OS/390

SecureWay Security Server RACF Migration

GC28-1920-08

OS/390

SecureWay Security Server RACF Migration

GC28-1920-08

Note

Before using this information and the product it supports, be sure to read the general information under “Appendix. Notices” on page 81.

Ninth Edition, December 2000

This is a major revision of GC28-1920-07. 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:

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

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

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

About This Book

This book contains information about the Resource Access Control Facility (RACF), which is a component of the SecureWay Security Server for OS/390 (Security Server). The Security Server is comprised of the following components:

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

For more information about these components, see the following documentation:

GC28-1938 *OS/390 Security Server (DCE) Overview*

SA22-7249 *OS/390 SecureWay Security Server Open Cryptographic Enhanced Plug-ins Guide and Reference*

SC24-5835 *OS/390 SecureWay Security Server Firewall Technologies Guide and Reference*

SC24-5861 *OS/390 SecureWay Security Server LDAP Server Administration and Usage Guide*

SC24-5878 *OS/390 SecureWay Security Server LDAP Client Application Development Guide and Reference*

SC24-5896 *OS/390 SecureWay Security Server Network Authentication and Privacy Service Administration*

SC24-5897 *OS/390 SecureWay Security Server Network Authentication and Privacy Service Programming*

Who Should Use This Book

This book provides planning information about installing and migrating to the RACF component of the OS/390 Version 2 Release 10 Security Server. This book should be used by those people who are responsible for migrating from an earlier release to this one and by those who are responsible for planning for this release.

How to Use This Book

This book is organized into the following sections:

- "Chapter 1. Migration Overview" on page 1, provides information to help you plan your installation's migration to the new release of RACF.
- "Chapter 2. Migration Roadmap" on page 7, describes high-level migration considerations for customers upgrading to the new release of RACF from previous levels of RACF.
- "Chapter 3. Version 2 Release 10.0 Overview" on page 11, provides an overview of the support introduced in the new release of OS/390 Version 2 Release 10.0.
- "Chapter 4. Version 2 Release 8.0 Overview" on page 29, provides an overview of the support introduced in OS/390 Version 2 Release 8.0.

- "Chapter 5. Summary of Interface Changes" on page 53, summarizes the specific RACF interfaces that have been updated in OS/390 Version 2 Release 10.0 and OS/390 Version 2 Release 8.0

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 Security Server, 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.

Summary of Changes

Summary of Changes
for GC28-1920-08
as Updated December, 2000

Updated Information

- The following sections have been updated to include new information about the R_PKIServ callable service (IRRSPX00) that is added with RACF APAR number OW45211 and SAF APAR number OW45212:
  - "Public Key Certificate Enhancements" on page 22
  - "Callable Services" on page 53
  - "Data Areas" on page 61
  - "SMF Records" on page 73
  - "Utilities" on page 77

This book includes terminology, maintenance, and editorial changes. Technical changes or additions to the text are indicated by a vertical line to the left of the change.

Summary of Changes
for GC28-1920-07
OS/390 Version 2 Release 10

This book contains new information about the RACF component of the SecureWay Security Server for OS/390 Version 2 Release 10.

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.

This book includes terminology, maintenance, and editorial changes. 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 GC28-1920-06
OS/390 Version 2 Release 8

This book contains primarily new information about the OS/390 Security Server (RACF) for OS/390 Version 2 Release 8.

Chapter 1. Migration Overview

Your plan for migrating to the new level of RACF should include information from a variety of sources. These sources of information describe topics, such as coexistence, service, hardware and software requirements, installation and migration procedures, and interface changes.

The following documentation, which is supplied with your product order, provides information about installing your OS/390 system. In addition to specific information about RACF, this documentation contains information about all of the OS/390 elements.

- *OS/390 Planning for Installation*

  This book describes the installation requirements for OS/390 at a system and element level. It includes hardware, software, and service requirements for both the driving and target systems. It also describes any coexistence considerations and actions.
- *OS/390 Program Directory*

  This document, which is provided with your OS/390 product order, leads you through the specific installation steps for RACF and the other OS/390 elements.
- *ServerPac Installing Your Order*

  This is the order-customized, installation book for using the ServerPac Installation method. Be sure to review “Appendix A. Product Information”, which describes data sets that are supplied, jobs or procedures that have been completed for you, and product status. IBM may have run jobs or made updates to PARMLIB or other system control data sets. These updates could affect your migration.

Within this book, you can find information about the specific updates and considerations that apply to this release of RACF.

- “Chapter 2. Migration Roadmap” on page 7

  This section identifies the migration paths that are supported with the current level of OS/390 Security Server (RACF). It also describes the additional publications that can assist you with your migration to the current level.
- “Chapter 3. Version 2 Release 10.0 Overview” on page 11

  This section describes the specific updates that were made to RACF for the current release. For each item, this section provides an overview of the change, a description of any migration and coexistence tasks that may need to be considered, and where you can find more detailed information in the RACF library or other OS/390 element libraries.
- “Chapter 4. Version 2 Release 8.0 Overview” on page 29

  This section describes the specific updates that were made to RACF for OS/390 Version 2 Release 8.0.For each item, this section provides an overview of the change, a description of any migration and coexistence tasks that may need to be considered, and where you can find more detailed information in the RACF library or other OS/390 element libraries.
- “Chapter 5. Summary of Interface Changes” on page 53

  This section provides a summary of the changes that were made to RACF user and programming interfaces for OS/390 Version 2 Release 10.0 (V2R10) and OS/390 Version 2 Release 8.0 (V2R8).

Terms You Need to Know

This section describes some terms you may need to know as you use this book.

Migration
Activities that relate to the installation of a new version or release of a program to replace an earlier level. Completion of these activities ensures that the applications and resources on your system will function correctly at the new level.

Coexistence
Two or more systems at different levels (for example, software, service or operational levels) that share resources. Coexistence includes the ability of a system to respond in the following ways to a new function that was introduced on another system with which it shares resources: ignore a new function, terminate gracefully, support a new function. The following are examples of multisystem configurations in which resource sharing can occur:

- A single system running multiple LPARs
- A single processor that is time-sliced to run different levels of the system (for example, during different times of the day)
- Two or more systems running separate processors
- A Parallel Sysplex configuration (also includes a basic sysplex)

Developing a Migration Strategy

The recommended steps for migrating to a new release of RACF are:

1. Become familiar with the supporting migration and installation documentation for the release.

   You should determine what updates are needed for products that are supplied by IBM, system libraries, and non-IBM products. Review the *OS/390 Planning for Installation* book and the *OS/390 Introduction and Release Guide* for information about RACF and other OS/390 elements.
2. Develop a migration plan for your installation.

   When planning to migrate to a new release of RACF, you must consider high-level support requirements, such as machine and programming restrictions, migration paths, and program compatibility.
3. Obtain and install any required program temporary fixes (PTFs) or updated versions of the operating system.

   Call the IBM Software Support Center to obtain the preventive service planning (PSP) upgrade for RACF, which provides the most current information about PTFs for RACF. Check RETAIN again just before testing RACF. For information about how to request the PSP upgrade, refer to the *OS/390 Program Directory*. Although the *OS/390 Program Directory* contains a list of the required PTFs, the most current information is available from the IBM Software Support Center.
4. Install the product using the *OS/390 Program Directory* or the *ServerPac Installing Your Order* documentation.
5. Contact programmers who are responsible for updating applications at your installation.

   Verify that your installation's applications will continue to run, and, if necessary, make changes to ensure compatibility with the new release.
6. Use the new release before initializing major new function.
7. If necessary, customize the new function for your installation.

8. Exercise the new functions.

Reviewing Changes to RACF Processing

As you define your installation's migration plan, consider how the new and changed RACF support might affect the following areas of RACF processing. For each item described in "Chapter 3. Version 2 Release 10.0 Overview" on page 11, you should review the "What This Change Affects" and "Migration Procedures" sections to determine how, or if, the support affects the tasks that are performed at your installation.

Administration

Security administrators must be aware of how changes introduced by a new product release can affect an installation's data processing resources. Changes to real and virtual storage requirements, performance, security, and integrity are of interest to security administrators or to system programmers who make decisions about the system resources used with a program.

Application Development

Application development programmers must be aware of new functions introduced in a new release of RACF. To ensure that existing programs run as before, your application programmers need to know about any changes in data areas and processing requirements. This book provides an overview of the changes that might affect existing application programs.

Auditing

Typically, auditors are responsible for ensuring proper access control and accountability for their installation. This book identifies any changes to security options, audit records, and report generation utilities.

Customization

To meet the specific requirements of your installation, you can customize RACF functions to take advantage of new support after the product is installed. For example, you can tailor RACF through the use of installation exit routines, class descriptor table (CDT) entries, or options to improve performance. This book lists changes to RACF that might require your installation to tailor the product, either to ensure that RACF runs as before or to accommodate new security controls that your installation may need.

General User

This book provides an overview of the changes that might affect existing procedures for general users. RACF general users can use a RACF-protected system to:

- Log on to the system
- Access resources on the system
- Protect their own resources and any group resources to which they have administrative authority

Operations

The new RACF release might introduce changes to its operating characteristics, such as changed

commands, new or changed messages, or in the methods of implementing new functions. This book identifies those changes for which you should provide user education before running this release of the product.

Reviewing Changes to RACF Interfaces

When defining your installation's migration plan, also consider that RACF interfaces may also be affected by the new or changed functions that are introduced in this release. These interfaces include:

- Callable services
- Class descriptor table (CDT)
- Commands
- Data areas
- Database templates
- Exits
- Macros
- Messages
- Panels
- SMF Records
- SYS1.SAMPLIB members
- Utilities

"Chapter 5. Summary of Interface Changes" on page 53 provides a summary of the changes that affect these interfaces for the release. This information is also listed in the "What This Change Affects" section that is provided for each release enhancement.

Actions Required for All Migrations

The following sections describe common activities and considerations that are typically required (or should be considered) whenever you migrate from a previous release of RACF to the current release.

Updating RACF Templates

To ensure that RACF functions properly, use the IRRMIN00 utility to update the RACF database with the database templates for the current release level. If an OS/390 Version 2 Release 10.0 RACF system shares its database with a lower-level RACF system, the lower level system is not impacted by the higher-level templates; the system performs the same.

To install the database template updates, run IRRMIN00 with PARM=UPDATE pointing to the templates that are supplied with RACF Version 2 Release 10.0 in the IRRTEMP1 SYS1.MODGEN member. You should do this **before** IPLing your OS/390 Version 2 Release 10.0 system. For more information, see *OS/390 Program Directory*, *ServerPac Installing Your Order* documentation, and *OS/390 SecureWay Security Server RACF System Programmer's Guide*.

Running Dynamic Parse

When new keywords are added to RACF commands, the dynamic parse table (IRRDPSDS) is also updated. After IPLing your system to use the updated RACF database, you should also issue the IRRDPI00 command to start dynamic parsing and use the updated parse table. For more information, see *OS/390 SecureWay Security Server RACF System Programmer's Guide*.

Using Automatic Direction of Application Updates (ADAU)

If your target system is synchronized with other systems in your sysplex, you can use Automatic Direction of Application Updates (ADAU) to propagate database changes to the other systems. If your systems are not synchronized, and you try to use ADAU to propagate changes, information will not be recognized by your target system. See *OS/390 SecureWay Security Server RACF Security Administrator's Guide* for additional information regarding automatic direction of application updates.

Checking for Duplicate Class Names

When new classes are shipped with RACF, you should verify that any installation-defined class names that have been added to the router table and class descriptor table (CDT) do not conflict with these new classes. If duplicate table entries are detected, you will receive the following error messages when the system is IPLed:

- For a duplicate router table entry, RACF issues message ICH527I and continues processing: `RACF DETECTED AN ERROR IN THE INSTALLATION ROUTER TABLE, ENTRY class_name, ERROR CODE 1`
- For a duplicate CDT entry, RACF issues message ICH564A and enters failsoft mode: `RACF DETECTED AN ERROR IN THE INSTALLATION CLASS DESCRIPTOR TABLE, ENTRY class_name, ERROR CODE 7`

If a conflict in class names occurs, you must:

1. Delete the profiles in the installation-defined class with the conflicting name.
2. Delete the CDT entry for the class.
3. Add a CDT entry with a different name.
4. Redefine the profiles.

Attention

Do not assemble the installation-defined CDT (ICHRRCDE) on an OS/390 Version 2 Release 10 system and attempt to use it on a system running RACF at a lower level than RACF/MVS Version 2 Release 2.

Year 2000 Support for RACF

RACF is an element of OS/390. Beginning with OS/390 Version 1 Release 2, OS/390 is certified as a Year 2000-ready operating system by the Information Technology Association of America (ITAA). Follow-on releases are also Year 2000 ready.

Previous products, such as RACF/MVS Release 2.2, are Year 2000 ready with maintenance applied.

RACF APAR OW24640 and OS/390 (MVS) APAR OW24641 provide additional Year 2000 support to enhance the support previously supplied. The additional support includes:

- RACROUTE REQUEST=EXTRACT supports the following parameters as part of TYPE=EXTRACT, EXTRACTN, or REPLACE:

  `DATEFMT=YYYYDDDF or DATEFMT=YYDDDF`

- The ICHEINTY macro supports the following parameters:

  `DATEFMT=YYYYDDDF or DATEFMT=YYDDDF`

The RACF report writer (RACFRW) uses SMF dates in the form *yyddd*. If you select a date range of records with a starting date that occurs before January 1, 2000 (for example, 99364) and an ending date that occurs on or after January 1, 2000 (for example, 00002), the report writer will reject your request. It will consider the year 00 as coming before the year 99. Similarly, when sorting records by date, the report writer will treat 00 as coming before 99. Because IBM has stabilized RACFRW and will not make functional improvements to it, IBM does not intend to enhance the RACF report writer to recognize this condition and to process the records differently. Other than this problem with record ordering, which should only occur if the input file has records both before and after January 1, 2000, RACFRW should properly process records with dates after January 1, 2000, as it would have handled those records if they had contained earlier dates.

For more information about the RACROUTE macro, see *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*; for more information about the ICHEINTY macro, see *OS/390 SecureWay Security Server RACF Macros and Interfaces*. See *OS/390 SecureWay Security Server RACF Auditor's Guide* for information about the RACF report writer.

For more information about Year 2000 support, refer to *The Year 2000 and 2-Digit Dates: Guide*, GC28-1251. For additional information about Year 2000, see the following URLs:

`http://www.ibm.com/IBM/year2000/`
`http://www.ibm.com/s390/racf/`

Chapter 2. Migration Roadmap

This section describes the migration paths that are supported by the current release of Security Server. It also provides information about how you can obtain the Security Server migration information from previous releases.

OS/390 V2R8 or V2R9 to V2R10

Table 1 summarizes the updates that have been introduced to RACF in OS/390 Version 2 Release 10 (V2R10). If you are migrating from a previous release, you should review the information in the detailed section for each item.

Table 1. Summary of RACF Updates for OS/390 Version 2 Release 10

For Information About:	Refer to Page:
Certificate Name Filtering	12
SecureWay Security Server Network Authentication and Privacy Service Support	16
Program Control Enhancements	18
Application Identity Mapping	19
Enhanced PassTicket Support	21
Public Key Certificate Enhancements	22
Enhanced OS/390 UNIX Superuser Granularity Support	24
Release FMID Update	25
Service Updates	26

OS/390 V2R6 or OS/390 V2R7 to OS/390 V2R10

This section is for those who are migrating from either OS/390 Version 2 Release 6 or Version 2 Release 7 to the current release. You should review the information in the detailed section for each item.

Table 2. Summary of RACF Updates for OS/390 Version 2 Release 8

For Information About:	Refer to Page:
Class Descriptor Table Enhancements	30
DB2 Support	33
ICETOOL Support	35
Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support	36
OS/390 UNIX Superuser Granularity	38
OS/390 UNIX User Limits	40
Protected User ID	42
Public Key Certificate Enhancements	44
R_admin SETROPTS Support	48
Release FMID Update	49
Service Updates	50
Changes introduced in OS/390 V2R10	

Table 2. Summary of RACF Updates for OS/390 Version 2 Release 8 (continued)

For Information About:	Refer to Page:
Certificate Name Filtering	12
SecureWay Security Server Network Authentication and Privacy Service Support	16
Program Control Enhancements	18
Application Identity Mapping	19
Enhanced PassTicket Support	21
Public Key Certificate Enhancements	22
Enhanced OS/390 UNIX Superuser Granularity Support	24
Release FMID Update	25
Service Updates	26

Security Server V2R5 and Earlier

If you are migrating from a release earlier than Security Server (RACF) V2R6, table Table 3 indicates which additional migration information you should review before migrating to the current release. To use the table, find the row that describes your current release or product level. An “X” or a note (described on page 8) in an associated column indicates an additional book or migration information that you should review before migrating to the current release. For example, if you are migrating from Security Server Version 2 Release 5 (V2R5), you would need to review an earlier edition of this book (GC28-1920-05) in addition to this current (GC28-1920-07) publication.

Table 3. Summary of Supported Migration Paths and Associated Migration Guides

Release You Are Migrating From	Review GC28-1920 Level							Note
	-07	-05	-04	-03	-02	-01	-00	
Security Server V2R5	X	X						
Security Server V2R4	X	X	X					
Security Server V1R3	X	X	X	X				
Security Server V1R2	X	X	X	X	X			
Security Server V1R1 or RACF/MVS 2.2	X	X	X	X	X	X		Note 1
RACF/MVS 2.1	X	X	X	X	X	X	X	
RACF/MVS 1.9.2	X	X	X	X	X	X	X	Note 2
RACF/MVS 1.9	X	X	X	X	X	X	X	Note 3

Notes:

1. Security Server for OS/390 V1R1 and RACF/MVS 2.2 (the standalone licensed product) are functionally equivalent.
2. For additional migration information, you should also review the following RACF/MVS 2.2 publication:

   GC23-3736-00 *RACF Planning: Installation and Migration*
3. If you are running RACF/MVS 1.9, you can migrate to the current release of Security Server if you are using the restructured RACF database and meet the current OS/390 release requirements.

If your database is not restructured, you must restructure it and perform appropriate testing of any installation-supplied code that uses the ICHEINTY or RACROUTE REQUEST=EXTRACT,TYPE=EXTRACT, or TYPE=REPLACE macros before installing the current release of Security Server.

In addition, you should review the following publications:

GC23-3736-00 *RACF Planning: Installation and Migration*, for RACF/MVS 2.1

GC23-3045-02 *RACF Migration and Planning*, for RACF/MVS 1.9.2

Note: If you are coming from a RACF/MVS release prior to 1.9, you first need to migrate to RACF/MVS 1.9, so that you can convert your RACF database to the restructured format. Contact IBM DIRECT to obtain a copy of the archived RACF/MVS 1.9 distribution tape. Also, in addition to the preceding publications, you should review the following book:

GC23-3045-01 *RACF Migration and Planning*, for RACF/MVS 1.9

Obtaining Previous Editions of Migration Information

You can obtain copies of the migration guides that support these previous levels of Security Server from the following locations:

- The OS/390 SecureWay Security Server bookshelf on the *IBM Online Library Omnibus Edition OS/390 Collection* CD-ROM.
- The *Online Library OS/390 SecureWay Security Server RACF Information Package* CD-ROM.
- OS/390 Online Library Web page, which is available at the following URL:

  `http://www.ibm.com/s390/os390/bkserv/`
- OS/390 RACF home page (select the “Migrating” topic), which is available at the following URL:

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

Migration Roadmap

Chapter 3. Version 2 Release 10.0 Overview

The following sections describe the new and changed RACF functions that are introduced for OS/390 Version 2 Release 10 (V2R10). The information about each item includes:

- Description
- Summary of the RACF tasks or interfaces that might be affected
- Coexistence considerations, if any, that are associated with the item
- Migration procedures, if any, that are associated with the item
- References to other publications that contain additional detailed information

Release Summary

Table 4 summarizes the updates that have been introduced to RACF in OS/390 Version 2 Release 10 (OS/390 V2R10). For more information, refer to the detailed section for each item.

Table 4. Summary of RACF Updates for OS/390 Version 2 Release 10

For Information About:	Refer to Page:
Certificate Name Filtering	12
SecureWay Security Server Network Authentication and Privacy Service Support	16
Program Control Enhancements	18
Application Identity Mapping	19
Enhanced PassTicket Support	21
Public Key Certificate Enhancements	22
Enhanced OS/390 UNIX Superuser Granularity Support	24
Release FMID Update	25
Service Updates	26

Certificate Name Filtering

Description

Certificate name filtering support associates many certificates to a single, shared RACF user ID without having to install each certificate into the RACF database. Certificate filters substantially decrease the amount of database storage and the system administration requirements associated with processing large numbers of certificates.

In addition, with certificate name filtering support, you can restrict the access a user ID has to global resources. Assigning restricted user IDs is an effective way to manage public or anonymous IDs, or IDs created for use with RACF's certificate filters. You can define a restricted user ID by assigning the RESTRICTED attribute through the ADDUSER or ALTUSER command. Restricted user IDs cannot be used to access protected resources they are not specifically authorized to access. Access authorization for restricted user IDs bypasses global access checking. In addition, the UACC of a resource and an ID(*) entry on the access list are not used to enable a restricted user ID to gain access.

Other highlights of certificate name filtering support include:

- Enhancements to the Remove ID utility and the RACDCERT command to remove orphan profiles (where the user ID associated with the profiles no longer exist) in the DIGTCERT and DIGTRING classes, as well as in the new DIGTNMAP class.
- Two new audit records are written by the initACEE callable service when the following occurs:
  - A certificate does not correspond to a RACF user ID
  - A certificate is not trusted.

  Console messages are also written when these conditions occur.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	To issue the MAP, ALTMAP, DELMAP and LISTMAP functions of the RACDCERT command, you must have one of the following authorities: • SPECIAL • Sufficient authority to resource IRR.DIGTCERT.*<function>* in the FACILITY class. For user IDs that are shared by multiple users, consider specifying the RESTRICTED parameter when issuing the ADDUSER and ALTUSER commands. The DELUSER command deletes user IDs and associated DIGTCERT, DIGTRING and DIGTNMAP profiles. Do not delete the irrmulti user ID; otherwise, information about the corresponding certificates will be deleted from your system. If you re-IPL your system, RACF automatically recreates the user ID; however, all of the information about the certificate filters may not be fully recovered.

Area	Considerations
Application Development	Attempts to specify the new irrmulti user ID on the RACROUTE REQUEST=VERIFY macro will fail; an audit record and console message will be generated.
Auditing	Two new audit records are written by the initACEE callable service when: • A certificate does not correspond to a RACF user ID • A certificate is not trusted. New command keywords on the RACDCERT, ADDUSER, and ALTUSER commands are audited as part of the command SMF records. The X.500 name is added to any SMF record written for an ACEE that contains a pointer to those values. Additional event code qualifiers were added to audit security related errors in initACEE that are not detected by a call to RACROUTE REQUEST=VERIFY. The SMF TYPE 80 record size increased, therefore a different space allocation method is needed when creating reports with DB2 from the SMF unload utility (IRRADU00). Contact your DB2 administrator for the appropriate buffer pool name to use for the SMF unload utility. The increase in DB2 buffer size will result in an increase in DB2 database storage usage for SMF unload reports.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Callable Services” on page 53, “Class Descriptor Table” on page 56, “Commands” on page 57, “Data Areas” on page 61, “Database Templates” on page 64, “Exits” on page 67, “Macros” on page 68, “Messages” on page 71, “Panels” on page 71, “SMF Records” on page 73, “SYS1.SAMPLIB Members” on page 75, and “Utilities” on page 77.

Coexistence Considerations

Note: Certificate name filtering support is only available on OS/390 Version 2 Release 10 and on OS/390 Version 2 Release 8 with APAR OW40129 applied.

- Do not issue the DELUSER command to delete a user ID that is associated with a mapping profile in the DIGTNMAP class on an OS/390 system that does not support certificate name filtering; residual DIGTNMAP profiles will inadvertently be left in a general resource class when the profile is deleted. Use the Remove ID utility to delete orphan profiles.
- For systems that support certificate name filtering, if RRSFDATA profiles are in effect for propagation of DIGTCERT and DIGTRING information, ensure that RRSFDATA profiles are created that cause propagation of DIGTNMAP and DIGTCRIT information in a consistent manner. The DIGTNMAP propagation is controlled using the resource name AUTODIRECT.*target-node*.DIGTNMAP.APPL with Automatic Direction of Application Updates (ADAU). The DIGTCRIT propagation is controlled using the resource name AUTODIRECT.*target-node*.DIGTCRIT.*command-name* with automatic command direction.
- If you use automatic command direction to propagate the ADDUSER and ALTUSER commands to systems that do not support certificate name filtering make sure that you do not specify the RESTRICTED or NORESTRICTED

keyword. These new keywords will not be recognized by your downlevel system, and as a result, will issue an error message indicating that an invalid keyword was detected.

- The SMF TYPE 80 record size increased, therefore DB2 requires additional space for the larger reports created when using the SMF unload utility (IRRADU00). Contact your DB2 administrator for the appropriate buffer pool name to use for the SMF unload utility.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if your installation uses the specified exits or macros.

Task	Condition	Reference Information
Verify compatibility APAR OW42339 is installed on all other members of your sysplex. The PTF numbers for compatibility APAR OW42339 are: • UW66589/RACF for OS/390 Version 1 Release 2 • UW66590/RACF for OS/390 Version 1 Release 3 • UW66591/RACF for OS/390 Version 2 Release 4 • UW66592/RACF for OS/390 Version 2 Release 6 • UW66593/RACF for OS/390 Version 2 Release 8	Required	
Run the IRRMIN00 utility	Required	“Updating RACF Templates” on page 4
Ensure that the new IBM–supplied class names (DIGTCRIT or DIGTNMAP) do not conflict with any installation-defined class names.	Required	“Checking for Duplicate Class Names” on page 5
The SMF TYPE 80 record size increased, therefore DB2 requires additional space for the larger reports created when using the SMF unload utility (IRRADU00). Contact your DB2 administrator for the appropriate buffer pool name to use for the SMF unload utility.	Required	
Determine the type of access users require to perform specific functions of the RACDCERT command.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator’s Guide*

For More Information

For more detailed information about this support in RACF, refer to the following publications:

- *OS/390 SecureWay Security Server RACF Auditor’s Guide*
- *OS/390 SecureWay Security Server RACF Callable Services*
- *OS/390 SecureWay Security Server RACF Command Language Reference*

- *OS/390 SecureWay Security Server RACF Data Areas*
- *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*
- *OS/390 SecureWay Security Server RACF Macros and Interfaces*
- *OS/390 SecureWay Security Server RACF Messages and Codes*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*
- *OS/390 SecureWay Security Server RACF System Programmer's Guide*

SecureWay Security Server Network Authentication and Privacy Service Support

Description

This support allows Network Authentication and Privacy Service principal and realm information to be stored and administered in a RACF database. The new principal and realm information is processed using a new KERB segment in the RACF user profiles and general resource profiles. Two new callable services, R_kerbinfo (IRRSMK00) and R_ticketserv (IRRSPK00) were created to support the Network Authentication and Privacy Service. R_kerbinfo retrieves the principal and realm information stored in RACF, and R_ticketserv enables OS/390 application servers to parse and extract principal names from GSS–API context tokens.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	None.
Auditing	A new event code (KTICKET) and event qualifiers (SUCCESS and FAILURE) have been added to the SMF Type 80 record.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Callable Services” on page 53, “Commands” on page 57, “Data Areas” on page 61, “Database Templates” on page 64, “Messages” on page 71, “Panels” on page 71, “SMF Records” on page 73, and “SYS1.SAMPLIB Members” on page 75.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if you choose to implement this function.

Task	Condition	Reference Information
Run the IRRMIN00 utility with PARM=UPDATE.	Required	“Updating RACF Templates” on page 4
Run the dynamic parse utility.	Required	“Running Dynamic Parse” on page 4
Use the TARGET command to define the local system as the local RACF remote sharing facility (RRSF) node.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator’s Guide*

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Callable Services*

- *OS/390 SecureWay Security Server RACF Command Language Reference*
- *OS/390 SecureWay Security Server RACF Macros and Interfaces*
- *OS/390 SecureWay Security Server RACF Data Areas*
- *OS/390 SecureWay Security Server RACF Diagnosis Guide*
- *OS/390 SecureWay Security Server RACF Messages and Codes*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*

Program Control Enhancements

Description

These enhancements were created to provide better security and integrity for OS/390 UNIX by making it easier to use OS/390 UNIX level security. You can select your level of security by defining BPX.DAEMON and BPX.SERVER in the Facility class. New messages assist the security administrator with diagnostics by providing the information needed for determining which PROGRAM definitions or WHEN(PROGRAM(...) conditional access list entries need modifications.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	OS/390 UNIX will use the IRRENS00 service to instruct RACF to do the following: • keep the environment clean • mark the environment dirty, or • reset the keep-controlled indicator
Auditing	None.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Callable Services” on page 53, “Data Areas” on page 61, and “Macros” on page 68.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Callable Services*
- *OS/390 SecureWay Security Server RACF Macros and Interfaces*
- *OS/390 SecureWay Security Server RACF Data Areas*
- *OS/390 SecureWay Security Server RACF Diagnosis Guide*
- *OS/390 SecureWay Security Server RACF Messages and Codes*
- *OS/390 SecureWay Security Server RACF Security Administrator’s Guide*

For more information about OS/390 UNIX, refer to:

- *OS/390 UNIX System Services Planning*

Application Identity Mapping

Description

Application identity mapping provides an improved method for associating identities defined by OS/390 UNIX, Lotus Notes for OS/390, and Novell Directory Services for OS/390 applications to RACF user IDs. A new utility, IRRIRA00, replaces the UNIXMAP, NOTELINK and NDSLINK mapping profiles with alias index entries, which require less space on the RACF database. Updates to the ADDUSER and ALTUSER commands will prevent you from associating application user identities for Lotus Notes for OS/390 and Novell Directory Services for OS/390 with more than one RACF user ID.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	None.
Auditing	None.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Commands” on page 57, “Data Areas” on page 61, “Database Templates” on page 64, “Macros” on page 68,“Messages” on page 71, “SYS1.SAMPLIB Members” on page 75, and “Utilities” on page 77.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if your installation uses the specified exits or macros.

Task	Condition	Reference Information
You should not migrate directly to the improved application identity mapping support; follow the conversion process described in *OS/390 SecureWay Security Server RACF System Programmer's Guide* to implement this support. Ensure that you run the IRRMIN00 utility with PARM=UPDATE; do NOT run IRRMIN00 with PARM=NEW.	Required	*OS/390 SecureWay Security Server RACF System Programmer's Guide*

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 UNIX System Services Planning*
- *OS/390 SecureWay Security Server RACF Callable Services*

Application Identity Mapping

- *OS/390 SecureWay Security Server RACF Macros and Interfaces*
- *OS/390 SecureWay Security Server RACF Data Areas*
- *OS/390 SecureWay Security Server RACF Diagnosis Guide*
- *OS/390 SecureWay Security Server RACF Messages and Codes*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*
- *OS/390 SecureWay Security Server RACF System Programmer's Guide*

For more information about OS/390 UNIX, refer to:

- *OS/390 UNIX System Services Planning*

Enhanced PassTicket Support

Description

With enhanced PassTicket support, the security administrator can enter the `NO REPLAY PROTECTION` text string in the APPLDATA field of the PTKTDATA RACF general resource class profile to bypass PassTicket replay protection. Once the replay protection is bypassed, shared user IDs can be allowed access to the same application (such as CICS) at the same time.

Attention

The option to bypass replay protection should only be used in secure environments where access to generated PassTickets is limited within a secure or internal network.

PassTicket support was also enhanced for determining the application name during TSO signon PassTicket evaluation. With this support, RACF checks for a VTAM generic resource name for the particular TSO application environment. If a generic resource name exists, RACF uses that name for the PassTicket evaluation process. See the *OS/390 SecureWay Security Server RACF Security Administrator's Guide* for complete details.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	If you use a RACF SAF exit to handle a VTAM generic resource name for TSO, verify that the exit still performs as intended.
Auditing	None.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to "Commands" on page 57.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*
- *OS/390 SecureWay Security Server RACF System Programmer's Guide*
- *OS/390 SecureWay Security Server RACF Command Language Reference*

Public Key Certificate Enhancements

Description

These updates expand RACF's support of digital certificates. Updates to the initACEE (IRRSIA00) and R_datalib (IRRSDL00) callable services enable RACF to perform these additional functions:

- Registering and deregistering user certificates
- Replacing certificate-authority certificates
- Supporting hostIDMapping extensions
- Extracting private keys
- Managing certificate serial numbers

The new R_PKIServ (IRRSPX00) callable service is added with RACF APAR number OW45211 and SAF APAR number OW45212. IRRSPX00 can be used by applications, such as web servers and their clients, to request the generation and retrieval of X.509 V.3 certificates.

The RACDCERT ALTER, EXPORT, GENCERT, GENREQ and ADD commands have been updated for this support.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	CONTROL authority to the IRR.DIGTCERT.GENCERT resource in the FACILITY class allows a server to retrieve the private keys of CERTAUTH and SITE certificates. READ authority to the IRR.HOST.<*host-name*> resource in the SERVAUTH class allows a server to accept client logins for the host name specified in the resource name. READ authority to the IRR.RADMIN.<*command-name*> resource in the FACILITY class allows a problem state program to execute the RACF TSO command *command-name* using the R_Admin SAF (IRRSEQ00) callable service. Sufficient authority to the IRR.RPKISERV.<*function*> resource in the FACILITY class allows applications, such as web servers and their clients, to request generation and retrieval of X.509 V.3 certificates using the R_PKIServ callable service (IRRSPX00). See *OS/390 SecureWay Security Server RACF Security Administrator's Guide* for information about authorizing servers and clients to use IRRSPX00.
Application Development	None.

Area	Considerations
Auditing	The SMF unload utility (IRRADU00) audits the following: • New extensions that mark the certificate authorities as highly trusted (HIGHTRUST) on the ALTNAME and KEYUSAGE keywords • Certificates exported in a PKCS#12 format (PKCS12DER) on the RACDCERT command. Additional diagnostic information for RACDCERT invoked ICHEINTY ALTER, RACROUTE REQUEST=EXTRACT, and RACROUTE REQUEST=DEFINE failures will be displayed when DEBUG is specified on the RACDCERT command.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Callable Services” on page 53, “Commands” on page 57, “Data Areas” on page 61, “Panels” on page 71, and “Utilities” on page 77.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if your installation uses the specified exits or macros.

Task	Condition	Reference Information
Examine existing profiles and verify that they meet your security requirements.	Required	

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF System Programmer’s Guide*
- *OS/390 SecureWay Security Server RACF Macros and Interfaces*
- *OS/390 SecureWay Security Server RACF Data Areas*
- *OS/390 SecureWay Security Server RACF Diagnosis Guide*
- *OS/390 SecureWay Security Server RACF Messages and Codes*
- *OS/390 SecureWay Security Server RACF Security Administrator’s Guide*
- *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*
- *OS/390 SecureWay Security Server RACF Callable Services*

Enhanced OS/390 UNIX Superuser Granularity Support

Description

This enhanced support verifies that an OS/390 UNIX user has the necessary privilege to perform a chmount. OS/390 UNIX checks the authority information by calling the check privilege (ck_priv) callable service (IRRSKP00), which determines if the user requesting the chmount has superuser privileges, or the authority to the appropriate resource in the UNIXPRIV class.

Note: This support is available on OS/390 Version 2 Release 9 with APAR OW39896 applied.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	The ck_priv callable service (IRRSKP00) checks authority to the SUPERUSER.FILESYS.MOUNT resource in the UNIXPRIV class if a user does not have superuser authority. UPDATE authority is required for chmount when `setuid` is specified; READ authority is required when `setuid` is not specified.
Application Development	None.
Auditing	An SMF TYPE 80 record with a ck_priv event code is written when an authorization check is requested to find users with superuser privileges.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Data Areas” on page 61.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Auditor’s Guide*
- *OS/390 SecureWay Security Server RACF Data Areas*

For more information about OS/390 UNIX, see the following publications:

- *OS/390 UNIX System Services Command Reference*
- *OS/390 UNIX System Services Planning*

Release FMID Update

Description

The RACF and SAF mapping macros have been updated with constants to indicate the new FMID. For compatibility with previous releases, the FMID HRF7703 is used as the RACF level, and is represented by the value 7703. The RACROUTE, ICHEINTY, ICHETEST and ICHEACTN macros have also been updated to accept the RELEASE=7703 parameter.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	If you specify RELEASE=7703 on the RACROUTE macro, you must assemble the application on a system that is running OS/390 V2R10. Also, if the application contains any other keywords on the RACROUTE macro that require RELEASE=7703, you must execute the application on an OS/390 V2R10 system. However, you do not have to update or reassemble existing programs that specify a previous RACF level on the RELEASE= operand. The TSO/E CLIST variable &SYSLRACF and TSO/E REXX SYSVAR(SYSLRACF) functions return 7703 as the RACF release.
Auditing	SMF records written by RACF will indicate the new FMID value.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Data Areas” on page 61, “Macros” on page 68, and “SMF Records” on page 73.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Data Areas*
- *OS/390 SecureWay Security Server RACF Diagnosis Guide*
- *OS/390 SecureWay Security Server RACF Macros and Interfaces*
- *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*

For more information about the TSO/E functions that return this information, refer to the following publications:

- *OS/390 TSO/E CLISTs*
- *OS/390 TSO/E REXX Reference*

Service Updates

Description

Note: This section describes changes from authorized program analysis reports (APARs) or other service updates that have also been incorporated into this release.

- APAR OW39128 provides new entries in the SMF record; the library name (the partitioned data set containing the program) and the volume serial. The additional information makes program control much easier to audit. Use the RACF SMF data unload utility (IRRADU00) or the SYS1.SAMPLIB members IRRADUTB and IRRADULD to view this information.
- APAR OW38799 includes the LIST operand in the SMF Type 80 record as one of the options specified on the SETROPTS command.
- APAR OW39279 checks for programs invoking a RACROUTE REQUEST=DEFINE with the EXPDT keyword (which only allows a date range of 1900–1999) and issues a warning that the keyword EXPDTX (which allows a date range of 2000–2155) should be used instead.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	None.
Auditing	Library and volume serial information are added to the SMF record whenever an attempt is made to load a controlled program. The LIST option, when specified on the SETROPTS command, is included in the SMF Type 80 record.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “SMF Records” on page 73.

Migration Procedures

The following migration tasks are associated with these service enhancements. An **optional** task need only be performed if you implement the indicated function.

Task	Condition	Reference Information
Examine any applications that use the RACROUTE REQUEST=DEFINE macro with the EXPDT keyword.	Optional	*OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*

For More Information

For more detailed information about these updates, refer to the RACF following publications:

- *OS/390 SecureWay Security Server RACF Callable Services*

- *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*

Service Updates

Chapter 4. Version 2 Release 8.0 Overview

The following sections describe the new and changed RACF functions that are introduced for OS/390 Version 2 Release 8 (V2R8). The information about each item includes:

- Description
- Summary of the RACF tasks or interfaces that might be affected
- Coexistence considerations, if any, that are associated with the item
- Migration procedures, if any, that are associated with the item
- References to other publications that contain additional detailed information

Release Summary

Table 5 summarizes the updates that have been introduced to RACF in OS/390 Version 2 Release 8 (OS/390 V2R8). For more information, refer to the detailed section for each item.

Table 5. Summary of RACF Updates for OS/390 Version 2 Release 8

For Information About:	Refer to Page:
Class Descriptor Table Enhancements	30
DB2 Support	33
ICETOOL Support	35
Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support	36
OS/390 UNIX Superuser Granularity	38
OS/390 UNIX User Limits	40
Protected User ID	42
Public Key Certificate Enhancements	44
R_admin SETROPTS Support	48
Release FMID Update	49
Service Updates	50

Class Descriptor Table Enhancements

Description

The RACF class descriptor table (CDT) has been updated to provide additional support for the following program products:

- CICS Transaction Server

  The SCICSTST and UCICSTST classes can now support resource (profile and member) names that contain up to 25 characters. This support enables CICS to enhance its support of temporary storage queues in a sysplex; you can specify longer and more meaningful resource names for CICS regions.
- OS/390 SecureWay Communication Server

  The new SERVAUTH class provides improved security for TN3270 access to OS/390 systems. OS/390 SecureWay Communication Server can use the SERVAUTH class to perform authorization checks and determine if specific users can connect to servers using specific communication ports.
- Java for OS/390

  The new JAVA class has been created to enable Java for OS/390 applications to define and check access to application-specific resources.

What This Change Affects

This support might affect the following areas of RACF processing.

Note: The following considerations are also applicable to any installation-defined classes that are based on the updated SCICSTST and UCICSTST classes. If your installation-defined classes do not support the longer resource names, no additional migration actions are required.

Area	Considerations
Administration	Incompatibilities might occur between systems that share the RACF database, if the CDT on each system has not been updated with the class changes. See “Coexistence Considerations” on page 31 for more information.
Application Development	Programs that use the following operand combinations on the RACROUTE or ICHEINTY macros might experience problems if the buffer specified for ENTITYX or ENTITY is too small to contain the larger resource names that are possible for the SCICSTST and UCICSTST classes: • RACROUTE REQUEST=EXTRACT – ENTITYX – TYPE=EXTRACTN or TYPE=EXTRACT with MATCHGN=YES • ICHEINTY – ENTITYX – NEXT or NEXTC • RACROUTE REQUEST=EXTRACT – ENTITY – TYPE=EXTRACTN
Auditing	SMF records and IRRADU00 output records might contain longer SCICSTST and UCICSTST member, profile, and resource names. They might also refer to the new JAVA and SERVAUTH classes.
Customization	Installation-defined exits that process requests for the SCICSTST or UCICSTST classes might need to be updated to support the longer names.

Area	Considerations
General User	None.
Operations	None.
Interfaces	Refer to “Class Descriptor Table” on page 56 and “Data Areas” on page 61.

Coexistence Considerations

If your installation shares the RACF database between a system with the changed SCICSTST or UCICSTST class descriptor table definitions (an “up-level” system) and any system without the changed definitions (a “lower-level” system), you should review the following considerations:

- Do not define profiles or members that use the longer names, if the classes have been made active by the SETROPTS CLASSACT command. You should not experience problems unless you have defined profiles or members with the longer names.
- Do not use RACF remote sharing to manually or automatically direct commands to a lower-level system, if the commands reference an SCICSTST or UCICSTST profile or member with the longer name. The command will work on the local system but will fail on the target system.
- Do not have the RACGLIST function active for either of the changed classes. RACGLIST shares RACLISTed profiles between classes that share the database. Because the SCICSTST and UCICSTST classes can support longer resource names, the RACLISTed profiles are not compatible across the systems. You must ensure that you have not issued either of the following commands:
  - SETROPTS CLASSACT(RACGLIST)
  - RDEFINE RACGLIST *class_name* for the SCICSTST or UCICSTST class

  If you have issued the SETROPTS CLASSACT(RACGLIST) command and have also issued the RDEFINE RACGLIST command for one of these classes, you should issue one of the following commands:
  - RDELETE RACGLIST *class_name* for each affected class (the preferred method)
  - SETROPTS NOCLASSACT(RACGLIST)

Also, on a lower-level system, the RACF utilities would be able to process a database that contained the names for the SCICSTST and UCICSTST classes. However, due to the longer names, you can not issue the commands that are generated by IRRRID00 on the lower-level system.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if your installation uses the specified exits or macros.

Task	Condition	Reference Information
Ensure the names of any installation-defined classes do not conflict with the names of the new classes that are supplied by IBM.	Required	“Checking for Duplicate Class Names” on page 5

CDT Enhancements

Task	Condition	Reference Information
Review the following exits to ensure that they can support CICS resource names that contain 25 characters: • SAF router exit (ICHRTX00) • RACROUTE REQUEST=FASTAUTH (ICHRFX01 - ICHRFX04) • RACROUTE REQUEST=AUTH (ICHRCX01 and ICHRCX02)	Optional	*OS/390 SecureWay Security Server RACF System Programmer's Guide*
Review applications to ensure the buffer specified on the ENTITYX operand of the ICHEINTY or RACROUTE REQUEST=EXTRACT macros can support the larger CICS resource names.	Optional	*OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*
Review applications to ensure the buffer specified on the ENTITY operand of the RACROUTE REQUEST=EXTRACT macro can support the larger CICS resource names.	Optional	*OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Command Language Reference*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*
- *OS/390 SecureWay Security Server RACF System Programmer's Guide*
- *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*

DB2 Support

Description

RACF introduces eight new classes, which support the following types of DB2 Version 6 objects:

- User-defined distinct types
- User-defined functions
- Schemas
- Stored procedures

The RACF/DB2 external security module (IRR@XACS) has also been updated to map access requests for these DB2 objects and privileges into the new RACF classes.

The RACF/DB2 external security module also supports TRIGGER, which is a new DB2 Version 6 privilege to control the ability to create a trigger on a table.

The eight new classes that support the new DB2 Version 6 objects are supplied with OS/390 Version 2 Release 8. However, the additional support provided by the RACF/DB2 external security module (IRR@XACS) is available with APAR OW38710.

In addition, implicit ownership of a PLAN or PACKAGE (which are objects that were included in the RACF support for DB2 Version 5) now allows a user some, but not all, of the privileges that are associated with these objects. A list of the objects and associated privileges follows:

Object	Privilege Required
PLAN	BINDAUT
PACKAGE	BINDAUT and COPYAUT

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	None.
Auditing	None.
Customization	The IRR@XACS sample exit routine that is supplied with RACF has been updated to support the new DB2 objects and privilege.
General User	None.
Operations	None.
Interfaces	Refer to “Class Descriptor Table” on page 56, “Exits” on page 67, and “SYS1.SAMPLIB Members” on page 75.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if you choose to implement this function.

DB2 Support

Task	Condition	Reference Information
Ensure the names of any installation-defined classes do not conflict with the names of the new classes that are supplied by IBM.	Required	"Checking for Duplicate Class Names" on page 5
Define RACF profiles for the new DB2 objects; otherwise, the RACF/DB2 external security module will not be active when you start DB2.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*
Assemble and install the sample exit code that is supplied with RACF in the SAMPLIB member IRR@XACS.	Optional	*OS/390 SecureWay Security Server RACF System Programmer's Guide*
Stop and restart your DB2 subsystem to use the RACF/DB2 external security module.	Optional	*OS/390 SecureWay Security Server RACF System Programmer's Guide*

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Macros and Interfaces*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*
- *OS/390 SecureWay Security Server RACF System Programmer's Guide*

For more information about DB2, see the following publications:

- *DB2 Administration Guide*
- *DB2 Command Reference*

ICETOOL Support

Description

The DFSORT program product provides a reporting facility called ICETOOL. With this support, you can now create ICETOOL reports, based on the output files from the RACF database unload utility (IRRDBU00) or the SMF data unload utility (IRRADU00). The SYS1.SAMPLIB member IRRICE contains the DFSORT statements that are needed to select records. It also contains the ICETOOL statements to produce and format a variety of reports.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	None.
Auditing	You can use this support to generate additional types of auditing reports, which are based on the output of the RACF database unload utility (IRRDBU00) and the SMF data unload (IRRADU00) utility.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “SYS1.SAMPLIB Members” on page 75.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Auditor’s Guide*
- *OS/390 SecureWay Security Server RACF Security Administrator’s Guide*

For more information about DFSORT and ICETOOL statements, refer to the following publications:

- *DFSORT Application Programming Guide R14*
- *DFSORT Getting Started R14*

Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support

Description

This enhancement enables RACF to map a user identity from a Lotus Notes for OS/390 or Novell Directory Services for OS/390 application to a RACF user ID. The new callable service, IRRSIM00 (R_usermap), provides user identity mapping functions. After the application has determined a user's RACF user ID, it may then choose to use this user ID when accessing MVS resources, such as data sets, and OS/390 UNIX System Services (OS/390 UNIX) files. As such, existing OS/390 UNIX functions, resources, and operating system security can be maintained while application servers are consolidated.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	User IDs might need to be defined for the applications. In addition, these user IDs will need to be granted READ access to the IRR.RUSERMAP resource in the FACILITY class.
Application Development	None.
Auditing	Additional fields (for the LNOTES and NDS segments) will be displayed in the Type 44 relocate sections of the Type 80 records that produced for the ADDUSER and ALTUSER commands.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to "Callable Services" on page 53, "Class Descriptor Table" on page 56, "Commands" on page 57, "Data Areas" on page 61, "Database Templates" on page 64, "Messages" on page 71, "Panels" on page 71, "SYS1.SAMPLIB Members" on page 75, and "Utilities" on page 77.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if you choose to implement this function.

Task	Condition	Reference Information
Run the IRRMIN00 utility.	Required	"Updating RACF Templates" on page 4
Run the dynamic parse utility.	Required	"Running Dynamic Parse" on page 4
Define a user ID for the application.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*

Task	Condition	Reference Information
Give the user ID that is associated with the application READ access to the IRR.RUSERMAP resource in the FACILITY class.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Callable Services*
- *OS/390 SecureWay Security Server RACF Command Language Reference*
- *OS/390 SecureWay Security Server RACF General User's Guide*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*
- *OS/390 SecureWay Security Server RACF System Programmer's Guide*

OS/390 UNIX Superuser Granularity

Description

This support introduces the new UNIXPRIV class, which enables you to define profiles that grant RACF authorization for certain OS/390 UNIX privileges. These privileges are automatically defined for all users that are defined with OS/390 UNIX superuser authority. Now, by defining profiles in the UNIXPRIV class, you can specifically grant certain superuser privileges, with a high degree of granularity, to users who do not have superuser authority. With this approach, you can reduce the number of users who have superuser authority at your installation.

In addition, if you define the discrete profile CHOWN.UNRESTRICTED in the UNIXPRIV class, you can enable all OS/390 UNIX users on your system to issue the **chown** command. With this support, these users can then use this command to transfer ownership of their own files to any other OS/390 UNIX user identifier (UID) or OS/390 UNIX group identifier (GID) on the system.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	Users can be granted authority to perform individual OS/390 UNIX superuser functions; they no longer require authority to all superuser functions.
Application Development	None.
Auditing	UNIXPRIV profiles can be used to audit successful uses of superuser functions. Multiple audit records might be produced for the same OS/390 UNIX operations.
Customization	None.
General User	If the administrator has created the UNIXPRIV profile CHOWN.UNRESTRICTED, users can issue the **chown** command to transfer ownership of their own OS/390 UNIX files.
Operations	None.
Interfaces	Refer to “Callable Services” on page 53, “Class Descriptor Table” on page 56, “Data Areas” on page 61, and “Exits” on page 67.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if you choose to implement this function.

Task	Condition	Reference Information
Ensure the name of any installation-defined class does not conflict with the name of the new class that is supplied by IBM.	Required	“Checking for Duplicate Class Names” on page 5
Create the required profiles in the UNIXPRIV class (such as, SUPERUSER.* and CHOWN.UNRESTRICTED).	Optional	*OS/390 SecureWay Security Server RACF Security Administrator’s Guide*

Task	Condition	Reference Information
Activate and RACLIST the UNIXPRIV class.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*
Remove superuser authority from any user ID that no longer requires it.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Auditor's Guide*
- *OS/390 SecureWay Security Server RACF Callable Services*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*

For more information about OS/390 UNIX, see the following publications:

- *OS/390 UNIX System Services Command Reference*
- *OS/390 UNIX System Services Planning*

OS/390 UNIX User Limits

Description

With this support, you can control the amount of system resources that are consumed by individual OS/390 UNIX users. Resource limits for most OS/390 UNIX users are determined by the BPXPRMxx member of the PARMLIB. Using the ADDUSER and ALTUSER commands, you can specify and adjust the following limits, which are stored in the OMVS segment of the user profile:

- CPUTIMEMAX
- ASSIZEMAX
- FILEPROCMAX
- PROCUSERMAX
- THREADSMAX
- MMAPAREAMAX

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	The OMVS segment of individual users might need to be updated if their OS/390 UNIX system requirements differ from the system-defined defaults.
Application Development	The changes to the SMF records and the SMF data unload records are compatible with lower-level systems. However, programs that are sensitive to the length of the data returned might be affected by the increase in size of the unloaded SMF Type 80 data.
Auditing	Additional OS/390 UNIX fields will be displayed in the Type 44 relocate sections of the Type 80 records that are produced for the ADDUSER and ALTUSER commands.
Customization	None.
General User	None.
Operations	TSO message IKJ56702I will be issued if you do not specify a valid value for the OS/390 UNIX limits.
Interfaces	Refer to “Callable Services” on page 53, “Commands” on page 57, “Data Areas” on page 61, “Database Templates” on page 64, “Panels” on page 71, “SYS1.SAMPLIB Members” on page 75, and “Utilities” on page 77.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if you choose to implement this function.

Task	Condition	Reference Information
Run the IRRMIN00 utility.	Required	“Updating RACF Templates” on page 4
Run the dynamic parse utility.	Required	“Running Dynamic Parse” on page 4

Task	Condition	Reference Information
Identify any user IDs with OS/390 UNIX system requirements that differ from the system-defined defaults.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*
Remove superuser authority from any user ID that no longer requires it.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Callable Services*
- *OS/390 SecureWay Security Server RACF Command Language Reference*
- *OS/390 SecureWay Security Server RACF General User's Guide*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*

For more information about setting OS/390 UNIX limits, see *OS/390 UNIX System Services Planning*.

Protected User ID

Description

This support allows you to define RACF user IDs that cannot be used for activities such as logging on to TSO or signing on to CICS. A user ID becomes a protected user ID when it is given the NOPASSWORD and NOOIDCARD attributes by an ADDUSER or ALTUSER command. The user IDs that are defined for OS/390 UNIX, OS/390 UNIX daemons, and other important subsystems or started tasks can be protected from being used for other purposes. These user IDs can also be protected from being revoked after several unsuccessful attempts to enter a password. This support protects these user IDs from being misused if the RACF administrator does not change the password of the user ID from the default group to a more secure value.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	Determine which user IDs are required to be protected. IBM recommends that you assign a protected user ID to the RACF subsystem.
Application Development	Applications that check the FLAG7 field in the user profile might have to be updated to process the new bit values. Applications that process output from the IRRDBU00 utility might need to be updated to support the new value (“PRO”) that might be returned by the utility.
Auditing	None.
Customization	None.
General User	None.
Operations	Message ICH01002I will no longer be issued if the OIDCARD parameter is not specified with the NOPASSWORD parameter on the ADDUSER command. For the ALTUSER command, message ICH21007I is no longer issued for the following cases: • NOOIDCARD and NOPASSWORD operands are both in effect (a protected user ID is created) • NOOIDCARD is specified while NOPASSWORD is in effect • NOPASSWORD is specified while NOOIDCARD is in effect
Interfaces	Refer to “Commands” on page 57, “Data Areas” on page 61, “Database Templates” on page 64, “Macros” on page 68, “Messages” on page 71, “Panels” on page 71, and “Utilities” on page 77.

Coexistence Considerations

A protected user ID that is created on a OS/390 V2R8 system could also be used as a system user ID on any lower level systems that share the OS/390 V2R8 RACF database. On the lower level systems, however, the user ID will not be considered a protected user ID; it might still be revoked by malicious or careless users entering incorrect passwords.

If a LISTUSER command is issued on the lower level system, it will not indicate that this is a protected user ID. If the database unload utility is run from the lower level system, the USBD_NOPWD field will also indicate that this user ID is not protected. Also, if the protected user ID was created using ADDUSER or ALTUSER on the OS/390 V2R8 system, do not issue ALTUSER commands for this user on the lower level system that specify the PASSWORD/NOPASSWORD or OIDCARD/NOOIDCARD operands.

Migration Procedures

The following migration tasks are associated with this enhancement. An **optional** task need only be performed if you choose to implement this function.

Task	Condition	Reference Information
Define a protected user ID for the RACF subsystem. If you have already defined a user ID for the RACF subsystem, use the ALTUSER command to define protect attributes for that user ID.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide* *OS/390 SecureWay Security Server RACF Command Language Reference*
Identify any other user IDs that you might need to define, or alter, as protected user IDs.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*
Review any applications that check the FLAG7 field in the user profile; they should be able to process the new bits that are added to this field.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Command Language Reference*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*
- *OS/390 SecureWay Security Server RACF System Programmer's Guide*
- *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*

Public Key Certificate Enhancements

Description

These updates expand RACF's support of digital certificates and Open Cryptographic Enhanced Plug-ins (OCEP), which is a component of the OS/390 Security Server. Updates to the RACDCERT command and the new DIGTRING class and IRRSDL00 callable service enable RACF to perform additional functions, including:

- Generating certificates and private keys for server applications
- Processing certificate requests that were generated elsewhere
- Providing support for the OCEP Data Storage Library and Trust Policy service provider modules, which are designed to be used with Open Cryptographic Services Facility (OCSF).

This support also introduces the irrcerta and irrsitec user IDs. These user IDs are defined in profiles that are supplied with RACF and they cannot be defined by your installation. The user IDs anchor certificate authority and site certificates. User certificates that are added by specifying the CERTAUTH option of the RACDCERT ADD command are associated with the irrcerta user ID. User certificates that are added by specifying the SITE option of the RACDCERT ADD command are associated with the irrsitec user ID.

Combined, these enhancements enable RACF to function as a limited certificate authority. RACF can accept certificate requests and sign those certificate requests with a certificate authority that is managed by RACF.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	To perform certain functions of the RACDCERT command, a user must be authorized to access IRR.DIGTCERT.*function* resources in the FACILITY class. The DELUSER command can be used to delete any key rings that are associated with a user; you do not need to issue the RACDCERT command to delete the key rings that are associated with a user ID. Do not delete the irrcerta or irrsitec user IDs; otherwise, information about the corresponding certificates will be deleted from your system. If you re-IPL your system, RACF automatically re-creates these user IDs; however, it might not be able to recover all of the information about the certificates.

Area	Considerations
Application Development	Attempts to specify the new irrcerta or irrsitec user IDs on the RACROUTE REQUEST=VERIFY macro will fail; an audit record and console message will be produced. The automatic direction of application updates (ADAU) function of RACF's remote sharing facility (RRSF) has been updated as follows: • Private key information is not propagated to remote RACF databases. • Changes to user profiles that were made as a result of a digital certificate being updated are controlled by AUTODIRECT profiles for the DIGTCERT class, instead of by AUTODIRECT profiles for the USER class. • Digital certificate additions and updates are controlled by AUTODIRECT profiles for the DIGTCERT and DIGTRING classes. The Type 6 relocation section of the RACDCERT command has been updated.
Auditing	None.
Customization	None.
General User	None.
Operations	The RACDCERT ADD command cannot be used to change the label that is associated with a digital certificate. Instead, you should use the NEWLABEL keyword of the RACDCERT ALTER command. The irrcerta and irrsitec user IDs might appear in the responses from the SEARCH CLASS(USER) and LISTUSER commands.
Interfaces	Refer to "Callable Services" on page 53, "Class Descriptor Table" on page 56, "Commands" on page 57, "Data Areas" on page 61, "Database Templates" on page 64, "Macros" on page 68, "Messages" on page 71, "Panels" on page 71, "SMF Records" on page 73, "SYS1.SAMPLIB Members" on page 75, and "Utilities" on page 77.

Coexistence Considerations

If your OS/390 V2R8 (an "up-level" system) installation shares the RACF database between "lower-level" systems, you should review the following considerations:

- To ensure that profile information is synchronized across the systems:
  - All RACDCERT commands must be issued from the up-level system.
  - All DELUSER commands that specify a user ID that has associated certificates or key rings must be issued from the up-level system
- If you run the IRRRID00 utility on a lower-level system against the IRRDBU00 output from an up-level system, IRRRID00 will generate RALTER commands that attempt to change the owner of the default certificate authority profiles. You should edit the IRRRID00 output to remove these commands.

Migration Procedures

The following migration tasks are associated with this enhancement. A **required** task must be performed regardless of whether you implement this function at your installation. An **optional** task need only be performed if you choose to implement this function.

Public Key Certificate Enhancements

Task	Condition	Reference Information
Run the IRRMIN00 utility.	Required	"Updating RACF Templates" on page 4
Run the dynamic parse utility.	Required	"Running Dynamic Parse" on page 4
Ensure the name of any installation-defined class does not conflict with the name of the new class that is supplied by IBM.	Required	"Checking for Duplicate Class Names" on page 5
Determine the type of access users require to perform specific functions of the RACDCERT command; authorize the users to access the appropriate IRR.DIGTCERT.*function* resources in the FACILITY class.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide* *OS/390 SecureWay Security Server RACF Command Language Reference*
If your installation uses an RRSFDATA profile to control the automatic direction of application updates for the DIGTCERT class (for example, AUTODIRECT.*target-node*.DIGTCERT.APPL), create a new RRSFDATA profile for the DIGTCERT and DIGTRING classes (for example, AUTODIRECT.*target-node*.DIGT*.APPL). Then, delete the profile AUTODIRECT.*target-node*.DIGTCERT.APPL. This will ensure consistent propagation across these classes.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*
Examine your RRSFDATA profiles that control the automatic direction of application updates for the USER class. You might need to adjust the access lists on your RRSFDATA profiles. Before OS/390 V2R8, any updates in the USER class that were related to digital certificates were propagated based on the RRSFDATA profile AUTODIRECT.*target-node*.USER.APPL. Now, profile AUTODIRECT.*target-node*.DIGTCERT.APPL is the basis for propagating these USER class updates.	Optional	*OS/390 SecureWay Security Server RACF Security Administrator's Guide*

For More Information

For more detailed information about this support in RACF, refer to the following publications:

- *OS/390 SecureWay Security Server RACF Callable Services*
- *OS/390 SecureWay Security Server RACF Command Language Reference*
- *OS/390 SecureWay Security Server RACF Macros and Interfaces*
- *OS/390 SecureWay Security Server RACF Messages and Codes*
- *OS/390 SecureWay Security Server RACF Security Administrator's Guide*
- *OS/390 SecureWay Security Server RACF System Programmer's Guide*

For more information about the OCEP component of the OS/390 Security Server, refer to *OS/390 SecureWay Security Server Open Cryptographic Enhanced Plug-ins Guide and Reference*.

For more detailed information about OCSF support, refer to the following publications:

- *OS/390 Open Cryptographic Services Facility Application Developer's Guide and Reference*
- *OS/390 Open Cryptographic Services Facility Service Provider Module Developer's Guide and Reference*

R_admin SETROPTS Support

Description

With this enhancement, you can use the R_admin callable service (IRRSEQ00) to set (alter) and retrieve RACF SETROPTS information. The R_admin callable service can be used by any application that is running in supervisor state and key 0. Information can be retrieved in two formats. One format is equivalent to the format of the data supplied on the alter request; the other format returns the data as a series of SMF data unload output records.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	The changes to the SMF records and the SMF data unload records are compatible with lower level systems. However, programs that are sensitive to the length of the data returned might be affected by the increased size of the unloaded SMF Type 81 data.
Auditing	The SMF Type 81 record has been updated. The SMF81BOX field contains new indicators relating to the RVARY SWITCH and RVARY STATUS passwords in effect. The Type 81 basic data record (RACFINIT) now provides data from relocate section 32 (X'20') at the end of the record mapping. Also, two fields are added to indicate the settings of the RVARY SWITCH and RVARY STATUS passwords in effect.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Callable Services” on page 53, “Data Areas” on page 61, “SMF Records” on page 73, “SYS1.SAMPLIB Members” on page 75, and “Utilities” on page 77.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Callable Services*
- *OS/390 SecureWay Security Server RACF Data Areas*
- *OS/390 SecureWay Security Server RACF Macros and Interfaces*

Release FMID Update

Description

The RACF and SAF mapping macros have been updated with constants to indicate the new FMID. For compatibility with previous releases, the FMID HRF2608 is used as the RACF level, and is represented by the value 2608. The RACROUTE, ICHEINTY, ICHETEST and ICHEACTN macros have also been updated to accept the RELEASE=2608 parameter.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	If you specify RELEASE=2608 on the RACROUTE macro, you must assemble the application on a system that is running OS/390 V2R8. Also, if the application contains any other keywords on the RACROUTE macro that require RELEASE=2608, you must execute the application on an OS/390 V2R8 system. However, you do not have to update or reassemble existing programs that specify a previous RACF level on the RELEASE= operand. The TSO/E CLIST variable &SYSLRACF and TSO/E REXX SYSVAR(SYSLRACF) functions return 2608 as the RACF release.
Auditing	SMF records written by RACF will indicate the new FMID value.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Data Areas” on page 61, “Macros” on page 68, and “SMF Records” on page 73.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

For more detailed information about this support, refer to the following RACF publications:

- *OS/390 SecureWay Security Server RACF Data Areas*
- *OS/390 SecureWay Security Server RACF Diagnosis Guide*
- *OS/390 SecureWay Security Server RACF Macros and Interfaces*
- *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*

For more information about the TSO/E functions that return this information, refer to the following publications:

- *OS/390 TSO/E CLISTs*
- *OS/390 TSO/E REXX Reference*

Service Updates

Description

Note: This section describes changes from authorized program analysis reports (APARs) or other service updates that have also been incorporated into this release.

- APAR OW33566 provides updates that enable RACF to support the services provided by the NOSECURITY operand of the OS/390 UNIX MOUNT command. The following RACF callable services have been updated to recognize, and accept, the security credentials of a system caller (a CRED with a user type of system):
  - IRRSCA00 (R_chaudit)
  - IRRSCS00 (clear_setid)
  - IRRSMF00 (make_fsp)
- APAR OW34996 changed how RACROUTE REQUEST=FASTAUTH, in non-cross memory invocations and with no ACEEALET or ENVRIN parameter specified, locates the profile that protects a resource for classes that were RACLISTed by the RACROUTE REQUEST=LIST, GLOBAL=YES macro. If the caller is in system key (0-7) or supervisor state, RACF first tries to use the ACEE= parameter to find the RACLISTed profiles. If no input ACEE is specified or the caller is not in system key (0-7) or in supervisor state, RACF tries the task ACEE (TCBSENV) pointer in the TCB. If there is no TCB (which is the case for SRB mode) or if the task ACEE pointer is zero, RACF uses the main ACEE for the address space.
- APAR OW36832 changes the format in which dates that are extracted from uninitialized data fields in the RACF database are reported. When the DATEFMT=YYYYDDDF operand is specified with TYPE=EXTRACT or TYPE=EXTRACTN operands, the ICHEINTY and RACROUTE REQUEST=EXTRACT macros will return the values 0000000F or FFFFFFFF.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	Customers should investigate any applications that utilize RACROUTE REQUEST=FASTAUTH for a possible impact.
Auditing	None.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Callable Services” on page 53 and “Macros” on page 68.

Migration Procedures

The following migration tasks are associated with these service enhancements. An **optional** task need only be performed if you implement the indicated function.

Task	Condition	Reference Information
Examine any applications that use the RACROUTE REQUEST=FASTAUTH macro.	Optional	*OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*

For More Information

For more detailed information about these updates, refer to the RACF following publications:

- *OS/390 SecureWay Security Server RACF Callable Services*
- *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*

For more information about the OS/390 UNIX MOUNT command, refer to the *OS/390 UNIX System Services Command Reference*.

Service Updates

Chapter 5. Summary of Interface Changes

This section summarizes the new and changed interface components of RACF.

Callable Services

Table 6 lists the new and updated callable services. See *OS/390 SecureWay Security Server RACF Callable Services* for more detailed information.

Table 6. Summary of New and Changed Callable Services

Callable Service Name	Release	Description	Related Support
IRRSCA00	V2R8	Updated to accept a CRED with a user type of system.	Service Updates (APAR OW33566)
IRRSCI00	V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	OS/390 UNIX Superuser Granularity
IRRSCO00	V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	OS/390 UNIX Superuser Granularity
IRRSCS00	V2R8	Updated to accept a CRED with a user type of system.	Service Updates (APAR OW33566)
IRRSC200	V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	OS/390 UNIX Superuser Granularity
IRRSDL00	V2R10	Updated to extract private keys and to manage certificate serial numbers.	Public Key Certificate Enhancements
	V2R8	**New:** the R_datalib callable service supports the data library functions that are provided by Open Cryptographic Enhanced Plug-ins.	Public Key Certificate Enhancements

Table 6. Summary of New and Changed Callable Services (continued)

Callable Service Name	Release	Description	Related Support
IRRSEQ00	V2R10	1. **New:** User Administration and General Resource Administration fields were added in support of the SecureWay Security Server Network Authentication and Privacy Service. 2. Updated to support the restricted access attribute in the user base segment. 3. Updated to support public key certificate enhancements.	1. SecureWay Security Server Network Authentication and Privacy Service Support 2. Certificate Name Filtering 3. Public Key Certificate Enhancements
	V2R8	1. Updated to support the LNOTES and NDS segments. 2. Function codes ADMN_ADD_USER, ADMN_ALT_USER, and ADMN_LST_USER have been updated to support the additional fields in the OMVS segment. 3. Updated to support the following function codes that enable RACF SETROPTS information to be listed or changed: ADMN_ALT_SETR, ADMN_XTR_SETR, and ADMN_UNL_SETR	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. OS/390 UNIX User Limits 3. R_admin SETROPTS Support
IRRSFK00	V2R10	Updated to save and restore the following additional security information: controlled status, keep-controlled indicators, and saved messages.	Program Control Enhancements
IRRSIA00	V2R10	1. **New:** X500NAME and VARIABLE_LIST parameters were created in support of certificate name filtering. Updated to provide a new function for APPL_ID. 2. Updated to support public key certificate enhancements.	1. Certificate Name Filtering 2. Public Key Certificate Enhancements
	V2R8	Returns OUSP information that contains the new user limit values specified in the OMVS segment.	OS/390 UNIX User Limits

Table 6. Summary of New and Changed Callable Services (continued)

Callable Service Name	Release	Description	Related Support
IRRSIM00	V2R10	Updated with the ability to • Map local and foreign principals to RACF identities. • Map RACF identities to local principals. For local principals, the RACF USER profile must have a KERB segment containing a principal name; foreign principals must have an explicit KERBLINK profile created.	SecureWay Security Server Network Authentication and Privacy Service Support
	V2R8	**New:** R_usermap enables OS/390 application servers to determine the application user identity associated with a RACF user ID, or to determine the RACF user ID associated with an application user identity or digital certificate.	Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support
IRRSIU00	V2R8	Returns OUSP information that contains the new user limit values specified in the OMVS segment.	Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support
IRRSKA00	V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	OS/390 UNIX Superuser Granularity
IRRSKO00	V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	OS/390 UNIX Superuser Granularity
IRRSKP00	V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	OS/390 UNIX Superuser Granularity
IRRSMF00	V2R8	Updated to accept a CRED with user type of system.	Service Updates (APAR OW33566)
IRRSMK00	V2R10	**New:** The Network Authentication and Privacy Service is the only exploiter of the new R_kerbinfo service.	SecureWay Security Server Network Authentication and Privacy Service Support
IRRSPK00	V2R10	**New:** The R_ticketserv callable service enables OS/390 application servers to parse or extract principal names from the Network Authentication and Privacy Service GSS-API context token.	SecureWay Security Server Network Authentication and Privacy Service Support
IRRSPT00	V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	OS/390 UNIX Superuser Granularity
IRRSPX00	V2R10	**New:** The R_PKIServ callable service enables authorized applications, such as web servers and their clients, to request the generation and retrieval of X.509 V.3 certificates.	Public Key Certificate Enhancements
IRRSQF00	V2R8	Updated to check for the existence of the discrete profile CHOWN.UNRESTRICTED in the UNIXPRIV class.	OS/390 UNIX Superuser Granularity

Class Descriptor Table

Table 7 lists the new and changed classes that are provided in the class descriptor table (CDT), ICHRRCDX, that is supplied by IBM. The class name is part of the programming interface for the ICHEINTY and RACROUTE macros. For more information about these macros, see *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*.

New or changed classes are also reflected in the router table (ICHRFR0X) that IBM supplies. For detailed information, see *OS/390 SecureWay Security Server RACF Macros and Interfaces*.

Table 7. Summary of New and Changed Classes

Class Name	Release	Description	Related Support
DIGTCRIT	V2R10	**New:** maps the additional criteria found through the DIGTNMAP class to a RACF user ID.	Certificate Name Filtering
DIGTNMAP	V2R10	**New:** maps a subject's and/or issuer's distinguished name to a RACF user ID.	Certificate Name Filtering
DIGTRING	V2R8	**New:** contains a profile for each key ring and provides information about the digital certificates that are a part of each key ring.	Public Key Certificate Enhancements
GDSNSC	V2R8	**New:** provides the grouping class for DB2 schemas.	DB2 Support
GDSNSP	V2R8	**New:** provides the grouping class for DB2 stored procedures.	DB2 Support
GDSNUF	V2R8	**New:** provides the grouping class for DB2 user-defined functions.	DB2 Support
GDSNUT	V2R8	**New:** provides the grouping class for DB2 user-defined distinct types.	DB2 Support
JAVA	V2R8	**New:** contains profiles that are used by Java for OS/390 applications to perform authorization checks for Java resources.	Class Descriptor Table Enhancements
KERBLINK	V2R10	**New:** maps principal identities to RACF identities.	SecureWay Security Server Network Authentication and Privacy Service Support
MDSNSC	V2R8	**New:** provides the member class for DB2 schemas.	DB2 Support
MDSNSP	V2R8	**New:** provides the member class for DB2 stored procedures.	DB2 Support
MDSNUF	V2R8	**New:** provides the member class for DB2 user-defined functions.	DB2 Support
MDSNUT	V2R8	**New:** provides the member class for DB2 user-defined distinct types.	DB2 Support
NDSLINK	V2R8	**New:** provides the mapping class for Novell Directory Services for OS/390 user identities.	Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support

Table 7. Summary of New and Changed Classes (continued)

Class Name	Release	Description	Related Support
NOTELINK	V2R8	**New:** provides the mapping class for Lotus Notes for OS/390 user identities.	Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support
REALM	V2R10	**New:** contains registry information about realms.	SecureWay Security Server Network Authentication and Privacy Service Support
SCICSTST	V2R8	Updated to support profile and resource names that contain up to 25 characters. If any applications use the ENTITY operand on the RACROUTE REQUEST=EXTRACT macro to process SCICSTST profiles, you may have to update them to use the ENTITYX operand before you define SCICSTST profile names that contain more than 17 characters.	Class Descriptor Table Enhancements
SERVAUTH	V2R8	**New:** contains profiles that are used by OS/390 SecureWay Communication Server servers to check a client's authorization to use the server itself or the resources managed by the server.	Class Descriptor Table Enhancements
UCICSTST	V2R8	Updated to support profile and resource names that contain up to 25 characters. If any applications use the ENTITY operand on the RACROUTE REQUEST=EXTRACT macro to process UCICSTST profiles, you may have to update them to use the ENTITYX operand before you define UCICSTST profile names that contain more than 17 characters.	Class Descriptor Table Enhancements
UNIXPRIV	V2R8	**New:** contains profiles that are used to grant specific OS/390 UNIX privileges.	OS/390 UNIX Superuser Granularity

Commands

Table 8 on page 58 lists the changes to the RACF commands for this release. See *OS/390 SecureWay Security Server RACF Command Language Reference* for more detailed information about these commands. For information about BLKUPD, refer to *OS/390 SecureWay Security Server RACF Diagnosis Guide*.

Interface Changes

Table 8. Summary of Changed Commands

Command Name	Release	Description	Related Support
ADDUSER	V2R10	1. Updated to support the new keyword RESTRICTED. 2. Updated to support the new keyword KERB, with subkeywords MAXTKTLFE and KERBNAME.	1. Certificate Name Filtering 2. SecureWay Security Server Network Authentication and Privacy Service Support
	V2R8	1. Updated to support the new keywords LNOTES and NDS, and their supporting parameters. 2. Parameters have been added to the OMVS keyword to allow for additional fields to be specified in the OMVS segment of a user ID. 3. The behavior of NOPASSWORD and NOOIDCARD has changed. If both keywords are in effect for a user, a protected user ID will now be created.	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. OS/390 UNIX User Limits 3. Protected User ID
ADDSD	V2R10	UACC keyword updated.	Certificate Name Filtering
ALTDSD	V2R10	UACC keyword updated.	Certificate Name Filtering
ALTUSER	V2R10	1. Updated to support the new keywords RESTRICTED and NORESTRICTED. 2. Updated to support the new keyword KERB, with subkeywords: • KERBNAME • NOKERBNAME • MAXTKTLFE • NOMAXTKTLFE and keyword NOKERB, with subkeywords: • MAXTKTLFE • NOMAXTKTLFE	1. Certificate Name Filtering 2. SecureWay Security Server Network Authentication and Privacy Service Support
	V2R8	1. Updated to support the keywords LNOTES and NDS, and their supporting parameters. 2. Parameters have been added to the OMVS keyword to allow for additional fields to be specified in the OMVS segment of a user ID. 3. The behavior of the NOPASSWORD and NOOIDCARD keywords has changed. If both keywords are in effect for a user, a protected user ID will now be created.	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. OS/390 UNIX User Limits 3. Protected User ID

Table 8. Summary of Changed Commands (continued)

Command Name	Release	Description	Related Support
BLKUPD	V2R8	Updated to allow *entryname* and *string* values to be specified as lower-case or mixed-case characters.	Public Key Certificate Enhancements
DELUSER	V2R10	1. Deletes all DIGTNMAP profiles associated with the user ID being deleted. 2. Deletes KERBLINK profiles if the user has a KERBNAME.	1. Certificate Name Filtering 2. SecureWay Security Server Network Authentication and Privacy Service Support
LISTUSER	V2R10	1. Reports the value RESTRICTED in the attributes it displays. 2. Lists KERB segment data when the KERB keyword is specified.	1. Certificate Name Filtering 2. SecureWay Security Server Network Authentication and Privacy Service Support
	V2R8	1. Updated to support the new LNOTES and NDS keywords. 2. Updated to display additional fields in the OMVS segment for a user ID. 3. Updated to display the PROTECTED attribute, if the user has been defined as a protected user ID.	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. OS/390 UNIX User Limits 3. Protected User ID

Table 8. Summary of Changed Commands (continued)

Command Name	Release	Description	Related Support
RACDCERT	V2R10	Updated to support the following new keywords: • ALTMAP, with subkeywords – NEWCRITERIA – NEWLABEL – TRUST and NOTRUST • DEBUG • DELMAP and LISTMAP, with subkeyword, LABEL • MAP, with subkeywords: – SDNFILTER – IDNFILTER – CRITERIA – WITHLABEL – TRUST and NOTRUST The following keywords have been updated: • ADD, with new subkeyword, HIGHTRUST • ALTER, with new subkeyword, HIGHTRUST • EXPORT, with new subkeywords: – PKCS12DER – PKCS12B64 – PASSWORD • ID/MULTIID • LIST • GENCERT, with new subkeywords: – ALTNAME, with new subkeywords: - DOMAIN - EMAIL - IP - URI – KEYUSAGE, with new subkeywords: - CERTSIGN - DATAENCRYPT - DOCSIGN - HANDSHAKE	• Certificate Name Filtering • Public Key Certificate Enhancements
	V2R8	Updated to support the following new keywords and their associated subkeywords and parameters, which support digital certificates and key rings: • ADDRING • CONNECT • DELRING • EXPORT • GENCERT • GENREQ • LISTRING • REMOVE The following keywords have been updated: • ADD • DELETE • LIST	Public Key Certificate Enhancements

Table 8. Summary of Changed Commands (continued)

Command Name	Release	Description	Related Support
RALTER	V2R10	1. Updated to support the new keywords KERB and NOKERB, with subkeywords: • DEFTKTLFE and NODEFTKTLFE • KERBNAME and NOKERBNAME • MAXTKTLFE and NOMAXTKTLFE • MINTKTLFE and NOMINTKTLFE • PASSWORD and NOPASSWORD 2. Entering the value, ″No Replay Protection″ in the APPLDATA field of the PTKTDATA general resource class profile allows replay protection to be bypassed.	1. SecureWay Security Server Network Authentication and Privacy Service Support 2. Enhanced PassTicket Support
RDEFINE	V2R10	1. Updated to support the new keyword KERB, with subkeywords: • DEFTKTLFE • KERBNAME • MAXTKTLFE • MINTKTLFE • PASSWORD 2. Entering the value, ″No Replay Protection″ in the APPLDATA field of the PTKTDATA general resource class profile allows replay protection to be bypassed.	1. SecureWay Security Server Network Authentication and Privacy Service Support 2. Enhanced PassTicket Support
RLIST	V2R10	Updated to support the new keyword KERB.	SecureWay Security Server Network Authentication and Privacy Service Support
RVARY	V2R10	Issued from a console with master authority, RVARY ACTIVE, NODATASHARE, or SWITCH will accept YES as an alternative to the installation defined password.	None.
SETROPTS	V2R10	Updated to disallow GENERIC and GENCMD for REALM and KERBLINK classes.	SecureWay Security Server Network Authentication and Privacy Service Support

Data Areas

Table 9 on page 62 lists the new and changed data areas. For more information about the PICB data area, see *OS/390 SecureWay Security Server RACF Diagnosis Guide*. For detailed information about other the RACF data areas, see *OS/390 SecureWay Security Server RACF Data Areas*.

Interface Changes

Table 9. Summary of New and Changed Data Areas

Data Area Name	Release	Description	Related Support
ACEE	V2R10	The following new fields and constants have been added: • ACEEFLG6 — miscellaneous flags • ACEERAUI — restricted access user ID • ACEEX5PR — pointer to the X500 name structure	Certificate Name Filtering
	V2R8	Bit definitions in field ACEEFLG3 have been added to indicate a protected user ID that cannot access the system with a password.	Protected User ID
AFC	V2R10	The following new constants have been added: • AFC_CHMOUNT • AFC_CHMOUNT_SETUID	Enhanced OS/390 UNIX Superuser Granularity Support
	V2R8	The following constants have been added or updated: • AFC_MOUNT • AFC_UNMOUNT • AFC_QUIESCE • AFC_UNQUIESCE • AFC_QUIESCE_SETUID • AFC_UNQUIESCE_SETUID • AFC_MOUNT_SETUID • AFC_UNMOUNT_SETUID	OS/390 UNIX Superuser Granularity
CNST/CSNX (SAF)	V2R8	**New:** this structure supports the SAF version of the class descriptor table mapping macro, IRRPCNST.	Class Descriptor Table Enhancements

Table 9. Summary of New and Changed Data Areas (continued)

Data Area Name	Release	Description	Related Support
COMP	V2R10	1. **New:** Kerb field structure, field mapping, and constants have been added to support the new R_kerbinfo callable service. **New:** TKTS structures and constants have been added to support the new R_ticketserv callable service. 2. **New:** field structures and constants have been added to support public key certificate enhancements. 3. **New:** field structures and constants have been added to support certificate name filtering. Updated INTA_LAST_PARM.	1. SecureWay Security Server Network Authentication and Privacy Service Support 2. Public Key Certificate Enhancements 3. Certificate Name Filtering
	V2R8	1. The UMAP structure and constants have been added to support the IRRSIMOO (R_usermap) callable service. 2. Multiple structures and constants have been added to support the IRRSDL00 (R_datalib) callable service. 3. Multiple structures and constants have been added to support the IRRSEQ00 (R_admin) callable service.	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. Public Key Certificate Enhancements 3. R_admin SETROPTS Support
ICB	V2R10	Added a new byte, ICBALIAS, which indicates the current application identity mapping conversion stage.	Application Identity Mapping
FC	V2R10	Function code IRRSPX00# has been added to support the IRRSPX00 (R_PKIServ) callable service.	Public Key Certificate Enhancements
	V2R8	1. Function code IRRSIM00# has been added to support the IRRSIM00 (R_usermap) callable service. 2. Function code IRRSDL00# has been added to support the IRRSDL00 (R_datalib) callable service.	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. Public Key Certificate Enhancements
OUSP	V2R8	Multiple structures and constants have been added to support OS/390 UNIX user limit values.	OS/390 UNIX User Limits
PICB	V2R8	Constant ICB2608 has been added to represent the new FMID, HRF2608.	Release FMID Update

Table 9. Summary of New and Changed Data Areas (continued)

Data Area Name	Release	Description	Related Support
RCVT	V2R10	1. A new flag, RCVTENVS, indicates that the Environment Service, IRRENS00 is available. A new pointer, RCVTENVP, points to the Environment Service, IRRENS00. 2. A new byte, RCVTALIS has been added to support application identity mapping. 3. A new flag, RCVTX500, indicates that X500NAME support is available. 4. Constant RCVTVR73 has been added and RCVTVRMC has been updated to reflect the RACF FMID.	1. Program Control Enhancements 2. Application Identity Mapping 3. Certificate Name Filtering
	V2R8	Constant RCVTVR28 has been added and constant RCVTVRMC has been updated to reflect the RACF FMID.	Release FMID Update
RIPL	V2R10	The following field structures and constants have been added in support of X500NAME: • INITEND7 • INITIDN • INITIDNL • INITPRM7 • INITSDN • INITSDNL • INITX500 • INITX5PR • INITXLEN	Certificate Name Filtering
RIXP	V2R10	**New:** field RIXX5PRP contains the address of the X500 name if it exists.	Certificate Name Filtering
SAFP	V2R10	Constant SAFPRL73 has been added and constant SAFPCURR has been updated to reflect the RACF FMID.	Release FMID Update
	V2R8	Constant SAFPRL28 has been added and constant SAFPCURR has been updated to reflect the RACF FMID.	Release FMID Update

Database Templates

Table 10 on page 65 lists changes to RACF database templates. For detailed information, see *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference* or *OS/390 SecureWay Security Server RACF Macros and Interfaces*.

Table 10. Summary of Database Template Changes

Segment Name	Release	Description of Change	Related Support
General Resource Template			
Base segment	V2R10	The following new fields have been added to support certificate name filtering: • FILTERCT • FLTRLABL • FLTRNAME • FLTRSTAT • FLTRSVD1 • FLTRSVD2 • FLTRSVD3 • FLTRSVD4 • FLTRSVD5 • FLTRUSER	Certificate Name Filtering
CERTDATA	V2R8	The following new fields have been added to support digital certificates and key rings: • CERTCT • CERTDFLT • CERTEND • CERTLSER • CERTNAME • CERTPRVK • CERTPRVS • CERTPRVT • CERTRSV1 - CERTRSVK (reserved fields) • CERTSJDN • CERTSTRT • CERTUSAG • RINGCT • RINGNAME • RINGSEQN	Public Key Certificate Enhancements
COMBINATION	V2R10	The following new fields have been added to support certificate name filtering: • FLTRLST1 • FLTRLST2	Certificate Name Filtering
	V2R8	The following new fields have been added to support key ring information: • CERTRING • CERTRNG2 • CERTRNG3	Public Key Certificate Enhancements

Table 10. Summary of Database Template Changes (continued)

Segment Name	Release	Description of Change	Related Support
KERB	V2R10	The following new fields have been added to support SecureWay Security Server Network Authentication and Privacy Service: • CURKEY • CURKEYV • DEFTKTLF • ENCTYPE • KERB • KERBNAME • MAXTKTLF • MINTKTLF • PREVKEY • PREVKEYV • SALT	SecureWay Security Server Network Authentication and Privacy Service Support
Group Template			
OMVS	V2R10	The GID field, Flag 2 value has been changed to 10	Application Identity Mapping
User Template			
Base segment	V2R10	The following new fields have been added to support certificate name filtering: • FLAG9 • NMAPCT • NMAPLABL • NMAPNAME • NMAPRSV1 • NMAPRSV2 • NMAPRSV3 • NMAPRSV4 • NMAPRSV5	Certificate Name Filtering
	V2R8	1. Bit definitions in the FLAG7 field have been updated. 2. The CERTPUBK and CERTSJDN fields have been added.	1. Protected User ID 2. Public Key Certificate Enhancements
COMBINATION	V2R8	Updated with the new CERTLIST field.	Public Key Certificate Enhancements
KERB	V2R10	The following new fields have been added to support SecureWay Security Server Network Authentication and Privacy Service: • CURKEY • CURKEYV • DEFTKTLF • ENCTYPE • KERB • KERBNAME • MAXTKTLF • MINTKTLF • PREVKEY • PREVKEYV • SALT	SecureWay Security Server Network Authentication and Privacy Service Support

Table 10. Summary of Database Template Changes (continued)

Segment Name	Release	Description of Change	Related Support
LNOTES	V2R10	The SNAME field, Flag 2 value has been changed to 10	Application Identity Mapping
	V2R8	**New:** added for this release; includes the LNOTES and SNAME fields.	Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support
NDS	V2R10	The UNAME field, Flag 2 value has been changed to 10.	Application Identity Mapping
	V2R8	**New:** added for this release; includes the NDS and UNAME fields.	Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support
OMVS	V2R10	The UID field, Flag 2 value has been changed to 10.	Application Identity Mapping
	V2R8	Updated to contain the following new fields: • CPUTIME • ASSIZE • FILEPROC • PROCUSER • THREADS • MMAPAREA	OS/390 UNIX User Limits

Exits

Table 11 lists the changes that were made to RACF exits. For more information, refer to *OS/390 SecureWay Security Server RACF System Programmer's Guide*.

Table 11. Summary of Changed Exits

Exit Name	Release	Description	Related Support
ICHRFX01, ICHRFX03	V2R8	When a RACROUTE REQUEST=FASTAUTH request is invoked for the UNIXPRIV class, exit ICHRFX03 (if present) is always called instead of ICHRFX01, even in non-cross memory mode.	OS/390 UNIX Superuser Granularity
ICHRFX02, ICHRFX04	V2R8	When a RACROUTE REQUEST=FASTAUTH request is invoked for the UNIXPRIV class, exit ICHRFX04 is always called instead of ICHRFX02, even in non-cross memory mode.	OS/390 UNIX Superuser Granularity
ICHRTX00	V2R8	When a RACROUTE REQUEST=FASTAUTH request is invoked for the UNIXPRIV class, the FASTAUTH service is called directly from a callable service; this exit is not called.	OS/390 UNIX Superuser Granularity

Table 11. Summary of Changed Exits (continued)

Exit Name	Release	Description	Related Support
IRR@XACS	V2R8	With the availability of APAR OW38710, the RACF/DB2 external security module supports the following new DB2 Version 6 object types and their associated privileges. The object names and corresponding RACF class abbreviations follow: **M** Schemas (SC) **E** User-Defined Distinct Types (UT) **F** User-Defined Functions (UF) **O** Stored Procedures (SP) The RACF/DB2 external security module also supports TRIGGER, which is a new DB2 privilege to control the ability to create a trigger on a table. In addition, implicit ownership of PLAN or PACKAGE (which are objects that were already included in the RACF support for DB2 Version 5) now allows a user some, but not all, of the privileges that are associated with these objects. A list of the objects and associated privileges follows: **Object** — **Privilege Required** **PLAN** — BINDAUT **PACKAGE** — BINDAUT and COPYAUT	DB2 Support

Macros

Table 12 lists the changes that were made to the RACF executable macros. For more information, refer to *OS/390 SecureWay Security Server RACF Macros and Interfaces* or *OS/390 SecureWay Security Server External Security Interface (RACROUTE) Macro Reference*.

Table 12. Summary of Changed Executable Macros

Macro Name	Release	Description	Related Support
ICHEACTN	V2R10	Updated to accept the RELEASE=7703 keyword.	Release FMID Update
	V2R8	Updated to accept the RELEASE=2608 keyword.	Release FMID Update

Table 12. Summary of Changed Executable Macros (continued)

Macro Name	Release	Description	Related Support
ICHEINTY	V2R10	1. A new restriction, and new return and reason codes were added. 2. Updated to accept the RELEASE=7703 keyword.	1. Application Identity Mapping 2. Release FMID Update
	V2R8	1. Programs that use this macro to process the USER class may find the irrcerta and irrsitec user IDs, which are associated with digital certificates. These user IDs do not represent real users and cannot be used for RACROUTE REQUEST=VERIFY processing; as a result, your application may choose to ignore these user IDs. 2. Updated to accept the RELEASE=2608 keyword. 3. When DATEFMT=YYYYDDDF is specified with the TYPE=EXTRACT or TYPE=EXTRACTN operands, the values 0000000F or FFFFFFFF will be returned for any uninitialized data fields from the RACF database.	1. Public Key Certificate Enhancements 2. Release FMID Update 3. Service Updates (APAR OW36832)
ICHETEST	V2R10	Updated to accept the RELEASE=7703 keyword.	Release FMID Update
	V2R8	Updated to accept the RELEASE=2608 keyword.	Release FMID Update
RACROUTE	V2R10	Updated to accept the RELEASE=7703 keyword.	Release FMID Update
	V2R8	Updated to accept the RELEASE=2608 keyword.	Release FMID Update
RACROUTE REQUEST=AUTH	V2R10	1. Checks the RESTRICTED attribute to determine the correct authorization to grant. 2. Added a new reason code that will be set when a user has access to a data set but permission is denied because the environment is not controlled. .	1. Certificate Name Filtering 2. Program Control Enhancements

Table 12. Summary of Changed Executable Macros (continued)

Macro Name	Release	Description	Related Support
RACROUTE REQUEST=EXTRACT	V2R10	The ENVR object extracted from the ACEE includes the USP and X500 name if they exist.	Certificate Name Filtering
	V2R8	1. Applications that specify the TYPE=EXTRACTN and CLASS=USER keywords with this macro may find profiles for the irrsitec and irrcerta user IDs, which are associated with digital certificates. These user IDs do not represent real users and cannot be used for RACROUTE REQUEST=VERIFY processing; as a result, your application may choose to ignore these user IDs. 2. When DATEFMT=YYYYDDDF is specified with the TYPE=EXTRACT or TYPE=EXTRACTN operands, the values 0000000F or FFFFFFFF will be returned for any uninitialized data fields from the RACF database.	1. Public Key Certificate Enhancements 2. Service Updates (APAR OW36832)
RACROUTE REQUEST=FASTAUTH	V2R10	Checks the RESTRICTED attribute to determine the correct authorization to grant.	Certificate Name Filtering
	V2R8	For non-cross memory requests that do not specify the ACEEALET or ENVRIN keywords, if the caller is in system key (0-7) or in supervisor state, FASTAUTH uses the input ACEE to locate the profile that protects the resource for classes that are RACLISTed by the RACROUTE REQUEST=LIST,GLOBAL=YES macro. If no input ACEE is specified or the caller is not in system key or supervisor state, RACF uses the task ACEE (TCBSENV) pointer in the extended TCB. If there is no TCB (which is the case for SRB mode) or if the task ACEE pointer is zero, RACF uses the main ACEE for the address space.	Service Updates (APAR OW34996)

Table 12. Summary of Changed Executable Macros (continued)

Macro Name	Release	Description	Related Support
RACROUTE REQUEST=VERIFY	V2R10	Updated to allow an X500 name to be used in the creation of an ACEE. An MNOTE failure will be issued when an X500NAME is specified with an ENVIR other than CREATE.	Certificate Name Filtering
	V2R8	1. During processing, this macro determines if the specified *userid* has been defined as a protected user ID. If it has, and a password is specified or expected with the user, the request will fail. This support prevents a protected user ID from being used to log on to the system. 2. The irrsitec and irrcerta user IDs, which are associated with digital certificates, cannot be processed by this macro request.	1. Protected User ID 2. Public Key Certificate Enhancements
RACROUTE REQUEST=VERIFYX	V2R8	This macro has been updated to determine if the specified *userid* has been defined as a protected user ID. If it has, and a password is also specified or expected with the *userid*, the request will fail. This support prevents a protected user ID from being used to log on to the system.	Protected User ID

Messages

For detailed information about the new and changed RACF messages, see *OS/390 SecureWay Security Server RACF Messages and Codes*. For information about other OS/390 message changes that may affect your installation, refer to *OS/390 Summary of Message Changes*.

Panels

Table 13 on page 72 lists the new and changed RACF panels. Some panels may be updated by more than one release enhancement. The first part of the panel number indicates the type of panel that is affected:

ICHH Displays help information that is related to a panel or a task that you are performing

ICHM Displays message information that is related to a panel or a task that you are performing

ICHP Allows you to enter information such as a user ID or profile name

Interface Changes

Table 13. Summary of New and Changed Panels

Panel Number		Release	Description	Related Support
ICHPB80 **ICHPB82** **ICHPB83**	ICHPB81 ICHPB821 ICHPB831	V2R10	**New:** these panels provide support for certificate name filtering.	Certificate Name Filtering
ICHH21F **ICHH41N** **ICHHM17** **ICHP21F** **ICHP41N**	ICHH22F ICHH42N ICHHY03 ICHP22F ICHP42N	V2R10	**New:** these panels provide support for Network Authentication and Privacy Service.	SecureWay Security Server Network Authentication and Privacy Service Support
ICHCB02 **ICHCB73** **ICHH7B** **ICHH74** **ICHHT70** **ICHHT728** **ICHM85** **ICHP74**	ICHCB71 ICHH7A ICHH73 ICHH719 ICHHT71 ICHM73 ICHP73 ICHPB728	V2R10	**New:** these panels provide additional support for the RACDCERT command and certificate renewal.	Public Key Certificate Enhancements
ICHH21A **ICHH22A** **ICHM21** **ICHM41** **ICHP22A**	ICHH21OP ICHH28 ICHM22 ICHP21A ICHP28	V2R10	Updated to support Network Authentication and Privacy Service.	SecureWay Security Server Network Authentication and Privacy Service Support
ICHH41A1 **ICHP41A1** **ICHP48**	ICHH42A1 ICHP42A1 ICHM42	V2R10	Updated to support Network Authentication and Privacy Service.	SecureWay Security Server Network Authentication and Privacy Service Support
		V2R8	Updated to allow for users to specify new segment information.	Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support
ICHHB0 **ICHHB02** **ICHPB01A**	ICHHB01A ICHPB0 ICHPB02	V2R10	Updated for certificate name filtering and digital certificate support.	Certificate Name Filtering and Public Key Certificate Enhancements
		V2R8	Updated for digital certificate and key ring support.	Public Key Certificate Enhancements
ICHPB03 **ICHPB04** **ICHPB71**	ICHPB03B ICHPB70 ICHPB72	V2R10	Updated for certificate name filtering and digital certificate support.	Certificate Name Filtering and Public Key Certificate Enhancements
		V2R8	**New:** provide additional support for digital certificate and key ring tasks.	Public Key Certificate Enhancements

Table 13. Summary of New and Changed Panels (continued)

Panel Number		Release	Description	Related Support
ICHH41K1 **ICHH42K1** **ICHP41K** **ICHP42K**	ICHH41L1 ICHH42L1 ICHP41L ICHP42L	V2R8	**New:** these panels allow users to specify LNOTES and NDS segment information.	Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support
ICHH41GA **ICHH41GC** **ICHH41GE** **ICHH41G3** **ICHM41**	ICHH41GB ICHH41GD ICHH41GF ICHP41G3 ICHM42	V2R8	**New:** these panels allow users to enter values to update the new fields in the OMVS segment.	OS/390 UNIX User Limits
ICHHB021 **ICHHB03B** **ICHHT70** **ICHHT72** **ICHH712** **ICHH714** **ICHH716** **ICHH718** **ICHH75** **ICHH753** **ICHH754** **ICHPB03** **ICHPB04** **ICHPB71** **ICHP73** **ICHP75A** **ICHP753A** **ICHP755** **ICHM75**	ICHHB03 ICHHB04 ICHHT71 ICHH711 ICHH713 ICHH715 ICHH717 ICHH73 ICHH75A ICHH753A ICHH755 ICHPB03B ICHPB70 ICHPB72 ICHP75 ICHP753 ICHP754 ICHM73	V2R8	**New:** these panels provide additional support for digital certificate and key ring tasks, such as: generating certificate requests, generating certificate and key pairs, and writing a certificate to a data set.	Public Key Certificate Enhancements
ICHHM13 **ICHP41G1** **ICHP42G**	ICHP41G ICHP41G2	V2R8	Updated to reflect the new supported fields in the OMVS segment.	OS/390 UNIX User Limits
ICHHN10 **ICHM41**	ICHP41A ICHM42	V2R8	Updated to reflect changes in the OIDCARD and NOPASSWORD options.	Protected User ID
ICHH0B0 **ICHH00SM** **ICHP00** **ICHP141D** **ICHP141F** **ICHP142D** **ICHP41G1** **ICHP42G**	ICHH00 ICHPB021 ICHP00SM ICHP141E ICHP142B ICHP41G ICHP41G2 ICHM85	V2R8	Updated for digital certificate and key ring support.	Public Key Certificate Enhancements

SMF Records

Table 14 on page 74 lists the changes that were made to RACF SMF records. For more detailed information, refer to *OS/390 SecureWay Security Server RACF Macros and Interfaces* and *OS/390 SecureWay Security Server RACF Auditor's Guide*.

Interface Changes

Table 14. Summary of New and Changed RACF SMF Records

Record Type	Event Code/Field Name	Release	Description	Related Support
Type 80	Event code (all), except 68(44)	V2R10	Relocate sections 331 and 332 were added.	Certificate Name Filtering
	Event Code 66(42)	V2R10	1. Relocate sections 328, 329, and 330 have been added to contain the SDNFILTER, IDNFILTER, CRITERIA/NEWCRITERIA, the subject's distinguished name and the issuer's distinguished name values. 2. Extended relocate sections 336(150), 337(151), 338(152), and 339(153) have been added to contain the ALTNAME IP Address, ALTNAME Email, ALTNAME Domain, and ALTNAME URI values.	1. Certificate Name Filtering 2. Public Key Certificate Enhancements
		V2R8	Updated to reflect the additional keywords of the RACDCERT command. Relocate sections 320-327 have been added to contain the ring name and components of a subject's distinguished name.	Public Key Certificate Enhancements
	Event Code 67(43)	V2R10	The following event code qualifiers were added: • 4 — user ID not found for the certificate • 5 — certificate not trusted • 6 — successful CERTAUTH certificate registration • 7 — insufficient authority to register the CERTAUTH certificate.	Certificate Name Filtering and Public Key Certificate Enhancements
	Event Code 68(44)	V2R10	**New:** Relocate sections 333, 334, 335 have been added but are reserved for use by the Network Authentication and Privacy Service.	SecureWay Security Server Network Authentication and Privacy Service Support
	Event Code 69(45)	V2R10	**New:** Relocate sections 340—351 have been added for the R_PKIServ GENCERT request.	Public Key Certificate Enhancements
	Event Code 70(46)	V2R10	**New:** Relocate sections 343, 344, 351 have been added for the R_PKIServ EXPORT request.	Public Key Certificate Enhancements

Table 14. Summary of New and Changed RACF SMF Records (continued)

Record Type	Event Code/Field Name	Release	Description	Related Support
SMF80VRM	V2R10	Updated to show FMID 7703	Release FMID Update	
	V2R8	Updated to show FMID, 2608.	Release FMID Update	
Type 81	SMF81BOX	V2R8	Updated with new bits to indicate the type of password in effect for RVARY SWITCH and RVARY STATUS.	R_admin SETROPTS Support

SYS1.SAMPLIB Members

Table 15 identifies changes to the RACF members of SYS1.SAMPLIB.

Table 15. Summary of RACF Changes to SYS1.SAMPLIB

Member Name	Release	Description	Related Support
IRR@XACS	V2R8	With the availability of APAR OW38710, the RACF/DB2 external security module has been updated to process the following DB2 Version 6 objects and their associated privileges: • User-Defined Distinct Types • User-Defined Functions • Schemas • Stored Procedures The RACF/DB2 external security module also supports TRIGGER, which is a new DB2 privilege to control the ability to create a trigger on a table. In addition, implicit ownership of PLAN or PACKAGE (which are objects that were already included in the RACF support for DB2 Version 5) now allows a user some, but not all, of the privileges that are associated with these objects. A list of the objects and associated privileges follows: **Object** — **Privilege Required** **PLAN** — BINDAUT **PACKAGE** — BINDAUT and COPYAUT	DB2 Support

Table 15. Summary of RACF Changes to SYS1.SAMPLIB (continued)

Member Name	Release	Description	Related Support
IRRADULD	V2R10	1. Updated to include two new X500 name relocates at the end of every event type, except for the KTICKET event. 2. Updated to support the KTICKET event code(68).	1. Certificate Name Filtering 2. SecureWay Security Server Network Authentication and Privacy Service Support
	V2R8	Updated to reflect changes in SMF records.	R_admin SETROPTS Support
IRRADUTB	V2R10	1. Updated to include two new X500 name relocates at the end of every event type. The parameters specified for the DB2 CREATE TABLESPACE statement are also updated (from 4K to 32K) due to the increased size of the SMF records. 2. Updated to support the KTICKET event code(68).	1. Certificate Name Filtering 2. SecureWay Security Server Network Authentication and Privacy Service Support
	V2R8	Updated to reflect changes in SMF records.	R_admin SETROPTS Support
IRRICE	V2R8	**New:** this member contains the DFSORT statements for the selection criteria and the ICETOOL statements for the report format for all of the RACFICE reports.	ICETOOL Support
RACDBULD	V2R10	1. Updated to contain the new KERB record 2. Updated with a new USBD_ATTRIBS field in the User Basic Data record type and two new record types.	1. SecureWay Security Server Network Authentication and Privacy Service Support 2. Certificate Name Filtering
	V2R8	1. Updated to contain information about the LNOTES and NDS user records. 2. Updated to contain additional information about the resource limits that are defined for OS/390 UNIX users. 3. Updated to contain information about the key type, key size, and serial number that is associated with a digital certificate. For key rings, this information also includes the certificate label.	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. OS/390 UNIX User Limits 3. Public Key Certificate Enhancements

Table 15. Summary of RACF Changes to SYS1.SAMPLIB (continued)

Member Name	Release	Description	Related Support
RACDBUTB	V2R10	1. Updated to contain a new KERB record 2. Updated with a new USBD_ATTRIBS field in the User Basic Data record type and two new record types.	1. SecureWay Security Server Network Authentication and Privacy Service Support 2. Certificate Name Filtering
	V2R8	1. Updated to contain information about the LNOTES and NDS user records. 2. Updated to contain additional information about the resource limits that are defined for OS/390 UNIX users. 3. Updated to contain information about the key type, key size, and serial number that is associated with a digital certificate. For key rings, this information also includes the certificate label.	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. OS/390 UNIX User Limits 3. Public Key Certificate Enhancements
RACINSTL	V2R10	Updated to contain an entry to the index of samples pointing to RACJCL	Application Identity Mapping
	V2R8	Updated to contain an entry to the index of samples pointing to RACJCL and RACFICE.	ICETOOL Support
RACJCL	V2R10	Updated with sample JCL to run conversion utility IRRIRA00.	Application Identity Mapping
	V2R8	Updated with sample JCL to allocate a report data set and add the RACFICE reports in IEBUPDTE format.	ICETOOL Support

Utilities

Table 16 on page 78 lists the changes made to RACF utilities for this release. For information about the IRRDBU00 and IRRRID00 utilities, see *OS/390 SecureWay Security Server RACF Security Administrator's Guide*. For information about the IRRADU00 utility, see *OS/390 SecureWay Security Server RACF Auditor's Guide*. For more information about other RACF utilities, refer to *OS/390 SecureWay Security Server RACF System Programmer's Guide*.

Interface Changes

Table 16. Summary of Changed Utilities

Utility Name	Release	Description	Related Support
IRRADU00	V2R10	1. Updated to support the extension to the RACDCERT, ADDUSER, and ALTUSER type 6 relocate sections, the new RACDCERT relocate sections, the X500 name relocate sections, and the new event code qualifiers for event 67. 2. Updated to support the auditing of extensions to the RACDCERT command and for the new initACEE and R_PKIServ event qualifiers. 3. Updated to support event code 68.	1. Certificate Name Filtering 2. Public Key Certificate Enhancements 3. SecureWay Security Server Network Authentication and Privacy Service Support
	V2R8	Updated to unload additional fields in SMF Type 81 data.	R_admin SETROPTS Support

Table 16. Summary of Changed Utilities (continued)

Utility Name	Release	Description	Related Support
IRRDBU00	V2R10	1. Updated the User Basic Data record, and added the User Associated Mapping record and the Filter Data record. 2. Updated to support KERB segment data.	1. Certificate Name Filtering 2. SecureWay Security Server Network Authentication and Privacy Service Support
	V2R8	1. Updated to unload the following user record types **02B0** LNOTES Data **02C0** NDS Data 2. Updated to unload the following new fields in record type 0270 (USOMVS): • USOMVS_CPUTIMEMAX • USOMVS_ASSIZEMAX • USOMVS_FILEPROCMAX • USOMVS_PROCUSERMAX • USOMVS_THREADSMAX • USOMVS_MMAPAREAMAX 3. Updated to display the following values from the USBD_NOPWD field in the user record, which indicate the setting of FLAG7: **X'00'** NO; the user ID must log on with a password. **X'40'** PRO; the user ID may not be used to log on to the system. **X'80'** YES; the user ID does not need to specify a password to log on to the system. 4. Updated to unload the following general resource record types: **0560** Certificate Data Record **0561** Certificate References Record **0562** Key Ring Data Record	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. OS/390 UNIX User Limits 3. Protected User ID 4. Public Key Certificate Enhancements
IRRIRA00	V2R10	**New:** Converts an existing database to application identity mapping functionality using a four-staged approach.	Application Identity Mapping
IRRMIN00	V2R10	Updated to enable the new database for application identity mapping processing when PARM=NEW.	Application Identity Mapping

Table 16. Summary of Changed Utilities (continued)

Utility Name	Release	Description	Related Support
IRRRID00	V2R10	Updated to recognize KERBLINK profiles.	SecureWay Security Server Network Authentication and Privacy Service Support
	V2R8	1. Updated to find residual user IDs in the APPLDATA field of NOTELINK and NDSLINK profiles. If a residual user ID is found in a NOTELINK or NDSLINK profile, an RDELETE command will be produced. However, if the profile name contains lower case characters, the command cannot be executed successfully. To delete the profile, you must issue an ADDUSER command for the user ID with the corresponding LNOTES SNAME or NDS UNAME specified to re-establish the link. Then, you can issue a DELUSER command to delete the user and the NOTELINK or NDSLINK profile. 2. Updated to find and remove references to residual IDs that are associated with digital certificates and key rings. For digital certificates, it checks the APPLDATA field of the DIGTCERT profile. For key rings, it compares the user ID specified in the key ring to a list of valid user IDs. It does not search the OWNER field of the DIGTCERT or DIGTRING profiles.	1. Lotus Notes for OS/390 and Novell Directory Services for OS/390 Support 2. Public Key Certificate Enhancements
IRRUT200	V2R10	Updated to process the alias index structures to detect errors and to display the formatted alias index blocks.	Application Identity Mapping
IRRUT400	V2R10	Updated to build an alias index structure in the output RACF database.	Application Identity Mapping

Appendix. 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 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 pointers in this publication to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites. IBM accepts no responsibility for the content or use of non-IBM Web sites specifically mentioned in this publication or accessed through an IBM Web site that is mentioned in this publication.

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
Attention: Information Request

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.

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	DB2
DFSMS	DFSORT	IBM
IBMLink	Library Reader	MVS/ESA
OS/390	Parallel Sysplex	RACF
RETAIN	S/390	SecureWay
System/390	TalkLink	VM/ESA

Lotus and Lotus Notes are trademarks of Lotus Development Corporation in the United States, other countries, or both.

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.

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

Tivoli is a registered trademark or trademark of Tivoli Systems, Inc. in the United States, other countries, or both.

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

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

Index

Special Characters

A

B

C

D

E

F

G

I

J

K

L

M

N

O

P

R

S

T

U

Y

Readers' Comments — We'd Like to Hear from You

OS/390
SecureWay Security Server RACF
Migration

Publication No. GC28-1920-08

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
GC28-1920-08

IBM

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

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.

GC28-1920-08