z/OS

Security Server RACF Migration

GA22-7690-03

z/OS

Security Server RACF Migration

GA22-7690-03

Note

Before using this information and the product it supports, be sure to read the general information under “Notices” on page 147.

Fourth Edition, September, 2002

This is a major revision of GA22-7690-02. This edition applies to Version 1 Release 4 of z/OS (5694-A01), Version 1 Release 4 of z/OS.e (5655-G52), and to subsequent releases and modifications until otherwise indicated in new editions.

Order documents through your IBM® representative or the IBM branch office serving your locality. Documents are not stocked at the address below.

IBM welcomes your comments. A form for readers’ comments may be provided at the back of this document, 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/servers/eserver/zseries/zos/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 document
- Page number or topic related to your comment

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

Contents

Tables

About this document

This document supports z/OS (5694-A01) and z/OS.e (5655-G52)and contains information about Resource Access Control Facility (RACF), which is a component of the Security Server. The Security Server is comprised of the following components:

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

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

GC28-1938	*z/OS SecureWay Security Server DCE Overview*
SA22-7249	*z/OS SecureWay Security Server Open Cryptographic Enhanced Plug-ins Application Programming*
SC24-5835	*z/OS Security Server Firewall Technologies*
SC24-5861	*z/OS Security Server LDAP Server Administration and Use*
SC24-5878	*z/OS Security Server LDAP Client Programming*
SC24-5896	*z/OS Security Server Network Authentication Service Administration*
SC24-5897	*z/OS Security Server Network Authentication Service Programming*
SA22–7693	*z/OS Security Server PKI Services Guide and Reference*

Intended audience

This document provides planning information about installing and migrating to the RACF component of the z/OS Version 1 Release 3 Security Server. This document 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 document

This document 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 9, describes high-level migration considerations for customers upgrading to the new release of RACF from previous levels of RACF.
- Chapter 3, “z/OS Version 1 Release 4 Overview” on page 17, provides an overview of the support introduced in z/OS Version 1 Release 4.
- Chapter 4, “z/OS Version 1 Release 3 Overview” on page 31, provides an overview of the support introduced in z/OS Version 1 Release 3.
- Chapter 5, “z/OS Version 1 Release 2 Overview” on page 41, provides an overview of the support introduced in z/OS Version 1 Release 2.

- Chapter 6, “z/OS Version 1 Release 1 Overview” on page 59, provides an important note about z/OS Version 1 Release 1.
- Chapter 7, “OS/390 Version 2 Release 10 overview” on page 61, provides an overview of the support introduced in OS/390 Version 2 Release 10, and also available in z/OS Version 1 Release 1.
- Chapter 8, “OS/390 Version 2 Release 8 Overview” on page 79, provides an overview of the support introduced in OS/390 Version 2 Release 8.
- Chapter 9, “Summary of Interface Changes” on page 103, summarizes the specific RACF interfaces that have been updated in z/OS Version 1 Release 2, OS/390 Version 2 Release 10, and OS/390 Version 2 Release 8.

Where to find more information

Where necessary, this document references information in other publications. For complete titles and order numbers for all elements of z/OS™, see *z/OS Information Roadmap*.

Softcopy publications

The RACF® library is available on the following CD-ROMs. The CD-ROM online library collections include Library Reader™, which is a program that enables you to view the softcopy documents.

SK3T-4269 *z/OS Version 1 Release 4 Collection*

This collection contains the set of unlicensed documents for the current release of z/OS in both BookManager® and Portable Document Format (PDF) files. You can view or print the PDF files with the Adobe Acrobat reader.

SK3T-4272 *z/OS Security Server RACF Collection*

This softcopy collection kit contains the Security Server library for z/OS in both BookManager and Portable Document Format (PDF) files. You can view or print the PDF files with the Adobe Acrobat reader.

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

This softcopy collection contains the Security Server library for OS/390. It also contains the RACF/MVS Version 2 product libraries, the RACF/VM 1.10 product library, product documents from the OS/390® and VM collections, International Technical Support Organization (ITSO) documents (known as Redbooks™), and Washington System Center (WSC) documents (known as orange books) that contain information related to RACF. The collection 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®.

SK3T-7876 *IBM eServer zSeries™ Redbooks Collection*

This softcopy collection contains a set of documents called Redbooks that pertain to zSeries subject areas ranging from e-business application development and enablement to hardware, networking, Linux, solutions, security, Parallel Sysplex® and many others.

SK2T-2177 *IBM Redbooks S/390® Collection*

This softcopy collection contains a set of documents called Redbooks that pertain to S/390 subject areas ranging from application development and enablement to hardware, networking, security, Parallel Sysplex and many others.

RACF courses

The following RACF classroom courses are available:

ES840	*Implementing RACF Security for CICS/ESA® and CICS/TS*
H3917	*Basics of OS/390 Security Server RACF Administration*
H3927	*Effective RACF Administration*
ES88A	*Exploiting the Features of OS/390 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)

Using LookAt to look up message explanations

LookAt is an online facility that allows you to look up explanations for most messages you encounter, as well as for some system abends and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can access LookAt from the Internet at:

`http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/`

or from anywhere in z/OS where you can access a TSO/E command line (for example, TSO/E prompt, ISPF, z/OS UNIX System Services running OMVS). You can also download code from the *z/OS Collection* (SK3T-4269) and the LookAt Web site that will allow you to access LookAt from a handheld computer (Palm Pilot VIIx suggested).

To use LookAt as a TSO/E command, you must have LookAt installed on your host system. You can obtain the LookAt code for TSO/E from a disk on your *z/OS Collection* (SK3T-4269) or from the **News** section on the LookAt Web site.

Some messages have information in more than one document. For those messages, LookAt displays a list of documents in which the message appears.

Accessing z/OS licensed documents on the Internet

z/OS licensed documentation is available on the Internet in PDF format at the IBM Resource Link™ Web site at:

`http://www.ibm.com/servers/resourcelink`

Licensed documents are available only to customers with a z/OS license. Access to these documents requires an IBM Resource Link user ID and password, and a key code. With your z/OS order you received a Memo to Licensees, (GI10-0671), that includes this key code. [1]

1. z/OS.e™ customers received a Memo to Licensees, (GI10-0684) that includes this key code.

To obtain your IBM Resource Link user ID and password, log on to:
`http://www.ibm.com/servers/resourcelink`

To register for access to the z/OS licensed documents:

1. Sign in to Resource Link using your Resource Link user ID and password.
2. Select **User Profiles** located on the left-hand navigation bar.

Note: You cannot access the z/OS licensed documents unless you have registered for access to them and received an e-mail confirmation informing you that your request has been processed.

Printed licensed documents are not available from IBM.

You can use the PDF format on either **z/OS Licensed Product Library CD-ROM** or IBM Resource Link to print licensed documents.

IBM systems center publications

IBM systems centers produce documents known as red and orange books that can help you set up and use RACF. These documents 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 documents follows. Other documents 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*
GG24-3378	*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*
GG24-3970	*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*
SG24-4704	*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 *ibm.servers.mvs.racf* newsgroup for discussion of RACF-related topics. You can find this newsgroup on news (NNTP) server *news.software.ibm.com* using your favorite news reader client.

Internet sources

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

- **Online library**

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

  `http://www.ibm.com/servers/eserver/zseries/zos/bkserv/`

- **Redbooks**

  The documents known as Redbooks that are produced by the International Technical Support Organization (ITSO) are available at the following address:

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

- **Enterprise systems security**

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

  `http://www.ibm.com/servers/eserver/zseries/zos/security/`

- **RACF home page**

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

  `http://www.ibm.com/servers/eserver/zseries/zos/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, or go to ftp://ftp.software.ibm.com/eserver/zseries/zos/racf/.

  The code is also available from `ftp.software.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 or tool you want to download:

```
cd eserver/zseries/zos/racf/
```

An announcement will be posted on the RACF-L discussion list and on newsgroup *ibm.servers.mvs.racf* whenever something is added.

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

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

Restrictions

Because the sample code and tools are not officially supported,

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

To request copies of IBM publications

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

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

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

Summary of changes

Summary of changes
for GA22-7690-03
z/OS Version 1 Release 4

This document contains information previously presented in z/OS SecureWay Security Server RACF Migration, GA22-7690-02, which supports z/OS Version 1 Release 3.

The following summarizes the changes to that information.

New information

- Information is added to indicate this document supports z/OS.e.
- Chapter 3, “z/OS Version 1 Release 4 Overview” on page 17

Changed information

- Chapter 2, “Migration roadmap” on page 9 has been updated for z/OS Version 1 Release 4.
- Chapter 9, “Summary of Interface Changes” on page 103 has been updated for z/OS Version 1 Release 4.

This document contains 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.

Starting with z/OS V1R2, you may notice changes in the style and structure of some content in this document —for example, headings that use uppercase for the first letter of initial words only, and procedures that have a different look and format. The changes are ongoing improvements to the consistency and retrievability of information in our documents.

Summary of changes
for GA22-7690-02
z/OS Version 1 Release 3

This document contains information previously presented in z/OS SecureWay Security Server RACF Migration, GA22-7690-01, which supports z/OS Version 1 Release 2.

The following summarizes the changes to that information.

New information

- Chapter 4, “z/OS Version 1 Release 3 Overview” on page 31
- An appendix with z/OS product accessibility information was added.

The following summarizes the changes to that information.

Changed information

- Chapter 2, “Migration roadmap” on page 9 has been updated for z/OS Version 1 Release 3.
- Chapter 9, “Summary of Interface Changes” on page 103 has been updated for z/OS Version 1 Release 3.

Deleted information

- Note that the glossary has been removed from this document. You can now find the glossary in the *z/OS Security Server RACF Security Administrator's Guide*.

This document contains 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 GA22-7690-01 z/OS Version 1 Release 2

This document contains information previously presented in GA22-7690-00, which supports z/OS Version 1 Release 1 and OS/390 Version 2 Release 10.

The following summarizes the changes to that information.

New information

- Chapter 5, "z/OS Version 1 Release 2 Overview" on page 41.

Changed information

- Chapter 2, "Migration roadmap" on page 9 has been updated for z/OS Version 1 Release 2.
- Chapter 9, "Summary of Interface Changes" on page 103 has been updated for z/OS Version 1 Release 2.

This document contains terminology, maintenance, and editorial changes, including changes to improve consistency and retrievability.

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 z/OS system. In addition to specific information about RACF, this documentation contains information about all of the z/OS elements.

- *z/OS and z/OS.e Planning for Installation*

  This document describes the installation requirements for z/OS 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.
- *z/OS Program Directory*

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

  This is the order-customized, installation document 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 document, you can find information about the specific updates and considerations that apply to this release of RACF.

- Chapter 2, “Migration roadmap” on page 9

  This section identifies the migration paths that are supported with the current level of RACF. It also describes the additional publications that can assist you with your migration to the current level.
- Chapter 3, “z/OS Version 1 Release 4 Overview” on page 17

  This section describes the specific updates that were made to RACF for z/OS Version 1 Release 4. 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 z/OS element libraries.
- Chapter 4, “z/OS Version 1 Release 3 Overview” on page 31

  This section describes the specific updates that were made to RACF for z/OS Version 1 Release 3. 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 z/OS element libraries.
- Chapter 5, “z/OS Version 1 Release 2 Overview” on page 41

  This section describes the specific updates that were made to RACF for z/OS Version 1 Release 2. 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 z/OS element libraries.

- Chapter 6, “z/OS Version 1 Release 1 Overview” on page 59

  This section provides a special note about RACF for z/OS Version 1 Release 1.

  Note: RACF for z/OS Version 1 Release 1 and RACF for OS/390 Version 2 Release 10 are functionally equivalent.
- Chapter 7, “OS/390 Version 2 Release 10 overview” on page 61

  This section describes the specific updates that were made to RACF for OS/390 Version 2 Release 10. 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 z/OS element libraries.
- Chapter 8, “OS/390 Version 2 Release 8 Overview” on page 79

  This section describes the specific updates that were made to RACF for OS/390 Version 2 Release 8. 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 z/OS element libraries.
- Chapter 9, “Summary of Interface Changes” on page 103

  This section provides a summary of the changes that were made to RACF user and programming interfaces for z/OS Version 1 Release 2, OS/390 Version 2 Release 10, and OS/390 Version 2 Release 8.

Terms you need to know

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

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 *z/OS and z/OS.e Planning for Installation* and *z/OS Introduction and Release Guide* for information about RACF and other z/OS 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 *z/OS Program Directory*. Although *z/OS 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 *z/OS Program Directory* or *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 5, "z/OS Version 1 Release 2 Overview" on page 41, 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 document 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 document 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 document 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 document 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 document 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 9, "Summary of Interface Changes" on page 103 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.

Testing your new RACF database

You can create a test copies of your primary and backup RACF databases to test the new RACF release. This will allow you to run your own tests based on installation considerations, without affecting your production RACF environment. Before you copy your RACF databases, you should determine your strategy for synchronizing changes to your test and production databases. Once you copy your production RACF databases, any profile changes you make during testing to your test database may be lost if you do not have appropriate plans in place to migrate those changes. See “Synchronizing changes between your test and production databases” on page 6 for more information.

Attention

Do not attempt to use IRRUT400 to merge your production and test RACF databases.

Do not merge your production and test RACF databases using the merge function of the RACF utility IRRUT400. The IRRUT400 utility does not support the merging of RACF databases. Using IRRUT400 in this way may cause duplicate, missing or incomplete profiles in the merged database. See *z/OS Security Server RACF System Programmer's Guide* for information about the use of IRRUT400.

Creating your test RACF databases

You can verify and copy your primary and backup production databases to create test databases, and then upgrade your test databases using the following RACF utilities:

IRRUT200 Verifies your production RACF databases and identifies internal inconsistencies.

IRRUT400 Copies your production RACF databases and creates the test version.

IRRMIN00 Updates your test RACF databases using the new set of database templates associated with the new RACF release.

See *z/OS Security Server RACF System Programmer's Guide* for details about using IRRUT400.

Updating RACF database templates

To ensure that RACF functions properly, use the IRRMIN00 utility to update the test and production RACF databases with the database templates for the current release level. If you share the RACF 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 the current release level of RACF in the IRRTEMP1 SYS1.MODGEN member. You should do this **before** IPLing. For more information, see *z/OS Program Directory*, *ServerPac Installing Your Order* documentation, and *z/OS 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 *z/OS Security Server RACF System Programmer's Guide*.

Synchronizing changes between your test and production databases

If you upgrade a test copy of your RACF database with the new database templates and make profile changes on either your test or production RACF databases, you should consider the following ways to synchronize these changes. You can use one or more of these choices depending on the configuration of your systems, the nature of your testing, the daily volume of RACF database changes on your production system, and how long you plan to test the new release.

- Keep a record of all profiles added, changed, or deleted on the test database, and then add, change or delete these profiles from your production database through the use of RACF commands.

  Use this method when:

  1. You are testing the new release for a short period of time, and
  2. You will not replace your production RACF databases with your test RACF databases.

  You can use RACF auditing to track new, changed and deleted profiles. To do so, enter the SETROPTS AUDIT(*classnames*) command before making profile changes to your test databases. After testing is complete, use the SMF data unload utility (IRRADU00) to unload the audit records. Extract the audit records related to command usage and use the information in these records to recreate the profile changes from your test databases to your production databases.
- Use the RACF remote sharing facility (RRSF) to direct changes production databases to your test databases.

  Use this method when:

  1. Your systems are configured for RRSF, and
  2. There is a high volume of daily profile changes on your production RACF databases, and
  3. You will replace your production RACF databases with your test RACF databases.

  See "Using automatic direction of application updates (ADAU)" for more information.
- Migrate your test databases to the production databases after using the test databases for a limited period of time.

  Use this method when:

  1. You are testing the new release for a short period of time, and
  2. There is a low volume of daily profile changes on your production RACF databases, and
  3. You do not plan to configure your systems for RRSF, and
  4. You will not replace your production RACF databases with your test RACF databases.

  This method eliminates the need to synchronize the test and production databases.

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 *z/OS 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 a system running the current release level of RACF and attempt to use it on a system running RACF at a lower level than RACF/MVS Version 2 Release 2.

Migration overview

Chapter 2. Migration roadmap

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

z/OS V1R3 to z/OS V1R4

Table 1 summarizes the updates that were introduced by RACF in z/OS Version 1 Release 4. If you are migrating from z/OS V1R3 you should review the information in the detailed section for each item.

Table 1. Summary of RACF Updates for z/OS Version 1 Release 4

For Information About:	Refer to Topic:
Changes introduced in z/OS V1R4	
RACF Support for Enterprise Identity Mapping Services (EIM)	18
PKI Services	20
UNIX Security Management Usability Enhancements	22
Program Access to Data Sets (PADS)	25
Release FMID Update	26
Other Enhancements	27
Service Updates	29

z/OS V1R2 to z/OS V1R4

Table 2 summarizes the updates that were introduced by RACF in z/OS Version 1 Release 3 and z/OS Version 1 Release 4. If you are migrating from z/OS V1R2 you should review the information in the detailed section for each item.

Table 2. Summary of RACF Updates for z/OS Version 1 Release 3 and z/OS Version 1 Release 4

For Information About:	Refer to Topic:
Changes introduced in z/OS V1R3	
Access Control Lists (ACLs)	32
PKI Services	34
Policy Director Authorization Services for z/OS and OS/390	35
Release FMID Update	37
Other Enhancements	38
Service Updates	39
Changes introduced in z/OS V1R4	
RACF Support for Enterprise Identity Mapping Services (EIM)	18
PKI Services	20
UNIX Security Management Usability Enhancements	22
Program Access to Data Sets (PADS)	25
Release FMID Update	26
Other Enhancements	27

Table 2. Summary of RACF Updates for z/OS Version 1 Release 3 and z/OS Version 1 Release 4 (continued)

For Information About:	Refer to Topic:
Service Updates	29

OS/390 V2R10 or z/OS V1R1 to z/OS V1R4

Table 3 summarizes the updates that were introduced by RACF in z/OS Version 1 Release 2, z/OS Version 1 Release 3, and z/OS Version 1 Release 4. If you are migrating from OS/390 V2R10 or z/OS V1R1, you should review the information in the detailed section for each item.

Table 3. Summary of RACF Updates for z/OS Version 1 Release 2, z/OS Version 1 Release 3, and z/OS Version 1 Release 4

For Information About:	Refer to Topic:
Changes introduced in z/OS V1R2	
DB2 Version 7 Support	42
Enterprise Java Beans	44
Mixed-Case Profile Names	45
Network Authentication Service Support	48
SAF Trace	50
Universal Groups	51
Release FMID Update	54
Enhancements for z/OS UNIX	55
Other Enhancements	56
Service Updates	58
Changes introduced in z/OS V1R3	
Access Control Lists (ACLs)	32
PKI Services	34
Policy Director Authorization Services for z/OS and OS/390	35
Release FMID Update	37
Other Enhancements	38
Service Updates	39
Changes introduced in z/OS V1R4	
RACF Support for Enterprise Identity Mapping Services (EIM)	18
PKI Services	20
UNIX Security Management Usability Enhancements	22
Program Access to Data Sets (PADS)	25
Release FMID Update	26
Other Enhancements	27
Service Updates	29

OS/390 V2R8 or V2R9 to z/OS V1R4

Table 4 summarizes the updates that were introduced by RACF in OS/390 Version 2 Release 10, z/OS V1R2, z/OS V1R3, and z/OS V1R4. If you are migrating from OS/390 V2R8 or OS/390 V2R9, you should review the information in the detailed section for each item.

Note that RACF for z/OS Version 1 Release 1 and RACF for OS/390 Version 2 Release 10 are functionally equivalent.

Table 4. Summary of RACF Updates for OS/390 V2R10, z/OS V1R2, z/OS V1R3, and z/OS V1R4

For Information About:	Refer to Topic:
Changes introduced in OS/390 V2R10	
Certificate Name Filtering	62
Network Authentication Service	66
Program Control Enhancements	68
Application Identity Mapping	69
Enhanced PassTicket Support	71
Public Key Certificate Enhancements	72
Enhanced Superuser Granularity	74
IBM License Manager	75
Release FMID Update	76
Service Updates	78
Changes introduced in z/OS V1R2	
DB2 Version 7 Support	42
Enterprise Java Beans	44
Mixed-Case Profile Names	45
Network Authentication Service Support	48
SAF Trace	50
Universal Groups	51
Release FMID Update	54
Enhancements for z/OS UNIX	55
Other Enhancements	56
Service Updates	58
Changes introduced in z/OS V1R3	
Access Control Lists (ACLs)	32
PKI Services	34
Policy Director Authorization Services for z/OS and OS/390	35
Release FMID Update	37
Other Enhancements	38
Service Updates	39
Changes introduced in z/OS V1R4	
RACF Support for Enterprise Identity Mapping Services (EIM)	18
PKI Services	20

Table 4. Summary of RACF Updates for OS/390 V2R10, z/OS V1R2, z/OS V1R3, and z/OS V1R4 (continued)

For Information About:	Refer to Topic:
UNIX Security Management Usability Enhancements	22
Program Access to Data Sets (PADS)	25
Release FMID Update	26
Other Enhancements	27
Service Updates	29

OS/390 V2R6 or V2R7 to z/OS V1R4

Table 5 summarizes the updates that were introduced by RACF in OS/390 Version 2 Release 8, OS/390 Version 2 Release 10, z/OS V1R2, z/OS V1R3, and z/OS V1R4. If you are migrating from OS/390 V2R6 or OS/390 V2R7, you should review the information in the detailed section for each item.

Note that RACF for z/OS Version 1 Release 1 and RACF for OS/390 Version 2 Release 10 are functionally equivalent.

Table 5. Summary of RACF updates for OS/390 V2R8, OS/390 V2R10, z/OS V1R2, z/OS V1R3, and z/OS V1R4

For Information About:	Refer to Topic:
Changes introduced in OS/390 V2R8	
Class Descriptor Table Enhancements	80
DB2 Version 6 Support	83
ICETOOL Support	85
Lotus Notes for z/OS and Novell Directory Services for OS/390 Support	86
Superuser Granularity	88
z/OS UNIX User Limits	90
Protected User ID	92
Public Key Certificate Enhancements	94
R_admin SETROPTS	98
Release FMID Update	99
Service Updates	100
Changes introduced in OS/390 V2R10	
Certificate Name Filtering	62
Network Authentication Service	66
Program Control Enhancements	68
Application Identity Mapping	69
Enhanced PassTicket Support	71
Public Key Certificate Enhancements	72
Enhanced Superuser Granularity	74
IBM License Manager	75
Release FMID Update	76

Table 5. Summary of RACF updates for OS/390 V2R8, OS/390 V2R10, z/OS V1R2, z/OS V1R3, and z/OS V1R4 (continued)

For Information About:	Refer to Topic:
Service Updates	78
Changes introduced in z/OS V1R2	
DB2 Version 7 Support	42
Enterprise Java Beans	44
Mixed-Case Profile Names	45
Network Authentication Service Support	48
SAF Trace	50
Universal Groups	51
Release FMID Update	54
Enhancements for z/OS UNIX	55
Other Enhancements	56
Service Updates	58
Changes introduced in z/OS V1R3	
Access Control Lists (ACLs)	32
PKI Services	34
Policy Director Authorization Services for z/OS and OS/390	35
Release FMID Update	37
Other Enhancements	38
Service Updates	39
Changes introduced in z/OS V1R4	
RACF Support for Enterprise Identity Mapping Services (EIM)	18
PKI Services	20
UNIX Security Management Usability Enhancements	22
Program Access to Data Sets (PADS)	25
Release FMID Update	26
Other Enhancements	27
Service Updates	29

Security Server V2R5 and earlier

If you are migrating from a RACF release earlier than Security Server Version 2 Release 6, table Table 6 on page 14 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 in topic 14) in an associated column indicates an additional document or migration information that you should review before migrating to the current release. For example, if you are migrating from Security Server V2R5, you would need to review an earlier edition of this document (GC28-1920-05), in addition to the current version.

Migration roadmap

Table 6. 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 RACF if you are using the restructured RACF database and meet the current z/OS 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 RACF.

   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 document:

   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 RACF from the following locations:

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

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

http://www.ibm.com/servers/eserver/zseries/zos/racf/

Chapter 3. z/OS Version 1 Release 4 Overview

The following sections describe the new and changed RACF functions that were introduced with z/OS Version 1 Release 4. 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

RACF Support for Enterprise Identity Mapping Services (EIM)

Description

Enterprise Identity Mapping Services (EIM) defines a set of services and extensions to LDAP. It will be available on all Enterprise Server Group (ESG) platforms - i/Series (OS/400®), z/Series (z/OS), p/Series (AIX®) and LINUX. EIM is an infrastructure that user administration applications, servers, operating systems, and audit tools can use to provide complete solutions to two classes of problems you experience:

- transforming the user identity associated with a work request as it moves between systems through a multi-tiered application
- administering userids in a heterogeneous environment

The RACF support for EIM in this release enables you to configure z/OS and servers to use an EIM domain.

IBM is developing a new eLiza-driven technology that will help address the challenge of multiple heterogeneous security registries existing in and between enterprises. By managing the relationship between identities that are identified within multiple applications, platforms, and middle-ware, EIM services will make it possible for an application to use one registry for user authentication while using a different registry to associate users with resource access control rules.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	The new EIM keywords are ADDUSER, ALTUSER, REDEFINE, and RALTER.
Application Development	R_admin callable service (IRRSEQ00) results updated when you specify new EIM keywords.
Auditing	Use of new keywords.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Commands” on page 108, “Callable Services” on page 103, “Data Areas” on page 116, “Database Templates” on page 120, “Panels” on page 128, “SMF Records” on page 132, and “SYS1.SAMPLIB Members” on page 135.

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
New fields are added to RACF templates (IRRTEMP1). IRRMIN00 must be run with PARM=UPDATE to add the changed templates to existing RACF databases.	Required.	*z/OS Security Server RACF Diagnosis Guide*

For More Information

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

- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Command Syntax Summary*
- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF Auditor's Guide*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Callable Services*

PKI Services

Description

This support for PKI Services includes support for the following:

- Support Email notification for completed certificate requests and expiration warnings
- Support MAIL, STREET and POSTALCODE distinguished name qualifiers
- Enhance the RACDCERT command and R_PKIServ callable service to support PKCS#7 certificate chains
- Remove clear text LDAP passwords from the pkiserv.conf file by storing them in RACF profiles
- Use the PCI cryptographic coprocessor to generate key pair, eliminating software key exposures
- Update the list of default CERTAUTH certificates in RACF. Provide VSAM RLS for the ICL and ObjectStore VSAM data sets in support of SYSPLEX enablement

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	RACF's RACDCERT TSO command has improved support for PKCS#7 certificate hierarchies and the ability to generate RSA key pairs using the PCI Cryptographic Coprocessor. See *z/OS Security Server RACF Command Language Reference* for more information.
Application Development	None.
Auditing	None.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to "Data Areas" on page 116, "SYS1.SAMPLIB Members" on page 135, "SMF Records" on page 132, "Panels" on page 128, "Callable Services" on page 103, and "Commands" on page 108.

Migration Procedures

The default CA Certificate, * IBM World Registry™ CA, has been deleted. Thus, if you are not sharing the RACF database with a downlevel system, you can delete this CA Certificate from the RACF database. It is not necessary to do, but you can now do it without RACF recreating this digital certificate.

For More Information

For more information about support for PKI Services, see the following publications:

- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Command Syntax Summary*
- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Messages and Codes*

- *z/OS Security Server RACF Auditor's Guide*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server PKI Services Guide and Reference*

UNIX Security Management Usability Enhancements

Description

The main objective of UNIX Security Management Usability Enhancements is to aid the RACF administrator in making sure that RACF users and groups run with a unique UNIX identity.

- A system-wide setting prevents assignment of a UID or GID value that is already in use. To handle exceptions to the ″one user ID/one UID″ rule, a RACF command keyword will be provided that will override the system setting and allow assignment of a shared UID or GID.
- A SEARCH enhancement allows an administrator to determine the set of users or groups assigned a given UID or GID.
- A mechanism is provided to automatically assign an unused UID or GID value to a user or group, which helps reduce manual steps and potential administrative error.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	The new UID and GID keywords of the SEARCH command allow you to determine the set of users who are assigned a specified UID, or the set of groups that are assigned the same GID, respectively. The new SHARED keyword in the OMVS segment allows you to assign a UID or GID that is already in use (applicable only if you are controlling shared UNIX UIDs and GIDs). The new AUTOUID and AUTOGID keywords in the OMVS segment allow you to request that RACF automatically assign a unique UID or GID value to a user or group.

Area	Considerations
Application Development	If you have CLISTs or REXX execs that define OMVS segments for users and groups, you must be aware that ADDUSER, ALTUSER, ADDGROUP, and ALTGROUP commands will now fail if an administrator implements SHARED.IDS, and the CLIST is assigning a UID or GID value that is already in use. This can occur when defining a user that requires a UID of zero. On a z/OS Version 1 Release 4 system, or on a lower level system with OW52135 applied, you can alter your commands to specify the new SHARED keyword. If SHARED.IDS is not implemented, the SHARED keyword will be ignored. If SHARED.IDS is implemented, and the ID you are assigning is already in use, the command will succeed as long as the user running the CLIST or REXX exec is SPECIAL, or has at least READ access to the SHARED.IDS profile. There are potential changes to the command image that RACF presents to the Common Command Exit (IRREVX01) in the postprocessing call. Before z/OS Version 1 Release 4, if the preprocessing exit changed the content of the command image, RACF sent the altered command image to the postprocessing exit exactly as the preprocessing exit returned it. However, as documented, RACF re-parses an altered command image before invoking the RACF command processor. As such, it is more correct to present the re-parsed command image to the postprocessing exit, since this was the actual command image that was executed. With z/OS V1R4, RACF now sends the more correct (the re-parsed) command image to the postprocessing exit. The command will be functionally equivalent to the command returned by the preprocessing exit. However, if the exit added abbreviated keywords, these keywords will be expanded. Also, the preprocessing exit must place any new keywords at the end of the command image, but the order in which the keywords appears can be different in the re-parsed command image that is presented to the postprocessing exit.
Auditing	You can log both successful and failed attempts to assign a shared UID or GID by setting the auditing options in the SHARED.IDS profile in the UNIXPRIV class.
Customization	You can define the SHARED.IDS profile in the UNIXPRIV class to prevent assignment of UNIX UIDs and GIDs that are already in use. You can define the BPX.NEXT.USER profile in the FACILITY class with an appropriate APPLDATA string in order to enable automatic UID/GID assignment using the new AUTOUID and AUTOGID keywords in the OMVS segment.
General User	None.
Operations	None.
Interfaces	Refer to “Commands” on page 108, “Data Areas” on page 116, and“Panels” on page 128.

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.

UNIX Security Management Usability Enhancements (z/OS V1R4)

Task	Condition	Reference Information
UNIX Security Management Usability Enhancements needs to have application identity mapping set to at least stage 2. If you have not done so already, use the IRRIRA00 utility to convert the RACF database to AIM stage 2 or 3.	Optional	*z/OS Security Server RACF System Programmer's Guide*
All systems sharing the RACF database, or participating in an RRSF network, must be upgraded to z/OS V1R4 or have APAR OW52135 applied. Otherwise, RACF will not be able to guarantee ID uniqueness when updates are made from a downlevel system. Further, automatic assignment requests made on one RRSF node will fail when propagated to a downlevel node.	Optional	None.

For More Information

For more information about UNIX Security Management Usability Enhancements, see the following publications:

- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Command Syntax Summary*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF System Programmer's Guide*
- *z/OS UNIX System Services Planning*
- *z/OS UNIX System Services Command Reference*
-

Program Access to Data Sets (PADS)

Description

This enhancement provides improved usability and increased security when using Program Control, Program Access to Data Sets (PADS), and optionally UNIX servers and daemons.

The increased security allows implementation of a new ENHANCED mode for program security that can make systems more resistant to malicious attacks.

The improved usability allows specification in the conditional access list of the program the user actually executed and makes it simpler to specify conditional access lists for PADS and to reduce administrator error.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	Affects how programs are defined and how WHEN(PROGRAM(...)) entries are defined in a conditional access list. Use SETROPTS and RDEFINE to specify PGMSECURITY mode (ENHANCED or BASIC) and optionally use RDEFINE and RALTER to define programs as MAIN or BASIC when running in ENHANCED program security mode.
Application Development	None.
Auditing	Event code 2 has a new event code qualifier 14, X'0E', and 15 X'0F'.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Data Areas” on page 116, “SMF Records” on page 132, and “Commands” on page 108.

Migration Procedures

Before changing how you specify conditional access lists, ensure that all systems sharing the RACF database have z/OS Version 1 Release 4 installed.

For More Information

For more information about Program Access to Data Sets (PADS), see the following publications:

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

Release FMID Update

Description

For compatibility with previous releases, the FMID HRF7707 is used as the RACF level, and is represented by the value 7707. The ICHEINTY, ICHETEST, ICHEACTN and RACROUTE macros have also been updated to accept the RELEASE=7707 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=7707 on the RACROUTE macro, you must assemble the application on a system that is running z/OS Version 1 Release 4. Also, if the application contains any other keywords on the RACROUTE macro that require RELEASE=7707, you must execute the application on a z/OS Version 1 Release 4 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 7707 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 116, “Macros” on page 125, and “SMF Records” on page 132.

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:

- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACROUTE Macro Reference*

For more information about theTSO/E functions, refer to the following publications:

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

Other Enhancements

Description

This section describes other enhancements that have been incorporated into this release.

- MLS Compatibility Support

  Additional multi-level security support is being added:

  – The SETROPTS command has been changed to update the MLACTIVE and MLS options.

    Upon installation, an administrator will not be allowed to enable these options unless the SECLABEL class is active. Also, the installation will not be able to deactivate the SECLABEL class if either MLS or MLACTIVE have been enabled.

  – Two new messages, ICH14076I and ICH14077I, will replace ICH14037I and ICH14038I.

- IRRICE Reporting

  – A new report, NWPI, is added to IRRICE to support user IDs that have a password interval value of NOINTERVAL.

  – A new report, GIDS, is added to locate instances of shared UNIX GIDs. This is similar to the existing UIDS report.

- UNIX Access Enhancement (APAR OW52941)

  – Audit function code support for UNIX System Services is being added to RACF callable service, ck_access (IRRSKA00) to improve access checking for z/OS UNIX files and directories. In addition, UNIXPRIV authority will now be checked for the existing AFC_ACCESS audit function code, as long as the real, effective, and saved UIDs of the process are the same, and the real, effective, and saved GIDs of the process are the same.

- UNIX file group ownership option

  This enhancement provides administrators a system-wide mechanism of choosing how the group owner of a new HFS file is assigned. It can either come from the group owner of the parent directory, as it is prior to z/OS V1R4, or it can come from the effective GID of the creating process.

  If the administrator defines a UNIXPRIV profile named FILE.GROUPOWNER.SETGID, then the set-gid bit for a directory determines how the group owner is initialized for new objects created within the directory:

  – If the set-gid bit is on, then the owning GID is set to that of the directory

  – If the set-gid bit is off, then the owning GID is set to the effective GID of the process

  In order to use the FILE.GROUPOWNER.SETGID profile in a shared HFS environment, all nodes sharing HFS must be at Version 1 Release 4 (or higher). Between any two nodes sharing HFS, if either of them is downlevel, the group owner for a new file will always be set from the parent directory, regardless of whether FILE.GROUPOWNER.SETGID exists. If one node has a separate RACF database, then that node will be considered downlevel if the FILE.GROUPOWNER.SETGID profile does not exist, even if the node is at z/OS Version 1 Release 4.

- RACROUTE REQUEST=VERIFY(X) Suppression of RACF Abends

  – When there is an error with the RACF data manager during the use of REQUEST=VERIFY or REQUEST=VERIFY(X), an abend code 483 occurs. A

new keyword, ERROROPT, is added to this support to issue a return and reason code, instead of the abend code.

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 108, “Callable Services” on page 103 and “Data Areas” on page 116.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

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

- *z/OS Security Server RACF Auditor’s Guide*
- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Command Language Reference*

Service Updates

Description

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

- APAR OW50327 enables RACF to allow program control access READ to the modules in SYS1.LINKLIB if they are accessed via UACC(NONE) on a * or ** PROGRAM class profile. Otherwise, the specified access will be used. If any access entry of ID(*) with ACC(NONE) for this same profile is used with any UACC, then it will be changed to READ. Also, new message, ICH580I, will be issued by the SETR WHEN(PROGRAM) routine to indicate that one of these profiles were found.
- APAR OW54280 indicates that RACF commands that provide output listings (LISTDSD, LISTUSER, LISTGROUP, RLIST) are designed to be issued by users, not by programs. RACF list commands, such as `LISTUSER *` or `LISTGRP *`, can generate many thousands of lines of output. This consumes many address space resources. RACF does not support the command output as a programming interface.

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	None.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

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

- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Command Language Reference*

Service Updates (z/OS V1R4)

Chapter 4. z/OS Version 1 Release 3 Overview

The following sections describe the new and changed RACF functions that were introduced with z/OS Version 1 Release 3. 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

Access Control Lists (ACLs)

Description

This support for Access Control Lists (ACLs) allows you to control access to files and directories by individual user (UID) and group (GID). To manage an ACL for a file, you must either be the file owner or have superuser authority (UID=0 or have READ access to SUPERUSER.FILESYS.CHANGEPERMS in the UNIXPRIV class). UNIX file security on z/OS uses permission bits to control access to files, in accordance with the POSIX standard. However, the permission bit model does not allow for granting and denying access to specific users and groups, such as is possible using RACF profiles. This function will be provided by the introduction of Access Control Lists (ACLs) in the UNIX file system. An ACL is a SAF-owned construct which resides within the file system. The RESTRICTED attribute of a user will now be applicable to file and directory access.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	You can use the z/OS UNIX setfacl command to define ACLs.
Application Development	None.
Auditing	You can use SETROPTS LOGOPTIONS for the FSSEC class to audit changes to ACLs.
Customization	You need to determine whether you want to use the two UNIXPRIV profiles; one to make ACLs override UNIXPRIV authority and one to make ACLs work like RACF profiles regarding RESTRICTED users.
General User	You can use the z/OS UNIX setfacl command to define ACLs.
Operations	None.
Interfaces	Refer to “Utilities” on page 141, “SYS1.SAMPLIB Members” on page 135, “Data Areas” on page 116 and “Callable Services” on page 103.

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
Upgrade any systems that share HFS to z/OS V1R3 or, at a minimum, apply the compatibility APAR (OW50655 for SAF, and OW49334 for RACF) to the downlevel systems.	Optional	None.
Until you want ACLs to be used in access checks, make sure FSSEC is inactive. When you are ready to use ACLs, issue: SETROPTS CLASSACT(FSSEC). Note that ACLs can be defined (and inherited) while FSSEC is inactive.	Required	*z/OS Security Server RACF Security Administrator’s Guide*

For More Information

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

- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS UNIX System Services Planning*
- *z/OS UNIX System Services Command Reference*

PKI Services

Description

This support for PKI Services includes certificate support for the following:

- Administrative approval processes using a web–based interface for the selective approval, rejection, and revocation of certificates (life cycle management). Clients can also renew and revoke their own certificates.
- Certificates created are posted to an LDAP directory.
- Certificate revocation lists (CRLs) maintained and posted to an LDAP directory.
- Coexists with the RACF V2R10 SPE. Installation chooses certificate generation provider:
  - SAF - uses the existing limited Security Server (RACF) certificate support
  - PKI - uses new PKI Services component
- R_PKIServ SAF service extended to provide additional functions that support the programmatic request of certificates and certificate management used by the Web user and Web administrator functions.

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 “Callable Services” on page 103, “Utilities” on page 141, and “SYS1.SAMPLIB Members” on page 135.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

For more information about support for PKI Services, see the following publications:

- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server PKI Services Guide and Reference*

Policy Director Authorization Services for z/OS and OS/390

Description

This support for Policy Director Authorization Services Support includes the following:

- Support for a new callable service, R_cacheserv (IRRSCH00), which provides cache management services for application invokers.
- Support for another new callable service, R_proxyserv (IRRSPY00), which allows invokers to retrieve information from an LDAP directory, without requiring a POSIX environment.
- RACF SMF Unload (IRRADU00) support for new SMF Type 80 records cut by z/OS Policy Director Services Authorization Services for the aznAccess SAF callable service. The maximum output record size for IRRADU00 has been increased to 8192.
- RACF database profile segment and command enhancements.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	Authority to the new IRR.RCACHESERV.*cachename* resource in the FACILITY class will allow a server that is not running in supervisor state or with the system key to use the R_cacheserv callable service. UPDATE authority allows the server to utilize all the R_cacheserv callable service functions, while READ authority is all that is necessary to utilize the Fetch, X'0004', function. Authority to the new IRR.RPROXYSERV resource in the FACILITY class will also allow a server to use the R_proxyserv callable service. In an RRSF environment, commands defining base profiles in the new CACHECLS class should not be directed to downlevel systems because they will fail.
Application Development	None.
Auditing	New event code, decimal 71, and extended-length relocation section variable data types, decimal 352, 353, 354, 355, 356, and 372, have been added to the SMF Type 80 record. For IRRADU00, the LRECL on the OUTDD statement has been changed to 8192.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to "Commands" on page 108, "Data Areas" on page 116, "Callable Services" on page 103, "Class Descriptor Table (CDT)" on page 106, "Utilities" on page 141, "SYS1.SAMPLIB Members" on page 135, "Database Templates" on page 120, and "Panels" on page 128.

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 database templates” on page 5
Run the dynamic parse utility.	Required	“Running dynamic parse” on page 5
When using IRRADU00, ensure the LRECL on the OUTDD statement of the JCL is changed to 8192.	Required	*z/OS Security Server RACF Auditor's Guide*, Chapter 3, ″Using IRRADU00″

For More Information

For more information about Policy Director Authorization Services Support, see the following publications:

- *z/OS Security Server RACF Auditor's Guide*
- *z/OS Security Server RACF Callable Services*
- *Policy Director Authorization Services for z/OS and OS/390 Customization and Use*

Release FMID Update

Description

For compatibility with previous releases, the FMID HRF7706 is used as the RACF level, and is represented by the value 7706. The ICHEINTY, ICHETEST, ICHEACTN and RACROUTE macros have also been updated to accept the RELEASE=7706 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=7706 on the RACROUTE macro, you must assemble the application on a system that is running z/OS Version 1 Release 3. Also, if the application contains any other keywords on the RACROUTE macro that require RELEASE=7706, you must execute the application on a z/OS Version 1 Release 3 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 7706 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 116, “Macros” on page 125, and “SMF Records” on page 132.

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:

- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACROUTE Macro Reference*

For more information about theTSO/E functions, refer to the following publications:

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

Other Enhancements

Description

This section describes other enhancements that have been incorporated into this release.

- Audit Support for z/OS UNIX Shutdown Registration Service
  - New audit function code, AFC_SHUTDOWN_REG, is added to support the z/OS UNIX System Services shutdown registration service. The ck_priv callable service is updated to audit this event based on the SETR LOGOPTIONS setting of the PROCESS class.
- CDT Updates for PRINTSRV Class
  - A new class, PRINTSRV, is added to the class descriptor table (CDT) to support Infoprint Server, allowing them to protect printer definitions with RACF.
- ICEGENER Utility Update
  - Customers who have installed DFSORT release 14 may see new messages issued by the IRRUT200 utility. With DFSORT release 14, RACF can use the ICEGENER utility to copy the RACF database, as opposed to the IEBGENER utility which would have otherwise been used. ICEGENER produces more detailed messages than IEBGENER produces.

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 “Class Descriptor Table (CDT)” on page 106 and “Data Areas” on page 116.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

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

- *z/OS Security Server RACF Auditor’s Guide*
- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Macros and Interfaces*

Service Updates

Description

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

- APAR OW49124 modifies the RACF SMF Data Unload utility (IRRADU00) to store Relocate 47 data in the IRRADU00 utility output record.
- APAR OW46174 modifies the logic in callable service check_access to check the UNIXPRIV Class (superuser.filesys) for read authority when doing a directory search. Also, Open will check for read authority, instead of update, when doing a search and Opendir will check for read authority.

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 “Callable Services” on page 103 and *z/OS Security Server RACF Macros and Interfaces*.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

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

- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Macros and Interfaces*

Service Updates (z/OS V1R3)

Chapter 5. z/OS Version 1 Release 2 Overview

The following sections describe the new and changed RACF functions that were introduced with z/OS Version 1 Release 2. 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

The table below summarizes the RACF updates that were introduced with z/OS Version 1 Release 2. For more information, refer to the detailed section for each item.

Table 7. Summary of RACF Updates for z/OS Version 1 Release 2

For Information About:	Refer to Topic:
DB2 Version 7 Support	42
Enterprise Java Beans	44
Mixed-Case Profile Names	45
Network Authentication Service Support	48
SAF Trace	50
Universal Groups	51
Release FMID Update	54
Enhancements for z/OS UNIX	55
Other Enhancements	56
Service Updates	58

DB2 Version 7 Support

Description

This support introduces the following new classes to support the new DB2 Java archive (JAR) object introduced with DB2 Version 7. The RACF/DB2 external security module (IRR@XACS) is updated to map access requests for the new JAR object, and its USAGEAUTJ privilege, into the new RACF classes.

MDSNJR Member class for the DB2 Java archive (JAR) object.

GDSNJR Grouping class for the DB2 Java archive (JAR) object.

The RACF/DB2 external security module is updated to pass database names in support of DBADM authorization checking for the following privileges:

- CREATE VIEW
- ALTER INDEX
- DROP INDEX

The RACF/DB2 external security module is also updated to include support for the new `&ERROROPT` customization option for use with DB2 Version 7. This support includes new and changed initialization reason codes for `XAPLFUNC=1`, and new and changed RACF messages.

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 JAR object, the new `&ERROROPT` option, and enhanced authorization checking for the CREATE VIEW, ALTER INDEX and DROP INDEX privileges.
General User	None.
Operations	None.
Interfaces	Refer to “Class Descriptor Table (CDT)” on page 106, “Exits” on page 123, “Messages” on page 128 and “SYS1.SAMPLIB Members” on page 135.

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 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 7
Define RACF profiles for the new DB2 objects and activate the new classes.	Optional	*z/OS Security Server RACF Security Administrator's Guide*
Customize, assemble and install the sample exit code that is supplied with RACF in the SAMPLIB member IRR@XACS using the DB2 Version 7 libraries.	Optional	*z/OS Security Server RACF System Programmer's Guide*
Stop and restart your DB2 subsystem to use the RACF/DB2 external security module.	Optional	*z/OS Security Server RACF System Programmer's Guide*
If you share the RACF database with downlevel systems, install APAR OW45152 on systems running the following releases to share support for DB2 Version 7: • z/OS Version 1 Release 1 (HRF7703) • OS/390 Version 2 Release 10 (HRF7703) • OS/390 Version 2 Release 9 (HRF2608) • OS/390 Version 2 Release 8 (HRF2608) • OS/390 Version 2 Release 6 (HRF2260)	Optional	None.

For More Information

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

- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF System Programmer's Guide*

For more information about DB2, see the following publications:

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

Enterprise Java Beans

Description

This support for Enterprise Java Beans includes two new classes in the class descriptor table and corresponding entries in the RACF router table:

EJBROLE Member class for Enterprise Java Beans authorization roles.

GEJBROLE Grouping class for Enterprise Java Beans authorization roles.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	The new EJBROLE and GEJBROLE classes support mixed-case profile names. This allows for mixed-case Enterprise Java Beans authorization role names. See “Mixed-Case Profile Names” on page 45 for more information.
Application Development	None.
Auditing	None.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Class Descriptor Table (CDT)” on page 106.

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
If you share the RACF database with downlevel systems, install APAR OW46859 on systems running the following releases to share support for Enterprise Java Beans: • z/OS Version 1 Release 1 (HRF7703) • OS/390 Version 2 Release 10 (HRF7703) • OS/390 Version 2 Release 9 (HRF2608) • OS/390 Version 2 Release 8 (HRF2608)	Optional	None.

For More Information

For more information about support for Enterprise Java Beans, see the following publication:

- *WebSphere Application Server V4.0 for z/OS and OS/390: Assembling J2EE Applications*

Mixed-Case Profile Names

Description

This support allows mixed-case profile names to be used for classes that are defined in the class descriptor table (CDT) using the new `CASE=ASIS` operand of the ICHERCDE macro. The following commands have been updated as part of this support:

- ADDSD
- PERMIT
- RALTER
- RDEFINE
- RDELETE
- RLIST
- SEARCH

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	For classes defined in the CDT with the new CASE=ASIS operand allowing mixed-case profile names, RACF commands do not fold the characters of the profile name to uppercase, but now preserve the case as entered. For these classes, you should be sure to enter profile names in the exact case desired. ISPF panels display the name as it is entered and pass it to the command, which determines whether it needs to be converted to an uppercase name or preserved as a mixed-case name. If you have RACF remote sharing facility (RRSF) implemented, you should ensure that any CDT entries you define with CASE=ASIS are defined the same way on all participating RRSF nodes. If an inconsistency is created, commands will be folded to uppercase on source or target nodes where the class is defined, or defaulted to, CASE=UPPER. This will result in different profile names than were intended. The CLIST option of the SEARCH command is enhanced to preserve the case of character strings. If character strings are specified, the statement CONTROL ASIS appears in the first line of the output CLIST. If your installation has an automated process that processes the output CLIST, you should ensure that it works correctly with mixed-case strings and with the added statement.

Mixed-Case Profile Names (z/OS V1R2)

Area	Considerations
Application Development	The RACF command preprocessing exit (ICHCNX00) and the general command exit (IRREVX01) receive RACF command images as part of their input. In some cases, a profile name or member name will appear in the command image in the case in which it was entered, even for classes that support only uppercase profile names. If an exit examines this profile name, it must take into account the possibility that the profile or member name needs to be folded to uppercase. If the class is DATASET, the exit can always safely fold the name to uppercase. Otherwise, issue a RACROUTE REQUEST=STAT for the relevant class to retrieve a copy of the class descriptor table (CDT) entry for the class. If the CNSTCASE bit in the CDT entry is 0, the exit should fold the profile name to uppercase. Note that for ICHCNX00, the CNXRESNM field contains a pointer to the data set name for which the exit is being invoked. This copy of the data set name will always be in uppercase and fully qualified, and this field should be used instead of the data set name as it appears in the command image.
Auditing	None.
Customization	None.
General User	None.
Operations	Mixed-case profile names are not supported with RACF commands entered at the operator console.
Interfaces	Refer to “Commands” on page 108, “Data Areas” on page 116, “Macros” on page 125, and “Panels” on page 128.

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
If you share the RACF database with downlevel systems, install APAR OW46859 on systems running the following releases to share support for mixed-case profile names: • z/OS Version 1 Release 1 (HRF7703) • OS/390 Version 2 Release 10 (HRF7703) • OS/390 Version 2 Release 9 (HRF2608) • OS/390 Version 2 Release 8 (HRF2608)	Optional	None.
If you have programs that process the output CLIST created by the SEARCH command, you should ensure that they properly handle the new `CONTROL ASIS` statement.	Required	*z/OS Security Server RACF Command Language Reference*

For More Information

For more information about mixed-case profile names, see the following publication:

- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Macros and Interfaces*

- *z/OS Security Server RACF System Programmer's Guide*
- *z/OS Security Server RACF Data Areas*

Network Authentication Service Support

Description

This support provides the ability to store and retrieve keys encrypted using the DES3 and DESD (DES with derivation) encryption algorithms. Previously, DES was the only supported encryption algorithm. It also allows the administrator to choose which key types will be used for authentication of users and realms by setting new ENCRYPT options in the KERB segments of user and realm profiles. The new options are specified using the new KERB ENCRYPT operand of the ADDUSER, ALTUSER, RDEFINE and RALTER commands. This support also provides a new SETROPTS KERBLVL option to control use of the new key types on a system-wide basis.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	Once SETROPTS KERBLVL(1) in enabled, you should not reset to KERBLVL(0). This may create inconsistencies in the processing of encryption keys. See *z/OS Security Server RACF Security Administrator's Guide* for more information.
Application Development	None.
Auditing	None.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to "Callable Services" on page 103, "Commands" on page 108, "Database Templates" on page 120, "Messages" on page 128, "Panels" on page 128, "SMF Records" on page 132, "SYS1.SAMPLIB Members" on page 135 and "Utilities" on page 141.

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
Define a z/OS UNIX user identifier (UID) for the user ID associated with the RACF address space and for each user or administrator who generates keys. As an alternative, you may customize your z/OS UNIX environment to allow default OMVS segment processing.	Optional	*z/OS Security Server RACF Security Administrator's Guide* *z/OS Security Server RACF Command Language Reference*

Task	Condition	Reference Information
Ensure that all systems sharing your RACF database support the SETROPTS KERBLVL command before enabling KERBLVL(1). As an alternative, you may enable KERBLVL(1) if you ensure that no keys are generated or used from downlevel systems.	Optional	*z/OS Security Server RACF Security Administrator's Guide* *z/OS Security Server RACF Command Language Reference*

For More Information

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

- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF Auditor's Guide*

SAF Trace

Description

This support enables the capture of interface parameters and other useful debug information without setting slip traps and acquiring dumps. Time and resources spent with the IBM support center resolving RACF problems can be reduced. This support enhances the RACF SET TRACE command with several additional suboperands to enable tracing for RACROUTE macro executions, RACF database manager requests, callable services, address spaces, and jobs.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	Authority to issue the SET TRACE command is controlled by resource names in the OPERCMDS class with the following format: *subsystem*.SET.TRACE
Application Development	None.
Auditing	None.
Customization	None.
General User	None.
Operations	System performance can be negatively affected by enabling tracing of RACF events using the SET TRACE command. Use trace options judiciously and monitor system performance while trace options are in effect.
Interfaces	Refer to “Commands” on page 108.

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:

- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF System Programmer’s Guide*
- *z/OS Security Server RACF Diagnosis Guide*

Universal Groups

Description

This support provides the new UNIVERSAL operand for the ADDGROUP command to define a universal group. A universal group is a group that allows an unlimited number of users to be connected. The member list of a universal group contains only entries for users connected with a group authority higher than USE, or for those with group-SPECIAL, group-OPERATIONS, or group-AUDITOR attributes. Therefore, all members of a universal group may not be listed using the LISTGRP command.

To list all members of a universal group, you should use the RACF database unload utility (IRRDBU00). The following two sample RACFICE reports, based on IRRDBU00, were added to SYS1.SAMPLIB in support of universal groups:

CUG$ Lists group names of all universal groups.

GPRM Lists the user IDs of all members of a group, including a universal group.

A new message ICH05008I was also added to warn users who delete a universal group using the DELGROUP command that the remove ID utility (IRRRID00) should be run to ensure that all members are removed from the deleted group.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	All members of a universal group may not be listed using the LISTGRP command. To list all members of a universal group, you should use the output of the RACF database unload utility (IRRDBU00) to create reports with DB2 or RACFICE. Although you can use the DELGROUP command, you should use the remove ID utility (IRRRID00), specifying the group name, to delete a universal group. Be sure to execute the resulting REMOVE commands to ensure that all users are removed from the group. If you do not execute the REMOVE commands, user profiles for users who are not removed from the deleted group will contain residual data related to the deleted group connection. If you share your RACF database with downlevel systems: • You may delete and remove users from a universal group by issuing the DELUSER and REMOVE commands from a downlevel system. • When you connect a user to a universal group with group authority of USE from a downlevel system, the user ID will be added to the member list in the group profile. Issuing the ALTUSER command with AUTHORITY specified will also add the user to the member list. To remove a user from the member list of a universal group, you can issue a CONNECT command with AUTHORITY(USE) from an uplevel system that has universal group support. • When you delete a universal group that contains no members in the member list from a downlevel system, the DELGROUP will be successful. However, you will not receive a warning message indicating that you have deleted a universal group and that you should ensure that all members are removed. • An ADDGROUP command with UNIVERSAL specified will fail if directed to a downlevel system by RRSF.
Application Development	None.
Auditing	New UNIVERSAL operand of the ADDGROUP command is audited in the standard format of the SMF records associated with this commands.
Customization	None.
General User	None.
Operations	None.
Interfaces	Refer to “Callable Services” on page 103, “Commands” on page 108, “Database Templates” on page 120, “Messages” on page 128, “Panels” on page 128, “SMF Records” on page 132, “SYS1.SAMPLIB Members” on page 135 and “Utilities” on page 141.

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:

- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Callable Services*

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 HRF7705 is used as the RACF level, and is represented by the value 7705. The ICHEINTY, ICHETEST, ICHEACTN and RACROUTE macros have also been updated to accept the RELEASE=7705 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=7705 on the RACROUTE macro, you must assemble the application on a system that is running z/OS Version 1 Release 2. Also, if the application contains any other keywords on the RACROUTE macro that require RELEASE=7705, you must execute the application on a z/OS Version 1 Release 2 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 7705 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 116, “Macros” on page 125, and “SMF Records” on page 132.

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:

- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACROUTE Macro Reference*

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

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

Enhancements for z/OS UNIX

Description

This section describes enhancements that have been incorporated into this release in support of z/OS UNIX.

- As an enhancement to superuser granularity, the RACF `R_chmod` callable service (IRRSCF00) has been updated to check the caller's authorization to resource SUPERUSER.FILESYS.CHANGEPERMS in the UNIXPRIV class if the caller's user ID does not have UID(0) or is not the owner of the file. If the user executing the **chmod** command has at least READ authority to the resource, the user is authorized to change the file mode in the same manner as a user having UID(0).
- Processing for the ICH408I message has been enhanced to provide the user identifier (UID) and group identifier (GID) used to make access control decisions for z/OS UNIX resources. A new line in the ICH408I message will now contain the effective UID and effective GID for z/OS UNIX authorization failures.

Migration Procedures

No special migration procedures are required to user this support.

For More Information

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

- *z/OS UNIX System Services Planning*
- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Auditor's Guide*

Other Enhancements

Description

This section describes other enhancements that have been incorporated into this release.

- Reliability of RACF data sharing mode has been improved by reducing the occurrence of RACF abends due to coupling facility failures. This support allows RACF manager to retry requests that are in progress when a coupling facility rebuild takes place. This addresses APAR OW40605 which was closed as a suggestion.
- Performance has been enhanced for environments running in sysplex communication mode with Virtual Lookaside Facility (VLF) active. This support uses cross-system messaging facility (XCF) to improve ACEE VLF caching by reducing the number of times the VLF cache is purged. Performance improvements are provided only for systems running z/OS Version 1 Release 2 or higher. APAR OW46269 must be installed on all downlevel systems in sysplexes running in sysplex communication mode.
- The database unload utility (IRRDBU00) has changed its processing of the GRBD_UACC field in the General Resource Basic Data record (0500) for profiles in the DIGTCERT class. The following flags are now unloaded with the following UACC values:
  X'80' TRUST
  X'00' NOTRUST
  X'C0' HIGHTRST

  The RACFICE tool in SYS1.SAMPLIB member IRRICE has also been updated to exclude profiles in the DIGTCERT class when searching for general resource profiles with UACC other than NONE.
- The `R_admin` callable service (IRRSEQ00) has been updated. IRRSEQ00 will no longer allow unauthorized callers to specify subpool 0 for output messages, and will now restrict them to subpools 1–127. Unauthorized callers that specify subpool 0, or any other subpool outside this range, will receive return code 8 with reason code 4, indicating a parameter list error.
- The processing for exits ICHDEX01 and ICHDEX11 has been changed to add return code 16. When present, if one of these exits delivers return code 16 for an operation, RACF will use DES encryption for the storing of passwords. For the comparing of passwords, RACF will first use DES, and if DES processing fails, RACF will use masking. Effectively, if one of these exits delivers return code 16, RACF will process as if the exit were not present.

What This Change Affects

This support might affect the following areas of RACF processing.

Area	Considerations
Administration	None.
Application Development	Unauthorized callers of IRRSEQ00 are now limited to subpools 1–127 for output messages, and will receive return code 8 with reason code 4 (parameter list error) if subpool 0, or any other subpool outside this range, is specified.
Auditing	None.
Customization	None.

Area	Considerations
General User	None.
Operations	• Messages associated with a coupling facility failure may not appear as quickly following a failure as they did prior to installing z/OS Version 1 Release 2. In addition, some failure messages may now be followed by recovery action rather than an abend. • You may experience errors or outages on downlevel systems, if you install z/OS Version 1 Release 2 on a system in a sysplex running RACF in sysplex communication mode before installing required APAR OW46269 on all downlevel systems in your sysplex.
Interfaces	None.

Migration Procedures

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

Task	Condition	Reference Information
Before installing z/OS Version 1 Release 2 on a system in a sysplex running RACF in sysplex communication mode, you must install the appropriate PTFs for OW46269 on all downlevel systems in your sysplex. **UW79591** OS/390 Version 2 Release 6 (HRF2260) **UW79592** OS/390 Version 2 Release 8 (HRF2608) **UW79593** OS/390 Version 2 Release 10 (HRF7703) For installations that do not run RACF in sysplex communication mode, this task is not required.	Required	None.
If you have applications that process output from the IRRDBU00 utility, ensure that they are able to correctly process the changed 0500 data records for profiles in the DIGTCERT class.	Required	*z/OS Security Server RACF Macros and Interfaces*
If you have unauthorized programs that invoke the `R_admin` callable service (IRRSEQ00), ensure that they specify subpools in the range of 1–127 for output messages.	Required	*z/OS Security Server RACF Callable Services*

Service Updates

Description

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

APAR OW42913 modifies RACROUTE REQUEST=VERIFY processing to validate new passwords against the installation's syntax rules before it invokes the password processing exit (ICHPWX01). This processing sequence is changed to match the sequence of new-password validation processing used by the PASSWORD and ALTUSER commands. This support also adds more information, such as user name, to the SMF data unload (IRRADU00) output record for new-password failures processed by ICHPWX01.

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	With APAR OW42913, when RACROUTE REQUEST=VERIFY encounters multiple user errors, the order in which they are reported may be different than it was prior to installing z/OS Version 1 Release 2. Also, IRRADU00 output records may contain more information related to new-password failures that were processed by ICHPWX01.
Interfaces	None.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

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

- *z/OS Security Server RACF System Programmer's Guide*

Chapter 6. z/OS Version 1 Release 1 Overview

RACF for z/OS Version 1 Release 1 is functionally equivalent to RACF for OS/390 Version 2 Release 10. HRF7703 is the FMID for the RACF component of both z/OS Version 1 Release 1 and OS/390 Version 2 Release 10.

Considerations for migrating to z/OS Version 1 Release 1 are the same considerations for migrating to OS/390 Version 2 Release 10. See Chapter 7, “OS/390 Version 2 Release 10 overview” on page 61.

There are no unique migration considerations for migrating to z/OS Version 1 Release 1.

Chapter 7. OS/390 Version 2 Release 10 overview

The following sections describe the RACF functions that were introduced with OS/390 Version 2 Release 10 and are available with z/OS Version 1 Release 1. Note that RACF for z/OS Version 1 Release 1 and RACF for OS/390 Version 2 Release 10 are functionally equivalent. 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 8 summarizes the RACF updates that were introduced with OS/390 Version 2 Release 10 and are available with z/OS Version 1 Release 1. Note that RACF for z/OS Version 1 Release 1 and RACF for OS/390 Version 2 Release 10 are functionally equivalent. For more information, refer to the detailed section for each item.

Table 8. Summary of RACF updates for OS/390 Version 2 Release 10

For Information About:	Refer to Topic:
Certificate Name Filtering	62
Network Authentication Service	66
Program Control Enhancements	68
Application Identity Mapping	69
Enhanced PassTicket Support	71
Public Key Certificate Enhancements	72
Enhanced Superuser Granularity	74
IBM License Manager	75
Release FMID Update	76
Service Updates	78

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 (IRRRID00) 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 103, “Class Descriptor Table (CDT)” on page 106, “Commands” on page 108, “Data Areas” on page 116, “Database Templates” on page 120, “Exits” on page 123, “Macros” on page 125, “Messages” on page 128, “Panels” on page 128, “SMF Records” on page 132, “SYS1.SAMPLIB Members” on page 135, and “Utilities” on page 141.

Coexistence Considerations

Note: Certificate name filtering support is only available on z/OS Version 1 Release 1, 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 (IRRRID00) 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

Certificate name filtering (OS/390 V2R10)

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 database templates” on page 5
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 7
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	*z/OS Security Server RACF Security Administrator’s Guide*

For More Information

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

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

- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACROUTE Macro Reference*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF System Programmer's Guide*

Network Authentication Service

Description

This support allows principal and realm information for Security Server Network Authentication Service 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 Service. R_kerbinfo retrieves the principal and realm information stored in RACF, and R_ticketserv enables z/OS and 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 103, “Commands” on page 108, “Data Areas” on page 116, “Database Templates” on page 120, “Messages” on page 128, “Panels” on page 128, “SMF Records” on page 132, and “SYS1.SAMPLIB Members” on page 135.

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 database templates” on page 5
Run the dynamic parse utility.	Required	“Running dynamic parse” on page 5
Use the TARGET command to define the local system as the local RACF remote sharing facility (RRSF) node.	Optional	*z/OS Security Server RACF Security Administrator’s Guide*

For More Information

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

- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Command Language Reference*

- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF Security Administrator's Guide*

Program Control Enhancements

Description

These enhancements were created to provide better security and integrity for z/OS UNIX by making it easier to use z/OS 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	z/OS 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 103, “Data Areas” on page 116, and “Macros” on page 125.

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:

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

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

- *z/OS UNIX System Services Planning*

Application Identity Mapping

Description

Application identity mapping provides an improved method for associating identities defined by z/OS UNIX, Novell Directory Services for OS/390, and Lotus Notes for z/OS applications to RACF user IDs. A new utility, IRRIRA00, converts UNIXMAP, NOTELINK and NDSLINK mapping profiles to alias index entries that 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 z/OS 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 108, “Data Areas” on page 116, “Database Templates” on page 120, “Macros” on page 125,“Messages” on page 128, “SYS1.SAMPLIB Members” on page 135, and “Utilities” on page 141.

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 *z/OS 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	*z/OS Security Server RACF System Programmer's Guide*

For More Information

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

- *z/OS UNIX System Services Planning*
- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Macros and Interfaces*

Application Identity Mapping (OS/390 V2R10)

- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF System Programmer's Guide*

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

- *z/OS 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 PassTicket 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.

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 108.

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:

- *z/OS Security Server RACF Security Administrator’s Guide*
- *z/OS Security Server RACF System Programmer’s Guide*
- *z/OS 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 *z/OS 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 103, “Commands” on page 108, “Data Areas” on page 116, “Panels” on page 128, and “Utilities” on page 141.

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:

- *z/OS Security Server RACF System Programmer’s Guide*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Messages and Codes*
- *z/OS Security Server RACF Security Administrator’s Guide*
- *z/OS Security Server RACROUTE Macro Reference*
- *z/OS Security Server RACF Callable Services*

Enhanced Superuser Granularity

Description

This enhanced support verifies that a z/OS UNIX user has the necessary privilege to perform a **chmount**. z/OS 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 116.

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:

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

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

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

IBM License Manager

Description

This support for IBM License Manager is provided by APAR OW44238, and includes the new ILMADMIN class in the class descriptor table and a corresponding entry in the RACF router table.

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 “Class Descriptor Table (CDT)” on page 106.

Migration Procedures

No special migration procedures are required to use this support.

For More Information

For more information about IBM License Manager, see the following publication:

- *z/OS IBM License Manager: Administration*

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.

Note: HRF7703 is the FMID for the RACF component of both z/OS Version 1 Release 1 and OS/390 Version 2 Release 10. RACF for z/OS Version 1 Release 1 and RACF for OS/390 Version 2 Release 10 are functionally equivalent.

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 z/OS Version 1 Release 1 or OS/390 Version 2 Release 10. Also, if the application contains any other keywords on the RACROUTE macro that require RELEASE=7703, you must execute the application on a z/OS Version 1 Release 1 or OS/390 Version 2 Release 10 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 116, “Macros” on page 125, and “SMF Records” on page 132.

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:

- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACROUTE Macro Reference*

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

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

Service Updates

Description

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 132.

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	*z/OS Security Server RACROUTE Macro Reference*

For More Information

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

- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACROUTE Macro Reference*

Chapter 8. OS/390 Version 2 Release 8 Overview

The following sections describe the new and changed RACF functions that were introduced with OS/390 Version 2 Release 8. 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 9 summarizes the RACF updates that were introduced with OS/390 Version 2 Release 8. For more information, refer to the detailed section for each item.

Table 9. Summary of RACF Updates for OS/390 Version 2 Release 8

For Information About:	Refer to Topic:
Class Descriptor Table Enhancements	80
DB2 Version 6 Support	83
ICETOOL Support	85
Lotus Notes for z/OS and Novell Directory Services for OS/390 Support	86
Superuser Granularity	88
z/OS UNIX User Limits	90
Protected User ID	92
Public Key Certificate Enhancements	94
R_admin SETROPTS	98
Release FMID Update	99
Service Updates	100

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.
- z/OS Communication Server

  The new SERVAUTH class provides improved security for TN3270 access to z/OS and OS/390 systems. z/OS 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 z/OS

  The new JAVA class has been created to enable Java for z/OS 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 81 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 (CDT)” on page 106 and “Data Areas” on page 116.

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 7

CDT Enhancements (OS/390 V2R8)

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	*z/OS 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	*z/OS Security Server 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	*z/OS Security Server RACROUTE Macro Reference*

For More Information

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

- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF System Programmer's Guide*
- *z/OS Security Server RACROUTE Macro Reference*

DB2 Version 6 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 privileges.
General User	None.
Operations	None.
Interfaces	Refer to “Class Descriptor Table (CDT)” on page 106, “Exits” on page 123, and “SYS1.SAMPLIB Members” on page 135.

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 V6 Support (OS/390 V2R8)

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 7
Define RACF profiles for the new DB2 objects and activate the new classes.	Optional	*z/OS 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 using the new DB2 libraries.	Optional	*z/OS Security Server RACF System Programmer’s Guide*
Stop and restart your DB2 subsystem to use the RACF/DB2 external security module.	Optional	*z/OS Security Server RACF System Programmer’s Guide*

For More Information

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

- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACF Security Administrator’s Guide*
- *z/OS 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 135.

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:

- *z/OS Security Server RACF Auditor’s Guide*
- *z/OS 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 z/OS and Novell Directory Services for OS/390 Support

Description

This enhancement enables RACF to map a user identity from a Lotus Notes for z/OS 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. As such, existing 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 103, "Class Descriptor Table (CDT)" on page 106, "Commands" on page 108, "Data Areas" on page 116, "Database Templates" on page 120, "Messages" on page 128, "Panels" on page 128, "SYS1.SAMPLIB Members" on page 135, and "Utilities" on page 141.

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 database templates" on page 5
Run the dynamic parse utility.	Required	"Running dynamic parse" on page 5
Define a user ID for the application.	Optional	*z/OS Security Server RACF Security Administrator's Guide*
Give the user ID that is associated with the application READ access to the IRR.RUSERMAP resource in the FACILITY class.	Optional	*z/OS Security Server RACF Security Administrator's Guide*

For More Information

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

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

Superuser Granularity

Description

This support introduces the new UNIXPRIV class, which enables you to define profiles that grant RACF authorization for certain z/OS UNIX privileges. These privileges are automatically defined for all users that are defined with z/OS 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 z/OS 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 user identifier (UID) or 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 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 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 z/OS UNIX files.
Operations	None.
Interfaces	Refer to “Callable Services” on page 103, “Class Descriptor Table (CDT)” on page 106, “Data Areas” on page 116, and “Exits” on page 123.

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 7
Create the required profiles in the UNIXPRIV class (such as, SUPERUSER.* and CHOWN.UNRESTRICTED).	Optional	*z/OS Security Server RACF Security Administrator’s Guide*

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

For More Information

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

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

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

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

z/OS UNIX User Limits

Description

With this support, you can control the amount of system resources that are consumed by individual z/OS UNIX users. Resource limits for most z/OS 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 z/OS 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 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 z/OS UNIX limits.
Interfaces	Refer to “Callable Services” on page 103, “Commands” on page 108, “Data Areas” on page 116, “Database Templates” on page 120, “Panels” on page 128, “SYS1.SAMPLIB Members” on page 135, and “Utilities” on page 141.

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 database templates” on page 5
Run the dynamic parse utility.	Required	“Running dynamic parse” on page 5

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

For More Information

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

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

For more information about setting z/OS UNIX limits, see *z/OS 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 z/OS UNIX, z/OS 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 108, “Data Areas” on page 116, “Database Templates” on page 120, “Macros” on page 125, “Messages” on page 128, “Panels” on page 128, and “Utilities” on page 141.

Coexistence Considerations

A protected user ID that is created on a system running z/OS, or OS/390 Version 2 Release 8 or higher, can be used on a lower level system that shares the RACF database; however, the user ID will not be considered a protected user ID on the lower level system and may still be revoked by entering excessive 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, 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	*z/OS Security Server RACF Security Administrator's Guide* *z/OS Security Server RACF Command Language Reference*
Identify any other user IDs that you might need to define, or alter, as protected user IDs.	Optional	*z/OS 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	*z/OS Security Server RACF Security Administrator's Guide*

For More Information

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

- *z/OS Security Server RACF Command Language Reference*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF System Programmer's Guide*
- *z/OS Security Server 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 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 103, "Class Descriptor Table (CDT)" on page 106, "Commands" on page 108, "Data Areas" on page 116, "Database Templates" on page 120, "Macros" on page 125, "Messages" on page 128, "Panels" on page 128, "SMF Records" on page 132, "SYS1.SAMPLIB Members" on page 135, and "Utilities" on page 141.

Coexistence Considerations

If your OS/390 Version 2 Release 8 or higher ("up-level") systems share the RACF database with "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 (OS/390 V2R8)

Task	Condition	Reference Information
Run the IRRMIN00 utility.	Required	"Updating RACF database templates" on page 5
Run the dynamic parse utility.	Required	"Running dynamic parse" on page 5
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 7
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	*z/OS Security Server RACF Security Administrator's Guide* *z/OS 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	*z/OS 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 Version 2 Release 8, 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	*z/OS Security Server RACF Security Administrator's Guide*

For More Information

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

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

For more information about the OCEP component of Security Server, refer to *z/OS SecureWay Security Server Open Cryptographic Enhanced Plug-ins Application Programming*.

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

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

R_admin SETROPTS

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 103, “Data Areas” on page 116, “SMF Records” on page 132, “SYS1.SAMPLIB Members” on page 135, and “Utilities” on page 141.

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:

- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACF Data Areas*
- *z/OS 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 Version 2 Release 8. 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 Version 2 Release 8 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 116, “Macros” on page 125, and “SMF Records” on page 132.

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:

- *z/OS Security Server RACF Data Areas*
- *z/OS Security Server RACF Diagnosis Guide*
- *z/OS Security Server RACF Macros and Interfaces*
- *z/OS Security Server RACROUTE Macro Reference*

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

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

Service Updates

Description

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 **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 103 and “Macros” on page 125.

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	*z/OS Security Server RACROUTE Macro Reference*

For More Information

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

- *z/OS Security Server RACF Callable Services*
- *z/OS Security Server RACROUTE Macro Reference*

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

Service Updates (OS/390 V2R8)

Chapter 9. Summary of Interface Changes

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

Callable Services

Table 10 lists the new and updated callable services. See *z/OS Security Server RACF Callable Services* for more detailed information.

Table 10. Summary of New and Changed Callable Services

Callable Service Name	Release	Description	Related Support
IRRSCA00 (R_chaudit)	OS/390 V2R8	Updated to accept a CRED with a user type of system.	Service Updates (APAR OW33566)
IRRSCF00 (R_chmod)	z/OS V1R2	Updated to check for the caller's authorization to a UNIXPRIV resource.	Other Enhancements
IRRSCH00 (R_cacheserv)	z/OS V1R3	**New:** The R_cacheserv callable service provides a mechanism for the storage and retrieval of security relevant information from a cache.	Policy Director Authorization Services for z/OS and OS/390
IRRSCI00 (R_IPC_ctl)	OS/390 V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	Superuser Granularity
IRRSCO00 (R_chown)	OS/390 V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	Superuser Granularity
IRRSCS00 (clear_setid)	OS/390 V2R8	Updated to accept a CRED with a user type of system.	Service Updates (APAR OW33566)
IRRSC200 (ck_owner_two_files)	OS/390 V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	Superuser Granularity
IRRSCL00 (R_setfacl)	z/OS V1R3	**New:** The R_setfacl callable service is used to maintain the access lists for a UNIX file or directory.	Access Control Lists (ACLs)
IRRSDK00 (R_dcekey)	z/OS V1R4	Updated to support PKI Services.	PKI Services

Callable Service Changes

Table 10. Summary of New and Changed Callable Services (continued)

Callable Service Name	Release	Description	Related Support
IRRSDL00 (R_datalib)	z/OS V1R4	Updated to support PKI Services.	PKI Services
	OS/390 V2R10	Updated to extract private keys and to manage certificate serial numbers.	Public Key Certificate Enhancements
	OS/390 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
IRRSEQ00 (R_admin)	z/OS V1R4	1. Updated to support EIM. 2. Updated to support the AUTOUID, AUTOGID, and SHARED fields in the OMVS segment.	1. RACF Support for Enterprise Identity Mapping Services (EIM) 2. UNIX Security Management Usability Enhancements
	z/OS V1R3	Updated to support a new field name, PROXY, for the user and General Resource functions to the BASE Segment Fields table.	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	1. Updated to support the ENCRYPT field in the KERB segment for User and General Resource Administration functions, and the KERBLVL field in the base segment for System Options Administration functions. 2. Updated to support the UNIVERSAL field in the base segment of group profiles. 3. Updated to prevent unauthorized callers from using subpool 0, restricting them to subpools 1–127.	1. Network Authentication Service Support 2. Universal Groups 3. Other Enhancements
	OS/390 V2R10	1. **New:** User Administration and General Resource Administration fields were added. 2. Updated to support the restricted access attribute in the user base segment. 3. Updated to support public key certificate enhancements.	1. Network Authentication Service 2. Certificate Name Filtering 3. Public Key Certificate Enhancements
	OS/390 V2R8	1. Updated to support the LNOTES and NDS segments. 2. Function codes ADMN_ADD_USER, ADMN_ALT_USER, and ADMN_LST_USER were 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 z/OS and Novell Directory Services for OS/390 Support 2. z/OS UNIX User Limits 3. R_admin SETROPTS

Table 10. Summary of New and Changed Callable Services (continued)

Callable Service Name	Release	Description	Related Support
	OS/390 V2R8	1. Updated to support the LNOTES and NDS segments. 2. Function codes ADMN_ADD_USER, ADMN_ALT_USER, and ADMN_LST_USER were 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 z/OS and Novell Directory Services for OS/390 Support 2. z/OS UNIX User Limits 3. R_admin SETROPTS
IRRSFK00 (R_fork)	OS/390 V2R10	Updated to save and restore the following additional security information: controlled status, keep-controlled indicators, and saved messages.	Program Control Enhancements
IRRSIA00 (initACEE)	OS/390 V2R10	1. **New:** X500NAME and VARIABLE_LIST parameters were added. 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
	OS/390 V2R8	Returns OUSP information that contains the new user limit values specified in the OMVS segment.	z/OS UNIX User Limits
IRRSIM00 (R_usermap)	OS/390 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.	Network Authentication Service
	OS/390 V2R8	**New:** The R_usermap callable service enables 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 z/OS and Novell Directory Services for OS/390 Support
IRRSIU00 (initUSP)	OS/390 V2R8	Returns OUSP information that contains the new user limit values specified in the OMVS segment.	Lotus Notes for z/OS and Novell Directory Services for OS/390 Support
IRRSKA00 (ck_access)	z/OS V1R4	Updated to support improved access checking for z/OS UNIX files and directories.	Other Enhancements
	z/OS V1R3	Updated to include ACLs, and the related UNIXPRIV profiles, in the access checking algorithm.	Access Control Lists (ACLs)
	OS/390 V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	Superuser Granularity
IRRSKO00 (ck_process_owner)	OS/390 V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	Superuser Granularity
IRRSKP00 (ck_priv)	OS/390 V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	Superuser Granularity

Callable Service Changes

Table 10. Summary of New and Changed Callable Services (continued)

Callable Service Name	Release	Description	Related Support
IRRSMF00 (make_fsp)	z/OS V1R4	Updated to support z/OS UNIX.	UNIX Security Management Usability Enhancements
	z/OS V1R3	Updated to support ACL inheritance.	Access Control Lists (ACLs)
	OS/390 V2R8	Updated to accept a CRED with user type of system.	Service Updates (APAR OW33566)
IRRSMK00 (R_kerbinfo)	OS/390 V2R10	**New:** The Network Authentication Service is the only exploiter of the new R_kerbinfo service.	Network Authentication Service
IRRSPK00 (R_ticketserv)	OS/390 V2R10	**New:** The R_ticketserv callable service enables application servers to parse or extract principal names from the Network Authentication Service GSS-API context token.	Network Authentication Service
IRRSPT00 (R_ptrace)	OS/390 V2R8	Updated to check for the caller's authorization to a UNIXPRIV resource.	Superuser Granularity
IRRSPX00 (R_PKIServ)	z/OS V1R4	Updated to support PKI Services.	PKI Services
	z/OS V1R3	SAF trace information has been added to the Function section.	PKI Services
	OS/390 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
IRRSPY00 (R_proxyserv)	z/OS V1R3	**New:** The R_proxyserv callable service allows applications to retrieve directory information from LDAP.	Policy Director Authorization Services for z/OS and OS/390
IRRSQF00 (query_file_security_options)	z/OS V1R3	Updated to be able to query whether ACLs are supported or not.	Access Control Lists (ACLs)
	OS/390 V2R8	Updated to check for the existence of the discrete profile CHOWN.UNRESTRICTED in the UNIXPRIV class.	Superuser Granularity

Class Descriptor Table (CDT)

Table 11 on page 107 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 *z/OS Security Server RACROUTE Macro Reference*.

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

Table 11. Summary of New and Changed Classes

Class Name	Release	Description	Related Support
CACHECLS	z/OS V1R3	**New:** Controls backup (harden) and restore of `R_cacheserv` (IRRSCH00) managed caches to and from the RACF database.	Policy Director Authorization Services for z/OS and OS/390
DIGTCRIT	OS/390 V2R10	**New:** Maps the additional criteria found through the DIGTNMAP class to a RACF user ID.	Certificate Name Filtering
DIGTNMAP	OS/390 V2R10	**New:** Maps a subject's and/or issuer's distinguished name to a RACF user ID.	Certificate Name Filtering
DIGTRING	OS/390 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
EJBROLE	z/OS V1R2	**New:** Provides member class for Enterprise Java Beans authorization roles.	Enterprise Java Beans
GDSNJR	z/OS V1R2	**New:** Provides the grouping class for DB2 Java archive file (JAR) privileges.	DB2 Version 7 Support
GDSNSC	OS/390 V2R8	**New:** Provides the grouping class for DB2 schema privileges.	DB2 Version 6 Support
GDSNSP	OS/390 V2R8	**New:** Provides the grouping class for DB2 stored procedure privileges.	DB2 Version 6 Support
GDSNUF	OS/390 V2R8	**New:** Provides the grouping class for DB2 user-defined function privileges.	DB2 Version 6 Support
GDSNUT	OS/390 V2R8	**New:** Provides the grouping class for DB2 user-defined distinct type privileges.	DB2 Version 6 Support
GEJBROLE	z/OS V1R2	**New:** Provides grouping class for Enterprise Java Beans authorization roles.	Enterprise Java Beans
ILMADMIN	OS/390 V2R10	**New:** Contains profiles that control access to the administrative functions of IBM License Manager. Added with APAR OW44238.	IBM License Manager
JAVA	OS/390 V2R8	**New:** Contains profiles that are used by Enterprise Java Beans applications to perform authorization checks for Java resources.	Class Descriptor Table Enhancements
KERBLINK	OS/390 V2R10	**New:** Maps principal identities to RACF identities.	Network Authentication Service
MDSNJR	z/OS V1R2	**New:** Provides the member class for DB2 Java archive file (JAR) privileges.	DB2 Version 7 Support
MDSNSC	OS/390 V2R8	**New:** Provides the member class for DB2 schema privileges.	DB2 Version 6 Support
MDSNSP	OS/390 V2R8	**New:** Provides the member class for DB2 stored procedure privileges.	DB2 Version 6 Support
MDSNUF	OS/390 V2R8	**New:** Provides the member class for DB2 user-defined function privileges.	DB2 Version 6 Support

CDT Changes

Table 11. Summary of New and Changed Classes (continued)

Class Name	Release	Description	Related Support
MDSNUT	OS/390 V2R8	**New:** Provides the member class for DB2 user-defined distinct type privileges.	DB2 Version 6 Support
NDSLINK	OS/390 V2R8	**New:** Provides the mapping class for Novell Directory Services for OS/390 user identities.	Lotus Notes for z/OS and Novell Directory Services for OS/390 Support
NOTELINK	OS/390 V2R8	**New:** Provides the mapping class for Lotus Notes for z/OS user identities.	Lotus Notes for z/OS and Novell Directory Services for OS/390 Support
PRINTSRV	z/OS V1R3	**New:** Provides support for Infoprint Server, allowing protection of printer definitions with RACF.	Other Enhancements
REALM	OS/390 V2R10	**New:** Contains registry information about realms.	Network Authentication Service
SCICSTST	OS/390 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	OS/390 V2R8	**New:** Contains profiles that are used by z/OS 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	OS/390 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	OS/390 V2R8	**New:** Contains profiles that are used to grant specific z/OS UNIX privileges.	Superuser Granularity

Commands

Table 12 on page 109 lists the changes to the RACF commands for this release. See *z/OS Security Server RACF Command Language Reference* for more detailed information about these commands. For information about BLKUPD, refer to *z/OS Security Server RACF Diagnosis Guide*.

Table 12. Summary of Changed Commands

Command Name	Release	Description	Related Support
ADDGROUP	z/OS V1R4	Added AUTOGID and SHARED suboperands to the OMVS operand.	UNIX Security Management Usability Enhancements
	z/OS V1R2	Updated to support the UNIVERSAL operand.	Universal Groups
ADDUSER	z/OS V1R4	1. Added new EIM operand. 2. Added AUTOUID and SHARED suboperands to the OMVS operand.	1. RACF Support for Enterprise Identity Mapping Services (EIM) 2. UNIX Security Management Usability Enhancements
	z/OS V1R3	Added PROXY operand and the following suboperands: • LDAPHOST • BINDDN • BINDPW	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	Updated to support the ENCRYPT suboperand of the KERB operand.	Network Authentication Service Support
	OS/390 V2R10	1. Added RESTRICTED operand. 2. Added KERB operand and following suboperands: • MAXTKTLFE • KERBNAME	1. Certificate Name Filtering 2. Network Authentication Service
	OS/390 V2R8	1. Added LNOTES and NDS operands, and their supporting suboperands. 2. Added suboperands for the OMVS operand to allow additional fields to be specified in the OMVS segment of a user ID. 3. Changed behavior of NOPASSWORD and NOOIDCARD operands. When both operands are now in effect, the user ID is protected.	1. Lotus Notes for z/OS and Novell Directory Services for OS/390 Support 2. z/OS UNIX User Limits 3. Protected User ID
ADDSD	z/OS V1R2	Updated to support mixed-case profile names in the FROM operand.	Mixed-Case Profile Names
	OS/390 V2R10	Updated UACC operand.	Certificate Name Filtering
ALTDSD	OS/390 V2R10	UACC operand updated.	Certificate Name Filtering
ALTGROUP	z/OS V1R4	Added AUTOGID and SHARED suboperands to the OMVS operand.	UNIX Security Management Usability Enhancements

Command Changes

Table 12. Summary of Changed Commands (continued)

Command Name	Release	Description	Related Support
ALTUSER	z/OS V1R4	1. A new EIM operand has been added. 2. Added AUTOUID and SHARED suboperands to the OMVS operand.	1. RACF Support for Enterprise Identity Mapping Services (EIM) 2. UNIX Security Management Usability Enhancements
	z/OS V1R3	Added PROXY operand and the following suboperands: • LDAPHOST • NOLDAPHOST • BINDDN • NOBINDDN • BINDPW • NOBINDPW NOPROXY operand was also added.	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	Updated to support the new ENCRYPT suboperand of the KERB operand.	Network Authentication Service Support
	OS/390 V2R10	1. Added RESTRICTED and NORESTRICTED operands. 2. Added KERB operand and following suboperands: • KERBNAME • NOKERBNAME • MAXTKTLFE • NOMAXTKTLFE Added NOKERB operand and following suboperands: • MAXTKTLFE • NOMAXTKTLFE	1. Certificate Name Filtering 2. Network Authentication Service
	OS/390 V2R8	1. Added LNOTES and NDS operands, and their supporting suboperands. 2. Added suboperands for the OMVS operand to allow additional fields to be specified in the OMVS segment of a user ID. 3. Changed behavior of NOPASSWORD and NOOIDCARD operands. When both operands are now in effect, the user ID is protected.	1. Lotus Notes for z/OS and Novell Directory Services for OS/390 Support 2. z/OS UNIX User Limits 3. Protected User ID
BLKUPD	OS/390 V2R8	Updated to allow *entryname* and *string* values to be specified with lowercase or mixed-case characters.	Public Key Certificate Enhancements
DELUSER	OS/390 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. Network Authentication Service
LISTGRP	z/OS V1R2	Updated to display the new UNIVERSAL operand.	Universal Groups

Table 12. Summary of Changed Commands (continued)

Command Name	Release	Description	Related Support
LISTUSER	z/OS V1R4	A new EIM operand has been added.	RACF Support for Enterprise Identity Mapping Services (EIM)
	z/OS V1R3	Updated to list PROXY segment data when the PROXY suboperand is specified.	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	Updated to support the ENCRYPT suboperand of the KERB operand.	Network Authentication Service Support
	OS/390 V2R10	1. Updated to list RESTRICTED attribute. 2. Updated to list KERB segment data when the KERB suboperand is specified.	1. Certificate Name Filtering 2. Network Authentication Service
	OS/390 V2R8	1. Updated to support new LNOTES and NDS operands. 2. Updated to list additional fields in the OMVS segment for a user ID. 3. Updated to list PROTECTED attribute.	1. Lotus Notes for z/OS and Novell Directory Services for OS/390 Support 2. z/OS UNIX User Limits 3. Protected User ID
PERMIT	z/OS V1R2	Updated to support mixed-case profile names.	Mixed-Case Profile Names

Command Changes

Table 12. Summary of Changed Commands (continued)

Command Name	Release	Description	Related Support
RACDCERT	z/OS V1R4	Updated to support PKCS#7 certificate packages and key generation by PCI cryptographic coprocessor.	PKI Services
	OS/390 V2R10	Added the following new operands: Added the following new operands: • ALTMAP, with suboperands – NEWCRITERIA – NEWLABEL – TRUST and NOTRUST • DEBUG • DELMAP and LISTMAP, with suboperand, LABEL • MAP, with suboperands: – SDNFILTER – IDNFILTER – CRITERIA – WITHLABEL – TRUST and NOTRUST Updated the following operands: • ADD, with new suboperand, HIGHTRUST • ALTER, with new suboperand, HIGHTRUST • EXPORT, with new suboperands: – PKCS12DER – PKCS12B64 – PASSWORD • ID/MULTIID • LIST • GENCERT, with new suboperands: – ALTNAME, with suboperands: - DOMAIN - EMAIL - IP - URI – KEYUSAGE, with suboperands: - CERTSIGN - DATAENCRYPT - DOCSIGN - HANDSHAKE	Certificate Name Filtering Public Key Certificate Enhancements
	OS/390 V2R8	Updated to support the following new operands and their associated suboperands: • ADDRING • CONNECT • DELRING • EXPORT • GENCERT • GENREQ • LISTRING • REMOVE Updated the following operands: • ADD • DELETE • LIST	Public Key Certificate Enhancements

Table 12. Summary of Changed Commands (continued)

Command Name	Release	Description	Related Support
RALTER	z/OS V1R4	1. A new EIM operand has been added. 2. New support has been added for enhanced program security.	1. RACF Support for Enterprise Identity Mapping Services (EIM) 2. Program Access to Data Sets (PADS)
	z/OS V1R3	Added PROXY operand and the following suboperands: • LDAPHOST • NOLDAPHOST • BINDDN • NOBINDDN • BINDPW • NOBINDPW NOPROXY operand was also added.	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	1. Updated to support the new ENCRYPT suboperand of the KERB operand. 2. Updated base command and following operands: • ADDMEM • FROM	1. Network Authentication Service Support 2. Mixed-Case Profile Names
	OS/390 V2R10	1. Updated to support the new operands KERB and NOKERB, with suboperands: • DEFTKTLFE and NODEFTKTLFE • KERBNAME and NOKERBNAME • MAXTKTLFE and NOMAXTKTLFE • MINTKTLFE and NOMINTKTLFE • PASSWORD and NOPASSWORD 2. Updated to support `No Replay Protection` value in the APPLDATA field of the PTKTDATA profile in the general resource class.	1. Network Authentication Service 2. Enhanced PassTicket Support

Command Changes

Table 12. Summary of Changed Commands (continued)

Command Name	Release	Description	Related Support
RDEFINE	z/OS V1R4	1. A new EIM operand has been added. 2. Updated support for APPLDATA.	1. RACF Support for Enterprise Identity Mapping Services (EIM) 2. Program Access to Data Sets (PADS)
	z/OS V1R3	Added PROXY operand and the following suboperands: • LDAPHOST • BINDDN • BINDPW	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	1. Updated to support the new ENCRYPT suboperand of the KERB operand. 2. Updated base command and following operands: • ADDMEM • FROM	1. Network Authentication Service Support 2. Mixed-Case Profile Names
	OS/390 V2R10	1. Updated to support the new operand KERB, with suboperands: • DEFTKTLFE • KERBNAME • MAXTKTLFE • MINTKTLFE • PASSWORD 2. Updated to support `No Replay Protection` value in the APPLDATA field of the PTKTDATA profile in the general resource class.	1. Network Authentication Service 2. Enhanced PassTicket Support
RDELETE	z/OS V1R3	Updated to provide special processing if the **profile-name** entered on a RDELETE for a profile in the CACHECLS is just the *cachename*, rather than a specific *cachename_ddd_nnnnn*.	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	Updated to support mixed-case profile names.	Mixed-Case Profile Names
RLIST	z/OS V1R4	A new EIM operand has been added.	RACF Support for Enterprise Identity Mapping Services (EIM)
	z/OS V1R3	Updated to list PROXY segment data when the PROXY suboperand is specified.	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	1. Updated to list key encryption types. 2. Updated to accept mixed-case profile names.	1. Network Authentication Service Support 2. Mixed-Case Profile Names
	OS/390 V2R10	Updated to support the KERB operand.	Network Authentication Service
RVARY	OS/390 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.

Table 12. Summary of Changed Commands (continued)

Command Name	Release	Description	Related Support
SEARCH	z/OS V1R4	Added UID and GID keywords.	UNIX Security Management Usability Enhancements
	z/OS V1R2	Updated the following operands: • CLIST • FILTER • MASK	Mixed-Case Profile Names
SET	z/OS V1R3	Updated to allow trace enablement for both the new R_cacheserv and R_proxyserv SAF callable services, as well as the new aznAccess and aznCreds SAF callable services supported by Policy Director Authorization Services.	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	Updated to support the following suboperands of the TRACE operand, and their associated suboperands: • ALLASIDS • ALLJOBNAMES • ASID • CALLABLE • DATABASE • JOBNAME • NOASID • NOCALLABLE • NODATABASE • NOJOBNAME • NORACROUTE • RACROUTE	SAF Trace
SETROPTS	z/OS V1R4	1. A new EIM operand has been added. 2. New output for LIST has been added.	1. RACF Support for Enterprise Identity Mapping Services (EIM) 2. Program Access to Data Sets (PADS)
	z/OS V1R2	Updated to support the new KERBLVL operand.	Network Authentication Service Support
	OS/390 V2R10	Updated to disallow GENERIC and GENCMD for REALM and KERBLINK classes.	Network Authentication Service

Data Areas

Table 13 lists the new and changed data areas. For detailed information about RACF data areas, see *z/OS Security Server RACF Data Areas*.

Table 13. Summary of New and Changed Data Areas

Data Area Name	Release	Description	Related Support
ACEE	z/OS V1R3	The following new flags were added: • ACEERUAA • ACEERUAV	Access Control Lists (ACLs)
	OS/390 V2R8	Bit definitions in field ACEEFLG3 were added to indicate a protected user ID that cannot access the system with a password.	Protected User ID
	OS/390 V2R10	The following new fields and constants were added: • ACEEFLG6 • ACEERAUI • ACEEX5PR	Certificate Name Filtering
AFC	z/OS V1R4	The following new audit function code was added: • AFC_EACCESS	Other Enhancements
	z/OS V1R3	The following new constants were added: • AFC_SETFACL • AFC_SHUTDOWN_REG	Access Control Lists (ACLs)
	OS/390 V2R10	The following new constants were added: • AFC_CHMOUNT • AFC_CHMOUNT_SETUID	Enhanced Superuser Granularity
	OS/390 V2R8	The following constants were added or updated: • AFC_MOUNT • AFC_UNMOUNT • AFC_QUIESCE • AFC_UNQUIESCE • AFC_QUIESCE_SETUID • AFC_UNQUIESCE_SETUID • AFC_MOUNT_SETUID • AFC_UNMOUNT_SETUID	Superuser Granularity
CNST/CSNX (SAF)	z/OS V1R2	A new flag, CNSTCASE, added to indicate mixed-case profile names.	Mixed-Case Profile Names
	OS/390 V2R8	**New:** This structure supports the SAF version of the class descriptor table mapping macro, IRRPCNST.	Class Descriptor Table Enhancements

Table 13. Summary of New and Changed Data Areas (continued)

Data Area Name	Release	Description	Related Support
COMP	z/OS V1R4	Updated to define data areas and constants for the R_PKIServ, R_dcekey, and R_datalib callable services.	PKI Services
	z/OS V1R3	1. **New:** Field structures added to support the following callable services: • IRRSCH00 (`R_cacheserv`) • IRRSPY00 (`R_proxyserv`) 2. **New:** Function specific parameter lists were added to support R_PKIServ callable service. 3. **New:** Function specific parameter list was added to support R_setfacl callable service and the mapping for the area pointed to by RACL_Edit@ was added.	1. Policy Director Authorization Services for z/OS and OS/390 2. PKI Services 3. Access Control Lists (ACLs)
	OS/390 V2R10	1. **New:** KERB field structure, field mapping, and constants were added to support the new R_kerbinfo callable service. **New:** TKTS structures and constants were added to support the new `R_ticketserv` callable service. 2. **New:** Field structures and constants were added. 3. **New:** Field structures and constants were added. Updated INTA_LAST_PARM.	1. Network Authentication Service 2. Public Key Certificate Enhancements 3. Certificate Name Filtering
	OS/390 V2R8	1. The UMAP structure and constants were added to support the IRRSIM00 (`R_usermap`) callable service. 2. Multiple structures and constants were added to support the IRRSDL00 (`R_datalib`) callable service. 3. Multiple structures and constants were added to support the IRRSEQ00 (`R_admin`) callable service.	1. Lotus Notes for z/OS and Novell Directory Services for OS/390 Support 2. Public Key Certificate Enhancements 3. R_admin SETROPTS
CRED	z/OS V1R3	Updated to support ACLs.	Access Control Lists (ACLs)
FACL	z/OS V1R3	**New:** IRRPFACL has been added.	Access Control Lists (ACLs)

Data Area Changes

Table 13. Summary of New and Changed Data Areas (continued)

Data Area Name	Release	Description	Related Support
FC	z/OS V1R3	1. **New:** Function codes added to support the following callable services: • IRRSCH00 (`R_cacheserv`) • IRRSPY00 (`R_proxyserv`) 2. **New:** A new function code has been added to support R_setfacl.	1. Policy Director Authorization Services for z/OS and OS/390 2. Access Control Lists (ACLs)
	OS/390 V2R10	Function code IRRSPX00# has been added to support the IRRSPX00 (`R_PKIServ`) callable service.	Public Key Certificate Enhancements
	OS/390 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 z/OS and Novell Directory Services for OS/390 Support 2. Public Key Certificate Enhancements
ICB	z/OS V1R4	• Constant ICB7707 has been added to represent the new FMID, HRF7707.	• Release FMID Update
	z/OS V1R3	• Constant ICB7706 has been added to represent the new FMID, HRF7706.	• Release FMID Update
	z/OS V1R2	• A new field, ICBKRBLV, has been added to indicate the current SETROPTS KERBLVL setting. • Constant ICB7705 has been added to represent the new FMID, HRF7705.	• Network Authentication Service Support • Release FMID Update
	OS/390 V2R10	• Added a new byte, ICBALIAS, which indicates the current application identity mapping conversion stage. • Constant ICB7703 has been added to represent the new FMID, HRF7703.	• Application Identity Mapping • Release FMID Update
	OS/390 V2R8	Constant ICB2608 has been added to represent the new FMID, HRF2608.	Release FMID Update
IFSP	z/OS V1R3	Updated to indicate the presence of ACLs for a given file system object.	Access Control Lists (ACLs)
OUSP	OS/390 V2R8	Multiple structures and constants were added.	z/OS UNIX User Limits

Table 13. Summary of New and Changed Data Areas (continued)

Data Area Name	Release	Description	Related Support
RCVT	z/OS V1R4	1. Updated to support z/OS UNIX. 2. Updated to add new flags. 3. Updated for EIM registry. 4. Constant RCVTVR77has been added and RCVTVRMC has been updated to reflect the RACF FMID.	1. UNIX Security Management Usability Enhancements 2. Program Access to Data Sets (PADS) 3. RACF Support for Enterprise Identity Mapping Services (EIM) 4. Release FMID Update
	z/OS V1R3	Constant RCVTVR76 has been added and RCVTVRMC has been updated to reflect the RACF FMID.	Release FMID Update
	z/OS V1R2	Constant RCVTVR75 has been added and RCVTVRMC has been updated to reflect the RACF FMID.	"Release FMID Update" on page 54
	OS/390 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 4. Release FMID Update
	OS/390 V2R8	Constant RCVTVR28 has been added and constant RCVTVRMC has been updated to reflect the RACF FMID.	Release FMID Update
RIPL	z/OS V1R4	A new flag value was added to indicate ERROROPT status.	Other Enhancements
	OS/390 V2R10	The following field structures and constants were added in support of X500NAME: • INITEND7 • INITIDN • INITIDNL • INITPRM7 • INITSDN • INITSDNL • INITX500 • INITX5PR • INITXLEN	Certificate Name Filtering
RIXP	z/OS V1R4	A new flag value was added to indicate ERROROPT status.	Other Enhancements
	OS/390 V2R10	**New:** Field RIXX5PRP contains the address of the X500 name if it exists.	Certificate Name Filtering

Data Area Changes

Table 13. Summary of New and Changed Data Areas (continued)

Data Area Name	Release	Description	Related Support
SAFP	z/OS V1R3	Constant SAFPRL76 was added and constant SAFPCURR was updated to reflect the RACF FMID.	Release FMID Update
	z/OS V1R2	Constant SAFPRL75 was added and constant SAFPCURR was updated to reflect the RACF FMID.	Release FMID Update
	OS/390 V2R10	Constant SAFPRL73 was added and constant SAFPCURR was updated to reflect the RACF FMID.	Release FMID Update
	OS/390 V2R8	Constant SAFPRL28 was added and constant SAFPCURR was updated to reflect the RACF FMID.	Release FMID Update
SAFV	z/OS V1R2	Size of the SAFV data area was increased from 48 bytes to 64 bytes.	SAF Trace

Database Templates

Table 14 lists changes to RACF database templates. For detailed information, see *z/OS Security Server RACROUTE Macro Reference* or *z/OS Security Server RACF Macros and Interfaces*.

Table 14. Summary of Database Template Changes

Segment Name	Release	Description of Change	Related Support
General Template			
Base segment	z/OS V1R3	The RACDHDR field was added.	Policy Director Authorization Services for z/OS and OS/390
	OS/390 V2R10	The following new fields were added: • FILTERCT • FLTRLABL • FLTRNAME • FLTRSTAT • FLTRSVD1 • FLTRSVD2 • FLTRSVD3 • FLTRSVD4 • FLTRSVD5 • FLTRUSER	Certificate Name Filtering

Table 14. Summary of Database Template Changes (continued)

Segment Name	Release	Description of Change	Related Support
CERTDATA	OS/390 V2R8	The following new fields were added: • CERTCT • CERTDFLT • CERTEND • CERTLSER • CERTNAME • CERTPRVK • CERTPRVS • CERTPRVT • CERTRSV1 - CERTRSVK (reserved fields) • CERTSJDN • CERTSTRT • CERTUSAG • RINGCT • RINGNAME • RINGSEQN	Public Key Certificate Enhancements
COMBINATION	OS/390 V2R10	The following new fields were added: • FLTRLST1 • FLTRLST2	Certificate Name Filtering
	OS/390 V2R8	The following new fields were added: • CERTRING • CERTRNG2 • CERTRNG3	Public Key Certificate Enhancements
KERB	z/OS V1R2	The ENCRYPT field was added.	Network Authentication Service Support
	OS/390 V2R10	The following new fields were added: • CURKEY • CURKEYV • DEFTKTLF • ENCTYPE • KERB • KERBNAME • MAXTKTLF • MINTKTLF • PREVKEY • PREVKEYV • SALT	Network Authentication Service Support
EIM	z/OS V1R4	The following new fields were added: • DOMAINDN • OPTIONS • LOCALREG	RACF Support for Enterprise Identity Mapping Services (EIM)
PROXY	z/OS V1R3	**New:**The following new fields were added: • PROXY • LDAPHOST • BINDDN • BINDPW • BINDPWKY	Policy Director Authorization Services for z/OS and OS/390
Group Template			
Base segment	z/OS V1R2	The UNVFLG field was added.	Universal Groups

Table 14. Summary of Database Template Changes (continued)

Segment Name	Release	Description of Change	Related Support
OMVS	OS/390 V2R10	The GID field, Flag 2 value was changed to 10.	Application Identity Mapping
User Template			
Base segment	OS/390 V2R10	The following new fields were added: • FLAG9 • NMAPCT • NMAPLABL • NMAPNAME • NMAPRSV1 • NMAPRSV2 • NMAPRSV3 • NMAPRSV4 • NMAPRSV5	Certificate Name Filtering
	OS/390 V2R8	1. Bit definitions in the FLAG7 field were updated. 2. The CERTPUBK and CERTSJDN fields were added.	1. Protected User ID 2. Public Key Certificate Enhancements
COMBINATION	OS/390 V2R8	Updated with the new CERTLIST field.	Public Key Certificate Enhancements
EIM	z/OS V1R4	The LDAPPROF field was added.	RACF Support for Enterprise Identity Mapping Services (EIM)
KERB	z/OS V1R2	The ENCRYPT field was added.	Network Authentication Service Support
	OS/390 V2R10	The following new fields were added: • CURKEY • CURKEYV • DEFTKTLF • ENCTYPE • KERB • KERBNAME • MAXTKTLF • MINTKTLF • PREVKEY • PREVKEYV • SALT	Network Authentication Service
LNOTES	OS/390 V2R10	The SNAME field, Flag 2 value was changed to 10.	Application Identity Mapping
	OS/390 V2R8	**New:** Added for this release; includes the LNOTES and SNAME fields.	Lotus Notes for z/OS and Novell Directory Services for OS/390 Support
NDS	OS/390 V2R10	The UNAME field, Flag 2 value was changed to 10.	Application Identity Mapping
	OS/390 V2R8	**New:** Added for this release; includes the NDS and UNAME fields.	Lotus Notes for z/OS and Novell Directory Services for OS/390 Support

Table 14. Summary of Database Template Changes (continued)

Segment Name	Release	Description of Change	Related Support
OMVS	OS/390 V2R10	The UID field, Flag 2 value was changed to 10.	Application Identity Mapping
	OS/390 V2R8	Updated to contain the following new fields: • CPUTIME • ASSIZE • FILEPROC • PROCUSER • THREADS • MMAPAREA	z/OS UNIX User Limits
PROXY	z/OS V1R3	**New:**The following new fields were added: • PROXY • LDAPHOST • BINDDN • BINDPW • BINDPWKY	Policy Director Authorization Services for z/OS and OS/390

Exits

Table 15 lists the changes that were made to RACF exits. For more information, refer to *z/OS Security Server RACF System Programmer's Guide*.

Table 15. Summary of Changed Exits

Exit Name	Release	Description	Related Support
ICHDEX01, ICHDEX11	z/OS V1R2	Return code 16 has been added to indicate that RACF will use DES encryption for storing passwords, and will first use DES for comparing passwords, reverting to masking if the comparison fails. Effectively, if the exit returns 16, RACF will process as if the exit were not present.	Other Enhancements
ICHRFX01, ICHRFX03	OS/390 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.	Superuser Granularity
ICHRFX02, ICHRFX04	OS/390 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.	Superuser Granularity
ICHRTX00	OS/390 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.	Superuser Granularity

Table 15. Summary of Changed Exits (continued)

Exit Name	Release	Description	Related Support
IRR@XACS	z/OS V1R2	The RACF/DB2 external security module supports a new object, Java archive file (JAR), and its associated privilege called `USAGEAUTJ`. The corresponding RACF class abbreviation is `J`. The RACF/DB2 external security module has also been updated to pass database names in support of DBADM authorization checking for the following privileges: • CREATE VIEW • ALTER INDEX • DROP INDEX The RACF/DB2 external security module has also been updated to include support for the new `&ERROROPT` customization option and includes new and changed initialization reason codes for `XAPLFUNC=1`.	DB2 Version 7 Support
	OS/390 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 **E** User-defined distinct types **F** User-defined functions **O** 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 Version 6 Support

Macros

Table 16 lists the changes that were made to the RACF executable macros. For more information, refer to *z/OS Security Server RACF Macros and Interfaces* or *z/OS Security Server RACROUTE Macro Reference*.

Table 16. Summary of Changed Executable Macros

Macro Name	Release	Description	Related Support
ICHEACTN	z/OS V1R4	Updated to accept the RELEASE=7707 keyword.	Release FMID Update
	z/OS V1R3	Updated to accept the RELEASE=7706 keyword.	Release FMID Update
	z/OS V1R2	Updated to accept the RELEASE=7705 keyword.	Release FMID Update
	OS/390 V2R10	Updated to accept the RELEASE=7703 keyword.	Release FMID Update
	OS/390 V2R8	Updated to accept the RELEASE=2608 keyword.	Release FMID Update
ICHERCDE	z/OS V1R2	Updated to accept the CASE operand.	Mixed-Case Profile Names
ICHEINTY	z/OS V1R4	Updated to accept the RELEASE=7707 keyword.	Release FMID Update
	z/OS V1R3	Updated to accept the RELEASE=7706 keyword.	Release FMID Update
	z/OS V1R2	Updated to accept the RELEASE=7705 keyword.	Release FMID Update
	OS/390 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
	OS/390 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)

Table 16. Summary of Changed Executable Macros (continued)

Macro Name	Release	Description	Related Support
ICHETEST	z/OS V1R4	Updated to accept the RELEASE=7707 keyword.	Release FMID Update
	z/OS V1R3	Updated to accept the RELEASE=7706 keyword.	Release FMID Update
	z/OS V1R2	Updated to accept the RELEASE=7705 keyword.	Release FMID Update
	OS/390 V2R10	Updated to accept the RELEASE=7703 keyword.	Release FMID Update
	OS/390 V2R8	Updated to accept the RELEASE=2608 keyword.	Release FMID Update
RACROUTE	z/OS V1R4	Updated to accept the RELEASE=7707 keyword.	Release FMID Update
	z/OS V1R3	Updated to accept the RELEASE=7706 keyword.	Release FMID Update
	z/OS V1R2	Updated to accept the RELEASE=7705 keyword.	Release FMID Update
	OS/390 V2R10	Updated to accept the RELEASE=7703 keyword.	Release FMID Update
	OS/390 V2R8	Updated to accept the RELEASE=2608 keyword.	Release FMID Update
RACROUTE REQUEST=AUTH	OS/390 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 16. Summary of Changed Executable Macros (continued)

Macro Name	Release	Description	Related Support
RACROUTE REQUEST=EXTRACT	OS/390 V2R10	The ENVR object extracted from the ACEE includes the USP and X500 name if they exist.	Certificate Name Filtering
	OS/390 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	OS/390 V2R10	Checks the RESTRICTED attribute to determine the correct authorization to grant.	Certificate Name Filtering
	OS/390 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)

Macro Changes

Table 16. Summary of Changed Executable Macros (continued)

Macro Name	Release	Description	Related Support
RACROUTE REQUEST=VERIFY	z/OS V1R4	Added new keyword, ERROROPT.	Other Enhancements
	OS/390 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
	OS/390 V2R8	1. During processing, this macro determines if the specified *userid* was 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	z/OS V1R4	Added new keyword, ERROROPT.	Other Enhancements
	OS/390 V2R8	This macro was updated to determine if the specified *userid* was 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 *z/OS Security Server RACF Messages and Codes*. For information about other message changes that may affect your installation, refer to *z/OS Summary of Message Changes*.

Panels

Table 17 on page 129 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

Table 17. Summary of New and Changed Panels

Panel Number		Release	Description	Related Support
ICHH39 ICHH39B ICHH41GU ICHH49 ICHH49A ICHH49B ICHH312 ICHH322 ICHM31 ICHM39 ICHM49	ICHM41 ICHM42 ICHM49 ICHP39 ICHP41G ICHP42G ICHP49 ICHP49A ICHP312 ICHH39 ICHH49	z/OS V1R4	**New:** and updated to support for z/OS UNIX.	UNIX Security Management Usability Enhancements
ICHH73 ICHH716 ICHHT71 ICHM73 ICHP73	ICHPB02 ICHPB03B ICHPB04 ICHPB71	z/OS V1R4	Updated to support for PKI Services.	PKI Services
ICHHL07 ICHHL08 ICHHL09 ICHHR15 ICHHR16 ICHH21A ICHH22A ICHH28 ICHH41A1 ICHH42A1 ICHH56 ICHH56F ICHM21 ICHM22 ICHM56	ICHP21A ICHP21K ICHP21L ICHP21M ICHP22A ICHP22K ICHP22L ICHP22M ICHP28 ICHP41A1 ICHP41S ICHP42A1 ICHP42S ICHP48 ICHP56	z/OS V1R4	**New** and updated to provide support for Enterprise Identity Mapping Services.	RACF Support for Enterprise Identity Mapping Services (EIM)
ICHHM18 ICHHM19 ICHHY04 ICHHY05 ICHP21G ICHP21H ICHP21I ICHP21J ICHP22G ICHP22H	ICHP22I ICHP22J ICHP41O ICHP41P ICHP41Q ICHP41R ICHP42O ICHP42P ICHP42Q ICHP42R	z/OS V1R3	**New:** Provide support for Policy Director Authorization Services.	Policy Director Authorization Services for z/OS and OS/390
ICHH21A ICHH21OP ICHH22A ICHH22OP ICHH28 ICHH41A1 ICHH42A1 ICHM21 ICHM22	ICHM41 ICHM42 ICHP21A ICHP22A ICHP28 ICHP41A1 ICHP42A1 ICHP48	z/OS V1R3	Updated to support Policy Director Authorization Services.	Policy Director Authorization Services for z/OS and OS/390
ICHHN12		z/OS V1R2	**New:** Provide support for mixed-case profile names.	Mixed-Case Profile Names

Panel Changes

Table 17. Summary of New and Changed Panels (continued)

Panel Number		Release	Description	Related Support
ICHP115 ICHP191 ICHP20B ICHP215 ICHP241A ICHHP04	ICHP141A ICHP20A ICHP214 ICHP224 ICHP29	z/OS V1R2	Updated to support mixed-case profile names.	Mixed-Case Profile Names
ICHP58	ICHM57	z/OS V1R2	**New:** Provide support for Network Authentication Service.	Network Authentication Service Support
ICHP41N ICHP42N ICHP21F ICHP22F ICHP50	ICHH41N ICHH42N ICHH21F ICHH22F	z/OS V1R2	Updated to support Network Authentication Service.	Network Authentication Service Support
ICHHU20		z/OS V1R2	**New:** Provide support for the UNIVERSAL attribute.	Universal Groups
ICHP31 ICHM31	ICHH31	z/OS V1R2	Updated to support the UNIVERSAL attribute.	Universal Groups
ICHHM13 ICHH41GD	ICHHY03	z/OS V1R2	Updated to reflect the z/OS version name.	None.
ICHPB80 ICHPB82 ICHPB83	ICHPB81 ICHPB821 ICHPB831	OS/390 V2R10	**New:** Provide support for certificate name filtering.	Certificate Name Filtering
ICHH21F ICHH41N ICHHM17 ICHP21F ICHP41N	ICHH22F ICHH42N ICHHY03 ICHP22F ICHP42N	OS/390 V2R10	**New:** Provide support for Network Authentication Service.	Network Authentication Service
ICHCB02 ICHC73 ICHH7B ICHH74 ICHHT70 ICHHT728 ICHM85 ICHP74	ICHCB71 ICHH7A ICHH73 ICHH719 ICHHT71 ICHM73 ICHP73 ICHPB728	OS/390 V2R10	**New:** Provide additional support for the RACDCERT command and certificate renewal.	Public Key Certificate Enhancements
ICHH21A ICHH22A ICHM21 ICHM41 ICHP22A	ICHH21OP ICHH28 ICHM22 ICHP21A ICHP28	OS/390 V2R10	Updated to support Network Authentication Service.	Network Authentication Service
ICHH41A1 ICHP41A1 ICHP48	ICHH42A1 ICHP42A1 ICHM42	OS/390 V2R10	Updated to support Network Authentication Service.	Network Authentication Service
		OS/390 V2R8	Updated to allow for users to specify new segment information.	Lotus Notes for z/OS and Novell Directory Services for OS/390 Support

Table 17. Summary of New and Changed Panels (continued)

Panel Number		Release	Description	Related Support
ICHHB0 ICHHB02 ICHPB01A	ICHHB01A ICHPB0 ICHPB02	OS/390 V2R10	Updated for certificate name filtering and digital certificate support.	Certificate Name Filtering Public Key Certificate Enhancements
		OS/390 V2R8	Updated for digital certificate and key ring support.	Public Key Certificate Enhancements
ICHPB03 ICHPB04 ICHPB71	ICHPB03B ICHPB70 ICHPB72	OS/390 V2R10	Updated for certificate name filtering and digital certificate support.	Certificate Name Filtering Public Key Certificate Enhancements
		OS/390 V2R8	**New:** Provide additional support for digital certificate and key ring tasks.	Public Key Certificate Enhancements
ICHH41K1 ICHH42K1 ICHP41K ICHP42K	ICHH41L1 ICHH42L1 ICHP41L ICHP42L	OS/390 V2R8	**New:** Allow users to specify LNOTES and NDS segment information.	Lotus Notes for z/OS and Novell Directory Services for OS/390 Support
ICHH41GA ICHH41GC ICHH41GE ICHH41G3 ICHM41	ICHH41GB ICHH41GD ICHH41GF ICHP41G3 ICHM42	OS/390 V2R8	**New:** Allow users to enter values to update the new fields in the OMVS segment.	z/OS 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	OS/390 V2R8	**New:** 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	OS/390 V2R8	Updated to reflect the new supported fields in the OMVS segment.	z/OS UNIX User Limits
ICHHN10 ICHM41	ICHP41A ICHM42	OS/390 V2R8	Updated to reflect changes in the OIDCARD and NOPASSWORD options.	Protected User ID

Panel Changes

Table 17. Summary of New and Changed Panels (continued)

Panel Number		Release	Description	Related Support
ICHH0B0 ICHH00SM ICHP00 ICHP141D ICHP141F ICHP142D ICHP41G1 ICHP42G	ICHH00 ICHPB021 ICHP00SM ICHP141E ICHP142B ICHP41G ICHP41G2 ICHM85	OS/390 V2R8	Updated for digital certificate and key ring support.	Public Key Certificate Enhancements

SMF Records

Table 18 on page 133 lists the changes that were made to RACF SMF records. For more detailed information, refer to *z/OS Security Server RACF Macros and Interfaces* and *z/OS Security Server RACF Auditor's Guide*.

Table 18. 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)	OS/390 V2R10	Relocate sections 331 and 332 were added.	Certificate Name Filtering
	Event code 2(2)	z/OS V1R4	New event qualifiers were added.	"Program Access to Data Sets (PADS)" on page 25
	Event code 9(9)	z/OS V1R2	Updated to include a new flag in the data type 6 record for the UNIVERSAL operand of the ADDGROUP command.	Universal Groups
	Event code 24(18)	z/OS V1R4	Relocate section 6 is updated to support EIM.	"RACF Support for Enterprise Identity Mapping Services (EIM)" on page 18
		z/OS V1R2	Updated to include a new byte in the data type 6 for the KERBLVL setting of SETROPTS command.	Network Authentication Service Support
	Event code 28(1C)	z/OS V1R3	New values in extended relocate section 268 were added.	Access Control Lists (ACLs)
	Event code 29(1D)	z/OS V1R3	New values in extended relocate section 268 were added.	Access Control Lists (ACLs)
	Event code 30(1E)	z/OS V1R3	New values in extended relocate section 268 were added.	Access Control Lists (ACLs)
	Event Code 71 (47)	z/OS V1R3	**New:** Added for Policy Director Authorization Services. Extended relocate sections 352, 353, 354, 355, 356, and 372 were added but are reserved for Policy Director Authorization Services.	Policy Director Authorization Services for z/OS and OS/390
	Event Code 72 (48)	z/OS V1R4	Extended relocate section 373 was added.	PKI Services
		z/OS V1R3	**New:** Added to audit the function provided by the new IRRSPX00 callable service.	PKI Services
	Event Code 73 (49)	z/OS V1R3	**New:** Added to audit the function provided by the new IRRSPX00 callable service.	PKI Services
	Event Code 66(42)	OS/390 V2R10	1. Relocate sections 328, 329, and 330 were 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) were added to contain the ALTNAME IP Address, ALTNAME Email, ALTNAME Domain, and ALTNAME URI values.	1. Certificate Name Filtering 2. Public Key Certificate Enhancements
		OS/390 V2R8	Updated to reflect the additional operands of the RACDCERT command. Relocate sections 320-327 were added to contain the ring name and components of a subject's distinguished name.	Public Key Certificate Enhancements

SMF Changes

Table 18. Summary of New and Changed RACF SMF Records (continued)

Record Type	Event Code/Field Name	Release	Description	Related Support
Type 80 (cont.)	Event Code 67(43)	OS/390 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 Public Key Certificate Enhancements
	Event Code 68(44)	OS/390 V2R10	**New:** Relocate sections 333, 334, 335 were added but are reserved.	Network Authentication Service
	Event Code 69(45)	z/OS V1R4	1. Updated for the `R_PKIServ` GENCERT function. 2. Extended relocate section 373 was added.	PKI Services
		z/OS V1R3	Updated to add new PKI Services qualifiers and relocate sections.	PKI Services
		OS/390 V2R10	**New:** Relocate sections 340–351 were added for the `R_PKIServ` GENCERT function.	Public Key Certificate Enhancements
	Event Code 70(46)	z/OS V1R3	Updated to add new PKI Services qualifiers and relocate sections.	PKI Services
		OS/390 V2R10	**New:** Relocate sections 343, 344, 351 were added for the `R_PKIServ` EXPORT function.	Public Key Certificate Enhancements
	Event Code 75(4B)	z/OS V1R3	**New:** Added to record changes to ACL entries.	Access Control Lists (ACLs)
	Event Code 76 (4C)	z/OS V1R3	**New:** Added to record changes to ACL.	Access Control Lists (ACLs)
	Event Code 74 (50)	z/OS V1R3	**New:** Added to audit the function provided by the new IRRSPX00 callable service.	PKI Services
	SMF80VRM	z/OS V1R4	Updated for FMID 7707.	Release FMID Update
		z/OS V1R3	Updated for FMID 7706.	Release FMID Update
		z/OS V1R2	Updated for FMID 7705.	Release FMID Update
		OS/390 V2R10	Updated for FMID 7703.	Release FMID Update
		OS/390 V2R8	Updated for FMID 2608.	Release FMID Update
Type 81	SMF81KBL	z/OS V1R2	**New:** Added to indicate the level of KERB segment processing in effect.	Network Authentication Service Support
	SMF81BOX	OS/390 V2R8	Updated with new bits to indicate the type of password in effect for RVARY SWITCH and RVARY STATUS.	R_admin SETROPTS

Table 18. Summary of New and Changed RACF SMF Records (continued)

Record Type	Event Code/Field Name	Release	Description	Related Support
Type 83	SMF83VRM	z/OS V1R4	Updated for FMID 7707.	Release FMID Update
		z/OS V1R3	Updated for FMID 7706.	Release FMID Update
		z/OS V1R2	Updated for FMID 7705.	Release FMID Update
		OS/390 V2R10	Updated for FMID 7703.	Release FMID Update
		OS/390 V2R8	Updated for FMID 2608.	Release FMID Update

SYS1.SAMPLIB Members

Table 19 on page 136 identifies changes to the RACF members of SYS1.SAMPLIB.

SAMPLIB Changes

Table 19. Summary of RACF Changes to SYS1.SAMPLIB

Member Name	Release	Description	Related Support
IRR@XACS	z/OS V1R2	The RACF/DB2 external security module supports a new object, Java archive file (JAR), and its associated privilege called USAGEAUTJ. The corresponding RACF class abbreviation is J. The RACF/DB2 external security module has also been updated to pass database names in support of DBADM authorization checking for the following privileges: • CREATE VIEW • ALTER INDEX • DROP INDEX The RACF/DB2 external security module has also been updated to include support for the new &ERROROPT customization option and includes new and changed initialization reason codes for XAPLFUNC=1.	DB2 Version 7 Support
	OS/390 V2R8	With the availability of APAR OW38710, the RACF/DB2 external security module was 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 Version 6 Support

Table 19. Summary of RACF Changes to SYS1.SAMPLIB (continued)

Member Name	Release	Description	Related Support
IRRADULD	z/OS V1R4	Updated to support PKI Services.	PKI Services
	z/OS V1R3	1. **New:** Contains new event codes and associated fields to support ACLs. 2. Updated to support PKI Services. 3. Contains new event code and associated fields to support Policy Director Authorization Services.	1. Access Control Lists (ACLs) 2. PKI Services 3. Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	Updated to support SMF changes for ENCRYPT values and SETROPTS KERBLVL setting.	Network Authentication Service Support
	OS/390 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. Network Authentication Service
	OS/390 V2R8	Updated to reflect changes in SMF records.	R_admin SETROPTS
IRRADUTB	z/OS V1R4	Updated to support PKI Services.	PKI Services
	z/OS V1R3	1. **New:** Contains new event codes and associated fields to support ACLs. 2. Updated to support PKI Services. 3. Contains new event code and associated fields to support Policy Director Authorization Services.	1. Access Control Lists (ACLs) 2. PKI Services 3. Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	Updated to support SMF changes for ENCRYPT values and SETROPTS KERBLVL setting.	Network Authentication Service Support
	OS/390 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. Network Authentication Service
	OS/390 V2R8	Updated to reflect changes in SMF records.	R_admin SETROPTS

SAMPLIB Changes

Table 19. Summary of RACF Changes to SYS1.SAMPLIB (continued)

Member Name	Release	Description	Related Support
IRRICE	z/OS V1R4	1. Updated with a new sample report. 2. Updated with new GID report. 3. Updated with a new sample report.	1. Other Enhancements 2. UNIX Security Management Usability Enhancements 3. Program Access to Data Sets (PADS)
	z/OS V1R2	1. Updated with a new sample report. 2. Updated to exclude DIGTCERT class profiles when searching for general resource profiles with UACC other than NONE.	1. Universal Groups 2. Other Enhancements
OS/390 V2R8	**New:** Contains the DFSORT statements for the selection criteria and the ICETOOL statements for the report format for all of the RACFICE reports.	ICETOOL Support	

Table 19. Summary of RACF Changes to SYS1.SAMPLIB (continued)

Member Name	Release	Description	Related Support
RACDBULD	z/OS V1R3	Updated to support the following new data records: **02E0** User PROXY **0590** General Resource PROXY	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	1. Updated to support new fields containing information about key encryption types in the following data records: **02D0** User KERB **0580** General Resource KERB 2. Updated to support new field containing information about the UNIVERSAL attribute in the Group Basic data record (0100).	1. Network Authentication Service Support 2. Universal Groups
	OS/390 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. Network Authentication Service 2. Certificate Name Filtering
	OS/390 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 z/OS 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 z/OS and Novell Directory Services for OS/390 Support 2. z/OS UNIX User Limits 3. Public Key Certificate Enhancements
RACDBUQR	z/OS V1R2	Updated with a new sample query.	Universal Groups

SAMPLIB Changes

Table 19. Summary of RACF Changes to SYS1.SAMPLIB (continued)

Member Name	Release	Description	Related Support
RACDBUTB	z/OS V1R3	Updated to support the following new data records: **02E0** User PROXY **0590** General Resource PROXY	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	1. Updated to support new fields containing information about key encryption types in the following data records: **02D0** User KERB **0580** General Resource KERB 2. Updated to support new field containing information about the UNIVERSAL attribute in the Group Basic data record (0100).	1. Network Authentication Service Support 2. Universal Groups
	OS/390 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. Network Authentication Service 2. Certificate Name Filtering
	OS/390 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 z/OS 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 z/OS and Novell Directory Services for OS/390 Support 2. z/OS UNIX User Limits 3. Public Key Certificate Enhancements
RACINSTL	OS/390 V2R10	Updated to contain an entry to the index of samples pointing to RACJCL	Application Identity Mapping
	OS/390 V2R8	Updated to contain an entry to the index of samples pointing to RACJCL and RACFICE.	ICETOOL Support
RACJCL	OS/390 V2R10	Updated with sample JCL to run conversion utility IRRIRA00.	Application Identity Mapping
	OS/390 V2R8	Updated with sample JCL to allocate a report data set and add the RACFICE reports in IEBUPDTE format.	ICETOOL Support
IRRDBU00	z/OS V1R4	Updated to support EIM.	RACF Support for Enterprise Identity Mapping Services (EIM)
IRRADU00	z/OS V1R4	1. Updated to support EIM. 2. Updated to support PADS.	1. RACF Support for Enterprise Identity Mapping Services (EIM) 2. Program Access to Data Sets (PADS)

Utilities

Table 20 lists the changes made to RACF utilities for this release. For information about the IRRDBU00 and IRRRID00 utilities, see *z/OS Security Server RACF Security Administrator's Guide*. For information about the IRRADU00 utility, see *z/OS Security Server RACF Auditor's Guide*. For more information about other RACF utilities, refer to *z/OS Security Server RACF System Programmer's Guide*.

Table 20. Summary of Changed Utilities

Utility Name	Release	Description	Related Support
IRRADU00	z/OS V1R3	1. Field name xxxx_ACCESS_TYPE, of records DIRSRCH, DACCESS, and FACCESS, has 4 new values added ('ACLERROR', 'ACLGROUP', 'ACLUSER', and 'RSTD'). 2. Updated to support event code 71. Minimum LRECL of OUTDD output dataset changed from 5096 to 8192.	1. Access Control Lists (ACLs) 2. Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	Updated to support new flag in the data type 6 relocate section for the ADDGROUP command.	Universal Groups
	OS/390 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. Network Authentication Service
	OS/390 V2R8	Updated to unload additional fields in SMF Type 81 data.	R_admin SETROPTS

Table 20. Summary of Changed Utilities (continued)

Utility Name	Release	Description	Related Support
IRRDBU00	z/OS V1R3	Updated to support PROXY segment data.	Policy Director Authorization Services for z/OS and OS/390
	z/OS V1R2	1. Updated the following data records to add new fields containing information about key encryption types: **02D0** User KERB **0580** General Resource KERB 2. Updated the Group Basic Data Record (0100) to add the GPBD_UNIVERSAL field. 3. Updated processing of the GRBD_UACC field in the General Resource Basic Data record (0500) for profiles in the DIGTCERT class. The following flags are now unloaded with the following UACC values: **X'80'** TRUST **X'00'** NOTRUST **X'C0'** HIGHTRST	1. Network Authentication Service Support 2. Universal Groups 3. Other Enhancements
	OS/390 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. Network Authentication Service

Table 20. Summary of Changed Utilities (continued)

Utility Name	Release	Description	Related Support
	OS/390 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 z/OS and Novell Directory Services for OS/390 Support 2. z/OS UNIX User Limits 3. Protected User ID 4. Public Key Certificate Enhancements
IRRIRA00	OS/390 V2R10	**New:** Converts an existing database to application identity mapping functionality using a four-staged approach.	Application Identity Mapping
IRRMIN00	OS/390 V2R10	Updated to enable the new database for application identity mapping processing when PARM=NEW.	Application Identity Mapping

Utility Changes

Table 20. Summary of Changed Utilities (continued)

Utility Name	Release	Description	Related Support
IRRRID00	OS/390 V2R10	Updated to recognize KERBLINK profiles.	Network Authentication Service
	OS/390 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 z/OS and Novell Directory Services for OS/390 Support 2. Public Key Certificate Enhancements
IRRUT200	OS/390 V2R10	Updated to process the alias index structures to detect errors and to display the formatted alias index blocks.	Application Identity Mapping
IRRUT400	OS/390 V2R10	Updated to build an alias index structure in the output RACF database.	Application Identity Mapping

Appendix. Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in z/OS enable users to:

- Use assistive technologies such as screen-readers and screen magnifier software
- Operate specific or equivalent features using only the keyboard
- Customize display attributes such as color, contrast, and font size

Using assistive technologies

Assistive technology products, such as screen-readers, function with the user interfaces found in z/OS. Consult the assistive technology documentation for specific information when using it to access z/OS interfaces.

Keyboard navigation of the user interface

Users can access z/OS user interfaces using TSO/E or ISPF. Refer to *z/OS TSO/E Primer*, *z/OS TSO/E User's Guide*, and *z/OS ISPF User's Guide Volume I* for information about accessing TSO/E and ISPF interfaces. These guides describe how to use TSO/E and ISPF, including the use of keyboard shortcuts or function keys (PF keys). Each guide includes the default settings for the PF keys and explains how to modify their functions.

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:

BookManager
CICS
CICS/ESA
DB2
DFSORT
eLiza
IBM
IBMLink
Infoprint
Library Reader
MVS
OS/390
OS/400
Parallel Sysplex
RACF
Redbooks
Resource Link
RETAIN
S/390
SecureWay
System/390
TalkLink
VM/ESA
VTAM
WebSphere

z/OS
z/OS.e
zSeries

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Tivoli and NetView are trademarks of International Business Machines Corporation or 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.

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

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

S

T

U

Z

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

z/OS
Security Server RACF
Migration

Publication No. GA22-7690-03

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
GA22-7690-03

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

GA22-7690-03

Cut or Fold
Along Line

Program Number: 5694-A01, 5655-G52

Printed in U.S.A.

GA22-7690-03