the same user IDs on different nodes belong to the same user.

For example, suppose your installation is using automatic password direction and you have the user ID CLAIRE on three different nodes: NODE1, NODE2, and NODE3. When you change your password on NODE1, a password synchronization request is automatically directed to be processed for CLAIRE on NODE2 and CLAIRE on NODE3. You will receive a TSO SEND message on NODE1 telling you whether the password synchronization request completed successfully or unsuccessfully.

In addition, depending on how automatic password direction is set up at your installation, the output from the password synchronization request is either discarded, sent to an administrator, or returned to you and appended in your RRSFLIST user data set. If automatic password direction is set up at your installation so that you receive this output and you do not have an RRSFLIST user data set, RACF allocates one and adds the results. The RRSFLIST data set name is '*prefix.userid*.RRSFLIST', where *prefix* is your TSO prefix at the time you changed your password. If *prefix* matches *userid* or if you specified PROFILE NOPREFIX via the TSO PROFILE command, the data set name used is '*userid*.RRSFLIST'.

You are responsible for maintaining this data set. If your data set becomes full, the output is transmitted to your user ID. In order for RACF to append to your RRSFLIST user data set again, you must edit and delete some of the returned output in this data set.

Notes:

1. If your installation is using automatic password direction, do not establish peer user ID associations with password synchronization enabled between same user IDs across multiple RRSF nodes. Doing so causes duplicate password synchronization requests. If you are not sure whether your installation is using automatic password direction, contact your RACF security administrator.
2. You can use peer user ID associations with password synchronization enabled between user IDs that are not the same in environments with automatic password direction, because automatic password direction only synchronizes passwords between the same user IDs on multiple RRSF nodes.
3. Password synchronization and automatic password direction only synchronize passwords for user IDs that are not revoked.

RRSF password synchronization requests run asynchronously, that is, the command issuer does not wait until the command completes processing, and results and output from the commands are returned as specified by the SET AUTOPWD command.

Format of Output

Figure 41 on page 42 shows the format of output produced by automatic password direction. The format of the output is the same for both your RRSFLIST data set and for the output transmitted when your data set is full.

```
==============================================================================

Password synchronization request issued at 15:03:58 on 02/28/98 was
processed at NODE2.TSOUSER on 02/28/98 at 15:04:00

 Request was propagated by automatic direction from NODE1.TSOUSER

 REQUEST ISSUED: From user TSOUSER at NODE1

 REQUEST OUTPUT:
 IRRC013I Password synchronized successfully for TSOUSER at NODE2 and
 TSOUSER at NODE1.

==============================================================================
```

Figure 41. Automatic Password Direction: Sample Output

Logging On to a Group Other Than Your Default Group

As a RACF user, you belong to a default group. You are automatically connected to that group when you log on. However, you may be defined to more than one group. If you need the resources of another group, your security administrator may give you authority to log on to that other group. For example, a particular group may use a data set containing a report that is critical to a presentation you are preparing. You need the information, so you log on to the group that has access to it.

To log on to a group other than your default group:

Note to the Reader

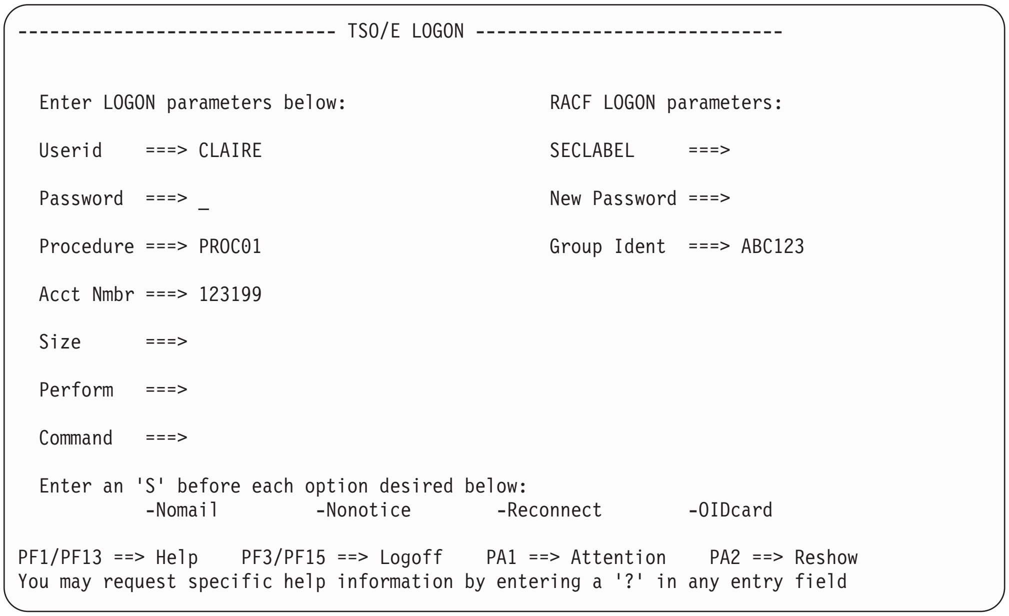
Use this procedure *only if* your installation does not have list-of-groups processing in effect. To find out if list-of-groups processing is in effect, ask your RACF security administrator.

If you belong to more than one group, and have no trouble accessing information belonging to the various groups, you need not use this procedure.

1. Determine what groups you belong to.

   You must first belong to a group before you can log on to it. If you know that you belong to the group you need, proceed with Step 2. If you do not know whether you belong to the group you need, use the LISTUSER command, as described in “Finding Out How You Are Defined to RACF” on page 14, to see a list of the groups you belong to.
2. Log on to a group other than your default group.

   Enter the group name you want to log on to in the **Group Ident** field of the logon panel. Figure 42 on page 43 shows a a user logging on to group ABC123.



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


  Enter LOGON parameters below:                  RACF LOGON parameters:

  Userid    ===> CLAIRE                          SECLABEL     ===>

  Password  ===> _                               New Password ===>

  Procedure ===> PROC01                          Group Ident  ===> ABC123

  Acct Nmbr ===> 123199

  Size      ===>

  Perform   ===>

  Command   ===>

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

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

Figure 42. Logging On To Another Group

Logging On with a Security Label Other Than Your Default Security Label

Your installation can define its own security classifications. These classifications are security levels, security categories, and security labels. A security level is a name for a numeric security classification indicator. For example, a security level could be SECRET. A security category is a name corresponding to a department or area within an organization with similar security requirements. For example, an employee in the payroll department may be in the security category PAYROLL.

A security label is used to represent the association between a particular security level and a set of zero or more security categories. For example, the security categories PAYROLL and PERSONNEL may both be associated with the security level SECRET by the security label PPSECR.

If your installation uses security classifications, RACF stores the security classifications for each user and each data set in user and data set profiles. When you request access to a data set, RACF checks your user profile and the data set profile to see if your security label is equal to or greater than the security label of the data set. RACF denies you access if you do not have the appropriate level.

Your security administrator defines a default security label for you. However you may be able to log on with a different security label if you have been authorized. This alternate security label allows you access to resources that have the same security label.

Note to the Reader

If you want to log on with a security label, your installation must have the security label class (SECLABEL) class active. Check with your security administrator.

Changing Your System Definitions

1. Determine what security labels you have authority to use.

   You must first have authority to a security label before you can log on with it. If you know what security label you need, proceed with Step 2.

   If you do not know whether you can use a particular security label, RACF can give you a list of all the profiles in the SECLABEL class you are authorized to use.

   To see this list, log on with your default security label and enter the following command:

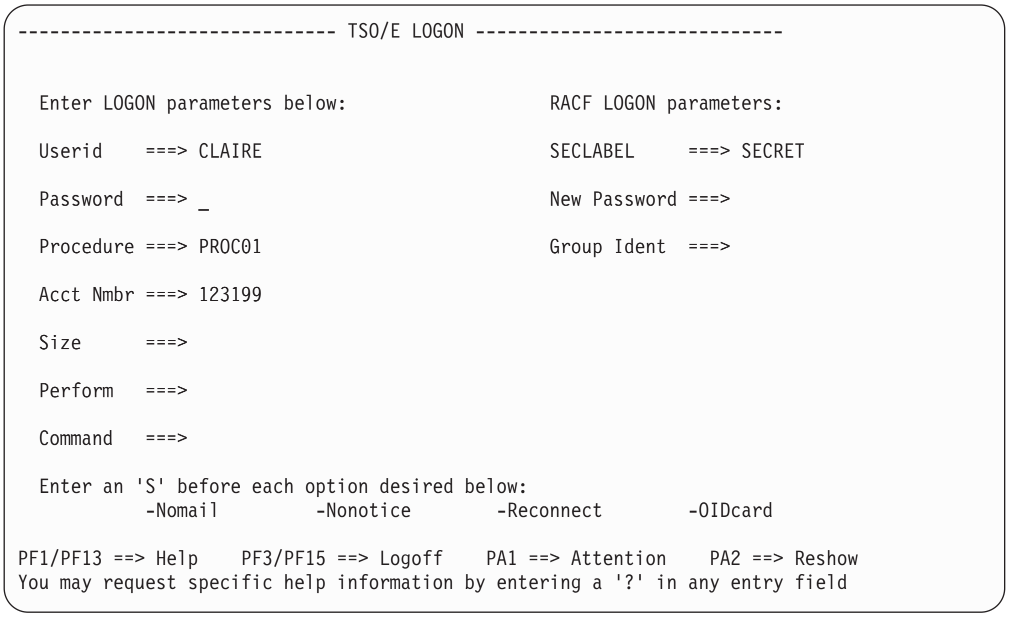
   ```
   SEARCH CLASS(SECLABEL)
   ```

   The profile names listed are the security labels you are authorized to use.

   ```
   LOGOFF
   ```

2. Log on using a security label other than your default security label.

   Enter the security label you want to log on with in the SECLABEL field of the logon panel. Figure 43 shows a user logging on with security label SECRET.



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


  Enter LOGON parameters below:                   RACF LOGON parameters:

  Userid    ===> CLAIRE                           SECLABEL     ===> SECRET

  Password  ===> _                                New Password ===>

  Procedure ===> PROC01                           Group Ident  ===>

  Acct Nmbr ===> 123199

  Size      ===>

  Perform   ===>

  Command   ===>

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

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

Figure 43. Logging On With Another Security Label

Once you log on with a different security label, that new security label is associated with your user ID until you change it. The new security label appears in the SECLABEL field of the logon panel the next time you log on. If you blank out this field, your security label returns to the default security label your security administrator assigned to you.

Allowing Another User to Submit Your Jobs

You can authorize another user to submit jobs on your behalf. This user is called a surrogate user. You are the execution user. For example, if you need certain jobs submitted while you are on vacation, you can authorize a surrogate user to submit these jobs for you. You do not have to give the surrogate user access to the data sets the jobs use. You also do not have to give the surrogate user your password, although the jobs will execute under your user ID.

The use of surrogate users might not be allowed on some systems. Contact your RACF security administrator to see if this is allowed on your system.

> **Attention**
>
> Do not allow another user to act as surrogate user for you *unless the surrogate user can be trusted as much as you are trusted*. This is because the surrogate user can do anything you can do (unless the surrogate user lacks access to a security label that protects a resource). For example, the surrogate user can submit a job to copy, alter, or delete your data.

To give a surrogate user authority to submit a job for you:

1. If security labels are used on your system, determine if the surrogate user has access to the security label the job will run under.

   To determine if the surrogate user has access to the security label under which the job will run, ask the surrogate user to enter the following command:

   ```
   SEARCH CLASS(SECLABEL)
   ```

   If the security label under which the job will run does not appear in the list of security labels, the surrogate user cannot run the job for you. Ask your RACF security administrator for assistance or find a different surrogate user who does have the correct security label authority.
2. Determine if the surrogate user has authority to submit your job.

   Determine if a profile called *your-userid*.SUBMIT exists and if it has an access list identifying the surrogate user with at least READ authority.

   To list information about the *your-userid*.SUBMIT profile, enter the following command:

   ```
   RLIST SURROGAT your-userid.SUBMIT AUTHUSER
   ```

   If the profile exists, RACF lists information about the profile, including the access list. If the surrogate user is on the access list and has an access authority of at least READ, proceed to Step 3.

   If the profile does not exist, RACF gives you an error message. You can create the profile yourself if you have class authority to the SURROGAT class. When the SECLABEL class is active, both you and the surrogate user must have authority to the security label of your job. If you need help creating the SURROGAT class profile, ask your security administrator.
3. Give the surrogate user authority to submit your job.

   To give the surrogate user READ access to the *your-userid*.SUBMIT profile, enter the following command:

   ```
   PERMIT your-userid.SUBMIT CLASS(SURROGAT)
          ID(surrogate-userid) ACCESS(READ)
   ```

   See “When Data Set Profile Changes Take Effect” on page 83 to find out when the surrogate user will have the necessary access authority after you enter this command. Proceed to Step 4.
4. Make sure the surrogate user has access to the data set containing the job control language (JCL) for that job.

   The user does not necessarily need access to the data sets the job uses, only to the data set containing the JCL. You can give the surrogate user this access by either sending a copy of the data set or giving the surrogate user READ access to it. For more information about giving someone READ access to a data set, see “Permitting an Individual or a Group to Use a Data Set” on page 70.

Note: Make sure the USER parameter on the JOB statement in the JCL is present and specifies your user ID. For surrogate processing to be performed, the PASSWORD parameter must not be specified.

5. To revoke a surrogate user’s authority to submit your jobs, enter the following command; the user will no longer be a surrogate user who can submit your jobs:

```
PERMIT your-userid.SUBMIT CLASS(SURROGAT)
       ID(surrogate-userid) DELETE
```

User ID Associations

A RACF user ID can have multiple user ID associations, that is, associations defined between your user ID and another user ID. There are two types of user ID associations: peer and managed.

With a peer user ID association, either user ID in the association can direct allowed RACF commands to run under the authority of the other user ID. See “Directing Commands” on page 8 for information on directing commands. A peer user ID association can be defined with or without password synchronization, and can be deleted by either user.

With a managed user ID association, the managing user ID in the association can direct allowed RACF commands to run under the authority of the managed user ID. Users of the managed user ID cannot direct RACF commands to run under the authority of the managing user ID. See “Directing Commands” on page 8 for information on directing commands. A managed user ID association cannot be defined with password synchronization, but can be deleted by either user.

Note: Your RACF security administrator determines whether you can define user ID associations. If you are not sure, contact your RACF security administrator. Also, an authorized user can establish user ID associations between your user ID and another user ID provided that user has the authority to do so. You receive a notification message to indicate any such activity.

Defining A Peer User ID Association

With Password Synchronization

To see the user ID associations that are already established for your user ID or are pending approval, see “Finding Out What User ID Associations Are Defined for You” on page 34.

To define a peer user ID association with password synchronization, enter the RACLINK command with the DEFINE keyword as follows:

```
RACLINK DEFINE(target-node.target-userid
       [/target-userid-password]) PEER(PWSYNC)
```

For example, to define a peer association between your two user IDs, JOHN on MVS01 and JDOE on MVS03, enter the following command from your user ID JOHN on MVS01:

```
RACLINK DEFINE(MVS03.JDOE/password-of-JDOE) PEER(PWSYNC)
```

Because you specified the password for your JDOE user ID in the preceding example, the user ID association between your user IDs is established and approved without requiring you to logon to your JDOE user ID to issue a subsequent RACLINK APPROVE command.

If you didn't specify the password for JDOE on MVS03 in the preceding example, the user ID association would be pending until JDOE on MVS03 issued a subsequent RACLINK APPROVE command.

Note: User IDs do not need the same password to request an association. Passwords are synchronized automatically when either of the associated user IDs changes a password after the peer association with password synchronization has been established.

Without Password Synchronization

To see the user ID associations that are already established for your user ID or are pending your approval, see "Finding Out What User ID Associations Are Defined for You" on page 34.

To define a peer user ID association without password synchronization, enter the RACLINK command with the DEFINE keyword as follows:

```
RACLINK DEFINE(target-node.target-userid
     [/target-userid-password]) PEER(NOPWSYNC)
```

For example, to define a peer association between your user ID JOHN on MVS01 and a co-worker's user ID SMITH on MVS01, enter the following command from your user ID JOHN on MVS01:

```
RACLINK DEFINE(MVS01.SMITH/password-of-SMITH) PEER(NOPWSYNC)
```

Because you specified the password of your co-worker's user ID SMITH on MVS01 in the preceding example, the user ID association between the two user IDs is established and approved without requiring the owner of the SMITH user ID on MVS01 to issue a subsequent RACLINK APPROVE command.

If you didn't specify the password for SMITH on MVS01 in the preceding example, the user ID association would be pending until SMITH on MVS01 issued a subsequent RACLINK APPROVE command.

Defining A Managed User ID Association

To see the user ID associations that are already established for your user ID or are pending your approval, see "Finding Out What User ID Associations Are Defined for You" on page 34.

To define a managed user ID association, enter the RACLINK command with the DEFINE keyword as follows:

```
RACLINK DEFINE(target-node.target-userid
        [/target-userid-password]) MANAGED
```

The user ID that issues this RACLINK command manages the target user ID.

For example, suppose you want your user ID JOHN on MVS01 to manage another user ID: OPER2 on MVS03. To define a managed association between JOHN and OPER2, enter the following command from your user ID JOHN on MVS01:

```
RACLINK DEFINE(MVS03.OPER2) MANAGED
```

Because user ID JOHN did not enter the password of OPER2 to approve the user ID association between JOHN and OPER2, OPER2 will receive a notification message that this user ID association is in the process of being established. The association will be pending until OPER2 issues a subsequent RACLINK APPROVE command.

Approving User ID Associations

To see the user ID associations that are already established for your user ID or are pending your approval, see “Finding Out What User ID Associations Are Defined for You” on page 34.

To approve a pending user ID association, enter the RACLINK command with the APPROVE keyword as follows:

```
RACLINK APPROVE(node.userid)
```

To approve the association in the previous example, OPER2 on MVS03 would issue the following command:

```
RACLINK APPROVE(MVS01.JOHN)
```

Deleting User ID Associations

To see the user ID associations that are already established for your user ID or are pending your approval, see “Finding Out What User ID Associations Are Defined for You” on page 34.

To reject a pending association or to delete an existing association, enter the RACLINK command with the UNDEFINE keyword as follows:

```
RACLINK UNDEFINE(node.userid)
```

To reject the association in the previous example, OPER2 on MVS03 would issue the following command:

```
RACLINK UNDEFINE(MVS01.JOHN)
```

Chapter 6. Protecting a Data Set

RACF can protect your data sets from other users by controlling who has authority to access them and at what authority level they can do so. You can use RACF to protect data sets by creating profiles for them. When you attempt to use a data set, RACF checks your user profile as well as the data set profile to decide whether to allow you to use it.

A data set profile contains:

- The data set name.
- The data set owner.
- The access list, which is a list of specific users and groups who may use a data set and how they may use it.
- The universal access authority (UACC), which is the default level of access authority allowed for all users or groups not specified in the access list.
- Auditing information. RACF can audit the use of each data set. The audit can be general or specific. For example, you can set up a resource profile for your data set to audit every attempt to use that data set. Or, you can define the profile to audit only the attempts to update the data set.

You can protect a data set by identifying specific users or groups with the access you want them to have in the access list. You can give all other RACF-defined users a certain access. Just put ID(*) in the access list with the access authority you want them to have. All other users are allowed the access you specify as the universal access authority (UACC). The access authorities you can specify are: NONE, READ, UPDATE, CONTROL, ALTER, and EXECUTE. See topic 51 for more information about each. To protect a data set most effectively, you should initially specify a UACC of NONE and selectively give certain users specific access authority to the data set.

You can use RACF to protect your data sets by doing the tasks described in this chapter.

Choosing Between Discrete and Generic Profiles

Data set profiles contain a description of a data set, including the authorized users and the access authority of each user. They can either be discrete or generic.

A *discrete* profile protects a single data set that has unique security requirements. The name of a discrete profile must exactly match the name of the data set it protects. The data set SMITH.PAYROLL.INFO would be protected by the discrete data set profile SMITH.PAYROLL.INFO.

You would choose a discrete profile to protect one data set with unique security requirements.

To create a discrete profile, see “Creating a Discrete Profile to Protect a Data Set” on page 51.

A *generic* profile protects several data sets that have a similar naming structure and security requirements. The name of a generic data set profile need not exactly match the names of the data sets it protects. Rather, it can contain generic characters which match any other characters. You may protect many data sets with similar characteristics with a generic profile. Two advantages of a generic profile are that:

- Data sets protected by a generic profile do not have to be individually defined to RACF
- The generic profile protects all copies of the data sets on all volumes in all locations in the system.

If a data set is protected by both a generic profile and a discrete profile, the discrete profile sets the level of protection for the data set. If a data set is protected by multiple generic profiles, the most specific generic profile sets the level of protection for the data set.

In general, given two profiles that match a data set, you can find the more specific one by comparing the profile name from left to right. Where they differ, a non-generic character is more specific than a generic character. In comparing generics, a % is more specific than an *, and an * is more specific than **. Another way to determine the most specific is with the SEARCH command, as there are some rare exceptions to the general rule. SEARCH always lists the profiles in the order of the most specific to the least specific.

A generic profile might already exist to protect your data set. However, that profile might not provide the exact protection you want. In this case, you can create a more specific generic profile or a discrete profile for the data set.

You would choose a generic profile for one of the following reasons:

- To protect more than one data set with the same security requirements. The data sets protected by a generic profile must have some identical characters in their names. The profile name contains one or more generic characters (*, **, or %).
- If you have a single data set that might be deleted, then re-created, and you want the protection to remain the same, you can create a *fully-qualified* generic profile. The name of a fully-qualified generic profile matches the name of the data set it protects. Unlike a discrete profile, a fully-qualified generic profile is not deleted when the data set itself is deleted. Also, with a fully-qualified generic profile, you can have multiple data sets with the same name all protected with the same profile.

To create a generic profile, see “Creating a Generic Profile to Protect a Data Set” on page 53.

Notes:

1. Deleting a data set that is protected with a discrete profile causes RACF to delete the data set profile from the RACF database.
2. If your installation is usingautomatic direction of application updates, you may receive output from an automatic direction of application update request when you do any of the following:
   - Define a data set when you have the ADSP attribute
   - Delete a data set that is protected with a discrete profile
   - Rename a data set that is protected with a discrete profile

   See “Automatic Direction of Application Updates” on page 84 for more information.

3. All the members of a partitioned data set (PDS) are protected by the profile that protects the data set. The members of a PDS cannot have different protection. If different protection is desired, those members should be moved to a different PDS.
4. All the components of a VSAM data set are protected by the profile that protects the cluster name. You do not need to create profiles that protect the index and data components of a cluster.
5. For a generic profile, unit and volume information, if specified, is ignored because the data sets that are protected under the generic profile can be on many different volumes.

Creating a Discrete Profile to Protect a Data Set

Create a discrete profile to protect a data set if you have a single data set with unique security requirements. To create a discrete profile:

1. Decide which RACF protections to use:

   There are different options you can use depending on how much protection you want.

   Note: To give specific authority to a certain user you could include that user on the access list for that data set. To do that see "Permitting an Individual or a Group to Use a Data Set" on page 70.

   The following options provide different degrees of general protection for your data set:

   - UACC (universal access authority).

     Universal access authority specifies the authority any user not on the access list has to use the data set. The UACC can be one of the following:

     NONE Does not allow users to access the data set.

     > **Attention**
     >
     > Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you may want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Permitting an Individual or a Group to Use a Data Set" on page 70 for information on how to permit selected users or groups to access a data set.)

     READ Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

     UPDATE
     Allows users to read from, copy from, or write to the data set. UPDATE does not, however, authorize a user to delete, rename, move, or scratch the data set.

     CONTROL
     For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform

control-interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER

ALTER allows users to read, update, delete, rename, move, or scratch the data set.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list*. However, ALTER does not allow users to change the owner of the profile.

When specified in a generic profile, ALTER gives users *no* authority over the profile itself.

When specified in a generic profile, ALTER allows users to create new data sets that are covered by that profile.

EXECUTE

For a private load library, EXECUTE allows users to load and execute, but not read or copy, programs (load modules) in the library.

Note: In order to specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

- NOTIFY user ID.

  The NOTIFY user ID is sent a message whenever someone tries to use a data set, and RACF denies the access.

  For example, if your user ID is specified on the NOTIFY keyword, and a user with READ access attempts to update a protected data set, you receive a message identifying the user who attempted the access and what kind of access was attempted.

  Note: If you do not specify a user ID on the NOTIFY keyword, your user ID is the default NOTIFY user ID.

- Erase-on-scratch.

  You might want to specify that the data set protected by this profile be physically erased when the data set is deleted (scratched) or released for re-use. Erasing the data set means overwriting all allocated extents with binary zeros. To use erase-on-scratch, specify the ERASE operand on the ADDSD command.

- WARNING option.

  Specifying WARNING allows *unauthorized* users to access a data set. RACF issues a warning message to the user requesting access, then allows the access.

  > **Attention**
  >
  > WARNING is generally used only during a transition period when RACF is first installed. If you use WARNING, it is equivalent to no protection.

- Your installation may have other security requirements for protecting data, including audit type, level, and security label. See your RACF security administrator for specific information.

2. Create the profile for the data set.

To create a discrete profile for a cataloged data set, enter the ADDSD command as follows:

```
ADDSD 'dataset-name' UACC(access-authority)
```

Note: A cataloged data set is one that is represented in an index in the system catalog.

For example, to create a discrete profile for data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD 'SMITH.PROJ.ONE' UACC(NONE)
```

To create a discrete profile for a data set that is not cataloged, you must specify the unit type and volume serial number of the data set. Enter the ADDSD command as follows:

```
ADDSD 'dataset-name' UNIT(type) VOLUME(volume-serial) +
      UACC(access-authority)
```

For example, to create a discrete profile for data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD 'SMITH.PROJ.ONE' UNIT(3380) VOLUME(ABC123) +
      UACC(NONE)
```

To create a discrete profile with a NOTIFY user ID, enter the ADDSD command as follows:

```
ADDSD 'data-set-name' UACC(access-authority) NOTIFY(userid)
```

For example, if your user ID is SMITH, and you want to be notified when RACF denies access to data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD 'SMITH.PROJ.ONE' UACC(NONE) NOTIFY
```

If your user ID is SMITH, and you want JONES to be notified when RACF denies access to data set SMITH.PROJ.ONE, enter the following command:

```
ADDSD 'SMITH.PROJ.ONE' UACC(NONE) NOTIFY(JONES)
```

To create a discrete profile for a VSAM data set, you can use the VSAM cluster name on the ADDSD command. The following example illustrates how this is done.

SMITH has created a VSAM cluster using the following command:

```
DEFINE CLUSTER(NAME('SMITH.SAMPLE') VOLUMES(VSAM02) ) +
  INDEX(NAME('SMITH.SAMPLEI') TRACKS(1 1) ) +
  DATA(NAME('SMITH.SAMPLED') CYLINDERS(1 1) KEYS(128 0) +
  CONTROLINTERVALSIZE(X'1000') )
```

SMITH can protect this cluster with a profile named 'SMITH.SAMPLE', as follows:

```
ADDSD 'SMITH.SAMPLE' UACC(NONE) NOTIFY
```

Creating a Generic Profile to Protect a Data Set

Create a generic profile if you have several data sets that have the same security requirements and that have some identical characters in their names. To create a generic profile:

1. Decide how to specify the profile name.

To define a generic profile you either include one or more generic characters (%, *, **) in the profile name or you specify the profile as a generic profile.

You can use the following generic characters when naming generic profiles:

% (percent sign)
A percent sign matches one and only one character. For example, a generic data set profile named AB.CD.% protects data sets named AB.CD.E and AB.CD.F, but not AB.CD.EF.

*** (asterisk)**
An asterisk used as a qualifier in the middle of a profile name (for example, ABC.*.DEF) matches one and only one qualifier.

An asterisk used as a character at the end of a qualifier in the middle of a profile name (for example, ABC.DE*.FGH) matches zero or more characters until the end of the qualifier.

An asterisk used at the end of a profile name has different meanings depending upon whether enhanced generic naming (EGN) is active.

- When enhanced generic naming is not active:
  An asterisk used as a character at the end of a profile name (for example, ABC.DEF*) matches zero or more characters until the end of the name, zero or more qualifiers until the end of the name, or both.
  An asterisk used as a qualifier at the end of a profile name (for example, ABC.DEF.*) matches one or more qualifiers until the end of the name.
- When enhanced generic naming is active:
  An asterisk used as a character at the end of a profile name (for example, ABC.DEF*) matches zero or more characters until the end of the qualifier.
  An asterisk used as a qualifier at the end of a profile name (for example, ABC.DEF.*) matches one and only one qualifier.

To find out whether EGN is active at your installation, ask your security administrator.

**** (double asterisk)**
A double asterisk matches zero or more qualifiers. For example, a generic data set profile named AB.CD.** protects data sets named AB.CD, AB.CD.EF, and AB.CD.EF.XYZ.

Note: The double asterisk (**) is allowed with the DATASET class if enhanced generic naming (EGN) is active. Ask your security administrator if EGN is active at your installation.

If a data set matches more than one generic profile, the most specific profile sets the level of protection for the data set. For example, assume there are two generic profiles, USERID.** and USERID.GAMES.*. A data set named USERID.GAMES.INDOOR would be protected by profile USERID.GAMES.*. Profile USERID.** would not protect the data set.

To create a generic profile for your user data set, the high-level qualifier must be your user ID. For example, for user ASMITH to protect data set ASMITH.PROJ.ONE, ASMITH must specify a profile name beginning with ASMITH (such as ASMITH.PROJ.* or ASMITH.PROJ.**).

You create a generic profile in the same manner as a discrete profile, except that you include one or more generic characters (% or *) in the profile name or you include the GENERIC keyword on the ADDSD command.

See “Profile Names for Data Sets” on page 80 for information about generic profile names with enhanced generic naming active and inactive.

How to specify the generic characters depends on whether your installation uses *enhanced generic naming.* Ask your RACF security administrator if enhanced generic naming is active.

If enhanced generic naming is active, see “Generic Profile Rules When Enhanced Generic Naming Is Active” on page 82 for a description of how to specify generic characters in profile names.

If enhanced generic naming is *not* active, see “Generic Profile Rules When Enhanced Generic Naming Is Inactive” on page 80 for a description of how to specify generic characters in profile names.

Note: Profiles created *before* an installation converts to enhanced generic naming are *not* affected by the conversion. Profiles created *after* the installation converts to enhanced generic naming are governed by the new rules.

2. Decide which RACF protections to use.

There are different options you can use depending on how much protection you want.

Note: To give specific authority to a certain user you could include that use on the access list for that data set. To do that see “Permitting an Individual or a Group to Use a Data Set” on page 70.

The following options provide different degrees of general protection for your data set:

- UACC (universal access authority)

  Universal access authority specifies the authority any user that is not on the access list has to use the data set. The UACC can be one of the following:

  NONE Does not allow users to access the data set.

Attention

Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you may want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See “Permitting an Individual or a Group to Use a Data Set” on page 70 for information on how to permit selected users or groups to access a data set.)

  READ Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

UPDATE
Allows users to read from, copy from, or write to the data set. UPDATE does not, however, authorize a user to delete, rename, move, or scratch the data set.

CONTROL
For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform control-interval access (access to individual VSAM data blocks), and to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER
ALTER allows users to read, update, delete, rename, move, or scratch the data set.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list*. However, ALTER does not allow users to change the owner of the profile.

When specified in a generic profile, ALTER gives users *no* authority over the profile itself.

When specified in a generic profile, ALTER allows users to create new data sets that are covered by that profile.

EXECUTE
For a private load library, EXECUTE allows users to load and execute, but not read or copy, programs (load modules) in the library.

Note: To specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

Note: If you do not specify UACC, the system uses the value specified in the UACC field in your current connect group. (For more information, see “Finding Out What Authority You Have as a Member of a Group” on page 17.)

- NOTIFY user ID.

  The NOTIFY user ID is sent a message whenever someone tries to use a data set, and RACF denies the access.

  For example, if your user ID is specified on the NOTIFY keyword, and a user with READ access attempts to update a protected data set, you receive a message identifying the user who attempted the access and what kind of access was attempted.

  Note: If you do not specify a user ID on the NOTIFY keyword, your user ID is the default NOTIFY user ID.

- Erase-on-scratch.

  If allowed by your installation, you can specify that a data set protected by this profile be physically erased when the data set is deleted (scratched) or released for re-use. Erasing the data set means overwriting all allocated extents with binary zeros. To use erase-on-scratch, specify the ERASE operand on the ADDSD command.

  Note: Only the data set that is deleted is erased. For example, the profile SMITH.SAMPLE*.DATA protects data sets SMITH.SAMPLE1.DATA and SMITH.SAMPLE2.DATA. If SMITH.SAMPLE1.DATA is deleted, only SMITH.SAMPLE1.DATA is erased. SMITH.SAMPLE2.DATA is not affected.

- WARNING option.

  Specifying WARNING allows *unauthorized* users to access a data set. RACF issues a warning message to the user requesting access, then allows the access.

> **Attention**
>
> WARNING is generally used only during a transition period when RACF is first installed. If you use WARNING, it is equivalent to no protection.

Your installation may have other security requirements for protecting data, including audit type, level, and security label. See your RACF security administrator for specific information.

3. Create the profile.

   To create a generic profile, enter the ADDSD command as follows:

   ```
   ADDSD 'profile-name-with-generic-character' UACC(access-authority)
   ```

   To create a fully-qualified generic profile, enter the ADDSD command as follows:

   ```
   ADDSD 'profile-name' UACC(access-authority) GENERIC
   ```

   Note: Changes to the profile will take effect for other users when they log off and log on again. For additional information, see "When Data Set Profile Changes Take Effect" on page 83.

   Example 1. A generic profile for all data sets not otherwise protected

   You can create a generic profile to protect all of your data sets that are not protected by more specific profiles. To do this, enter one of the following commands:

   - If your system has enhanced generic naming:

     ```
     ADDSD 'prefix.**' UACC(NONE)
     ```

   - If your system does not have enhanced generic naming:

     ```
     ADDSD 'prefix.*' UACC(NONE)
     ```

   where *prefix* is your user ID. The profile created allows a universal access authority (UACC) of NONE.

   Example 2. A generic profile for data sets whose last qualifier is TESTDATA

   You can create a generic profile to protect all of your data sets that have three qualifiers whose last qualifier is TESTDATA. To do this, enter the following command:

   ```
   ADDSD 'prefix.*.TESTDATA' UACC(NONE)
   ```

   where *prefix* is your user ID. The profile created allows a universal access authority (UACC) of NONE. You can permit or deny specific users or groups access to these data sets. For more information, see "Permitting an Individual or a Group to Use a Data Set" on page 70 or "Denying an Individual or a Group Use of a Data Set" on page 71.

Example 3. A generic profile for group data sets

You can create a generic profile to protect all of a group's data sets that are not protected by more specific profiles. To do this, enter one of the following commands:

- If your system has enhanced generic naming:
  ```
  ADDSD 'groupname.**' UACC(NONE)
  ```
- If your system does not have enhanced generic naming:
  ```
  ADDSD 'groupname.*' UACC(NONE)
  ```

where *groupame* is the group name. The profile that is created allows a universal access authority (UACC) of NONE.

Example 4. A fully-qualified generic profile

You want to allow a universal access of READ to a particular listing file that you will be deleting and recreating. To do this, enter the following command:

```
ADDSD 'prefix.SAMPLE.LISTING' UACC(READ) GENERIC
```

where *prefix* is your user ID. The profile created allows a universal access authority (UACC) of READ.

Finding Out How a Data Set is Protected

If you are the owner of a data set, you may want to determine what protection the data set has. For example, you might want to find out what users and groups can access the data set.

Note: Contact your security administrator if any problems occur with your data set protection.

To see how a data set is protected:

1. Determine if a discrete profile protects the data set by issuing the LISTDSD command as follows:
   ```
   LISTDSD DATASET('dataset-name') ALL
   ```

   You will see one of the following on your screen:
   - A listing for that profile, if the data set is protected by a discrete profile.
   - A listing for the generic profile, if the data set is not protected by a discrete profile but is protected by a fully-qualified generic profile, and generic profile command processing is active. (A generic profile is identified by a "G" in parentheses following the profile name.)
   - A message stating that no profile was found, if the data set is not protected by a discrete profile.

     Note: If generic profile checking is active, and you get the message that no profile was found, you must do Step 2 to check for generic profiles.

   If the command succeeds, you will see a listing of the profile similar to that shown in Figure 44 on page 60.
2. Determine if the data set is protected by a generic profile by entering the LISTDSD command with the GENERIC operand as follows:
   ```
   LISTDSD DATASET('dataset-name') ALL GENERIC
   ```

You will see one of the following on your screen:

- A listing for that profile, if the data set is protected by a fully-qualified generic profile.
- A listing for the most specific generic profile that protects the data set, if the data set is not protected by a fully-qualified generic profile but is protected by a generic profile.
- A message stating that no profile was found, if the data set is not protected by a generic profile.

If the command succeeds, you will see a listing of the profile, similar to that shown in Figure 44 on page 60.

If the command indicates that a profile is not found, protect the data set with a discrete or generic profile. See “Creating a Discrete Profile to Protect a Data Set” on page 51 or “Creating a Generic Profile to Protect a Data Set” on page 53 for more information. If the command fails, contact your RACF security administrator.

```
INFORMATION FOR DATASET profile-name

LEVEL    OWNER        UNIVERSAL ACCESS     WARNING     ERASE
-----    -----        ----------------     -------     -----
 00      SMITH            READ               NO          NO

AUDITING
----------
SUCCESS(UPDATE)

NOTIFY
--------
NO USER TO BE NOTIFIED

YOUR ACCESS          CREATION GROUP        DATASET TYPE
--------------        ----------------      --------------
   READ                   DEPTD60              NON-VSAM

VOLUMES ON WHICH DATASET RESIDES             UNIT
----------------------------------           ------
           21345                             SYSDA

INSTALLATION DATA
-------------------
PL/1 LINK LIBRARY

           SECURITY LEVEL
------------------------------------------------
NO SECURITY LEVEL

CATEGORIES
-----------
NOCATEGORIES

SECLABEL
-----------
NO SECLABEL

CREATION DATE     LAST REFERENCE DATE     LAST CHANGE DATE
(DAY)  (YEAR)      (DAY)     (YEAR)        (DAY)   (YEAR)
-------------     -------------------     ---------------
 070    95          090       98            090     98

ALTER COUNT    CONTROL COUNT    UPDATE COUNT    READ COUNT
-----------    -------------    ------------    ----------
 00000            00000            00002          00000

   ID       ACCESS      ACCESS COUNT
--------   --------    --------------
JONES       UPDATE         00009

   ID     ACCESS      ACCESS COUNT   CLASS            ENTITY NAME
--------  -------    -------------- -------- -----------------------
NO ENTRIES IN CONDITIONAL ACCESS LIST

DFP INFORMATION

RESOWNER
--------
SMITH
```

Figure 44. LISTDSD Command: Sample Output

Check the following fields for the most important security information about how the data set is protected:

- LEVEL field (if used at your installation)
- OWNER field
- UNIVERSAL ACCESS field
- WARNING field
- SECURITY LEVEL field (if used at your installation)
- CATEGORIES field (if used at your installation)
- SECLABEL field (if used at your installation)
- ID field and its related ACCESS and ACCESS COUNT fields
- PROGRAM field and its related ID, ACCESS, and ACCESS COUNT fields

Here are detailed descriptions of the fields appearing in the output:

INFORMATION FOR DATASET *profile-name*

This phrase appears for each data set profile listed.

Note: If the profile is a generic profile, the phrase looks like the following:

```
INFORMATION FOR DATASET profile-name (G)
```

LEVEL

A security classification indicator used by each individual installation. If anything other than 00 appears in this field, see your RACF security administrator for an explanation of the number.

OWNER

Each RACF-defined data set has an owner, which may be a user ID or a group. When you create a data set and then RACF-protect the data set without specifying an owner, RACF names you as the owner of the data set profile. The owner of the profile may modify the data set profile.

UNIVERSAL ACCESS

Each data set protected by RACF has a universal access authority (UACC). The UACC permits users or groups to use the data set in the manner specified in this field. In this example, the UACC is READ. Anyone may read this data set. (The only exception is if the user or group is specifically named in the access list with ACCESS of NONE.)

WARNING

If this field contains YES, RACF permits a user to access this resource *even though his or her access authority is insufficient*. RACF issues a warning message *to the user who is attempting access;* you are notified only if your user ID is the NOTIFY user ID.

If this field contains NO, RACF denies access to users with insufficient authority to access this resource.

ERASE

If this field contains YES, and erase-on-scratch is in effect on your system, data management physically erases the DASD data set extents when the data set is deleted. If this field contains NO, data management will not erase DASD data set extents when the data set is deleted.

Exception

Your installation could specify erase-on-scratch for all data sets that have a security level equal to or greater than the security level specified by the installation. If this data set's security level is equal to or greater than the security level specified by the installation, this data set will be erased even if the ERASE field in the profile contains NO.

AUDITING
The type of access attempts that are recorded. In this example, the AUDITING is SUCCESS(UPDATE). RACF records all successful attempts to update the data set.

NOTIFY
The user ID of a RACF-defined user that RACF notifies when denying access to a data set protected by this profile.

YOUR ACCESS
How you may access this data set.

If you must work with the listed data set but do not have the required authority, ask the owner (OWNER field) to issue a PERMIT command to give you access to the data set.

CREATION GROUP
The group under which the profile was created.

DATASET TYPE
The data set type. It may be either VSAM, NON-VSAM, MODEL, or TAPE.

VOLUME ON WHICH THE DATASET RESIDES
The volume on which a non-VSAM data set resides or the volume on which the catalog for a VSAM data set resides.

UNIT
The unit type for a non-VSAM data set.

INSTALLATION-DATA
Any information your installation keeps in this data set profile.

CREATION DATE
The date the profile was created.

SECURITY-LEVEL
Your installation can define its own security levels. This security level is a name associated with the numeric value shown in the LEVEL field earlier in this output. The security level displayed is the minimum security level you need to access a data set protected by this profile.

CATEGORIES
Your installation can define its own security categories. The names displayed are the security categories you need to access a data set protected by this profile.

SECURITY-LABEL
Your installation can define its own security labels. This security label is a name used to represent the association between a particular security level and a set of zero or more security categories. The security label displayed is the minimum security label you need to access a data set protected by this profile.

LAST REFERENCE DATE
The last time the profile was accessed.

LAST CHANGE DATE
The last time the profile was changed.

ALTER COUNT
The total number of times the data set protected by the profile was altered (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

CONTROL COUNT
The total number of times the data set protected by the profile was successfully accessed with CONTROL authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

UPDATE COUNT
The total number of times the data set protected by the profile was successfully accessed with UPDATE authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

READ COUNT
The total number of times the data set protected by the profile was successfully accessed with READ authority (not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

ID, ACCESS, and ACCESS COUNT
These fields describe the standard access list. ID is the user ID or group name given the access authority listed in the ACCESS field. ACCESS COUNT is the number of times the user listed in the ID field accessed the data set (ACCESS COUNT is not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, this value does not change.

ID, ACCESS, ACCESS COUNT, CLASS, and ENTITY NAME
These fields refer to entries in the conditional access list. A conditional access list is an access list in the data set profile that specifies another condition which must be satisfied for a user to get the specified access authority.

The CLASS and ENTITY NAME fields describe one of the following conditions which must be satisfied before authorization to the data set is granted to the user in the ID field.

1. If CLASS is APPCPORT, the ENTITY NAME is the name of the APPC port of entry, or logical unit (LU), through which the user must enter the system.
2. If CLASS is CONSOLE, the ENTITY NAME is the name of the system console from which the request must be sent.
3. If CLASS is JESINPUT, the ENTITY NAME is the name of the JES input device through which the user must enter the system.
4. If CLASS is PROGRAM, the ENTITY NAME is the name of the program the user must be running.
5. If CLASS is TERMINAL, the ENTITY NAME is the name of the terminal through which the user must enter the system.

ACCESS is the level of access to the data set that RACF grants when the condition is satisfied.

ACCESS COUNT is the number of times the user has accessed the data set under the condition described (ACCESS COUNT is not present for generic profiles).

Note: If your RACF security administrator has chosen not to record statistics for the DATASET class, the ACCESS COUNT value does not change.

DFP INFORMATION / RESOWNER
The RESOWNER field contains the user ID or group name of the owner of the resource. In this case, the resource is the data set; the owner of the data set need not be the same as the owner of the profile.

Finding Out What Data Set Profiles You Have

You can have RACF list the names of the profiles you own. If you want to see what data set profiles you have:

1. Find out what data set profiles you have, by entering the SEARCH command as follows:

   ```
   SEARCH
   ```

   RACF lists all of your profiles that are in the DATASET class. If you do not have any DATASET profiles, RACF displays a message telling you that no entries meet the search criteria.
2. Review the list of profiles, comparing them with the names of the data sets you need to protect.

   Any profile name that matches a data set name protects that data set.

   Any profile name that includes generic characters (% or *) may or may not protect data sets. See “Profile Names for Data Sets” on page 80 for information on the rules for specifying generic characters.

Deleting a Data Set Profile

When you delete a data set profile, any data set previously protected by that profile:

- Is protected by the most specific generic profile if the profile deleted was a discrete data set profile.
- Is protected by the next most specific generic profile if the profile deleted was a generic data set profile.
- Has no RACF protection if no generic profiles exist which protect the data set.

Attention

When you remove RACF protection from a data set, anyone (RACF-defined or not) can access, change, or delete your data set. You can selectively “remove” protection by using the PERMIT command to permit or deny access to your data set by selected users and groups. See “Permitting an Individual or a Group to Use a Data Set” on page 70 and “Denying an Individual or a Group Use of a Data Set” on page 71.

To delete a data set profile:

1. Find the name of the profile that currently protects the data set. To do this, see “Finding Out How a Data Set is Protected” on page 58.
2. Remove RACF protection.

   If the data set is protected by a discrete profile, or if you are removing protection from all data sets covered by a generic profile, delete the data set profile by issuing the DELDSD command as follows:

   ```
   DELDSD 'profile-name'
   ```

This deletes the profile, but leaves the data set intact.

Example 1:

To remove RACF protection from data set SMITH.PROJ.ONE, which is protected by a discrete profile, type:

```
DELDSD 'SMITH.PROJ.ONE'
```

Example 2:

To remove RACF protection from data sets SMITH.FIRST.DATA, SMITH.SECOND.DATA, and SMITH.THIRD.DATA, which are protected by profile SMITH.*.DATA, enter the following command:

```
DELDSD 'SMITH.*.DATA'
```

Attention

Be careful when you delete a generic profile that you are not inadvertently removing RACF protection from a data set that should remain protected. In the previous example, RACF protection would be removed from any data set whose name matched the profile name, such as SMITH.OTHER.DATA.

To list all catalogued data sets that are protected by a profile, enter the following command:

```
LISTDSD DA(profile-name) DSNS NORACF
```

You can then check which data sets are protected by the profile before deleting it.

Note also that when you delete a discrete or generic profile, the data set might still be protected by another generic profile. In the examples above, the data sets might be protected by profile SMITH.** (if enhanced generic naming is in effect) or profile SMITH.* (if enhanced generic naming is not in effect).

Example 3:

To “remove protection” from a data set without deleting a profile or renaming the data set, protect the data set with a profile that has UACC(ALTER) and no names in the access list.

Note: Other security characteristics of the profile, such as LEVEL and SECLEVEL, might still be required by your installation and defined in the profile.

Example 4:

If data sets SMITH.PROJ.ONE and SMITH.PROJ.TWO are protected by generic profile SMITH.PROJ.*, and you want to remove protection from SMITH.PROJ.ONE, create a new profile SMITH.PROJ.ONE with a UACC of ALTER. For specific instructions on creating a discrete profile, see “Creating a Discrete Profile to Protect a Data Set” on page 51.

Chapter 7. Protecting Data on Tapes

RACF can protect your data on tapes. It can control who has what authority to access the data. You can use RACF to protect your data on tapes by creating profiles to protect your tape data sets.

> **Note**
>
> Your installation must have the tape data set protection (TAPEDSN) option active to protect data on tape. Ask your security administrator if the TAPEDSN option is active on your system.

Creating a Profile to Protect a Tape Data Set

You can use a data set profile to protect a tape data set. To protect a tape data set, perform the following steps:

1. Decide if you want to protect the data set with a discrete or generic profile.

   See“Choosing Between Discrete and Generic Profiles” on page 49 if you need more information about discrete and generic profiles.

   The following are some reasons why you would choose a generic or a discrete profile:

   - *Generic profile:* Choose a generic profile when you want to protect more than one data set with the same security requirements. The data sets protected by a generic profile must have some identical characters in their names. The profile name contains one or more generic characters (*, **, or %).
   - *Discrete profile:* Choose a discrete profile when you want to protect one data set with unique security requirements. The name of a discrete profile matches the name of the data set it protects.

   Note: Keep in mind that a generic profile might already exist under which the data set is protected. However, that profile might not provide the exact protection you want for your data set. In this case, you can create a more specific generic profile or a discrete profile for the data set.

   - If a data set is protected by both a generic profile and a discrete profile, the discrete profile sets the level of protection for the data set.
   - If a data set is protected by more than one generic profile, the most specific profile sets the level of protection for the data set.
2. Decide which RACF protections to use.
   - UACC (universal access authority).

     The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see “Creating a Discrete Profile to Protect a Data Set” on page 51 or “Creating a Generic Profile to Protect a Data Set” on page 53.

     Note: If you do not specify UACC, the system uses the value specified in the UACC field in your current connect group. (For more information, see “Finding Out What Authority You Have as a Member of a Group” on page 17.)
   - NOTIFY user ID.

     The NOTIFY user ID is sent a message whenever someone tries to use a data set, and RACF denies the access.

For example, if your user ID is specified on the NOTIFY keyword, and a user with READ access attempts to update a protected data set, you receive a message identifying the user who attempted the access and what kind of access was attempted.

- Your installation may have other security requirements for protecting data, including audit type, level, and security level. See your RACF security administrator for specific information.

3. Create the profile.

   If the data set is **cataloged**, issue the ADDSD command with the TAPE operand as follows:

   ```
   ADDSD 'data-set-name' TAPE UACC(access-authority)
   ```

   RACF protects the entire data set, even if it is a multivolume data set.

   If the data set is **uncataloged**, issue the ADDSD command with the TAPE, UNIT, VOLUME, and FILESEQ operands as follows:

   ```
   ADDSD 'data-set-name' TAPE UNIT(type) +
     VOLUME(volume-serial) FILESEQ(number) UACC(access-authority)
   ```

   If an uncataloged data set is a multivolume data set (it resides on more than one volume), you must first use the ADDSD command to create a discrete profile for one volume, then use the ALTDSD command to add the other volumes to the discrete profile (one ALTDSD command for each additional volume).

   Example 1. Cataloged Tape Data Set:

   You have a cataloged tape data set named SMITH.TEST.DATA1. To protect this data set with a discrete profile, enter the following command:

   ```
   ADDSD 'SMITH.TEST.DATA1' TAPE UACC(NONE)
   ```

   Example 2. Uncataloged Tape Data Set:

   You have a tape data set named SMITH.TEST.DATA residing on tape volume 111111 with a file sequence of 1. To protect this data set with a discrete profile, enter the following command:

   ```
   ADDSD 'SMITH.TEST.DATA2' TAPE UNIT(TAPE) +
     VOLUME(111111) FILESEQ(1) UACC(NONE)
   ```

   Example 3. Uncataloged Multivolume Tape Data Set:

   You have a tape data set named SMITH.TEST.DATA residing on tape volumes 111111, 222222, and 333333, with a file sequence of 1. To protect this data set with a discrete profile, enter the following commands:

   ```
   ADDSD 'SMITH.TEST.DATA3' TAPE UNIT(TAPE) +
     VOLUME(111111) FILESEQ(1) UACC(NONE)
   ALTDSD 'SMITH.TEST.DATA3' ADDVOL(222222)
   ALTDSD 'SMITH.TEST.DATA3' ADDVOL(333333)
   ```

Chapter 8. Changing Access to a Data Set

Situations may occur when you want to allow or deny someone the use of a data set that you have already protected. You may also want to change how users who are not on a particular data set's access list may use that data set. You can change the access to a data set using the methods described in this chapter.

Changing the Universal Access Authority to a Data Set

You can allow other users to access a data set by specifying a universal access authority. This access level would pertain to any user on the system. For example, if you added confidential research data to a data set, you might want to change the universal access authority of the data set.

To change a data set's UACC (universal access authority), you must enter the ALTDSD command with the appropriate operands. To change a data set's UACC:

1. Find the name of the profile that protects the data set. To do this, see "Finding Out What Data Set Profiles You Have" on page 64.

   Remember that changing the UACC for a generic profile changes the access to all data sets protected by the profile.
2. Decide which level of UACC to specify in the profile.

   The UACC can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access Authority for Data Sets" on page 79.

   Attention

   a. Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you may want to initially assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See "Permitting an Individual or a Group to Use a Data Set" on page 70 for information on how to permit selected users or groups to access a data set.)

   b. If you are changing the UACC to restrict access, be certain that any user or group specifically mentioned in the access list has the access to the resource that you intend. For example, if you change the UACC to NONE, and there is a user specifically named in the access list with any authority, that user still has that authority to the resource.
3. Change the UACC specified in the profile.

   To change the UACC, enter the ALTDSD command as follows:

   ```
   ALTDSD 'profile-name' UACC(access-authority)
   ```

   Example 1:

   Assume that data set 'SMITH.PROJ.ONE' is protected by a discrete profile. To change the UACC for this data set to NONE, enter the following command:

   ```
   ALTDSD 'SMITH.PROJ.ONE' UACC(NONE)
   ```

Example 2:

If you are changing the UACC specified in a generic profile, specify the name of the generic profile. For example, to change the UACC for generic profile SMITH.* to NONE, enter the following command:

```
ALTDSD 'SMITH.*' UACC(NONE)
```

Permitting an Individual or a Group to Use a Data Set

You can use a data set profile to protect the information you create and use to do your job. Besides protecting a data set with a universal access authority, you can give certain users different abilities to access it. By adding the users and the authority you want to give them to the access list in the data set profile.

Note: For a description of when a change to a user's access occurs, see "When Data Set Profile Changes Take Effect" on page 83.

To permit an individual or a group use of a data set:

1. Find the name of the profile that protects the data set. To do this, see "Finding Out How a Data Set is Protected" on page 58.
2. Decide whether to use the profile that protects the data set.
   - If the profile is a discrete profile, go on to Step 3.
   - If the profile is a generic profile, it might protect more than one data set. You need to decide whether to create a new profile for the data set. For more information, see "Choosing Between Discrete and Generic Profiles" on page 49 .
3. Decide which access authority to specify for the user.

   The access authority can be one of the following: NONE, READ, UPDATE, CONTROL, ALTER, or EXECUTE. For descriptions of these values, see "Access Authority for Data Sets" on page 79.
4. Allow access to the data set.

   To allow access to your data set, use the PERMIT command with the ACCESS keyword:

   ```
   PERMIT 'profile-name' ID(userID|groupname) ACCESS(level)
   ```

   Example 1. Permitting a user to read a data set

   Data set SMITH.PROJ.ONE is protected by a discrete profile. To permit user JONES to read data set SMITH.PROJ.ONE, enter the following command:

   ```
   PERMIT 'SMITH.PROJ.ONE' ID(JONES) ACCESS(READ)
   ```

   Example 2. Permitting more than one user to read a data set

   To permit users JONES and MOORE to read data set SMITH.PROJ.ONE, enter the following command:

   ```
   PERMIT 'SMITH.PROJ.ONE' ID(JONES, MOORE) ACCESS(READ)
   ```

   Example 3. Permitting more than one user or group to read a data set

   To permit group DEPTD60 and user JONES to read user data set SMITH.PROJ.ONE, enter the following command:

   ```
   PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60, JONES) ACCESS(READ)
   ```

Example 4. Permitting a user to read a group data set

To permit user SMITH to read group data set GROUPID.PROJ.ONE, enter the following command:

```
PERMIT 'GROUPID.PROJ.ONE' ID(SMITH) ACCESS(READ)
```

Denying an Individual or a Group Use of a Data Set

You can use a data set profile to protect the information in your data sets. You may want to deny an individual use of a data set. For example, a colleague who has left the department can still use a data set. For security reasons you wish to exclude the person from using the data set. You can deny anyone access to your data set by specifying a certain universal access or individual access authority.

Note: For a description of when a change to a user's access occurs, see "When Data Set Profile Changes Take Effect" on page 83.

To deny an individual or a group use of a data set:

1. Find the name of the profile that protects the data set. To do this, see "Finding Out How a Data Set is Protected" on page 58.
2. Decide whether to use the profile that protects the data set.
   - If the profile is a discrete profile, go on to Step 3.
   - If the profile is a generic profile, it might protect more than one data set. You need to decide whether to create a new profile for the data set. For more information, see "Choosing Between Discrete and Generic Profiles" on page 49 .
3. Use the PERMIT command to deny access to the data set.

   You can use the PERMIT command to do this in two ways:
   - One way to deny access is to include the user or group on the access list but assign the user or group an access of NONE. To assign an access of NONE is the best procedure to ensure that the user or group has no access to the data set. See "Including the Individual or Group on the Access List with ACCESS(NONE)".
   - The second way is to remove the name of the user or group from the access list. However, this denies access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher, the user or group can still access the data set. See "Removing the User or Group from the Access List" on page 72.

Including the Individual or Group on the Access List with ACCESS(NONE)

Including the user or group on the access list with ACCESS(NONE) ensures that the user or group is denied access the data set.

To deny access by assigning a user or group an access of NONE, enter the PERMIT command with the ACCESS keyword as follows:

```
PERMIT 'profile-name' ID(userid|groupname) ACCESS(NONE)
```

Example 1:

To deny user JONES the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES) ACCESS(NONE)
```

Example 2:

To deny users JONES and MOORE the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES, MOORE) ACCESS(NONE)
```

Example 3:

To deny group DEPTD60 the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60) ACCESS(NONE)
```

Example 4:

To deny groups DEPTD60 and DEPTD58 use of user data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60, DEPTD58) ACCESS(NONE)
```

Removing the User or Group from the Access List

To deny access by removing a user or a group from the access list, enter the PERMIT command with DELETE keyword as follows:

```
PERMIT 'profile-name' ID(userid|groupname) DELETE
```

Example 1:

To deny user JONES use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES) DELETE
```

Example 2:

To deny users JONES and MOORE use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(JONES, MOORE) DELETE
```

Example 3:

To deny group DEPTD60 the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60) DELETE
```

Example 4:

To deny groups DEPTD60 and DEPTD58 the use of data set SMITH.PROJ.ONE, enter the following command:

```
PERMIT 'SMITH.PROJ.ONE' ID(DEPTD60, DEPTD58) DELETE
```

Chapter 9. Protecting General Resources

The types of general resources that RACF can protect include:

- DASD volumes
- Tape volumes
- Load modules (programs)
- Application resources (such as resources for IMS, CICS, and DB2)
- Terminals
- Installation-defined resources

For a complete list, see “Description of RACF Classes” on page 85.

Resources are protected with profiles. A profile contains descriptive information about a user, a group, or resource. RACF uses the information in a profile to control use of protected resources. When you attempt to use a protected resource, RACF checks your user profile, as well as the resource profile, to decide whether to allow you to use the resource.

Resource profiles describe the information and the levels of authority needed to use the resource. A resource profile contains:

- The resource name and resource owner.
- The access list, which is a list of users who may use a resource and how they may use it.
- The universal access authority (UACC), which is the default level of access authority allowed for all users who are not listed in the access list.
- Auditing information. RACF can audit the use of each resource. The audit can be general or specific. For example, you can set up a resource profile for your resource to audit every attempt to use that resource. Or, you can define the profile to audit only the attempts to update the resource.

  You can protect a resource by identifying specific users with the access you want them to have in the access list. All other users are allowed the access you specify as the universal access authority (UACC). The access authorities you can specify are: NONE, READ, UPDATE, CONTROL, and ALTER. See “Access Authority for General Resources” on page 80 for more information about access authorities. To protect a resource most effectively, you should initially specify a UACC of NONE and selectively give certain users specific access authority to the resource.

Note: The security administrator is *generally* the person who defines, alters, or deletes a general resource profile.

You can use RACF to protect your general resources by doing the tasks defined in this chapter.

Searching for General Resource Profile Names

You can list the names of general resource profiles that you own by using the SEARCH command.

The SEARCH command searches the RACF database for the names of profiles (in a particular resource class) that match the criteria you specify. For example, you can search for all TERMINAL profiles. Profiles that are listed are those you are the owner of, or to which you have at least READ access authority.

The output of this command is in line mode unless you use ISPF panels. You can use the TSO session manager to scroll through the output from the listing commands. By using the CLIST operand, you can save the list of profile names in a data set.

Attention: Using the SEARCH command may slow the system's performance. Therefore, the SEARCH command should be used with discretion (or not at all) during busy system times.

1. Find the name of the class that represents the resource you want to search. Valid class names are DATASET, USER, GROUP, and those names specified in the class descriptor table (CDT). For a list of the general resource classes that are defined in the class descriptor table supplied by IBM, see "Description of RACF Classes" on page 85.
2. Request the list of RACF profiles for the class. To search the RACF database for general resource profiles that you own, use the SEARCH command with the CLASS operand. Enter `search class(`*`classname`*`)` to find all the general resources you can access, this must be done one class at a time.

Example:

To search for resource profiles in class TERMINAL, type: `SEARCH CLASS(TERMINAL)`

Other Operands of the SEARCH Command

These examples show only some of the operands that are available to use on the SEARCH command. The complete syntax of the SEARCH command, with descriptions of all the command operands, is described in *OS/390 SecureWay Security Server RACF Command Language Reference*. In particular, you may want to read about these operands:

- CLIST

  Specifies RACF commands (or other commands) to be saved with the profile names, generating a CLIST that you run against the profiles.
- FILTER

  Specifies a string of characters to be used in searching the RACF database. The filter string defines the range of profile names you want to select from the RACF database.

Listing the Contents of General Resource Profiles

You can list the contents of general resource profiles that you own by using the RLIST command.

The RLIST command lists the contents of general resource profiles in a particular resource class. If you specify a profile that you do not have access to, you may receive an "access violation" message from the RLIST command.

Note: To see the access list for a resource, you must be the owner of the resource, or have ALTER access to the resource.

1. Find the name of the class that represents the resource you want to search. Valid class names are those specified in the class descriptor table (CDT). For a list of general resource classes defined in the class descriptor table supplied by IBM, see "Description of RACF Classes" on page 85.

2. Specify the RACF profiles you want to list. To list the contents of general resource profiles that you own, use the RLIST command with the class name and a profile name. Type:

   ```
   RLIST classname profile-name
   ```

Example 1:

To list the contents of resource profile IDTERMS in class TERMINAL, type:

```
RLIST TERMINAL IDTERMS
```

Example 2:

To list the contents of all resource profiles in class TERMINAL, type:

```
RLIST TERMINAL *
```

Other Operands of the RLIST Command

These examples show only some of the operands that are available to use on the RLIST command. The complete syntax of the RLIST command, with descriptions of all the command operands, is described in *OS/390 SecureWay Security Server RACF Command Language Reference*. In particular, you might want to read about these operands:

- ALL

  Displays all information specified for each resource.

- AUTHUSER

  Displays the standard and conditional access lists for the profile. This is useful information to have before you use the PERMIT command to allow or deny access to the resource.

Permitting an Individual or a Group to Use a General Resource

You can give certain users or groups of users different access authorities to use a general resource. You add their user ID and the authority you want to give them to the access list on the resource profile. For example, if you would like J.E. Jones, whose user ID is JONES, to use your RACF-protected terminal, you would add his user ID to its access list.

To permit an individual or a group to use a general resource:

1. Find the name of the profile that protects the general resource. To do this, see “Searching for General Resource Profile Names” on page 73.
2. Decide which access authority to specify in the profile. The access authority can be one of the following: NONE, READ, UPDATE, CONTROL, and ALTER. For descriptions of these values, see “Access Authority for General Resources” on page 80.
3. Allow access to the general resource. To allow access to your general resource, use the PERMIT command with the ACCESS operand. Type:

   ```
   PERMIT profile-name CLASS(classname) ID(userid|groupname)
          ACCESS(access-authority)
   ```

Example 1:

To permit user Jones to have access to a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(JONES) ACCESS(READ)
```

Example 2:

To permit groups DEPTD60 and DEPTD58 to have access to a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(DEPTD60, DEPTD58) ACCESS(READ)
```

Other Operands of the PERMIT Command

These examples show only some of the operands that are available to use on the PERMIT command. The complete syntax of the PERMIT command, with descriptions of all the command operands, is described in *OS/390 SecureWay Security Server RACF Command Language Reference*.

Denying an Individual or a Group Use of a General Resource

You may want to deny an individual or group use of a general resource. For example, a colleague who has left the department can still use a general resource. For security reasons you would wish to exclude the person from using the general resource. You can deny a person access to your general resource by specifying a certain universal access or individual access authority.

To deny an individual or a group the use of a general resource:

1. Find the name of the profile that protects the general resource. To do this, see "Searching for General Resource Profile Names" on page 73.
2. Deny access to the general resource. You can deny access in one of two ways:
   - One way is to remove the name of the user or group from the access list. However, this denies access only if the UACC is NONE. For example, if you delete a user or group from the access list but the UACC is READ or higher, the user or group still has access to the general resource. See "Removing the Individual or Group from the Access List" on page 77.
   - The second way to deny access is to include the user or group on the access list but assign the user or group an access of NONE. By assigning an access of NONE, you make sure the user or group cannot access the general resource. See "Including the Individual or Group on the Access List with ACCESS(NONE)".

Including the Individual or Group on the Access List with ACCESS(NONE)

By including the user or group on the access list with ACCESS(NONE), you make sure that the user or group cannot access the general resource. To deny access by assigning a user or group an access of NONE, enter the PERMIT command with the ACCESS keyword as follows:

```
PERMIT profile-name CLASS(classname) ID(userid|groupname) ACCESS(NONE)
```

Example 1:

To deny user Jones use of a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(JONES) ACCESS(NONE)
```

Example 2:

To deny groups DEPTD60 and DEPTD58 use of a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(DEPTD60, DEPTD58) ACCESS(NONE)
```

Other Operands of the PERMIT Command

These examples show only some of the operands that are available to use on the PERMIT command. The complete syntax of the PERMIT command, with descriptions of all the command operands, is described in *OS/390 SecureWay Security Server RACF Command Language Reference*. In particular, you might want to read about this operand:

- RESET

  Deletes the entire contents of both the standard access list and the conditional access list of a profile.

Removing the Individual or Group from the Access List

To revert to the universal access authority for a user or a group, enter the PERMIT command with the DELETE operand. Type:

```
PERMIT profile-name CLASS(classname) ID(userid|groupname) DELETE
```

Example 1:

To remove user Jones from the access list for a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(JONES) DELETE
```

Access to the terminal for user Jones reverts to the universal access authority for the terminal.

Example 2:

To remove groups DEPTD60 and DEPTD58 from the access list for a terminal protected by general resource profile IDTERMS, type:

```
PERMIT IDTERMS CLASS(TERMINAL) ID(DEPTD60, DEPTD58) DELETE
```

Access to the terminal for groups DEPTD60 and DEPTD58 reverts to the universal access authority for the terminal.

Other Operands of the PERMIT Command

These examples show only some of the operands that are available to use on the PERMIT command. The complete syntax of the PERMIT command, with descriptions of all the command operands, is described in *OS/390 SecureWay Security Server RACF Command Language Reference*. In particular, you might want to read about this operand:

- RESET

  Deletes the entire contents of both the standard access list and the conditional access list of a profile.

Appendix A. Reference Summary

The following sections contain reference information about RACF.

Access Authority for Data Sets

These definitions apply both to UACC authority and to authority granted to individual users or groups in the data set profile access list. Access authority for data sets can be:

NONE Does not allow users to access the data set.

> **Attention**
>
> Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can downgrade it. For this reason, you will probably want to assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known. (See “Permitting an Individual or a Group to Use a Data Set” on page 70 for information on how to permit selected users or groups to access a data set.)

READ Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

UPDATE

Allows users to read from, copy from, or write to the data set. UPDATE does not, however, authorize a user to delete, rename, move, or scratch the data set.

Allows users to perform normal VSAM I/O (not improved control interval processing) to VSAM data sets.

CONTROL

For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform improved control interval processing. This is control-interval access (access to individual VSAM data blocks), and the ability to retrieve, update, insert, or delete records in the specified data set.

For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER

ALTER allows users to read, update, delete, rename, move, or scratch the data set.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list.*

Note: ALTER does not allow users to change the owner of the profile using the ALTDSD command. However, if a user with ALTER access authority to a discrete data set profile renames the data set, changing the high-level qualifier to his or her own user ID, then both the data set and the profile are renamed, *and* the OWNER of the profile is changed to the new user ID.

When specified in a generic profile, ALTER gives users *no* authority over the profile itself, but lets users create new data sets that are covered by that profile.

EXECUTE
For a private load library, EXECUTE lets users load and execute, but not read or copy, programs (load modules) in the library.

Note: In order to specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

Access Authority for General Resources

These definitions apply both to UACC authority and to authority granted to individual users or groups in the resource profile access list.

The UACC is the default **resource-access authority**. All users or groups of users in the system who are not specifically named in an access list of authorized users for that resource can still access the resource with the authority specified by the UACC. The UACC also applies to users not defined to RACF.

Note: These access authorities can have different meanings depending on the general resource they are protecting. *OS/390 SecureWay Security Server RACF Security Administrator's Guide* describes the meaning of the access authorities for each kind of general resource. Additional information should be found in the reference materials for the specific product.

The resource access authorities are:

ALTER
Specifies that the user or group have full control over the resource.

CONTROL
Is used only for VSAM data sets and specifies that the user or group have access authority that is equivalent to the VSAM control password.

UPDATE
Specifies that the user or group be authorized to access the resource for the purpose of reading or writing.

READ Specifies that the user or group be authorized to access the resource for the purpose of reading only.

EXECUTE
Specifies that the user or group can run programs but not read or copy them.

NONE Specifies that the user or group not be permitted to access the resource.

Profile Names for Data Sets

The enhanced generic naming (EGN) option changes the meaning of generic characters within profile names. To find out if EGN is active at your installation, ask your security administrator.

Generic Profile Rules When Enhanced Generic Naming Is Inactive

In the DATASET class, you can use generic characters as follows:

- Specify % to match any single character in a data set name

- Specify * as follows:
  - As a character at the end of a data set profile name (for example, ABC.DEF*) to match zero or more characters until the end of the name, zero or more qualifiers until the end of the data set name, or both
  - As a qualifier at the end of a profile name (for example, ABC.DEF.*) to match one or more qualifiers until the end of the data set name
  - As a qualifier in the middle of a profile name (for example, ABC.*.DEF) to match any one qualifier in a data set name
  - As a character at the end of a qualifier in the middle of a profile name (for example, ABC.DE*.FGH) to match zero or more characters until the end of the qualifier in a data set name.

Note: For profiles in the DATASET class, the high-level qualifier of the profile name must not be, nor may it contain, a generic character—for example, *.ABC, AB%.B, and AB*.AB are not allowed.

The following tables are provided to show the variety of profiles that can be created by using generics, and by using enhanced generic naming. They also show the effects on profile protection if enhanced generic naming is turned off.

Table 2 and Table 3 provide examples of data set names using generic naming. Enhanced generic naming has not been turned on (SETROPTS NOEGN, the default, is in effect).

Table 4 and Table 5 provide examples of data set names with enhanced generic naming (SETR EGN is on).

*Table 2. Generic Naming for Data Sets with Enhanced Generic Naming Inactive: * at the End*

Profile Name	**AB.CD***	**AB.CD.***
Resources protected by the profile	AB.CD AB.CDEF AB.CD.EF AB.CD.XY AB.CD.EF.GH	AB.CD.EF AB.CD.XY AB.CD.EF.GH
Resources not protected by the profile	ABC.DEF ABC.XY.XY.DEF	AB.CD AB.CDEF ABC.DEF AB.XY.XY.DEF

*Table 3. Generic Naming for Data Sets with Enhanced Generic Naming Inactive: * in the Middle or %*

Profile Name	**ABC.%EF**	**AB.*.CD**	**AB.CD*.EF**
Resources protected by the profile	ABC.DEF ABC.XEF	AB.CD.CD	AB.CDEF.EF AB.CDE.EF
Resources not protected by the profile	ABC.DEFGHI ABC.DEF.GHI ABC.DDEF	AB.CD AB.CD.EF AB.CDEF ABC.DEF ABC.XY.CD AB.XY.XY.CD	AB.CD.XY.EF

Generic Profile Rules When Enhanced Generic Naming Is Active

The *enhanced generic naming* option applies only to data sets and allows you to use double asterisks (**) in the DATASET class. It also changes the meaning of the single asterisk (*) at the end of a profile name.

Your RACF security administrator activates enhanced generic naming by issuing the SETROPTS command with the EGN operand. SETROPTS EGN makes the rules for data set and general resource profiles consistent with each other. Additionally, generic profiles can be more precise, and the generic profile names are more similar to other IBM products.

New installations should set EGN on immediately.

The following rules apply if you have enhanced generic naming in effect.

Specify * as follows:

- As a character at the end of a data set profile name to match zero or more characters until the end of the qualifier.
- As a qualifier at the end of a profile name to match *one* qualifier until the end of the data set name.

  Note: There are differences in the meaning of an ending asterisk, depending on whether an installation is using generic profiles with or without EGN.

Specify ** as follows:

- As either a middle or end qualifier in a profile name to match zero or more qualifiers. Only one occurrence of a double asterisk is allowed in a profile name.

  For example, ABC.DE.** is allowed; ABC.DE** is not allowed; and A.**.B.** is not allowed.

Note: RACF does not allow you to specify any generic characters in the high-level qualifier of a data set name.

Table 4 and Table 5 on page 83 show examples of generic profile names you can create when enhanced generic naming is active, and the resources protected and not protected by those profiles.

*Table 4. Generic Data Set Profile Names Created with Enhanced Generic Naming Active: * and ***

Profile Name	A.B*	A.B.*	A.B.**	A.B*.**	A.B.*.**
Resources protected by the profile	A.B A.BC	A.B.C A.B.X	A.B A.B.C A.B.C.D A.B.X	A.B A.B.C A.BC A.BC.D A.B.C.D A.B.X	A.B.C A.B.C.D A.B.X
Resources not protected by the profile	A.B.C A.B.C.D A.B.X AB.CD	A.B A.BC A.B.C.D AB.CD	A.BC A.BC.D AB.CD	AB.CD	AB.CD A.BC A.BC.D A.B AB.X.Y.C

*Table 5. Generic Data Set Profile Names Created with Enhanced Generic Naming Active: *, **, or % in the Middle*

Profile Name	ABC.%EF	AB.*.CD	AB.**.CD
Resources protected by the profile	ABC.DEF ABC.XEF	AB.CD.CD	AB.CD AB.X.CD AB.X.Y.CD
Resources not protected by the profile	ABC.DEFGHI ABC.DEF.GHI ABC.DDEF	AB.CD AB.CD.EF AB.CDEF ABC.DEF ABC.XY.CD ABC.XY.XY.CD	AB.CD.EF AB.CDEF ABC.X.CD.EF ABC.DEF ABX.YCD

Note: Although multiple generic profiles may match a data set name, only the most specific actually protects the data set. For example, AB.CD*, AB.CD.**, and AB.**.CD all match the data set AB.CD, but AB.CD* protects the data set.

In general, given two profiles that match a data set, you can find the more specific one by comparing the profile name from left to right. Where they differ, a non-generic character is more specific than a generic character. In comparing generics, a % is more specific than an *, and an * is more specific than **. Another way to determine the most specific is with the SEARCH command, as there are some rare exceptions to the general rule. SEARCH always lists the profiles in the order of the most specific to the least specific.

When Data Set Profile Changes Take Effect

If a user is currently using a data set, changing the data set profile protecting the data set may not affect the user's current access until that user logs on again.

The change affects the user's access immediately in the following cases:

- If the user is not logged on. You can check to see if a user is logged on with the TSO STATUS command:

  ```
  STATUS userid
  ```

  If the user is logged on, the system displays a message indicating that a job with the letters TSU in it is executing.
- If the user is logged on and has not yet opened the data set or a data set protected by the same generic profile (for example, by browsing or editing).

If the user is logged on and has opened the data set, and you change his access, two situations could occur:

- If the profile is a discrete profile, the user's access changes after closing the data set.
- If the profile is a generic profile, the user's access changes after *one* of the following occurs:
  - The user issues the LISTDSD command as follows:

    ```
    LISTDSD DATASET(data-set-protected-by-the-profile) GENERIC
    ```

    This places a fresh copy of the profile in the user's address space.
  - A SETROPTS GENERIC(DATASET) REFRESH is issued on the system the user is logged on to.

Note: This command cannot be issued by a general user. It can be issued only by someone with the SPECIAL, OPERATIONS, or AUDITOR attribute.

– The user references more than four data sets with different high-level qualifiers, and the data sets are protected by generic profiles.

– The user logs off and then logs back on.

Automatic Direction of Application Updates

While running, an application may make updates to the RACF database. For example, if a user enters an incorrect logon password, an application updates the RACF database to increment the count of incorrect passwords. Updates are also made when a user creates, deletes, or renames a data set that is protected by a discrete profile. In this case, updates are made to maintain the data set profile.

Automatic direction of application updates, a function of the RACF remote sharing facility, is primarily used to keep already-synchronized RACF profiles synchronized between two or more remote nodes. Automatic direction of application updates propagates each individual update. Propagation of an application update takes place only after the update has successfully completed on the node where the application is running and only if SET AUTOAPPL has been used to activate automatic direction on that node.

An installation decides who should be notified of results and output from automatically directed application updates, so a user may or may not see output or TSO SEND messages from automatically directed application updates. If you receive output or notification that an automatically directed application update failed, notify your RACF security administrator.

Format of Output

Figure 45 shows the sample output of a successful application update. In this example, RACF sets the revoke count for a non-valid password attempt.

```
========================================================================
Application update request issued at 15:49:27 on 03/17/98 was
processed at NODE4.RRSFU1 on 03/17/98 at 15:49:28
Request was propagated by automatic direction from NODE3.RRSFU1

 REQUEST ISSUED:  ICHEINTY ALTER operation from user NODE3.RRSFU1

 REQUEST OUTPUT:
 IRRR101I Application update request completed successfully
          for class USER, profile name RRSFU1.
========================================================================
```

Figure 45. A Successful Application Update: Sample Output

Figure 46 on page 85 shows the sample output when RACF attempts to set the revoke count for an non-valid password attempt, but fails because the user ID is already revoked.

```
========================================================================
Application update request issued at 15:49:27 on 03/17/98 was *not*
processed at NODE4.RRSFU1 on 03/17/98 at 15:49:28
Request was propagated by automatic direction from NODE3.RRSFU1

 REQUEST ISSUED:  ICHEINTY ALTER operation from user NODE3.RRSFU1

 ERROR INFORMATION:
 IRRC110I Unable to establish RACF environment for application update request
 IRRC021I ACCESS HAS BEEN REVOKED FOR USER ID RRSFU1.
========================================================================
```

Figure 46. When the User ID Is Revoked: Sample Output

Description of RACF Classes

The following sections describe the general resource classes that are supplied in the class descriptor table (CDT). See *OS/390 SecureWay Security Server RACF Macros and Interfaces* to find details (such as POSIT values) for each class.

Supplied Resource Classes for OS/390 Systems

Table 6 lists the supplied classes that can be used on OS/390 systems.

Table 6. Resource Classes for OS/390 Systems

Class Name	Description
ALCSAUTH	Supports the Airline Control System/MVS (ALCS/MVS) product.
APPCLU	Verifying the identity of partner logical units during VTAM session establishment.
APPCPORT	Controlling which user IDs can access the system from a given LU (APPC port of entry). Also, conditional access to resources for users entering the system from a given LU.
APPCSERV	Controlling whether a program being run by a user can act as a server for a specific APPC transaction program (TP).
APPCSI	Controlling access to APPC side information files.
APPCTP	Controlling the use of APPC transaction programs.
APPL	Controlling access to applications.
CBIND	Controlling the client’s ability to bind to the server.
CONSOLE	Controlling access to MCS consoles. Also, conditional access to other resources for commands originating from an MCS console.
CSFKEYS	Controlling use of Integrated Cryptographics Service Facility (ICSF) cryptographic keys. See also the GCSFKEYS class.
CSFSERV	Controlling use of Integrated Cryptographics Service Facility (ICSF) cryptographic services.
DASDVOL	DASD volumes. See also the GDASDVOL class.
DBNFORM	Reserved for future IBM use.
DEVICES	Used by MVS allocation to control who can allocate devices such as: • Unit record devices (printers and punches) (allocated only by PSF, JES2, or JES3) • Graphics devices (allocated only by VTAM) • Teleprocessing (TP) or communications devices (allocated only by VTAM)
DIGTCERT	Contains digital certificates and information related to them.

Table 6. Resource Classes for OS/390 Systems (continued)

Class Name	Description
DIGTCRIT	Specifies additional criteria for certificate name filters.
DIGTNMAP	Mapping class for certificate name filters.
DIGTRING	Contains a profile for each key ring and provides information about the digital certificates that are part of each key ring.
DIRAUTH	Setting logging options for RACROUTE REQUEST=DIRAUTH requests. Also, if the DIRAUTH class is active, security label authorization checking is done when a user receives a message sent through the TPUT macro or the TSO SEND, or LISTBC commands. Profiles are not allowed in this class.
DLFCLASS	The data lookaside facility.
FACILITY	Miscellaneous uses. Profiles are defined in this class so that resource managers (typically program products or components of MVS or VM) can check a user's access to the profiles when the users take some action. Examples are catalog operations (DFP) and use of the vector facility (an MVS component). RACF does not document all of the resources used in the FACILITY class by other products. For information on the FACILITY class resources used by a specific product (other than RACF itself), see the product's documentation.
FIELD	Fields in RACF profiles (field-level access checking).
GCSFKEYS	Resource group class for CSFKEYS class. [1]
GDASDVOL	Resource group class for DASDVOL class. [1]
GLOBAL	Global access checking table entry. [1]
GMBR	Member class for GLOBAL class (not for use on RACF commands).
GSDSF	Resource group class for SDSF class. [1]
GTERMINL	Resource group class for TERMINAL class. [1]
IBMOPC	Controlling access to OPC/ESA subsystems.
JESINPUT	Conditional access support for commands or jobs entered into the system through a JES input device.
JESJOBS	Controlling the submission and cancellation of jobs by job name.
JESSPOOL	Controlling access to job data sets on the JES spool (that is, SYSIN and SYSOUT data sets).
LOGSTRM	Reserved for MVS/ESA.
NODES	Controlling the following on MVS systems: • Whether jobs are allowed to enter the system from other nodes • Whether jobs that enter the system from other nodes have to pass user identification and password verification checks
NODMBR	Member class for NODES class (not for use on RACF commands).
OPERCMDS	Controlling who can issue operator commands (for example, JES and MVS, and operator commands). [2]
PMBR	Member class for PROGRAM class (not for use on RACF commands).
PROGRAM	Controlled programs (load modules). [1]
PROPCNTL	Controlling if user ID propagation can occur, and if so, for which user IDs (such as the CICS or IMS main task user ID), user ID propagation is *not* to occur.

Table 6. Resource Classes for OS/390 Systems (continued)

Class Name	Description
PSFMPL	Used by PSF to perform security functions for printing, such as separator page labeling, data page labeling, and enforcement of the user printable area.
PTKTDATA	PassTicket key class enables the security administrator to associate a RACF secured signon secret key with a particular mainframe application that uses RACF for user authentication. Examples of such applications are IMS, CICS, TSO, VM, APPC, and MVS batch.
RACGLIST	Class of profiles that hold the results of RACROUTE REQUEST=LIST,GLOBAL=YES or a SETROPTS RACLIST operation.
RACFVARS	RACF variables. In this class, profile names, which start with & (ampersand), act as RACF variables that can be specified in profile names in other RACF general resource classes.
RRSFDATA	Used to control RACF remote sharing facility functions.
RVARSMBR	Member class for RACFVARS (not for use on RACF commands).
SCDMBR	Member class for SECDATA class (not for use on RACF commands).
SDSF	Controls the use of authorized commands in the System Display and Search Facility (SDSF). See also GSDSF class.
SECDATA	Security classification of users and data (security levels and security categories). [1]
SECLABEL	If security labels are used, and, if so, their definitions. [2]
SERVAUTH	Contains profiles that are used by servers running on OS/390 to check a client's authorization to use the server or to use resources managed by the server.
SERVER	Controlling the server's ability to register with the daemon.
SMESSAGE	Controlling to which users a user can send messages (TSO only).
SOMDOBJS	Controlling the client's ability to invoke the method in the class.
STARTED	Used in preference to the started procedures table to assign an identity during the processing of an MVS START command.
SURROGAT	If surrogate submission is allowed, and if allowed, which user IDs can act as surrogates.
SYSMVIEW	Controlling access by the SystemView for MVS Launch Window to SystemView for MVS applications.
TAPEVOL	Tape volumes.
TEMPDSN	Controlling who can access residual temporary data sets. You cannot create profiles in this resource class.
TERMINAL	Terminals (TSO or VM). See also GTERMINL class.
VTAMAPPL	Controlling who can open ACBs from non-APF authorized programs.
WRITER	Controlling the use of JES writers.
Lotus Notes for OS/390 and Novell Directory Services for OS/390 classes	
NDSLINK	Mapping class for Novell Directory Services for OS/390 user identities.
NOTELINK	Mapping class for Lotus Notes for OS/390 user identities.
CICS classes	
ACICSPCT	CICS program control table. [2]
BCICSPCT	Resource group class for ACICSPCT class. [1]

Table 6. Resource Classes for OS/390 Systems (continued)

Class Name	Description
CCICSCMD	Used by CICS/ESA 3.1, or later, to verify that a user is permitted to use CICS system programmer commands such as INQUIRE, SET, PERFORM, and COLLECT. [1]
CPSMOBJ	Used by CICSPlex System Manager, which provides a central point of control when running multiple CICS systems, to determine operational controls within a CICS complex.
CPSMXMP	Used by CICSPlex System Manager to identify exemptions from security controls within a CICS complex.
DCICSDCT	CICS destination control table. [2]
ECICSDCT	Resource group class for DCICSDCT class. [1]
FCICSFCT	CICS file control table. [2]
GCICSTRN	Resource group class for TCICSTRN class. [2]
GCPSMOBJ	Resource grouping class for CPSMOBJ.
HCICSFCT	Resource group class for FCICSFCT class. [1]
JCICSJCT	CICS journal control table. [2]
KCICSJCT	Resource group class for JCICSJCT class. [1]
MCICSPPT	CICS processing program table. [2]
NCICSPPT	Resource group class for MCICSPPT class. [1]
PCICSPSB	CICS program specification blocks or PSBs
QCICSPSB	Resource group class for PCICSPSB class. [1]
SCICSTST	CICS temporary storage table. [2]
TCICSTRN	CICS transactions.
UCICSTST	Resource group class for SCICSTST class. [1]
VCICSCMD	Resource group class for the CCICSCMD class. [1]
	DB2 classes
DSNADM	DB2 administrative authority class
DSNR	Controls access to DB2 subsystems.
GDSNBP	Grouping class for DB2 buffer pool privileges
GDSNCL	Grouping class for DB2 collection privileges
GDSNDB	Grouping class for DB2 database privileges
GDSNPK	Grouping class for DB2 package privileges
GDSNPN	Grouping class for DB2 plan privileges
GDSNSC	Grouping class for DB2 schemas
GDSNSG	Grouping class for DB2 storage group privileges
GDSNSM	Grouping class for DB2 system privileges
GDSNSP	Grouping class for DB2 stored procedures
GDSNTB	Grouping class for DB2 table, index, or view privileges
GDSNTS	Grouping class for DB2 tablespace privileges
GDSNUF	Grouping class for DB2 user-defined functions
GDSNUT	Grouping class for DB2 user-defined distinct types
MDSNBP	Member class for DB2 buffer pool privileges

Table 6. Resource Classes for OS/390 Systems (continued)

Class Name	Description
MDSNCL	Member class for DB2 collection privileges
MDSNDB	Member class for DB2 database privileges
MDSNPK	Member class for DB2 package privileges
MDSNPN	Member class for DB2 plan privileges
MDSNSC	Member class for DB2 schemas
MDSNSG	Member class for DB2 storage group privileges
MDSNSM	Member class for DB2 system privileges
MDSNSP	Member class for DB2 stored procedures
MDSNTB	Member class for DB2 table, index, or view privileges
MDSNTS	Member class for DB2 tablespace privileges
MDSNUF	Member class for DB2 user-defined functions
MDSNUT	Member class for DB2 user-defined distinct types
DFSMS/MVS and MVS/DFP classes	
MGMTCLAS	SMS management classes.
STORCLAS	SMS storage classes.
SUBSYSNM	Authorizes a subsystem (such as a particular instance of CICS) to open a VSAM ACB and use VSAM Record Level Sharing (RLS) functions.
IMS classes	
AIMS	Application group names (AGN).
CIMS	Command.
DIMS	Grouping class for command.
FIMS	Field (in data segment).
GIMS	Grouping class for transaction.
HIMS	Grouping class for field.
OIMS	Other.
PIMS	Database.
QIMS	Grouping class for database.
SIMS	Segment (in database).
TIMS	Transaction (trancode).
UIMS	Grouping class for segment.
WIMS	Grouping class for other.
Information/Management (Tivoli Service Desk for OS/390) classes	
GINFOMAN	Grouping class for Information/Management (Tivoli Service Desk for OS/390) resources.
INFOMAN	Member class for Information/Management (Tivoli Service Desk for OS/390) resources.
Network Authentication and Privacy Service classes	
KERBLINK	Mapping class for user identities of local and foreign principals.
REALM	Used to define the local and foreign realms.
LFS/ESA classes	
LFSCLASS	Controls access to file services provided by LFS/ESA.

Table 6. Resource Classes for OS/390 Systems (continued)

Class Name	Description
	MQM MVS/ESA classes
GMQADMIN	Grouping class for MQM administrative options. [1]
GMQCHAN	Reserved for MQM/ESA.
GMQNLIST	Grouping class for MQM namelists. [1]
GMQPROC	Grouping class for MQM processes. [1]
GMQQUEUE	Grouping class for MQM queues. [1]
MQADMIN	Protects MQM administrative options.
MQCHAN	Reserved for MQM/ESA.
MQCMDS	Protects MQM commands.
MQCONN	Protects MQM connections.
MQNLIST	Protects MQM namelists.
MQPROC	Protects MQM processes.
MQQUEUE	Protects MQM queues.
	NetView classes
NETCMDS	Controlling which NetView commands the NetView operator can issue.
NETSPAN	Controlling which NetView commands the NetView operator can issue against the resources in this span.
NVASAPDT	NetView/Access Services.
PTKTVAL	Used by NetView/Access Services Secured Single Signon to store information needed when generating a PassTicket.
RMTOPS	NetView Remote Operations.
RODMMGR	NetView Resource Object Data Manager (RODM).
	OS/390 DCE classes
DCEUUIDS	Used to define the mapping between a user's RACF user ID and the corresponding DCE principal UUID.
KEYSMSTR	Holds a key to encrypt the DCE password.
	OS/390 UNIX classes
DIRACC	Controls auditing (using SETROPTS LOGOPTIONS) for access checks for read/write access to HFS directories. Profiles are not allowed in this class.
DIRSRCH	Controls auditing (using SETROPTS LOGOPTIONS) of HFS directory searches. Profiles are not allowed in this class.
FSOBJ	Controls auditing (using SETROPTS LOGOPTIONS) for all access checks for HFS objects except directory searches. Controls auditing (using SETROPTS AUDIT) of creation and deletion of HFS objects. Profiles are not allowed in this class.
FSSEC	Controls auditing (using SETROPTS LOGOPTIONS) for changes to the security data (FSP) for HFS objects. Profiles are not allowed in this class.
IPCOBJ	Controlling auditing and logging of IPC security checks.
JAVA	Contains profiles that are used by Java for OS/390 applications to perform authorization checking for Java for OS/390 resources.
PROCACT	Controls auditing (using SETROPTS LOGOPTIONS) of functions that look at data from, or affect the processing of, OS/390 UNIX processes. Profiles are not allowed in this class.

Table 6. Resource Classes for OS/390 Systems (continued)

Class Name	Description
PROCESS	Controls auditing (using SETROPTS LOGOPTIONS) of changes to UIDs and GIDs of OS/390 UNIX processes. Controls auditing (using SETROPTS AUDIT) of dubbing and undubbing of OS/390 UNIX processes. Profiles are not allowed in this class.
UNIXMAP	Contains profiles that are used to map OS/390 UNIX UIDs to RACF user IDs and OS/390 UNIX GIDs to RACF group names.
UNIXPRIV	Contains profiles that are used to grant OS/390 UNIX privileges.
	Tivoli classes
ROLE	Specifies the complete list of resources and associated access levels that are required to perform the particular job function this role represents and defines which RACF groups are associated with this role.
TMEADMIN	Maps the user IDs of Tivoli administrators to RACF user IDs.
	TSO classes
ACCTNUM	TSO account numbers.
PERFGRP	TSO performance groups.
TSOAUTH	TSO user authorities such as OPER and MOUNT.
TSOPROC	TSO logon procedures.

Notes:

1. You cannot specify this class name on the GENCMD, GENERIC, and GLOBAL/NOGLOBAL operands of the SETROPTS command.
2. You cannot specify this class name on the GLOBAL operand of SETROPTS or, if you do, the GLOBAL checking is not performed.

Supplied Resource Classes for VM Systems

Table 7 lists the supplied classes that can be used on VM systems. These classes are primarily relevant if you share your RACF database with a VM system.

Table 7. Resource Classes for VM Systems

Class Name	Description
DIRECTRY	Protection of shared file system (SFS) directories.
FACILITY	Miscellaneous uses. Profiles are defined in this class so resource managers (typically program products or components of MVS or VM) can check a user's access to the profiles when the users take some action. Examples are using combinations of options for tape mounts, and use of the RACROUTE interface. RACF does not document all of the resources used in the FACILITY class by other products. For information on the FACILITY class resources used by a specific product (other than RACF itself), see that product's documentation.
FIELD	Fields in RACF profiles (field-level access checking).
FILE	Protection of shared file system (SFS) files.
GLOBAL	Global access checking. [1]
GMBR	Member class for GLOBAL class (not for use on RACF commands).
GTERMINL	Terminals whose IDs do not fit into generic profile naming conventions. [1]

Table 7. Resource Classes for VM Systems (continued)

Class Name	Description
PSFMPL	When class is active, PSF/VM performs separator and data page labeling as well as auditing.
PTKTDATA	PassTicket key class.
PTKTVAL	Used by NetView/Access Services Secured Single Signon to store information needed when generating a PassTicket.
RACFVARS	RACF variables. In this class, profile names, which start with & (ampersand), act as RACF variables that can be specified in profile names in other RACF general resource classes.
RVARSMBR	Member class for RACFVARS (not for use on RACF commands).
SCDMBR	Member class for SECDATA class (not for use on RACF commands).
SECDATA	Security classification of users and data (security levels and security categories). [1]
SECLABEL	If security labels are used and, if so, their definitions. [2]
SFSCMD	Controls the use of shared file system (SFS) administrator and operator commands.
TAPEVOL	Tape volumes.
TERMINAL	Terminals (TSO or VM). See also GTERMINL class.
VMBATCH	Alternate user IDs.
VMBR	Member class for VMEVENT class (not for use on RACF commands).
VMCMD	Certain CP commands and other requests on VM.
VMEVENT	Auditing and controlling security-related events (called VM events) on VM/SP systems.
VMMAC	Used in conjunction with the SECLABEL class to provide security label authorization for some VM events. Profiles are not allowed in this class.
VMMDISK	VM minidisks.
VMNODE	RSCS nodes.
VMRDR	VM unit record devices (virtual reader, virtual printer, and virtual punch).
VMSEGMT	Restricted segments, which can be named saved segments (NSS) and discontiguous saved segments (DCSS).
VXMBR	Member class for VMXEVENT class (not for use on RACF commands).
VMXEVENT	Auditing and controlling security-related events (called VM events) on VM/ESA systems.
VMPOSIX	Contains profiles used by OpenEdition for VM/ESA (OpenEdition VM).
WRITER	VM print devices.

Notes:

1. You cannot specify this class name on the GENCMD, GENERIC, and GLOBAL/NOGLOBAL operands of the SETROPTS command.
2. You cannot specify this class name on the GLOBAL operand of the SETROPTS command or, if you do, the GLOBAL checking is not performed.

Appendix B. Notices

This information was developed for products and services offered in the USA. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described 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:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental. COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

This product contains code licensed from RSA Data Security Incorporated.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States, other countries, or both:

CICS
CICS/ESA
CICSPlex
DB2
DFSMS
DFSMS/MVS
DFSMSdss
Hiperbatch
IBM
IBMLink
IMS
Library Reader
MVS/DFP
MVS/ESA
OpenEdition
OS/390
Print Services Facility
RACF
S/390
SecureWay
System/390

SystemView
TalkLink
VM/ESA
VTAM
WebSphere

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

Lotus and Lotus Notes are registered trademarks of Lotus Development Corporation in the United States, other countries, or both.

Tivoli is a trademark of Tivoli Systems, Inc. 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.

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

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

RACF Glossary

This glossary defines technical terms and abbreviations used in Security Server documentation. If you do not find the term you are looking for, refer to the index of the appropriate Security Server manual or view the IBM Dictionary of Computing, located at: *www.ibm.com/networking/nsg/nsgmain.htm*

Sequence of Entries

For purposes of clarity and consistency of style, this glossary arranges the entries alphabetically on a letter-by-letter basis, which means:

- Only the letters of the alphabet are used to determine sequence, and
- Special characters and spaces between words are ignored.

Organization of Entries

Each entry consists of:

- A single-word term,
- A multiple-word term,
- An abbreviation for a term, or
- An acronym for a term.

This entry is followed by a commentary, which includes one or more items (definitions or references) and is organized as follows:

1. An item number, if the commentary contains two or more items.
2. A usage label, indicating the area of application of the term, for example, “In programming,” or “In TCP/IP.” Absence of a usage label implies that the term is generally applicable to IBM, or to data processing.
3. A descriptive phrase, stating the basic meaning of the term. The descriptive phrase is assumed to be preceded by “the term is defined as...”. The part of speech being defined is indicated by the opening words of the descriptive phrase: “To ...” indicates a verb, and “Pertaining to ...” indicates a modifier. Any other wording indicates a noun or noun phrase.
4. Annotative sentences, providing additional or explanatory information.
5. References, pointing to other entries or items in the dictionary.

References

The following cross-references are used in this glossary:

- **Contrast with.** This refers to a term that has an opposite or substantively different meaning.
- **Synonym for.** This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.
- **Synonymous with.** This is a reference from a defined term to all other terms that have the same meaning.
- **See.** This refers the reader to meanings for acronyms, multiple-word terms in which this term appears, or terms that have a related, but *not* synonymous, meaning.

Selection of Terms

A term is the word or group of words being defined. In this glossary, the singular form of the noun and the infinitive form of the verb are the terms most often selected to be defined. If the term has an acronym or abbreviation, it is given in parentheses immediately following the term. The abbreviation’s definition serves as a pointer to the term it abbreviates, and the acronym’s definition serves as a pointer to the term it represents.

A

access. The ability to use a protected resource.

access authority. (1) The privileges granted to a particular user or group when accessing a protected resource (such as the ability to read or to update a data set). For resources protected by RACF profiles, the access authorities are NONE, EXECUTE, READ, UPDATE, CONTROL, and ALTER. These authorities are hierarchical, with READ also granting EXECUTE, UPDATE granting READ, and so forth. (2) RACF also has access authorities of READ, WRITE, and EXECUTE (or SEARCH) when dealing with files and directories in the HFS. Note that these authorities are not hierarchical, and HFS files are not protected by RACF profiles, although they do have access authorities.

access list. Synonym for *standard access list*. See *conditional access list*.

accessor environment element (ACEE). A description of the current user’s security environment, including user ID, current connect group, user attributes, and group authorities. An ACEE is constructed during user identification and verification. See *ENVR object*.

ACEE. See *accessor environment element*.

ADAU. See *automatic direction of application updates*.

ADSP. See *automatic data set protection*.

ADSP attribute. Establishes an environment in which all permanent DASD data sets created by the user are automatically defined to RACF and protected with a discrete profile. See *automatic data set protection*.

Advanced Program-to-Program Communication (APPC). A set of interprogram communication services that support cooperative transaction processing in an SNA network. APPC is the implementation, on a given system, of SNA's LU type 6.2. See *LU type 6.2* and *APPC/MVS*.

application user identity. An alternate name by which a RACF user can be known. The name represents the RACF user through another product.

APF-authorized. The authorized program facility (APF) allows an installation to identify system or user programs that can use sensitive system functions. To maintain system security and integrity, a program must be authorized by the (APF) before it can access restricted functions, such as supervisor calls (SVC) or SVC paths.

API. See *application programming interface*.

APPC. See *Advanced Program-to-Program Communication*.

APPC application. See *transaction program (TP)*.

APPC/MVS. The implementation of SNA's LU 6.2 and related communication services in the MVS base control program.

application programming interface (API). (1) A software interface that enables applications to communicate with each other. An API is the set of programming language constructs or statements that can be coded in an application program to obtain the specific functions and services provided by an underlying operating system or service program. (2) In VTAM, the language structure used in control blocks so that application programs can reference them and be identified to VTAM.

appropriate privileges. Describes which users can perform an action (such as execute a command, issue a syscall, and so forth) in a UNIX environment. Usually refers to having superuser authority or an appropriate subset of superuser authority.

attribute. See *user attribute* and *group attribute*.

AUDIT request. The issuing of the RACROUTE macro with REQUEST=AUDIT specified. An AUDIT request is a general-purpose security request that a resource manager can use to audit.

AUDITOR attribute. Allows the user to specify logging options on the RACF commands and list any profile (including its auditing options) using the RACF commands.

AUTH request. The issuing of the RACROUTE macro with REQUEST=AUTH specified. The primary function of an AUTH request is to check a user's authorization to a RACF-protected resource or function. The AUTH request replaces the RACHECK function. See *authorization checking*.

authentication. (1) In computer security, verification of the identity of a user or the user's eligibility to access an object. (2) In computer security, verification that a message has not been altered or corrupted. (3) In computer security, a process used to verify the user of an information system or protected resources. (4) A process that checks the integrity of an entity. (5) See also *password*.

authority. The right to access objects, resources, or functions. See *access authority, class authority,* and *group authority*.

authorization checking. The action of determining whether a user is permitted access to a protected resource. Authorization checking refers to the use of RACROUTE REQUEST=AUTH, RACROUTE REQUEST=FASTAUTH, or any of the RACF callable services unless otherwise stated. Note, however, that other RACF functions can also perform authorization checking as a part of their processing. For example, RACROUTE REQUEST=VERIFY can also check a user's authority to use a terminal or application.

automatic command direction. An RRSF function that enables RACF to automatically direct certain commands to one or more remote nodes after running the commands on the issuing node. Commands can be automatically directed based on who issued the command, the command name, or the profile class related to the command. Profiles in the RRSFDATA class control to which nodes commands are automatically directed. See *automatic direction, automatic direction of application updates, automatic password direction,* and *command direction.*

automatic data set protection (ADSP). A system function, enabled by the SETROPTS ADSP specification and the assignment of the ADSP attribute to a user with ADDUSER or ALTUSER, that causes all permanent data sets created by the user to be automatically defined to RACF with a discrete RACF profile.

automatic direction. See *automatic command direction*, *automatic password direction*, and *automatic direction of application updates*.

automatic direction of application updates. An RRSF function that automatically directs ICHEINTY and RACROUTE macros that update the RACF database to one or more remote systems. Profiles in the RRSFDATA class control which macros are automatically directed, and to which nodes. See *automatic direction, automatic command direction*, and *automatic password direction*.

automatic password direction. An extension of password synchronization and automatic command direction that causes RACF to automatically change the password for a user ID on one or more remote nodes after the password for that user ID is changed on the local node. Profiles in the RRSFDATA class control for which users and nodes passwords are automatically directed. See *password synchronization, automatic command direction, automatic direction*, and *automatic direction of application updates*.

automatic profile. A tape volume profile that RACF creates when a RACF-defined user protects a tape data set. When the last data set on the volume is deleted, RACF automatically deletes the tape volume profile. See *nonautomatic profile*.

B

backup data set. A data set in the backup RACF database. For each data set in the primary RACF database, an installation should define a corresponding backup data set. See *primary RACF database*.

backup RACF database. A RACF database that reflects the contents of the primary RACF database. You can switch to the backup database without a re-IPL if the primary RACF database fails. You can have an ″active backup,″ which reflects the contents of the primary RACF database. You can also have an ″inactive backup,″ which doesn't reflect the contents of the primary RACF database. You can switch to the ″inactive backup″ in case of error, but it will contain downlevel information. See *primary RACF database*.

base segment. The portion of a RACF profile that contains the fundamental information about a user, group, or resource. The base segment contains information that is common to all applications that use the profile. Also called *RACF segment*.

basic sequential access method (BSAM). In the NetView Performance Monitor (NPM), the method by which all PIUs collected for selected LUs can be logged into a sequential data set as they pass through VTAM.

BER. This term represents the Basic Encoding Rules specified in ISO 8825 for encoding data units described in abstract syntax notation 1 (ASN.1). The rules specify the encoding technique, not the abstract. See also
| *DER*.

block update command (BLKUPD). A RACF diagnostic command used to examine or modify the content of individual physical records in a RACF data set.

BSAM. See *basic sequential access method (BSAM)*.

byte file system. On VM, a file system for POSIX files that is organized in a tree-like structure of directories. Each directory can contain files or other directories.

C

cache structure. A coupling facility structure that contains data accessed by systems in a sysplex. For more information, see *OS/390 SecureWay Security Server RACF System Programmer's Guide*.

callable service. In OS/390 UNIX System Services, a request by an active process for a service. See *syscall*.

category. See *security category*.

CDMF. See *Commercial Data Masking Facility*.

CDT. See *class descriptor table*.

certificate. See *digital certificate.*

certificate authority. An organization that issues certificates for end users or entities. In doing so the certificate authority will vouch for or validate the correctness of the information contained within the certificate according to its published Certificate Practice Statement (CPS). The certificate authority might or might not be a real ″third party″ from the end user's or entity's point of view. The certificate authority might belong to the same organization as the end entities it supports. The term ″certificate authority″ refers to the entity named in the issuer field of a certificate. The term ″root certificate authority″ indicates a certificate authority that is directly trusted by an end entity; that is, securely acquiring the value of a root certificate authority public key requires some out-of-band step or steps. This term is not meant to imply that a root certificate authority is necessarily at the top of any hierarchy, but that the certificate authority in question is trusted directly. A subordinate certificate authority is one that is not a root certificate authority for the end entity in question. Often, a subordinate certificate authority will not be a root certificate authority for any entity but this is not mandatory.

| **certificate-authority certificate.** See *digital certificate*.

| **certificate package.** Contains the end certificate with
| its private key, plus any signing certificates needed to
| complete the basing chain (hierarchy) from end
| certificate to self-signed root certificate.

child. See *child process.*

child process. A process that is created by a parent process to execute a request. Contrast with *parent process*. See *fork* and *process.*

CICS. See *Customer Information Control System*.

| **certificate name filter.** Used to map a certificate to multiple user IDs in order to simplify administration of digital certificates, conserve storage space in the RACF database, maintain accountability, or maintain access control granularity.

class. A collection of RACF-defined entities (users, groups, and resources) with similar characteristics. Classes are defined in the class descriptor table (CDT), except for the USER, GROUP, and DATASET classes.

class authority (CLAUTH). An attribute enabling a user to define RACF profiles in a class defined in the class descriptor table. A user can have class authorities to zero or more classes.

class descriptor table (CDT). A table consisting of an entry for each class except the USER, GROUP, and DATASET classes. The CDT contains the classes supplied by IBM and the installation-defined classes.

classification model 1. See *single-subsystem scope*.

classification model 2. See *multiple-subsystem scope*.

CLAUTH attribute. See *class authority*.

command direction. An RRSF function that allows a user to issue a command from one user ID and direct that command to run in the RACF address space on the same system or on a different RRSF node, using the same or a different user ID. Before a command can be directed from one user ID to another, a user ID association must be defined between them using the RACLINK command.

command interpreter. A program that reads the commands that you type in and then executes them. When you are typing commands into the computer, you are actually typing input to the command interpreter. The interpreter then decides how to perform the commands that you have typed. The UNIX shell is an example of a command interpreter. Synonymous with *command language interpreter*. See *shell*.

command language interpreter. Synonym for *command interpreter*.

command prefix facility (CPF). An MVS facility that provides a registry for command prefixes. CPF ensures that two or more subsystems do not have the same or overlapping command prefixes for MVS operator commands.

Commercial Data Masking Facility (CDMF). An encryption function that uses a weaker key (40 bit) of the Data Encryption Standard (DES) algorithm. RACF uses CDMF to mask the data portion of RRSF transaction processing message packets. CDMF is part of the IBM Common Cryptographic Architecture.

common programming interface (CPI). An evolving application programming interface (API), supplying functions to meet the growing demands from different application environments and to achieve openness as an industry standard for communications programming. CPI-C provides access to interprogram services such as sending and receiving data, synchronizing processing between programs, and notifying a partner of errors in the communication.

conditional access list. Includes user IDs, group names, and levels of access. It also allows access if the specified condition is true. For example, with program access to data sets, the condition is that the user must be executing the program specified in the access list. See *access list*. Contrast with *standard access list*.

coordinator system. In a RACF data sharing group, the system on which the system operator or administrator enters a RACF command that is propagated throughout the group. See *peer system*.

coupling facility. The hardware element that provides high-speed caching, list processing, and locking functions in a sysplex.

CPF. See *command prefix facility*.

CPI-C. See *common programming interface*.

current connect group. (1) The group specified by a user when logging on to the system, or the user’s default group if the user did not specify a group when logging on. With SETROPTS NOGRPLIST in effect, RACF uses the user’s authority and this group’s authority during access checking. With SETR GRPLIST in effect, RACF includes the authority of the user’s other groups, if any, but the user still has only one ″current connect group″. (2) You can use the &RACGPID variable in members of GLOBAL profiles to refer to the user’s current connect group. For more information, see *OS/390 SecureWay Security Server RACF Security Administrator’s Guide*. (3) Synonymous with *current working directory* and *working directory*.

current directory. The directory with which a user is associated for access-checking purposes during a terminal session or batch job.

current security label. The security label that RACF uses in RACF authorization checking if the SECLABEL class is active. For interactive users, this is the security label specified when the user logged on, or (if no security label was specified) the default security label in the user’s user profile. For batch jobs, this is the security label specified in the SECLABEL operand of the JOB statement, or (if no security label was specified) the user's current security label in the user profile associated with the job.

current working directory. Synonym for *current directory*.

Customer Information Control System (CICS). A program licensed by IBM that provides online transaction processing services and management for critical business applications. CICS runs on many platforms (from the desktop to the mainframe) and is used in various types of networks that range in size from a few terminals to many thousands of terminals. The CICS application programming interface (API) enables programmers to port applications among the hardware and software platforms on which CICS is available. Each product in the CICS family can interface with the other products in the CICS family, thus enabling interproduct communication.

D

DASDVOL authority. As an alternative to assigning the OPERATIONS or group-OPERATIONS attribute, DASDVOL authority allows you to authorize operations personnel to access only those volumes that they must maintain. Using DASDVOL authority is also more efficient for functions such as volume dumping, because only one authorization check for the volume needs to be issued, instead of individual requests for each data set on the volume. Note that modern data management software (such as DFSMSdss) does not require DASDVOL authority. See *OPERATIONS attribute*, and *group-OPERATIONS attribute*.

Data Facility Product (DFP). A facility that controls access to expanded storage.

Data Lookaside Facility (DLF). A facility that processes DLF objects. A DLF object contains data from a single data set managed by Hiperbatch. The user (an application program) is connected to the DLF object, and the connected user can then access the data in the object through normal QSAM or VSAM macro instructions.

data security. The protection of data from intentional or unintentional unauthorized disclosure, modification, or destruction.

data security monitor (DSMON). A RACF auditing tool that produces reports enabling an installation to verify its basic system integrity and data-security controls.

data set profile. A profile that provides RACF protection for one or more data sets. The information in the profile can include the data set profile name, profile owner, universal access authority, access list, and other data. See *discrete profile* and *generic profile*.

data sharing group, RACF. A collection of one or more instances of RACF in a sysplex that have been identified to XCF and assigned to the group defined for RACF sysplex data sharing. RACF joins group IRRXCF00 when enabled for sysplex communication. See *data sharing member*.

data sharing mode. An operational RACF mode that is available when RACF is enabled for sysplex communication. Data sharing mode requires installation of coupling facility hardware.

DB2 administrative authority. A set of privileges, often covering a related set of objects, and often including privileges that are not explicit, have no name, and cannot be specifically granted. For example, the ability to terminate any utility job is included in the SYSOPR authority.

DB2 explicit privilege. A privilege that has a name, and is held as the result of an SQL GRANT statement.

DCE. See *Distributed Computing Environment*.

default group. The group specified in a user profile that provides a default current connect group for the user. See *current connect group*.

DEFINE request. The issuing of the RACROUTE macro with REQUEST=DEFINE specified or using a RACF command to add or delete a resource profile causes a DEFINE request. The DEFINE request replaces the RACDEF function.

delegation. The act of giving users or groups the necessary authority to perform RACF operations.

DER. This term represents the Distinguished Encoding Rules, which are a subset of the Basic Encoding Rules. See also *BER.*

DFP. See *Data Facility Product*.

digital certificate. A data structure that represents the binding of a user's distinguished name and a public key. Certificates are typically signed to enable a recipient of the certificate to ensure that the binding of the user's distinguished name (DN) and public key have not been tampered with.

RACF allows you to manage three types of digital certificates:

- Certificate-authority certificate, which is a certificate that is associated with a certificate authority and is used to verify signatures in other certificates.
- Site certificate, which is a certificate that is associated with a server, or network entity other than a user or certificate authority.
- User certificate, which is a certificate that is associated with a RACF user ID and is used to authenticate the user's identity

| **DIRAUTH request.** The issuing of the RACROUTE macro with REQUEST=DIRAUTH specified. A DIRAUTH request works on behalf of the message-transmission managers to ensure that the receiver of a message meets security-label authorization requirements.

directed command. A RACF command that is issued from a user ID on an RRSF node. It runs in the RACF subsystem address space on the same or a different RRSF node under the authority of the same or a different user ID. A directed command is one that specifies AT or ONLYAT. See *command direction* and *automatic command direction*.

directory. (1) A construct for organizing computer files. As files are analogous to folders that hold information, a directory is analogous to a drawer that can hold a number of folders. Directories can also contain subdirectories, which can contain subdirectories of their own. (2) In an HFS, an index to files and other directories is organized hierarchically below the directory. (3) An index used by a control program to locate blocks of data that are stored in separate areas of a data set in direct access storage.

directory entry. In OS/390 UNIX System Services, an object that associates a file name with a file or directory. Several directory entries can associate names with the same file or directory. See *link*.

discrete profile. A resource profile that provides RACF protection for a single resource. Contrast with *generic profile*.

discretionary access control. An access control environment in which the resource owner determines who can access the resource. Contrast this with ″mandatory access control.″

disjoint. Two security labels are disjoint when the set of security categories that defines the first does not include the set of security categories that defines the second, and the set of security categories that defines the second does not include the set of security categories that defines the first. This also means that the first does not dominate the second and the second does not dominate the first. See *dominate*.

Distributed Computing Environment (DCE). The Open Group specification (or a product derived from this specification) that assists in networking. DCE provides such functions as authentication, directory service (DS), and remote procedure call (RPC).

DLF object. When DLF is active, the first attempt to access a QSAM or VSAM data set defined to DLF creates a DLF object. A DLF object contains data from a single data set managed by Hiperbatch. The user (an application program) is connected to the DLF object, and the connected user can then access the data in the object through normal QSAM or VSAM macro instructions.

dominate. One security label dominates a second security label when the security level that defines the first is equal to or greater than the security level that defines the second, and the set of security categories that defines the first includes the set of security categories that defines the second.

DSMON. See *data security monitor*.

dub. To make an MVS address space known to OS/390 UNIX System Services. Once dubbed, an address space is considered to be an OS/390 UNIX process. Address spaces created by **fork()** are automatically dubbed when they are created; other address spaces become dubbed if they invoke an OS/390 UNIX service. Dubbing also applies to MVS tasks. A dubbed task is considered an OS/390 UNIX “thread.” Tasks created by **pthread_create()** are automatically dubbed threads; other tasks are dubbed if they invoke an OS/390 UNIX service. See *undub*.

E

effective group identifier (effective GID). (1) When the user connects to the system (for example, logs on to a TSO/E session), one group is selected as the user’s current group. When a user becomes an OS/390 UNIX user, the GID of the user’s current group becomes the effective GID of the user’s process. The user can access resources available to members of the user’s effective GID. (2) Contrast with *OS/390 UNIX group identifier (GID)* and *real GID*.

effective user identifier (effective UID). (1) When a user becomes an OS/390 UNIX user, the UID from the user’s RACF user profile becomes the effective UID of the user’s process. The system uses the effective UID to determine if the user is a file owner. (2) Contrast with *OS/390 UNIX user identifier (UID)* and *real UID*.

ENVR object. A transportable form of the ACEE that can be used within a single system to create the original ACEE without accessing the RACF database. It can be used, with limits, elsewhere in a single sysplex to recreate the original ACEE without accessing the RACF database.

entity. A user, group, or resource (for example, a DASD data set) that is defined to RACF.

erase-on-scratch. The physical overwriting of data on a DASD data set when the data set is deleted (scratched).

EXTRACT request. The issuing of the RACROUTE macro with REQUEST=EXTRACT specified. An EXTRACT request retrieves or replaces certain specified fields from a RACF profile or encodes certain clear-text (readable) data. The EXTRACT request replaces the RACXTRT function.

F

failsoft processing. (1) Processing that occurs when no data sets in the primary RACF database are available (RACF is installed but inactive). RACF cannot make decisions to grant or deny access. The operator is prompted frequently to grant or deny access to data sets. The resource manager decides on the action for general resource classes with a return code of 4. (2) Failsoft processing can also occur as the result of RVARY INACTIVE (temporary failsoft) or as the result of a serious system error requiring a re-IPL (permanent failsoft).

FASTAUTH request. The issuing of the RACROUTE macro with REQUEST=FASTAUTH specified. The primary function of a FASTAUTH request is to check a user's authorization to a RACF-protected resource or function. A FASTAUTH request uses only in-storage profiles (brought into storage using RACF functions such as RACROUTE REQUEST=LIST) for faster performance than an AUTH request. The FASTAUTH request replaces the FRACHECK function. See *authorization checking*.

field-level access checking. The RACF facility by which a security administrator can control access to nonbase segments in a RACF profile and fields in those segments.

file permission bits. In OS/390 UNIX System Services, information about a file that is used, along with other information, to determine if a process has read, write, or execute/search permission to a file or directory. The bits are divided into three parts, which are owner, group, and other.

file security packet (FSP). In OS/390 UNIX System Services, a control block containing the security data (file's owner OS/390 UNIX user identifier (UID), owner OS/390 UNIX group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the OS/390 UNIX file system.

FMID. See *function modification identifier*.

fork. In OS/390 UNIX System Services, to create and start a child process. Forking is similar to creating an address space and attaching. Forking creates a copy of the parent process, including open file descriptors. Contrast with *spawn*.

FSP. See *file security packet*.

file transfer program (FTP). In the Internet suite of TCP/IP-related protocols, an application-layer protocol that transfers bulk-data files between machines or hosts.

FRACHECK request. RACROUTE REQUEST=FASTAUTH replaces the FRACHECK function. See *FASTAUTH request*.

FTP. See *File Transfer Protocol*.

fully-qualified generic profile. A generic DATASET profile that has a name with no generic characters. A fully qualified generic profile protects only resources whose names exactly match the name of the profile. Contrast with *discrete profile*.

function modification identifier (FMID). A 7-character identifier that is used in elements associated with OS/390 to identify the release of the element.

G

GDG. See *generation data group*.

general resource. Any resource, other than an MVS data set, that is defined in the class descriptor table (CDT). General resources include DASD volumes, tape volumes, load modules, terminals, IMS and CICS transactions, and installation-defined resource classes.

general resource profile. A profile that provides RACF protection for one or more general resources. The information in the profile can include the general resource profile name, profile owner, universal access authority, access list, and other data.

general user. A user who has limited RACF privileges, such as logging on, accessing resources, and creating data sets. General users typically use and create RACF-protected resources, but have no authority to administer resources other than their own.

generation data group (GDG). A collection of data sets with the same base name, such as PAYROLL, that are kept in chronological order. Each data set is called a generation data set, and has a name such as PAYROLL.G0001V00, PAYROLL.G0002V00, and so forth

generic profile. A resource profile that can provide RACF protection for zero or more profiles. The resources protected by a generic profile have similar names and identical security requirements, though with RACFVARS, a generic profile can protect resources with dissimilar names, too. For example, a generic data set profile can protect one or more data sets.

GID. See *OS/390 UNIX group identifier (GID)*.

global access checking. The ability to allow an installation to establish an in-storage table of default values for authorization levels for selected resources. RACF refers to this table before performing normal RACROUTE REQUEST=AUTH processing and grants the request without performing an AUTH request if the requested access authority does not exceed the global value. RACF uses this table to process AUTH requests faster and with less overhead (no checking of access lists, no auditing) when you have resources for which you decide to grant access to all users. If the requested access does not exceed the access granted by the table, RACF bypasses most of its normal AUTH processing. Global access checking can grant the user access to the resource, but it cannot deny access.

global resource serialization. An OS/390 mechanism using ENQ with the SYSTEMS option (or, in some older programs, the RESERVE option) to serialize resources across multiple OS/390 images. It is used by RACF to serialize access to its database and to in-storage tables and buffers.

globally RACLISTed profiles. In-storage profiles for RACF-defined resources that are created by RACROUTE REQUEST=LIST and that are anchored from an ACEE. Globally RACLISTed in-storage profiles are shared across a system, such as the way that in-storage profiles created by SETROPTS RACLIST are shared. See *SETR RACLISTed profiles*, *RACLISTed profiles*, and *locally RACLISTed profiles*.

group. A collection of RACF-defined users who can share access authorities for protected resources.

group-ADSP attribute. Similar to the ADSP attribute for a user, but assigned by using the CONNECT command to restrict its effect to those cases where the user creates data sets with that group as the high level qualifier of the data set name (or as determined by the naming convention table or exit).

group-AUDITOR attribute. Similar to the AUDITOR attribute for a user, but assigned by using the CONNECT command to restrict the user's authority to resources that are within the scope of the group.

group authority. An authority specifying which functions a user can perform in a group. The group authorities are USE, CREATE, CONNECT, and JOIN.

group data set. A RACF-protected data set in which either the high-level qualifier of the data set name or the qualifier supplied by an installation-naming convention table or exit routine is a RACF group name.

group-GRPACC attribute. Similar to the GRPACC attribute for a user, but assigned by using the CONNECT command to restrict its effect to the specific group.

group ID. See *group name*.

group name. A string of 1–8 characters that identifies a group to RACF. The first character must be A through Z, # (X'7B'), $ (X'5B'), or @ (X'7C'). The rest can be A through Z, #, $, @, or 0 through 9.

group-OPERATIONS attribute. (1) Similar to the OPERATIONS attribute for a user, but assigned by using the CONNECT command to restrict its effect to those resources that are within the scope of the group. (2) If a person needs to perform maintenance activities on DASD volumes, it is more efficient (for RACF processing) and better (for limiting the resources the person can access) to give the person authority to those volumes using the PERMIT command than to assign the person the OPERATIONS or group-OPERATIONS attribute. See *DASDVOL authority* and *OPERATIONS attribute*.

group profile. A profile that defines a group. The information in the profile includes the group name, profile owner, and users in the group.

grouping profile. A profile in a resource group class.

group-REVOKE attribute. Assigned through the CONNECT command, it prevents the user from using that group as the current connect group. Also prevents RACF from considering that group during authorization checking.

group-SPECIAL attribute. Similar to the SPECIAL user attribute, but it is assigned by the CONNECT command to restrict the user's authority to users, groups, and resources within the scope of the group. Within this scope, it gives the user full control over everything except auditing options. However, it does not give the user authority to change global RACF options that will affect processing outside the group's scope. See *SPECIAL attribute*.

group-related user attribute. A user attribute, assigned at the group level, that enables the user to control the resource, group, and user profiles associated with the group and its subgroups. Group-related user attributes include group-SPECIAL attribute, group-AUDITOR attribute, and group-OPERATIONS attribute.

GRPACC attribute. With this attribute, any group data sets that the user defines to RACF (through the ADSP attribute, the PROTECT operand on the DD statement, or the ADDSD command) are automatically made accessible to other users in the group at the UPDATE level of access authority if the user defining the profile is a member of the group.

H

handle. See *label*.

hard limit. Maximum resource value for a process.

HFS. See *hierarchical file system*.

hierarchical file system (HFS). The file system for OS/390 UNIX System Services that organizes data in a tree-like structure of directories.

I

ICB. See *inventory control block*.

interprocess communication facilities (IPC). IPC facilities are services that allow different processes to communicate. Message passing (using message queues), semaphore sets, and shared memory services are forms of interprocess communication facilities.

inventory control block (ICB). The first block in a RACF database. The ICB contains a general description of the database and, for the master primary data set, holds the RACF global options specified by SETROPTS.

ICHRIN03. See *started procedures table*.

IPC. See *interprocess communication facilities*.

issuer's distinguished name (IDN). The X.509 name that is associated with a certificate authority.

K

kernel. The part of OS/390 UNIX System Services that provides support for such services as UNIX I/O, process management, and general UNIX functionality.

kernel address space. The address space in which the OS/390 UNIX System Services kernel runs. See *kernel*.

key ring. A named collection of personal, site, and certificate-authority certificates for a specific user. Users might have more than one key ring. Each key ring represents a different trust policy in effect for the user. Note that in the S/390 implementation, this trust policy is a subset of the installation's trust policy.

L

label. A usable ″handle″ for a certificate. See *handle*.

LDAP. See *Lightweight Directory Access Protocol*.

Lightweight Directory Access Protocol (LDAP). A protocol to access directory services on a network.

link pack area (LPA). (1) In OS/390 UNIX System Services, an area of virtual storage containing reenterable routines from system libraries that are loaded at IPL time and can be used concurrently by all tasks in the system. (2) The LPA presence in main storage saves loading time.

LIST request. The issuing of the RACROUTE macro with REQUEST=LIST specified. A LIST request builds in-storage profiles for a RACF general resource class. The LIST request replaces the RACLIST function.

list-of-groups checking. A RACF option (SETROPTS GRPLIST) that enables a user to access all resources available to all groups of which the user is a nonrevoked member, regardless of the user's current connect group. For any particular resource, RACF allows access based on the highest access among the groups in which the user is a member.

local logical unit (local LU). (1) Local LUs are LUs defined to the local system; partner LUs are defined to remote systems. It is a matter of point of view. From the point of view of a remote system, LUs defined to that system are local LUs, and those on the local system are the partner LUs. (2) A partner LU might or might not be on the same system as the local LU. When both LUs are on the same system, the LU through which communication is initiated is the local LU, and the LU through which communication is received is the partner LU. (3) See *partner logical unit (partner LU)*.

local mode. An RRSF node is operating in local mode when it has no RRSF logical node connection with any other RRSF node.

local node. Whether a node is perceived as local or remote depends on the point of view. As an example, consider two RRSF nodes, MVSA and MVSB, that are logically connected. From MVSA's point of view, MVSA is the local node and MVSB is the remote node. From MVSB's point of view, however, MVSB is the local node and MVSA is the remote node. See *remote node and target node*.

local transaction program (local TP). (1) Whether a transaction program is a local TP or a partner TP usually depends on the point of view. From an OS/390 system's point of view, the TPs that reside on it are local TPs and the TPs on remote systems are partner TPs. From the remote system's point of view, the TPs that reside on it are local TPs and the TPs on the OS/390 system are partner TPs. (2) A local TP can initiate communication with one or more partner TPs. The partner TP might or might not reside on the local system. The local TP does not need to know whether the partner TP is on the same system or on a remote system.

logging. The recording of audit data about specific events.

logical connection. See *RRSF logical node connection*.

logical unit (LU). A port which provides formatting, state synchronization, and other high-level services. Depending on the LU being used, (LU 1 or LU 2), a user can communicate with a host system, a program can communicate with a host system, a program can communicate with a LU 6.2, or a program can communicate with another program over an SNA network.

logical unit type 6.2 (LU type 6.2). The SNA logical unit type that supports general communication between programs in a cooperative processing environment. Also, the SNA logical unit type on which CPI-C and APPC/MVS TP conversation services are built.

locally RACLISTed profiles. In-storage profiles for RACF-defined resources that are created by RACROUTE REQUEST=LIST and that are anchored from an ACEE. Locally RACLISTed in-storage profiles are not shared across a system, the way that in-storage profiles created by SETROPTS RACLIST are shared. See *SETR RACLISTed profiles*, *RACLISTed profiles*, and *globally RACLISTed profiles*.

LPA. See *link pack area*.

LU. See *logical unit*.

LU=local. In APPC/MVS, a situation in which a pair of communicating transaction programs are on the same MVS system and under the control of APPC/MVS.

LU type 6.2. See *logical unit type 6.2*.

M

MAC. See *mandatory access control*.

main system. The system on a multisystem RRSF node that is designated to receive most of the RRSF communications sent to the node.

managed user ID association. A user ID association in which one of the associated user IDs is a managing user ID, and the other is a managed user ID. The managing user ID can run allowed RACF commands under the authority of the managed user ID. The managed user ID cannot run commands under the authority of the managing user ID. A managed user ID association does not allow password synchronization between the associated user IDs.

mandatory access control (MAC). A means of restricting access to objects on the basis of the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (clearance) of subjects to access information of such sensitivity.

mask. Provides protection, if an encryption function is not available, against casual viewing of a password that has been defined or altered.

master primary data set. The first data set activated in the primary RACF database.

MCS. See *multiple console support*.

MCS console. A non-SNA device defined to MVS that is locally attached to an MVS system and is used to enter commands and receive messages.

member. A user belonging to a group.

member profile. A profile that defines a member and security level for that member.

member system. Any one of the MVS system images in a multisystem RRSF node.

modeling. See *profile modeling*.

mount. To logically associate a mountable file system to another file system. The TSO command to perform this action is MOUNT.

multiple console support (MCS). The operator interface in an MVS system.

multiple-subsystem scope. A RACF classification model used in conjunction with the RACF/DB2 external security module to construct DB2 resource names. Default for the highest-level qualifier is the DB2 subsystem or group name.

multisystem node. See *multisystem RRSF node*.

multisystem RRSF node. An RRSF node consisting of multiple MVS system images that share the same RACF database. One of the systems is designated to be the main system, and it receives the unsolicited RRSF communications sent to the node.

multiple virtual storage (MVS). A mainframe operating system that allows multiple users to work simultaneously using the full amount of virtual storage.

multi-subsystem scope. A classification model used in conjunction with the RACF/DB2 external security module to construct DB2 classes with the subsystem ID as part of the class name. Contrast with *single-subsystem scope*.

MVS. See *multiple virtual storage*.

N

U.S. Department of Defense National Computer Security Center (NCSC). Determines defense and security criteria.

NCSC. See *U.S. Department of Defense National Computer Security Center*.

network-qualified name. An identifier for a partner LU in the form *netid.luname*, where *netid* is a 1–8 character network identifier and *luname* is a 1–8 character LU name.

network file system. A protocol that allows any host in a network to mount another host's file directories. Once mounted, the file directory appears to reside on the local host. See *NFS*, *mount*, and *unmount*.

NFS. See *network file system*.

node. See *RRSF node*.

non-data sharing mode. One of two normal modes of operation when RACF is enabled for sysplex communication and is the mode in which RACF communicates information using sysplex facilities to other instances of RACF, but does not make use of the coupling facility in doing so.

nonautomatic profile. A tape volume profile that RACF creates when an RDEFINE command is issued or when tape data set protection is not active. A tape volume profile created in this manner is called a nonautomatic profile, because RACF never deletes the profile except in response to the RDELETE command. See *automatic profile*.

O

operator identification card (OIDCARD). A small card with a magnetic stripe encoded with unique characters and used to verify the identity of a terminal operator to RACF on an OS/390 system.

OPERATIONS attribute. (1) Grants, effectively, ALTER access to all data sets unless the user or one of the user's groups appears explicitly in the access list of a data set's profile. (2) If a person needs to perform maintenance activities on DASD volumes, it is more efficient (for RACF processing) and better (for limiting the resources the person can access) to give the person authority to those volumes using the PERMIT command than to assign the person the OPERATIONS or group-OPERATIONS attribute. See *DASDVOL authority* and *group-OPERATIONS attribute*. (3) Note that most modern data maintenance programs do not require the OPERATIONS attribute.

OS/390. A program licensed by IBM that not only includes and integrates functions previously provided by many IBM software products, including the MVS operating system, but also:

1. Is an open, secure operating system for the IBM S/390 family of enterprise servers
2. Complies with industry standards
3. Is Year 2000 ready and enabled for network computing and e-business
4. Supports technology advances in networking server capability, parallel processing, and object-oriented programming

OS/390 UNIX group identifier (GID). A number between 0 and 2 147 483 647 that identifies a group of OS/390 UNIX users to OS/390 UNIX. The GID is associated with a RACF group name when it is specified in the OMVS segment of the group profile. See *real GID*. Contrast with *effective group identifier (effective GID).*

OS/390 UNIX System Services (OS/390 UNIX). The portion of the OS/390 operating system that implements the UNIX-95 standards and programming interfaces.

OS/390 UNIX user identifier (UID). A number between 0 and 2 147 483 647 that identifies a user to OS/390 UNIX. The UID is associated with a RACF user ID when it is specified in the OMVS segment of the user profile. It can be contained in an object of type uid_t, that is used to identify a system user. When the identity of the user is associated with a process, a UID value is referred to as a real UID, an effective UID, or an (optional) saved set UID. See *real UID*. Contrast with *effective user identifier (effective UID)*.

owner. The user or group that creates a profile, or is specified as the owner of a profile. The owner can modify, list, or delete the profile.

P

PADS. See *program access to data sets (PADS)*.

parent. See *parent directory* and *parent process*.

parent directory. (1) The directory one level above the current directory. (2) When discussing a given directory, the directory that both contains a directory entry for the given directory and is represented by the path name ″..″ in the given directory. (3) When discussing other types of files, a directory containing a directory entry for the file under discussion.

parent process. A process (MVS, UNIX, and so forth) created to carry out a program. The parent process creates child processes to execute requests. See *child process*, *parent process ID* and *process*.

parent process ID (parent PID). An attribute of a new process after it is created by a currently active process. The parent process ID of a process is the process ID of its creator for the lifetime of the creator. See *process ID*.

partner logical unit (partner LU). A partner logical unit is one that resides on a remote system. See *local logical unit* and *logical unit*.

partner transaction program (partner TP). A partner TP is one that resides on a remote system. See *local transaction program (local TP)*.

PassTicket. An alternative to the RACF password that permits workstations and client machines to communicate with the host. It allows a user to gain access to the host system without sending the RACF password across the network.

password. In computer security, a string of characters known to a user who must specify it to gain full or limited access to a system and to the data stored within it. RACF uses a password to verify the identity of the user.

password synchronization. An option that can be specified when a peer user ID association is defined between two user IDs. If password synchronization is specified for a user ID association, then whenever the password for one of the associated user IDs is changed, the password for the other user ID is automatically changed to the newly defined password. See *automatic password direction*.

pathname. (1) A string that is used to identify a file. (2) In OS/390 UNIX System Services, a file name specifying all directories leading to the file.

peer system. In a RACF data sharing group, any system to which RACF propagates a command entered by the system operator or administrator. See *coordinator system*.

peer user ID association. A user ID association that allows either user ID to run allowed RACF commands under the authority of the other user ID using command direction. A peer user ID association can also establish password synchronization between the associated user IDs. Contrast with *managed user ID association*.

permission bits. In OS/390 UNIX System Services, part of security controls for directories and files stored in the hierarchical file system (HFS). Used to grant read, write, search (just directories), or execute (just files) access to owner, file or directory owning group, or all others.

persistent verification (PV). PV is an APPC term that represents a level of conversation security between two logical units (LUs). PV provides a way of reducing the number of password transmissions by eliminating the need to provide a user ID and password on each attach (allocate) during multiple conversations between a user and a partner LU. The user is verified during the signon process and remains verified until the user has been signed off the partner LU.

PID. See *process ID*.

POSIX. Portable Operating System Interface For Computer Environments. An IEEE standard for computer operating systems that is an evolving family of standards describing a wide spectrum of operating system components ranging from C language and shell interfaces to system administration.

POSIT. A number specified for each class in the class descriptor table that identifies a set of flags that control RACF processing options. See the description of the POSIT keyword in the *OS/390 SecureWay Security Server RACF Macros and Interfaces*.

primary data set. A data set in the primary RACF database. See *master primary data set*.

primary RACF database. The RACF database, designated in the data set name table (ICHRDSNT) or specified at IPL time, that contains the RACF profiles used for authorization checking. The primary RACF database may contain as many as 90 data sets. A backup RACF database may also be designated in the data set name table or specified at IPL time. See *backup RACF database*.

private key. For encrypting and decrypting data, one party uses a common, non-secret public key and the other party uses the individual, secret private key. These keys are complementary in that if one is used to encrypt data, the other is used to decrypt data. See *public key*.

problem state. A state during which a processing unit cannot execute input/output and other privileged instructions. Contrast with supervisor state.

process. (1) A function, created by a **fork()** request, with three logical sections:
- Text, which is the function's instructions.
- Data, which the instructions use but do not change.
- Stack, which is a push-down, pop-up save area of the dynamic data that the function operates upon.

(2) The three types of processes are:
- User processes, which are associated with a user at a workstation.
- Daemon processes, which do systemwide functions in user mode, such as printer spooling.
- Kernel processes, which do systemwide functions in kernel mode, such as paging.

A process can run in an OS/390 UNIX System Services user address space, an OS/390 UNIX forked address space, or an OS/390 UNIX kernel address space. In an MVS system, a process is handled like a task. See *task*. (3) The current state of a program that is running—including a memory image, the program data, the variables used, the general register values, the status of opened files used, and the current directory. Programs running in a process must be either operating system programs or user programs.

process ID (PID). A unique number assigned to a process that is running. See *parent process ID (parent PID)*.

profile. Data that describes the significant characteristics of a user, a group of users, or one or more computer resources. A profile contains a base segment, and optionally, a number of other segments. See *data set profile, discrete profile, general resource profile, generic profile, group profile,* and *user profile*.

profile list. A list of profiles indexed by class (for general resources) or by the high-level qualifier (for data set profiles) and built in storage by the RACF routines.

profile modeling. The ability for a user or an installation to copy information (such as universal access authority or access lists) from an existing resource profile when defining a new resource profile. This might occur automatically when using ADDSD based on the MODEL specification in a USER or group PROFILE, or manually with the FROM keyword of the ADDSD and RDEFINE commands, or with keywords on RACROUTE REQUEST=DEFINE.

program access to data sets (PADS). A RACF function that enables an authorized user or group of users to access one or more data sets at a specified access authority only while running a specified RACF-controlled program. See *program control*.

program control. A RACF function that enables an installation to control who can run RACF-controlled programs. See *program access to data sets*.

protected resource. A resource defined to RACF for the purpose of controlling access to the resource. Some of the resources that can be protected by RACF are DASD volumes, tape volumes, load modules, terminals, IMS and CICS transactions, and installation-defined resource classes.

protected user ID. A user ID that cannot enter the system by any means that requires a password, and cannot be revoked by invalid password attempts. Assigning a protected user ID to OS/390 UNIX, a UNIX daemon, or another important started task or subsystem assures that the ID cannot be used for other purposes, and that functions will not fail because the ID has been revoked.

public key. For encrypting and decrypting data, one party uses a common, non-secret public key and the other party uses the individual, secret private key. These keys are complementary in that if one is used to encrypt data, the other is used to decrypt data. See *private key*.

PV. See *persistent verification*.

Q

QSAM. See *queued sequential access method (QSAM)*.

queued sequential access method (QSAM). An extended version of the basic sequential access method (BSAM). When this method is used, a queue is formed of input data blocks that are awaiting processing or of output data blocks that have been processed and are awaiting transfer to auxiliary storage or to an output device.

R

RACDEF request. The DEFINE function replaces the RACDEF function. See *DEFINE request*.

RACF. See *Resource Access Control Facility*.

RACF/DB2 external security module. A RACF exit point that receives control from the DB2 access control authorization exit point (DSNX@XAC) to handle DB2 authorization checks.

RACF database. The repository for the security information that RACF maintains.

RACF data set. One of the data sets comprising the RACF database.

RACF-indicated. Pertaining to a data set for which the RACF indicator is set on. If a data set is RACF-indicated, a user can access the data set only if a RACF profile or an entry in the global access checking table exists for that data set. On a system without RACF, a user cannot access a RACF-indicated data set until the indicator is turned off. For VSAM data sets, the indicator is in the catalog entry. For non-VSAM data sets, the indicator is in the data set control block (DSCB). For data sets on tape, the indicator is in the RACF tape volume profile of the volume that contains the data set.

RACF manager. The routines within RACF that provide access to the RACF database. Contrast with *RACF storage manager*.

RACF-protected. Pertaining to a resource that has either a discrete profile or an applicable generic profile, and is protected with the File Security Packet (FSP). A data set that is RACF-protected by a discrete profile must also be RACF-indicated.

RACF remote sharing facility (RRSF). RACF services that function within the RACF subsystem address space to provide network capabilities to RACF.

RACF remove ID utility. A RACF utility that identifies references to user IDs and group names in the RACF database. The utility can be used to find references to residual user IDs and group names or specified user IDs and group names. The output from this utility is a set of RACF commands that can be used to remove the references from the RACF database after review and possible modification. See residual user ID.

RACF storage manager. Manages the allocation of storage for the RACF programs running on a system.

RACF report writer. A RACF function that produces reports on system use and resource use from information found in the RACF SMF records. However, it is recommended that you use RACF SMF Unload instead if possible.

RACF segment. Known as *base segment*.

RACF SMF data unload utility. A RACF utility that enables installations to create a sequential file from the security-relevant audit data. The sequential file can be viewed directly, used as input for installation-written programs, and manipulated with sort/merge utilities. It can also be uploaded to a database manager (such as DB2) to process complex inquiries and create installation-tailored reports. See *SMF records*.

RACHECK request. The AUTH request replaces the RACHECK function. See *AUTH request*.

RACINIT request. The RACINIT request replaces the RACINIT function. See *VERIFY request*.

RACLIST request. The LIST request replaces the RACLIST function. See *LIST request*.

RACLISTed profiles. See *locally RACLISTed profiles* and *SETR RACLISTed profiles*.

RACROUTE macro. An assembler macro that provides a means of calling RACF to provide security functions, including the *AUDIT request, AUTH request, DEFINE request, DIRAUTH request, EXTRACT request, FASTAUTH request, LIST request, SIGNON request, STAT request, TOKENBLD request, TOKENMAP request, TOKENXTR request, VERIFY request,* and *VERIFYX request*.

RACSTAT request. The STAT request replaces the RACSTAT function. See *STAT request*.

RACXTRT request. The EXTRACT request replaces the RACXTRT function. See *EXTRACT request*.

RBA. See *relative byte address*.

read-only mode. A recovery mode of operation when RACF is enabled for sysplex communication. Read-only mode does not allow updates to be made to the RACF database except for statistics generated during logon and job initiation.

real GID. The attribute of a process that, at the time of process creation, identifies the group of the user who created the process. See *OS/390 UNIX group identifier (GID)*. Contrast with *effective group identifier (effective GID)*.

real UID. The attribute of a process that, at the time of process creation, identifies the user who created the process. See *OS/390 UNIX user identifier (UID)*. Contrast with *effective user identifier (effective UID)*.

real user ID. See *user ID*.

relative byte address (RBA). The address in the RACF database.

relative pathname. (1) The name of a directory or file expressed as a sequence of directories followed by a file name, beginning from the current directory. Relative pathnames do not begin with a / (slash) but are relative to the current directory. (2) A pathname that does not begin with a slash. The predecessor of the first file name in the pathname is taken to be the current working directory of the process.

remote logical unit (remote LU). (1) Local LUs are LUs defined to the local system; partner LUs are defined to remote systems. It is a matter of point of view. From the point of view of a remote system, LUs defined to that system are local LUs, and those on the local system are the partner LUs. (2) A partner LU might or might not be on the same system as the local LU. When both LUs are on the same system, the LU through which communication is initiated is the local LU, and the LU through which communication is received is the partner LU. (3) See *partner logical unit (partner LU)*.

remote node. Whether a node is perceived as local or remote depends on the point of view. As an example, consider two RRSF nodes, MVSA and MVSB, that are logically connected. From MVSA's point of view, MVSA is the local node and MVSB is the remote node. From MVSB's point of view, however, MVSB is the local node and MVSA is the remote node. See *local node and target node*.

residual authority. References in the RACF database to group names and user IDs that have been deleted.

residual group name. References in the RACF database to a group name that has been deleted.

residual user ID. References in the RACF database to a user ID that has been deleted.

Resource Access Control Facility (RACF). A program (licensed by IBM) that provides access control by identifying and verifying the users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, logging unauthorized attempts to enter the system, and logging detected accesses to protected resources. RACF is included in the SecureWay Security Server for OS/390 and is also available as a separate program for the MVS and VM environments.

resource grouping class. A RACF class in which resource group profiles can be defined. A resource grouping class is related to another class, sometimes called a *member class*. For example, the resource grouping class GTERMINL is related to the class TERMINAL. See *resource group profile*.

resource group profile. A general resource profile in a resource grouping class. A resource group profile can provide RACF protection for one or more resources with *unlike* names. See *resource grouping class*.

resource profile. A profile that provides RACF protection for one or more resources. USER, GROUP, and CONNECT profiles are not resource profiles. The information in a resource profile can include the profile name, profile owner, universal access authority, access list, and other data. Resource profiles can be discrete profiles or generic profiles. See *discrete profile* and *generic profile*.

restricted user ID. Used for shared user IDs assigned to users (of servers) who do not identify themselves, as well as for those created for use with RACF's Certificate Name Filtering Support. This is a quick method for restricting the access to global resources because a restricted user ID must be on a global resource's access list before access will be granted.

REVOKE attribute. Prevents the RACF-defined user from entering the system.

role. A Tivoli product that is a functional grouping of user authorizations. A ROLE profile represents a role and identifies the authorizations associated with that role.

root. (1) The starting point in the file system. (2) The first directory in the system. (3) In OS/390 UNIX System Services, ROOT identifies and mounts the HFS data set to be used as the root file system. (4) Synonym for *superuser*.

root directory. (1) The directory that points to the directories one level lower than itself that might also contain some files. (2) The top directory in the file system tree, referred to as "/". UNIX and POSIX-conforming systems have a single root directory with mounted devices. (3) A directory, associated with a process, that is used in pathname resolution for pathnames that begin with a slash.

| **root user.** In the OS/390 UNIX operating system, a user who has superuser authority. See *superuser authority*.

RRSF. See *RACF remote sharing facility*.

RRSF logical node connection. Two RRSF nodes are logically connected when they are properly configured to communicate through APPC/MVS, and they have each been configured by the TARGET command to have an OPERATIVE connection to the other.

RRSF network. Two or more RRSF nodes that have established RRSF logical node connections to each other.

RRSF node. An MVS system image or a group of MVS system images sharing a RACF database, which has been defined as an RRSF node, single-system RRSF node, or multisystem RRSF node to RACF by a TARGET command. See *RRSF logical node connection*.

RTOKEN. The RACF resource security token. An RTOKEN is an encapsulation or representation of the security characteristics of a resource. Resource managers, for example JES, can assign RTOKENs to the resources they manage; for example, JES spool files. See *UTOKEN* and *STOKEN*.

S

SAF. See *System Authorization Facility*.

secured signon. A product, which has been replaced by GSO, providing an alternative to the RACF password and also providing enhanced security across a network.

SecureWay Security Server. A licensed feature of OS/390 that is comprised of Resource Access Control Facility (RACF), DCE Security Server, Lightweight Directory Access Protocol (LDAP) Server, OS/390 Firewall Technologies, and Open Cryptographic Enhanced Plug-ins.

security. See *data security*.

security category. An installation-defined name corresponding to a department or area within an organization whose members have similar security requirements.

security classification. The use of security categories, a security level, or both, to impose additional access controls on sensitive resources. An alternative way to provide security classifications is to use security labels.

security label. An installation-defined name that corresponds to a specific RACF security level with a set of zero or more security categories. This is equivalent to the NCSC term *sensitivity label*.

security level. An installation-defined name that corresponds to a numerical security level; the higher the number, the higher the security level.

Security Server. See *SecureWay Security Server*".

security token. A collection of identifying and security information that represents data to be accessed, a user, or a job. This contains a user ID, group name, security label, node of origin, and other information.

segment. A portion of a profile. The format of each segment is defined by a template.

SETR RACLISTed profiles. See *locally RACLISTed profiles* and *RACLISTed profiles*.

SFS. See *Shared File System*.

shared file system (SFS). On VM/ESA, a part of CMS that lets users organize their files into groups known as directories and selectively share those files and directories with other users.

shell. (1) A program that interprets and processes interactive commands from a pseudoterminal or from lines in a shell script. (2) A program that interprets sequences of text input as commands. It might operate on an input stream, or it might interactively prompt and read commands from a terminal. Synonymous with command language interpreter. [POSIX.2] (3) A software interface between a user and the operating system of a computer. Shell programs interpret commands and user interactions on devices such as keyboards, pointing devices and touch-sensitive screens and communicate them to the operating system. (4) The command interpreter that provides a user interface to the operating system and its commands. (5) The program that reads a user's commands and executes them. (6) The shell command language interpreter, a specific instance of a shell. [POSIX.2] (7) A layer, above the kernel, that provides a flexible interface between users and the rest of the system. (8) Software that allows a kernel program to run under different operating system environments. (9) See *command language interpreter*.

shell program. A program that accepts and interprets commands for the operating system.

signed-on-from list. A list of user entries identifying those users who have been signed on from a partner LU to a local LU. The list is part of the persistent verification receive support that is a feature of the APPC architecture of LU 6.2.

SIGNON request. The issuing of the RACROUTE macro with REQUEST=SIGNON specified. A SIGNON request is used to manage the signed-on lists associated with persistent verification (PV), a feature of the APPC architecture of LU 6.2.

single-subsystem scope. A classification model used in conjunction with the RACF/DB2 external security module to construct DB2 classes with the subsystem ID as part of the class name. Contrast with *multi-subsystem scope*.

single-system node. See *single-system RRSF node*.

single-system RRSF node. An RRSF node consisting of one MVS system image.

site certificate. See *digital certificate*.

SMF. See *System Management Facilities*.

SMF records. (1) Records and system or job-related information collected by the System Management Facilities (SMF) and used in billing users, reporting reliability, analyzing the configuration, scheduling jobs, summarizing direct access volume activity, evaluating data set activity, profiling system resource use, and maintaining system security. (2) Variable-length process or status records from the SMF data set that are written to the SMF log data set. These records vary in layout based on the type of system information they contain. See *RACF SMF unload utility*.

SMS. See *Storage Management Subsystem*.

SNA. See *System Network Architecture (SNA)*.

soft limit. Current resource value for a process.

source user ID. The source half of a source user ID and target user ID pair that has an established user ID association between them. For command direction the source user ID is the user ID that issued the command that is being directed. For password synchronization the source user ID is the user ID whose password changed, causing a change to the password of the target user ID. Contrast with *target user ID*.

SPECIAL attribute. Gives the user full control over all of the RACF profiles in the RACF database and allows the user to issue all RACF commands, except for commands and operands related to auditing.

split database. A RACF database that has been divided among multiple data sets.

standard access list. Includes user IDs and group names authorized to access the resource, and the level of access granted to each. See *access list*. Contrast with *conditional access list*.

started procedures table (ICHRIN03). Associates the names of started procedures with specific RACF user IDs and group names. It can also contain a generic entry that assigns a user ID or group name to any started task that does not have a matching entry in the table. However, it is recommended that you use the STARTED class for most cases rather than the started procedures table.

STAT request. The issuing of the RACROUTE macro with REQUEST=STAT specified. A STAT request determines if RACF is active and (optionally) if a given resource class is defined to RACF and active. The STAT request replaces the RACSTAT function.

STOKEN. A UTOKEN associated with a user who has submitted work. See *UTOKEN* and *RTOKEN*.

Storage Management Subsystem (SMS). A component of MVS/DFP that is used to automate and centralize the management of storage by providing the storage administrator with control over data class, storage class, management class, storage group, and automatic class selection routine definitions.

structure. See *cache structure*.

stub. (1) A function that connects with the specified library, but remains outside the specified library. (2) A protocol extension procedure.

subject’s distinguished name (SDN). The X.509 name in a digital certificate that is associated with the name of the subject.

superuser. In OS/390 UNIX System Services, a system user who operates with the special privileges needed to perform a specified administrative task.

superuser authority. In an OS/390 UNIX System Services operating system, the unrestricted authority to access and modify any part of the operating system, usually associated with the user who manages the system. See *root user*.

supervisor. The part of a control program that coordinates the use of resources and maintains the flow of processing unit operations. Synonym for *supervisory routine*.

supervisor state. A state during which a processing unit can execute input/output and other privileged instructions. Contrast with *problem state*.

supervisory routine. A routine, usually part of an operating system, that controls the execution of other routines and regulates the flow of work in a data processing system. Synonymous with *supervisor*.

syscall. See *callable service*.

sysplex (system complex). Multiple systems communicating and cooperating with each other through multisystem hardware elements and software services to process the installation's workloads.

sysplex communication. An optional RACF function that allows the system to use XCF services and communicate with other systems that are also enabled for sysplex communication.

system complex. See *sysplex*.

system authorization facility (SAF). An MVS component that provides a central point of control for security decisions. It either processes requests directly or works with RACF or another security product to process them.

system call. In OS/390 UNIX System Services, a synonym for *callable service*.

System Management Facility (SMF). The part of the OS/390 operating system that collects and records system and job-related information used in billing users, reporting reliability, analyzing the configuration, scheduling jobs, summarizing direct access volume activity, evaluating data set activity, profiling system resource use, and maintaining system security. The information is recorded in the SMF log data set.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

tape volume set. The collection of tape volumes on which a multivolume data set resides. A volume set is represented in one RACF profile.

tape volume table of contents (TVTOC). Information about a tape data set that RACF stores in the tape volume profile for the volume on which the data set resides. The TVTOC includes the data set name, data set sequence number, creation date, and an indicator as to whether a discrete tape data set profile exists.

target node. An RRSF node that a given RRSF node is logically connected to, as a result of a TARGET command. See *local node* and *remote node*.

target user ID. The target half of a source user ID and target user ID pair that has an established user ID association between them. For command direction, the target user ID is the user ID specified on the AT or ONLYAT keyword, and is the user ID under whose authority the command is run on the specified node. For password synchronization, the target user ID is the user ID whose password RACF automatically updates when the password for the source user ID is changed. Contrast with *source user ID*.

task. (1) A basic unit of work to be performed or a process and the procedures that run the process on OS/390. (2) In a multiprogramming or multiprocessing environment, one or more sequences of instructions treated by a control program as an element of work to be accomplished by a computer.

template. Contains mappings of the profiles on the RACF database.

TOKENBLD request. The issuing of the RACROUTE macro with REQUEST=TOKENBLD specified. A TOKENBLD request builds a UTOKEN.

TOKENMAP request. The issuing of the RACROUTE macro with REQUEST=TOKENMAP specified. A TOKENMAP request maps a token in either internal or external format, allowing a caller to access individual fields within the UTOKEN.

TOKENXTR request. The issuing of the RACROUTE macro with REQUEST=TOKENXTR specified. A TOKENXTR request extracts a UTOKEN from the current address space, task or a caller-specified ACEE.

TP. See *transaction program*.

tranquility. Keeping the security classification of a resource constant while it is in use; keeping the security classification of a user constant while active.

transaction program (TP). A program used for cooperative transaction processing within an SNA network. For APPC/MVS, any program on MVS that issues APPC/MVS or CPI-C calls, or is scheduled by the APPC/MVS transaction scheduler.

trust. As a characteristic of a digital certificate, trust indicates that the user has presented a valid certificate and that the private key related to this certificate has not been compromised. In OS/390 implementation, trust policy is a subset of the installation's trust policy.

TVTOC. See *tape volume table of contents*.

U

UACC. See *universal access authority*.

UADS. See *user attribute data set*.

UID. See *OS/390 UNIX user identifier (UID)*.

undub. In OS/390 UNIX System Services, the inverse of *dub.* Normally, a task (dubbed a thread) is undubbed when it ends. An address space (dubbed a process) is undubbed when the last dubbed thread ends. Contrast with *dub*.

universal access authority (UACC). The default access authority that applies to a resource if the user or group is not specifically permitted access to the resource. The universal access authority can be any of the access authorities.

unmount. To logically disassociate a mountable file system from another file system. The TSO command to perform this action is UNMOUNT or UMOUNT.

user. A person who requires the services of a computing system.

user attribute. The extraordinary privileges, restrictions, and processing environments assigned to a user. The user attributes are SPECIAL, AUDITOR, CLAUTH, OPERATIONS, GRPACC, ADSP, and REVOKE.

user attribute data set (UADS). In TSO, a partitioned data set with a member for each authorized user. Each member contains the appropriate passwords, user identifications, account numbers, LOGON procedure names, and user characteristics that define the user.

user certificate. See *digital certificate*.

user data set. A data set defined to RACF in which either the high-level qualifier of the data set name or the qualifier supplied by an installation exit routine is a RACF user ID.

user ID. A RACF user ID. A string of 1-8 alphanumeric characters that uniquely identifies a RACF user, procedure, or batch job to the system. For TSO users, the user ID cannot exceed 7 characters and must begin with an alphabetic, #, $, or @ character. The user ID is defined by a user profile in the RACF database and is used as the name of the profile.

user ID association. A relationship between two user IDs, established through the RACLINK command, which is required for command direction and password synchronization between the user IDs. See *peer user ID association* and *managed user ID association*.

user identification. See *user ID*.

user identification and verification. The acts of identifying and verifying a RACF-defined user to the system during logon or batch job processing. RACF identifies the user by the user ID and verifies the user by the password, PassTicket, verified digital certificate, DCE credentials, or operator identification card supplied during logon processing or the password supplied on a batch JOB statement.

user name. (1) In RACF, 1–20 alphanumeric characters that represent a RACF-defined user. (2) In OS/390 UNIX System Services, a string that is used to identify a user. Contrast with *user ID*.

user profile. A description of a RACF-defined user that includes the user ID, user name, default group name, password, profile owner, user attributes, and other information. A user profile can include information for subsystems such as TSO and DFP.

UTOKEN. The RACF user security token. A UTOKEN is an encapsulation or representation of the security characteristics of a user. RACF assigns a UTOKEN to each user in the system. See *STOKEN* and *RTOKEN*.

V

verification. See *user identification and verification*.

VERIFY request. The issuing of the RACROUTE macro with REQUEST=VERIFY specified. A VERIFY request is used to verify the authority of a user to enter work into the system. The VERIFY request replaces the RACINIT function.

VERIFYX request. The issuing of the RACROUTE macro with REQUEST=VERIFYX specified. A VERIFYX request verifies a user and builds a UTOKEN, and handles the propagation of submitter ID.

Virtual Machine (VM). (1) An operating system that appears to be at the exclusive disposal of the particular user, but whose functions are accomplished by sharing the resources of a real data processing system. (2) In VM/ESA, the operating system that represents the virtual processors, virtual storage, virtual devices, and virtual channel subsystem allocated to a single user. A virtual machine also includes any expanded storage dedicated to it.

Virtual Smart Card. Software component that provides the same behavior as a physical smart card. It provides a secure repository for key pairs, certificates, and certificate mappings. Access to keys and certificates is governed by a personal identification number (PIN) or some other secret shared between the holder of the card and the smart card.

VM. See *Virtual Machine*.

W

working directory. In OS/390 UNIX System Services, the active directory used to resolve pathnames that do not begin with a slash. In similar systems, a working directory might be called the *current directory* or the *current working directory*.

workspace data sets. VSAM data sets used by RACF for queuing requests sent to and received from target nodes in an RRSF environment.

X

XCF. See *cross-system coupling facility*.

Index

Readers' Comments — We'd Like to Hear from You

OS/390
SecureWay Security Server RACF
General User's Guide

Publication No. SC28-1917-07

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You
SC28-1917-07

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY
12601-5400

Fold and Tape **Please do not staple** Fold and Tape

SC28-1917-07

Cut or Fold
Along Line

Program Number: 5647-A01

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC28-1917-07