IBM

# CA-ACF2 to OS/390 Security Server

## Migration Guide

- Product design similarities and differences
- Planning the migration
- Conversion methodologies

Paul de Graaff
Ted Anderson
Julie Bergh
Peter Desforge
Lynn Kearney
Lori Halberts Kikuchi
Tony Nix
Mark Shell

Redbooks

ibm.com/redbooks

International Technical Support Organization

SG24-5678-00

# CA-ACF2 to OS/390 Security Server Migration Guide

October 2000

**Take Note!**

Before using this information and the product it supports, be sure to read the general information in Appendix D, “Special notices” on page 127.

**First Edition (October 2000)**

This edition applies to SecureWay Security Server Version 2, Release Number 10, Program Number 5645-001 for use with the OS/390 Operating System.

Comments may be addressed to:
IBM Corporation, International Technical Support Organization
Dept. HYJ  Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

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

# Contents

# Figures

# Tables

# Preface

CA-ACF2 and the OS/390 Security Server are both sophisticated products. In some areas their designs are similar, and in other areas the designs are very different. Planning a migration from CA-ACF2 to the RACF element of the OS/390 Security Server, without unduly disrupting an OS/390 production environment, requires considerable planning and understanding. With proper planning, and perhaps with specially skilled people to assist in certain areas, the migration can usually be accomplished in an orderly way.

Understanding the higher-level issues and differences between the two products is an important starting point. This redbook is intended to assist in this area.

## The team that wrote this redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization Poughkeepsie Center.

**Paul de Graaff**, the project leader, is a Certified IT Specialist at the International Technical Support Organization, Poughkeepsie Center. He writes extensively and teaches IBM classes worldwide on all areas of S/390 Security. Before joining the ITSO, Paul worked in IBM Global Services in the Netherlands as a Senior IT Specialist.

**Ted Anderson** is a Senior IT Specialist with IBM's Software Migration Project Office (SMPO). He is a previous redbook author with 19 years of large systems experience. His areas of expertise include, but are not limited to, OS/390 systems programming, RACF and RACF migrations, and numerous other OS/390 system software products. He holds a BA degree in Biology from Bethel College.

**Julie Bergh** is an IT Specialist currently with IBM's Software Migration Project Office (SMPO) in North America. She has over 20 years of IT experience in MVS and related areas. Her areas of expertize include, but are not limitied to, OS/390 systems programming, RACF and RACF migrations from competitive security software, OS/390 system software products, business continuity planning, security administration, applications programming, auditing, project management, and quality assurance. Julie holds an external certification as a Certified Business Continuation Professional (CBCP). She holds a bachelor of science degree in Management Information Systems from the University of Wisconsin, Superior and a masters degree in Computer Resource Management from Webster Univerity in St. Louis, Missouri.

**Peter Desforge** is a Certified Senior IT Specialist currently working with the IBM Software Migration Project Office - Security Team. He has over 18 years of IT experience in a variety of areas, including system and application programming, managing user support and security administration, project management, user training and consulting Since joining the SMPO in 1994, he has been involved in well over 100 migrations to RACF from both CA-ACF2 and CA-Top Secret. He is also a senior member of the team that is responsible for the design and development of the IBM tools that convert CA-ACF2 and CA-Top Secret to RACF.

**Lynn Kearney** is a Certified Senior IT Specialist currently working with the Software Migration Project Office from Dallas, TX. She has over 30 years of IT experience in a variety of areas. She worked for 15 years in Poughkeepsie, NY in MVS development doing testing, design, development and running Early Support Programs. She moved to Texas in 1982 where she supported an 11 state area with MVS and security hotline calls and did ASKQ responses. While in the Area Systems Center, she was a systems programmer, security administrator, security analysis, and systems availability consultant. She did security audits for internal IBM sites and for customers. Since joining the SMPO in 1993, she has been involved in over 100 migrations to RACF from both CA-ACF2 and CA-Top Secret. .

**Lori Halberts Kikuchi** has worked for IBM for 17 years. Since the mid 1980s Lori has specialized in the area of security. Currently, Lori is a Certified Sales Specialist in the IBM System 390 Software Sales in the Americas. Her main goal is to sell the IBM SecureWay Security Server OS/390's RACF Element and RACF migration services to competitively installed clients. Lori's other positions in IBM were retail banking specialist, storage specialist, RACF Brand Manger, and Manager of the SMPO Security team.

**Tony Nix** s a Certified Senior IT Specialist currently working with the Software Migration Project Office from Costa Mesa, CA. He has 17 years of IT experience in a variety of areas, including computer operations, systems and applications programming, project management, line management, security administration, training and consulting. As a member of the SMPO for nearly four years, Tony has been involved in many diverse migrations. Tony holds an external CISSP certification (Certified Information Systems Security Professional).

**Mark Shell** is an Advisory IT Specialist currently working with the Software Migration Project Office from Dallas, TX. Mark was in the military for 9 years before he began his computer industry career. He has 13 years of IT experience in a variety of areas. Mark worked with the SMPO for 4 years as an external customer converting multiple security databases before joining the SMPO Team over 2 years ago.

A special thank you to Marilyn Thornton, manager of the RACF Software Migration Project Office, without whose leadership and dedication this book would not have been written. Marilyn's perspective on IBM's security has led to a better environment for all RACF users.

Thanks to the following people for their invaluable contributions to this project:

Kurt Meiser
ITSS International, Inc.

Kleber Candido de Melo
IBM Brazil

George Dawson
ISSC Australia

Bill Ogden
ITSS International, Inc.

Cees Kingma
IBM International Technical Support Organization

Gunnar Myhre
ITSS International, Inc.

Walt Farrell
IBM RACF Development

Rich Miles
IBM Software Migration Project Office

Terry Barthel, Alison Chandler, and Al Schwab
International Technical Support Organization, Poughkeepsie Center

## Comments welcome

**Your comments are important to us!**

We want our Redbooks to be as helpful as possible. Please send us your comments about this or other Redbooks in one of the following ways:

- Fax the evaluation form found in “IBM Redbooks review” on page 139 to the fax number shown on the form.
- Use the online evaluation form found at **ibm.com**/redbooks
- Send your comments in an Internet note to redbook@us.ibm.com

# Chapter 1. The value of SecureWay Security Server for OS/390

This chapter describes the advantages of using the OS/390 Security Server versus competitive security software from Computer Associates. The value is presented both from a functional point of view, component by component, to the monetary savings of the OS/390 Security Server.

## 1.1 Overview of the Security Server

In 1996 the IBM corporation offered a newly packaged operating system for mainframes, named OS/390. The base of OS/390 is the MVS operating system. OS/390 integrates MVS in addition to about 30 other products, which are pretested, integrated, and packaged together under the new name OS/390. This integration, performed by IBM, is very beneficial to the users of OS/390 because now only one product needs to be ordered: There is no need to test 30 separate products each time an operating system upgrade is performed, and it even costs less. Most of the products packaged in OS/390, like JES2 and VTAM, became standard features of OS/390. Other products, like SecureWay Security Server for OS/390 and DFSMS, became optional features of OS/390. Both standard and optional features are packaged, tested and delivered with every license of OS/390, but to use the optional features you must order the feature codes from IBM and enable the features on your system.

When IBM moved from MVS to OS/390 there was a perception in the marketplace that the name of RACF had been changed to SecureWay Security Server for OS/390. Actually, SecureWay Security Server for OS/390 is more than just a new name for IBM's RACF for MVS. IBM created a “security umbrella” as a delivery vehicle for IBM OS/390 security-oriented software. RACF is but one of the elements in the Security Server. In SecureWay Security Server for OS/390 2.10, there are six elements:

1. IBM RACF
2. OS/390 DCE Security Server
3. OS/390 Firewall Technologies
4. OS/390 LDAP Server
5. Network Authentication and Privacy Service (Kerberos)
6. Open Cryptographic Enhanced Plug-ins (OCEP)

IBM has positioned the SecureWay Security Server for OS/390 as the security product that will deliver the support and exploitation of new technology inside the glass house and in the e-business arena.

### 1.1.1 Business benefits of the Security Server

The job of your security product is to protect your information while allowing your business to move ahead with new ventures and technologies. RACF is the leader in this area. RACF integrates seamlessly upon availability of new versions and releases of IBM subsystems (e.g., CICS, DB2) and technologies (e.g., Sysplex Coupling Facility). This allows your business to move ahead with its objectives and applications as quickly as you choose. Many non-RACF customers have been held back for months by their current mainframe security product.

With the LDAP V3 Protocol Server, IBM continues this tradition outside of the glass house. The SecureWay Security Server for OS/390 delivered the LDAP Server as one of its elements before many companies even knew about the new Lightweight Directory Access Protocol. Now those same companies are ready to roll out applications and directories that will make use of the LDAP Server on OS/390, and they can do that with the confidence of knowing that the server was delivered as part of the SecureWay Security Server for OS/390 -- and it is ready and waiting for them.

Now any authorized LDAP client throughout the enterprise can search, extract, add and delete information from any OS/390 LDAP server (from the IBM brochure *Secureway Security Server for OS/390*, G221-4102-04). As of OS/390 2.7 it became possible to extract information from the RACF database into an LDAP directory. In OS/390 2.8 this support was enhanced to allow an authorized LDAP client user in your enterprise to access the RACF database and use the functions to add, delete and retrieve RACF user and group profile information. This ability opens the door to many enterprise-wide uses based on RACF information.

The Firewall Technology element of the Security Server delivers a set of features that can be used alone or with the Firewall Technologies that already ship in the OS/390 Communications Server, a standard part of the OS/390 Operating System. When used together, you have a full function OS/390 Firewall ready to use. The Virtual Private Network (IPsec) support of the OS/390 Firewall is one of the areas where it excels.

The RACF element of SecureWay Security Server for OS/390 2.4 first introduced support for Digital Certificates and Public Key Infrastructure (PKI). In September of 1999, SecureWay Security Server for OS/390 2.8 greatly enhanced that support. Again, RACF has new technology ready and waiting for you to move into the world of e-business. The following is a high-level list of the supported technology features:

- Digital Certificate Authentication providing integration between PKI technology and traditional RACF Authentication
- Certificate mapped to RACF userid, to provide seamless access to OS/390 resources
- User self-registration of digital certificates
- Processing of Certificate Revocation Lists by the IBM HTTP Server for OS/390
- RACF can generate digital certificates

### 1.1.2 Financial benefits of the Security Server

This section details the monetary savings of using the OS/390 Security Server.

#### 1.1.2.1 Identifying monetary savings based on product price

The five elements are delivered for virtually the same price as RACF alone. This is great news for RACF users! Non-RACF users who want to use any of these exclusive features will have to license the Security Server to use any of the elements other than the LDAP Server. Then, non-RACF businesses will be paying for both Security Server and their non-RACF security package. New releases become available every six months in conjunction with the OS/390 operating system.

If you are a Novell Directory Services (NDS) user, there is another benefit to having the SecureWay Security Server for OS/390: Novell Network Services for OS/390 incorporates Novell NDS Version 4 and comes free of charge when customers license SecureWay Security Server for OS/390.

There are many scenarios where the value of the SecureWay Security Server for OS/390 is evident, not the least of which is the scenario of upgrading CPUs. IBM's pricing policies are flexible yet predictable. There are no surprises regarding huge software upgrade bills.

#### 1.1.2.2 Identifying productivity savings

The SecureWay Security Server for OS/390 is an optional feature of the OS/390 operating system. The benefit of being a feature of OS/390 is that the Security Server is integrated and pretested with the OS/390 operating system. This reduces the amount of testing that your systems staff devotes to your security package. Most of our customers see a 40- to 120-hour time savings each time a new release of the operating system or non-RACF mainframe security product is installed. The savings to your systems programming organization will reflect these savings (40-150 hours) multiple times per year.

## 1.2 RACF administrative highlights

This section highlights the administration of the RACF element of the OS/390 Security Server and some of the recent administration enhancements made to RACF.

### 1.2.1 RACF administrative enhancements

It is beyond the scope of this document to try and communicate all of the product benefits that the SecureWay Security Server for the OS/390 RACF element (RACF) provides, so we limit this list to the new administrative features, the exciting features that support the UNIX System Services “side” of OS/390, and open computing.

Historically, RACF has brought out day-one support and exploitation of new software and hardware technologies. This is beneficial to corporations who like to be on the leading edge with new technology. For example, many customers with RACF have enjoyed the benefits of having RACF make use of the Coupling Facility since day one.

The RACF product performs extremely well. For detailed technical information you can review the RACF Performance White Paper written by Mark Nelson of RACF development and design (see `http://www.s390.ibm.com/products/racf/racfperf.html`).

RACF's Remote Sharing Facility (RRSF) is an integrated feature of the RACF element (RACF), which allows you to administer and synchronize multiple RACF databases. RRSF is extremely granular which allows you to make the choices that fit your business. For example, some or all commands and/or passwords can be synchronized automatically or they can be specifically targeted to one or more of the databases being managed. IBM has delivered this integrated feature with the utmost of integrity by encrypting the transmission of data and by providing automatic recovery if the transmission is interrupted.

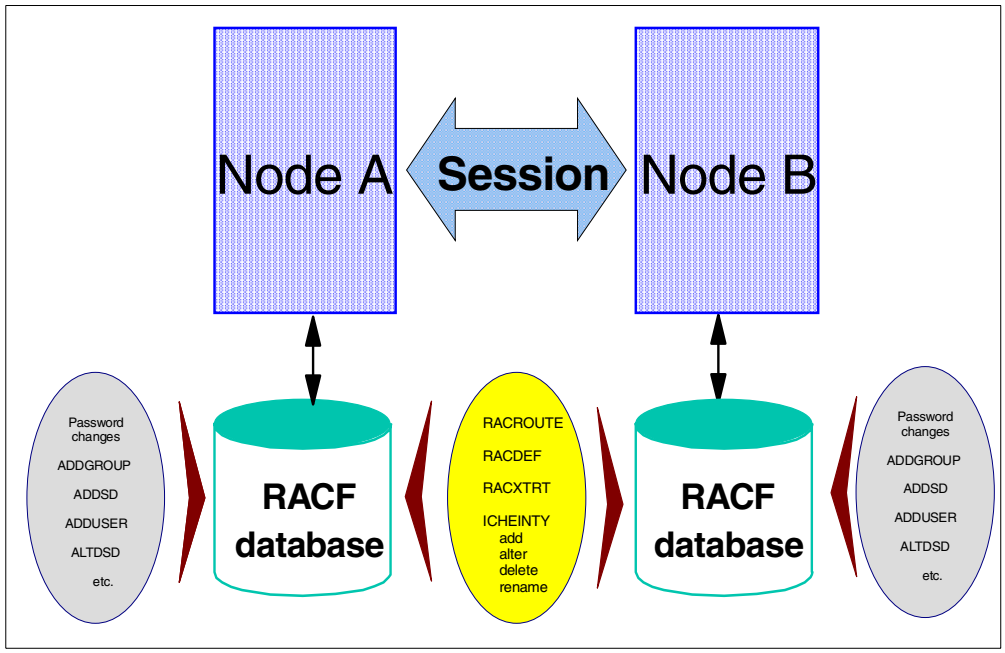


*Figure 1. RRSF overview*

RACF provides four reporting options. The traditional RACF reporting features are the Data Security Monitor (DSMON) and the RACF Report Writer. DSMON delivers “canned” RACF database and OS/390 auditing reports. The RACF Report Writer allows for ad hoc violation reporting. The Report Writer has been stabilized, which means it will not report on some of the new functions that RACF provides. This feature was not removed from RACF.

Both the Report Writer and DSMON are still supported and shipped with SecureWay Security Server for OS/390's RACF element. A few years ago IBM met customer requirements by adding two additional reporting options:

1. The RACF Database Unload feature
2. The SMF Unload feature

These features allow you to unload the RACF database and the violation records from SMF into flat files. IBM ships a comprehensive set of DB2 based reporting queries to meet your needs. In addition, you can use any SQL- based language

or product to create reports from the flat files. This method of reporting allows you to combine data stores to create more informative trend analysis reports on a user, system, or across platforms.

The RACF element delivered with version 2.8 includes an administrative enhancement for reporting called RACFICE, which was formerly only available via the Web. This feature includes over 30 sample reports, and it uses the DFDSS ICETOOL report generator. This is very beneficial to organizations that do not have DB2, and they can now easily make use of the database and SMF Unload utilities without having to write their own queries. Additional reporting options can be found in the IBM product Performance Reporter for OS/390. Performance Reporter includes 11 canned reports for RACF in its extensive list of performance-related reports.

The RACF Remove ID utility is a helpful new feature of RACF that greatly enhances the productivity of security administrators. This utility allows the administrator to search for an occurrence of a user ID or group. The results of the returned search are a set of RACF commands to delete the user ID or group and its related access permissions. The administrator can then mark the ones to delete, as it may not be appropriate to delete all occurrences. The administrator can then submit the results and the deletions will take place.

### 1.2.2 RACF/DB2 security administration overview

SecureWay Security Server for OS/390 2.4 introduced the RACF/DB2 administration feature with DB2 Version 5. This feature allows security administrators to manage DB2 security administration via RACF. The RACF/DB2 external security module is shipped with the Security Server.

RACF and CA-Top Secret have Identification, Authentication and the use of Secondary Authorization IDs in their base support -- this is not the issue. We are comparing the RACF/DB2 external security module to the CA-Top Secret DB2 add-on product. Using either the CA add-on products or the RACF/DB2 feature you can realize the benefits of moving your DB2 security administration function out of DB2 and into your OS/390 security product. DB2 is an outstanding database product, but its internal security structure does not provide the robust level of security administration that most organizations desire. Figure 2 on page 6 shows an overview of DB2 external (RACF) security.

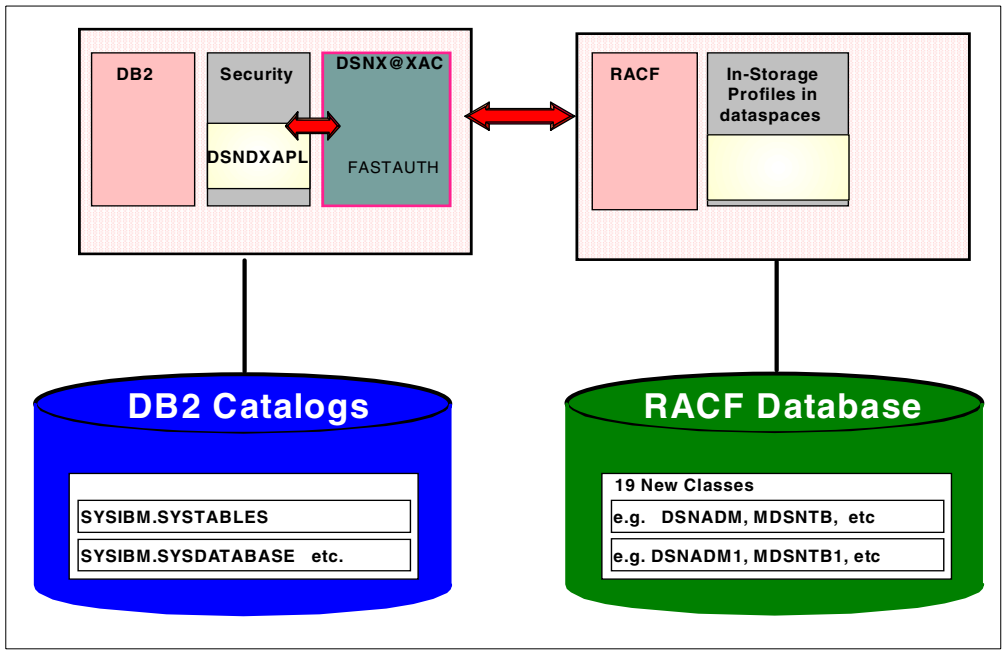


*Figure 2. DB2 external security (RACF) overview*

### 1.2.2.1 Benefits of using RACF to administer your DB2 security

The following benefits are gained when you use RACF for DB2 security:

- Separation of duties
- Single point of control for administration and auditing
- Ability to define security rules before a DB2 object is created
- Ability to allow security rules to persist when a DB2 object is dropped
- Ability to protect multiple DB2 objects with one security rule
- Eliminate the need to create multiple, and sometimes duplicate, security rules
- Ability to use RACF generic profiles and/or Member/Grouping profiles
- Eliminate DB2 cascading revoke
- Flexibility for multiple DB2 subsystems:
  - One set of RACF classes for multiple DB2 subsystems, or
  - One set of RACF classes for each DB2 subsystem

### 1.2.2.2 Migration issues: protection of DB2 resources via RACF

For organizations currently using the CA-Top Secret/DB2 product, the IBM SMPO Security Team's migration tools have built-in functions that can convert your DB2 add-on product data into the appropriate RACF commands to provide you with equivalent function via the RACF/DB2 external security model.

For organizations currently using internal DB2 security administration, RACF will allow you to phase in the RACF/DB2 function while you move from internal to external DB2 security administration. Once you have begun protecting DB2 resources via the RACF external security module, the RACF/DB2 external security module will look at the RACF profiles first. If there is not a RACF profile to protect the DB2 object, then the RACF/DB2 external security module passes

control to DB2's internal security authorization catalogs. This allows you to move over to external security in a manner best suited for your organization.

#### 1.2.2.3 Product benefits

Since the administrative function is included in RACF, there is no additional maintenance that needs to be done. The CA solution is delivered in a separate product, so there is an additional product to maintain, upgrade and test.

The external security module is shipped in the SAMPLIB member IRR@XACS. It is coded and fully supported by the IBM RACF development team. This means that you can call the IBM support center if you have any problems with this code, and they will support you and accept APARs if it is determined that a problem does exist.

The external security module is installed in DB2 at the Access Control Authorization Exit point. This allows RACF and DB2 to make use of the standard SAF interface, which eliminates the need install or modify any DB2 product code. IBM's implementation of the external security module provides any vendor the ability to perform DB2 security administration within its product without the requirement of modifying or overlaying DB2 code by simply using the industry standard SAF interface.

The IBM RACF development team works in concert with the DB2 development team to make sure that this module works and that it continues to work as each product comes out with new releases and versions. As a user of this function, you can feel confident that you will have day-one support of new releases and versions.

#### 1.2.2.4 Financial benefits

The RACF/DB2 external security module code is shipped with RACF for use with DB2 V5 and higher at no additional cost. The competitive product, CA-Top Secret/DB2, is sold as a separate product.

***Identifying monetary savings based on product price***

If you have already purchased this add-on product from CA then you will see an annual savings equal to your current maintenance charges. Most contracts that organizations have negotiated with CA do not have "out" clauses. Therefore, you will probably not realize these savings until the end of the contract period.

If you are trying to cost justify the migration to RACF and currently have funds for the CA DB2 add-on product allocated in your budget, then you can free up all OTC funds and the annual maintenance fee. In most cases, the amount of money that is saved can be used to cover the migration charges for the SMPO's Security Migration Team to advise and assist you with your migration.

Don't forget that these CA products will most likely be subject to upgrade charges when your CPU is upgraded or a new CPU is purchased.

CA has purchased Platinum, the company that came out with the RC Secure product. If you are currently using RC Secure, then you may also be able to discontinue that product when you implement the RACF/DB2 function. Once your contract has ended for RC Secure, you will also realize those savings.

***Identifying productivity savings***
The maintenance effort for RACF is easy to identify and quantify. It should take your systems programmer less than an hour to initially get the RACF/DB2 external security module installed. Annually, this should require minimal maintenance, if any at all. As of January 2000, our staff has spent less than 10 minutes over the past two years maintaining this module on our OS/390 system.

If you are currently using the CA DB2 add-on product, then you can easily quantify the benefits of migrating to RACF. You will need to quantify the number of hours the systems programming staff expends installing and maintaining this product on an annual basis. Subtract one hour per year from that number and you will arrive at the annual savings in hours that your organization should realize after migrating to RACF.

## 1.3 RACF market penetration

RACF has been securing data in the MVS environment for 24 years. Most companies chose their security products in the early eighties. The main choices then, as now, are RACF from IBM and CA-ACF2 and CA-Top Secret. At that time CA did not own the products. Most organizations chose CA-ACF2 or CA-Top Secret over RACF, because at that time RACF was not an extremely robust product.

Since the early to mid nineties organizations began taking a second look at RACF. Often the initial reason to consider migrating was, and still is, a dissatisfaction with their current vendor. Once these organizations began to research the implications of migrating to RACF, they also saw that RACF had become a robust product. It became very clear that IBM had committed itself to making RACF the best security product on the MVS operating system.

In 1986 RACF had roughly a 28% market share in the United States. This is based on the number of RACF licenses billing in MVS environments. RACF was the number three product behind CA-ACF2 and CA-Top Secret.

In 1993 the penetration had grown to approximately 38%, and by 1998 the penetration was 70%. The rise in market share in the United States had finally caught up with the rest of the world, and as of 1998 the penetration rates are based on the world-wide penetration of RACF on MVS and OS/390 systems.

As of the end of 1999, the RACF penetration rate has exceeded 70%. Some machines have more than one security product running in separate LPARs. Therefore, the marketplace actually exceeds 100%. We estimate that there is probably a 110% penetrated market, meaning that RACF is licensed on over 70% of MVS and OS/390 licenses. The remaining 40% or so of the market is shared between CA-Top Secret and CA-ACF2.

Since so many migrations have taken place in just the past five years, CA may still be receiving a revenue stream on unused licenses due to their practice of long-term contracts. This could mean that internally they show a higher penetration.

Many organizations are confused when we tell them that RACF has such a high penetration rate, and that it is the top security product in the MVS and OS/390 arena. The reason for this confusion lies with understanding the basis for the

penetration rates that are quoted by various vendors. Be sure to ask other vendors how many operating systems and how many products are included in their penetration number. Remember, IBM's penetration rate only includes actual revenue producing licenses only on the MVS and OS/390 operating systems.

# Chapter 2. SecureWay Security Server for OS/390

This chapter gives a high-level overview of the SecureWay Security Server for OS/390 and the security enhancements of the SecureWay Communication Server for OS/390.

## 2.1 SecureWay branding

IBM SecureWay software provides integrated directory, connectivity, and security between users and applications for e-business in a networked world. Every e-business application requires the ability to: locate resources, such as people, information and applications in the network; connect customers, partners, and employees to those resources across multiple systems; address the concern about how to secure communications, data, and transactions. SecureWay integrates these infrastructure requirements to provide the secure network platform needed for e-business. IBM SecureWay software is supported on multiple platforms, including OS/390.

With Release 8, the eNetwork Communications Server for OS/390 has been renamed SecureWay Communications Server for OS/390, and the OS/390 Security Server is renamed SecureWay Security Server for OS/390.

## 2.2 Introduction to the SecureWay Security Server for OS/390

Advances in the use of, and general familiarity with, small computers and data processing have increased the need for data security. OS/390 incorporates the SecureWay Security Server for OS/390, which provides a platform that gives you solid security for your entire enterprise, including support for the latest technologies. As a feature of OS/390, the SecureWay Security Server for OS/390 comes with the major components described in the following sections.

### 2.2.1 Resource Access Control Facility (RACF)

The primary component of the SecureWay Security Server for OS/390 is the Resource Access Control Facility (RACF). RACF works closely with OS/390 to protect its vital resources. Building from a strong security base provided by the RACF component, the Security Server is able to incorporate additional components that aid in securing your system as you make your business data and applications accessible by your intranet, extranets, or the Internet.

Using an entity known as the RACF user ID, RACF can identify users requesting access to the system. The RACF user password (or valid substitute, such as RACF PassTicket or digital certificate) authenticates the RACF user ID. RACF supports the user of PassTickets as other products use this to present a single sign-on environment to end users at their workstations. Once a user is authenticated, RACF and the resource managers control the interaction between that user and the objects it tries to gain access to. Figure 3 on page 12 shows an overview of RACF and its functions.

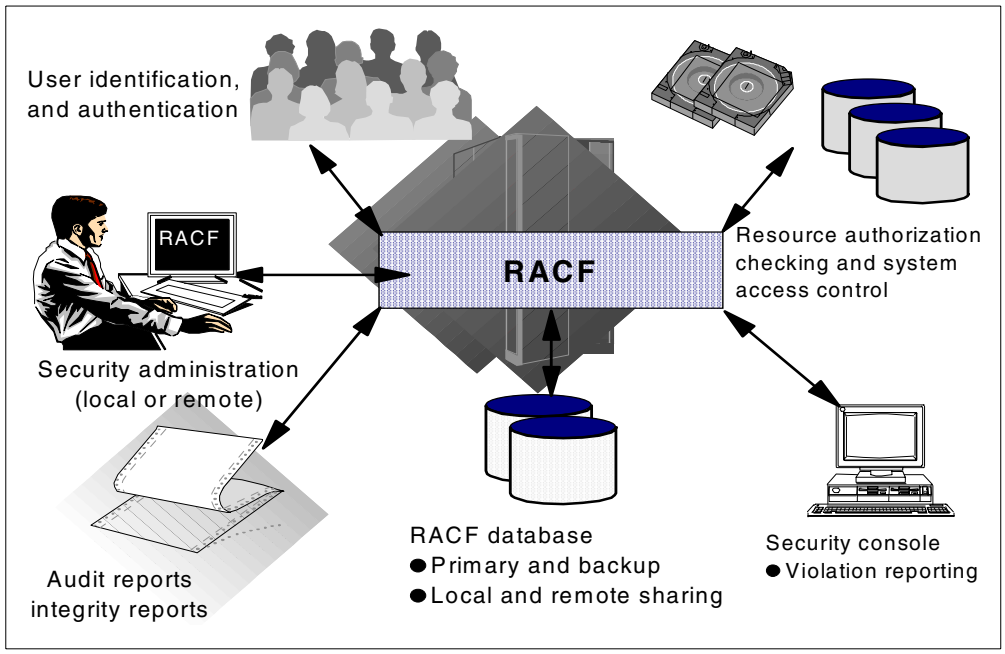


*Figure 3. RACF overview*

Digital Certificates can be mapped to the RACF user ID to provide seamless access to OS/390 resources, as shown in Figure 4.

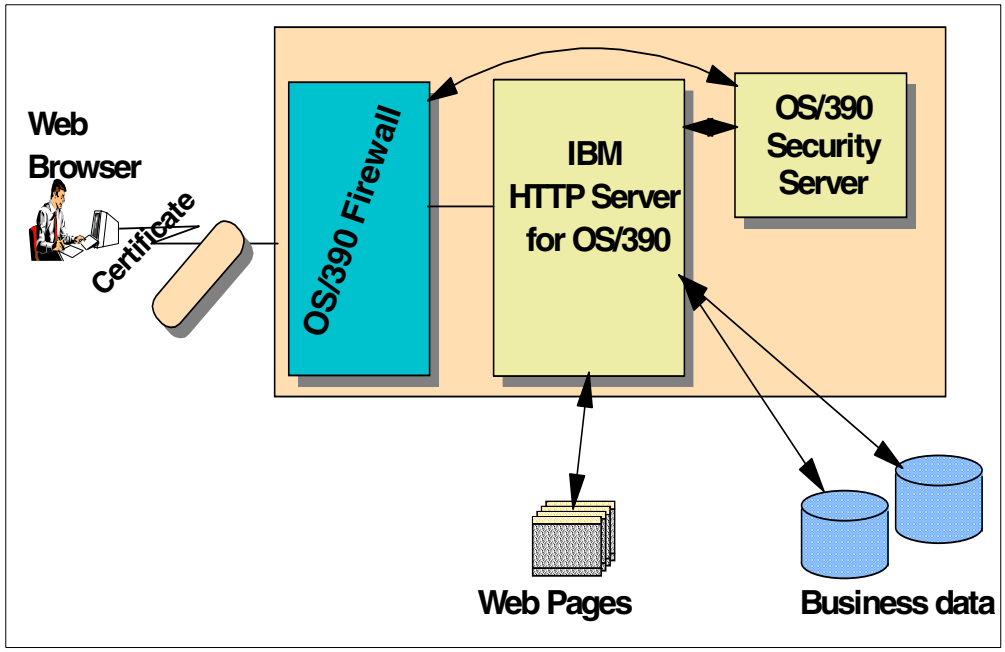


*Figure 4. Seamless access to OS/390 resources using digital certificates*

Users can be enabled to self-register their digital certificates, as shown in Figure 5 on page 13, to ease the administration of digital certificates.

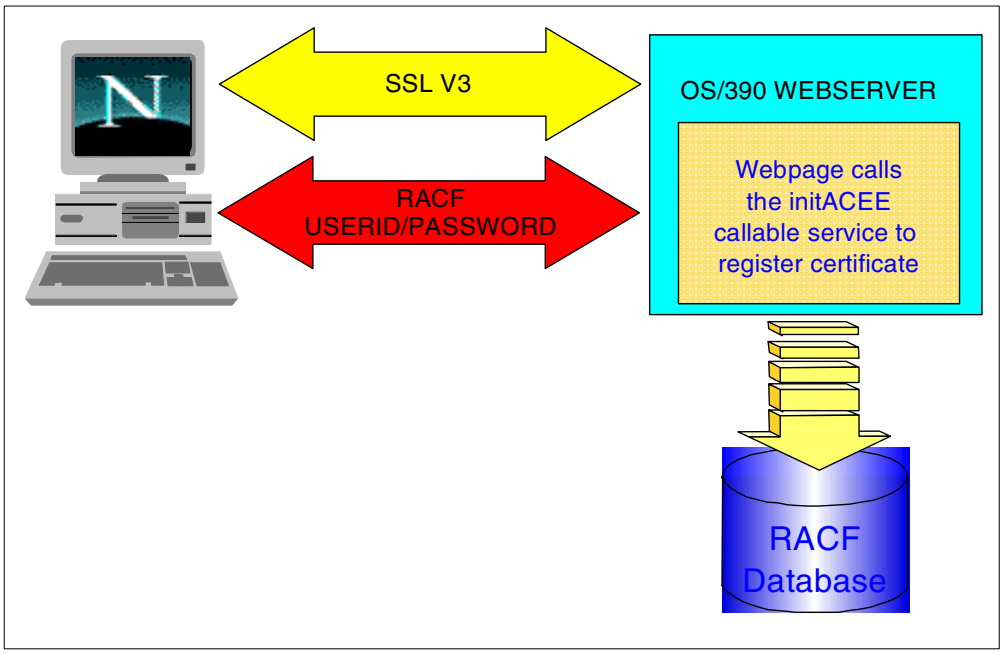


*Figure 5. Overview of the self-registration process*

Certificate name filtering support was added to associate 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 number of certificates.

With network authentication and privacy services support, it allows privacy services principal and realm information to be stored and administered in a RACF database.

RACF program control enhancement were created to provide better security and integrity of OS/390 UNIX server and daemon programs. This is accomplished by providing more control over the execution environment and preventing uncontrolled programs from entering into a controlled environment. Environment control is accomplished through a new services, IRRENS00, which marks an environment as either controlled (clean) or uncontrolled (dirty).

Application identity mapping provides an improved method for associating identities defined by OS/390 UNIX and Lotus Notes for OS/390.

### 2.2.2 The DCE Security Server

The DCE Security Server provides user and server authentication for applications using the client-server communications technology contained in the Distributed Computing Environment for OS/390. The DCE Security Server can also interoperate with users and servers that make use of the Kerberos V5 technology developed at the Massachusetts Institute of Technology and can provide authentication based on Kerberos tickets.

Through integration with RACF, OS/390 DCE support allows RACF-authenticated OS/390 users to access DCE-based resources and application servers without

having to further authenticate themselves to DCE. In addition, DCE application servers can, if needed, convert a DCE-authenticated user identity into a RACF identity and then access OS/390 resources on behalf of that user, with full RACF access control. Figure 6 shows an overview of the DCE and RACF interoperation.

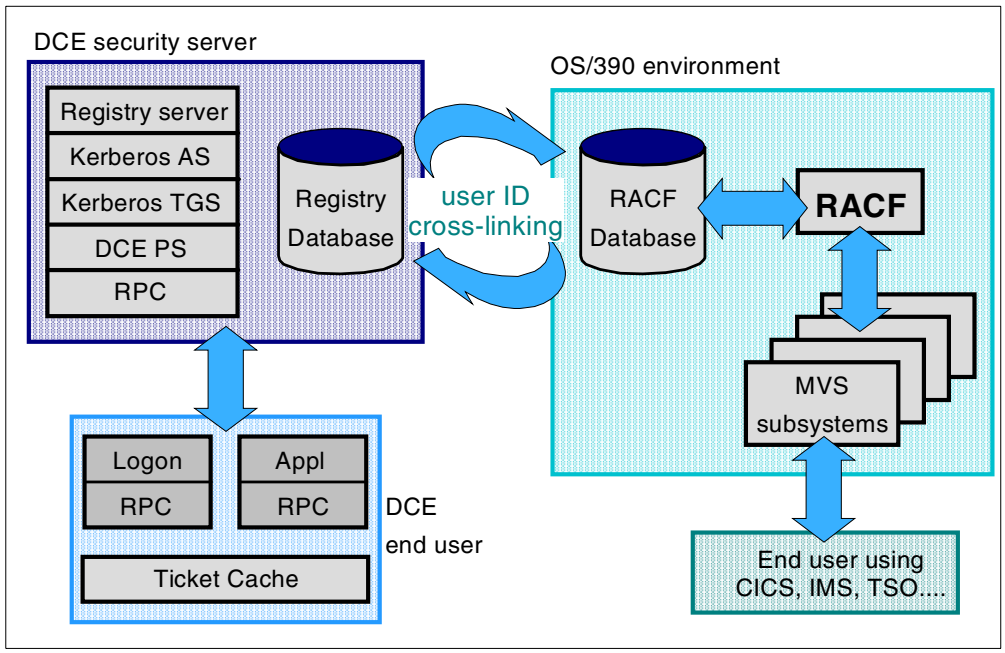


*Figure 6. DCE-RACF interoperation*

### 2.2.3 OS/390 firewall technologies

Implemented partly in the Security Server and partly in the SecureWay Communications Server for OS/390, OS/390 firewall technologies provide basic firewall capabilities on the OS/390 platform to reduce or eliminate the need for non-OS/390 platform firewalls in many customer installations.

The Communications Server provides the firewall functions of IP packet filtering, IP security (VPN or tunnels), and Network Address Translation (NAT).

The Security Server provides the firewall functions of FTP proxy support, SOCKS daemon support, logging, configuration, and administration.

OS/390 Firewall Technologies has support for On-Demand Dynamic Virtual Private Networks (VPNs). On-Demand VPNs allow an outbound Security Association (SA) to be set up automatically when the designated network traffic requires that it be transmitted securely through a VPN. Figure 7 on page 15 shows the potential usage of VPN technology.

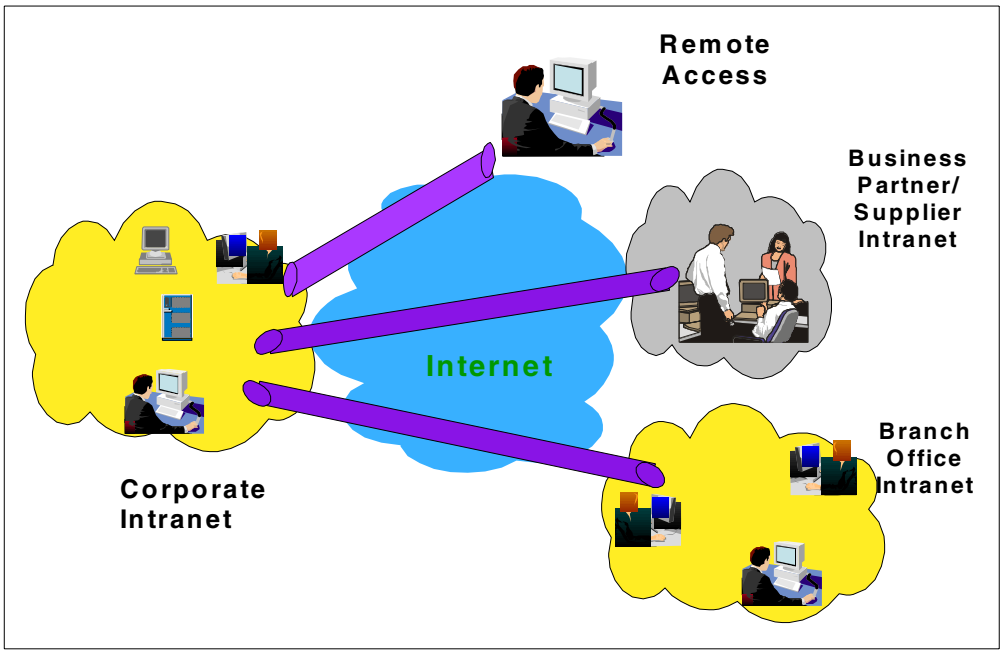


*Figure 7. Usage of VPN technology*

### 2.2.4 The LDAP Server

The LDAP Server provides secure access from applications and systems on the network to directory information held on OS/390 using the Lightweight Directory Access Protocol (LDAP). A directory is typically employed to store information used to locate computing resources, information about people in an enterprise, or configuration information for systems and services.

RACF data presents a large set of user, group, and profile information that is useful to applications in other environments or on other systems. This item makes RACF information that is accessible through SAF interfaces available via an OS/390 LDAP server to programs on and off the OS/390 platform. Figure 8 on page 16 shows an overview of the OS/390 LDAP server and the back-end systems it supports.

User ID and password authentication of LDAP client access to OS/390 LDAP Directory Server can be optionally handled by Security Server RACF rather than by accessing user IDs and passwords stored within the LDAP Server Directory.

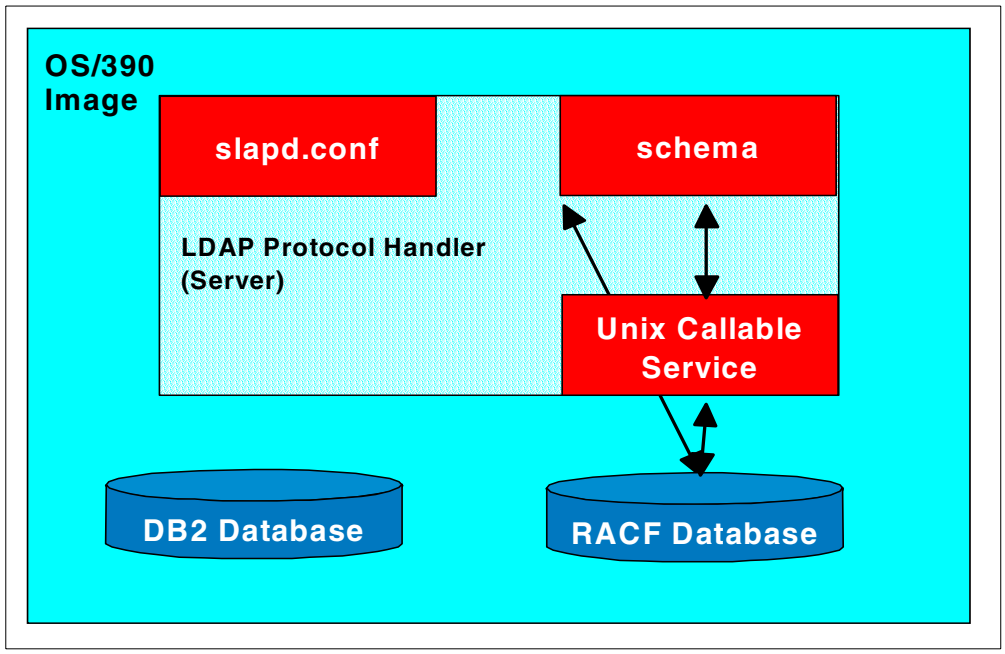


*Figure 8. Overview of the OS/390 LDAP Server and supported back-end systems*

### 2.2.5 Network Authentication and Privacy Service (Kerberos)

This is a new component of the SecureWay Security Server for OS/390. It is an implementation of MIT's Kerberos Version 5. It provides authentication, delegation, and data confidentiality services which are interoperable with other industry implementations based on the MIT Kerberos Version 5 reference implementation.

The Network Authentication Server provides the basis of consistent user identification and authentication in a heterogeneous networked environment when combined with Kerberos-aware applications that can span OS/390 and other platforms which support the MIT Version 5 Kerberos reference implementation.

The security client locates the security server through one of three methods:

1. Using LDAP, when the LDAP server is specified in the Kerberos configuration files.
2. Using the Domain Name Service (DNS), when DNS lookup is specified in the Kerberos configuration files.
3. Using static information contained in the Kerberos configuration files, when the LDAP or DNS server is not available or the target realm is not defined in the directory.

   **Note 1:** This is new function delivered as part of the Security Server, but is shipped *always-enabled*, like the LDAP Server. This means that it does not require a Security Server license in order to use it, but it does require that some new functions and fields be implemented in RACF.

   **Note 2:** Network Authentication and Privacy Service is a new implementation of Kerberos and does not require DCE.

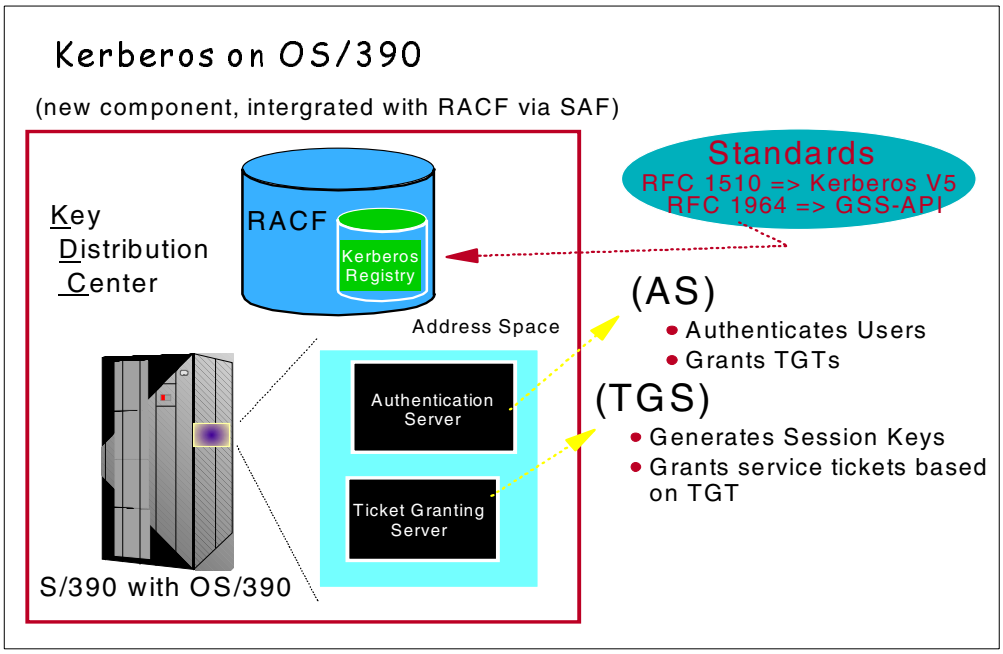


*Figure 9. Kerberos implementation on OS/390*

Figure 9 shows an overview of the various Kerberos pieces:

1. Kerberos registry integrated into RACF registry
2. Kerberos KDC executes within OS/390 address space
3. OS/390 KDC behaves like any other Kerberos “realm”
4. Kerberos realm-to-realm function supported

### 2.2.6 OS/390 Open Cryptographic Services Facility (OCSF)

Cryptography comprehensively helps meet multiple security needs, such as confidentiality, authentication and non-repudiation. Open Cryptographic Service Facility (OCSF) for OS/390 addresses these requirements in the emerging Internet, intranet, and extranet application domains. The primary application interface to this function is provided by Open Cryptographic Enhanced Plug-ins (OCEP), a component of Security Server.

OCEP functions are to be used by applications complying with Common Data Security Architecture (CDSA) standard interfaces. This makes it easier for application developers and independent software vendors (ISVs) to develop and port applications to the S/390 platform. It also helps customers apply consistent security rules to e-business applications that use digital certificates. Figure 10 on page 18 shows an overview of the OCSF and OCEP.

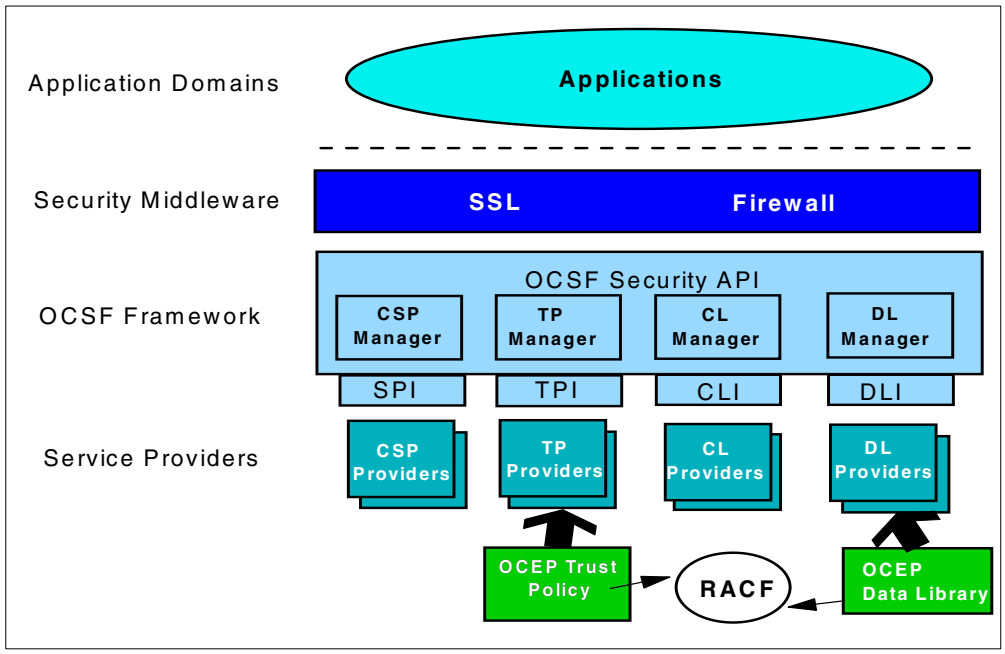


*Figure 10. OCSF -OCEP infrastructure overview*

The optional PCI Cryptographic Coprocessor (PCICC) brings additional cryptographic processing capacity and function to S/390 Parallel Enterprise G5 and G6 Servers. The PCICC feature is *integrated* into S/390 and OS/390. (Some people mistakenly think it is an external box.)

PCICC works in conjunction with the CMOS Cryptographic Coprocessor that is standard on those servers. PCICC is not a substitute for CMOS crypto coprocessors and in fact *requires* that the CMOS crypto coprocessors be enabled. Transparently to applications, OS/390 will route requests to the appropriate crypto engines for processing. OS/390 V2 R9 is the minimum release level required for PCICC support.

The SecureWay Security Server for OS/390 provides “one-stop shopping” for security on OS/390. With its integration of RACF and DCE security, its contribution to the OS/390 Firewall Technologies, the LDAP server, and RACF support for client authentication via digital certificates, the Security Server provides complete security both for traditional host-based data processing and for safely expanding your enterprise onto the Internet.

# Chapter 3. RACF overview

The Secureway Security Server for OS/390, also known as Resource Access Control Facility (RACF), is an IBM program product designed to provide OS/390 and VM users with an effective tool for managing access control, an increasingly important user responsibility and concern.

The objective of RACF access control is to protect data sets and other data processing resources from unauthorized destruction, modification, or disclosure, whether by accident or design. To be effective, security procedures should be easy to use and place no additional burden upon data processing management. RACF controls users and protects resources.

Users are identified by a *user ID* and authenticated by a *password*. A RACF user is identified by an alphanumeric user ID. However, a RACF user does not have to be an individual. For instance, a user ID can be associated with a started task address space or a batch job.

Resources can be divided into two categories, data sets and general resources. General resources include:

- CICS/VS resources
- DASD volumes
- DB2
- IMS/VS resources
- JES resources
- NODES
- Programs
- Tape volumes
- Terminals
- VM

There are many other resources that can be protected. For a full list of resource types (or resource classes), see *OS/390 Security Server (RACF) System Programmer's Guide.*

Before describing RACF resource definitions and resource access authorizations, we will explain how RACF is started and its main components. It may prove very useful when we discuss conversion problems from another security product.

RACF is started during system IPL. There is no specific command to start RACF. So, there is no specific command to stop it.

At startup time, RACF requires the name of the data sets containing user and resource definitions. Names can be provided either by a table (ICHRDSNT), or by a DD statement in MSTRJCL. If MSTRJCL does not contain a proper DD statement, and the name table is empty or contains invalid names, the operator is prompted for the name of the RACF database.

Some advantages and disadvantages of each of the three methods are:

- MSTRJCL

  You can define only one RACF database (the primary database). No secondary RACF database definition is allowed.

- Operator reply

  Very suitable for early tests, a conversion is an iterative process. Replying the RACF database name at IPL time may provide flexibility to back out to a previous iteration stage if errors are encountered and the current IPL is in error.

- ICHRDSNT (database name table)

  Recommended for standard implementation. No reply is needed at IPL time. Primary and secondary database names are allowed. The number of resident data and index blocks in storage is also specified.

## 3.1 Information flow

For all resources, security is processed through the system as summarized in Figure 11 on page 21. In this process, the components involved are listed in the leftmost part of the figure. They are (top to bottom):

- A subsystem (such as JES) or an application
- The System Authorization Facility (SAF), which is part of OS/390
- RACF
- The RACF database

The role of each component in the security process is discussed in later topics. The information that is passed is discussed in the following sections.

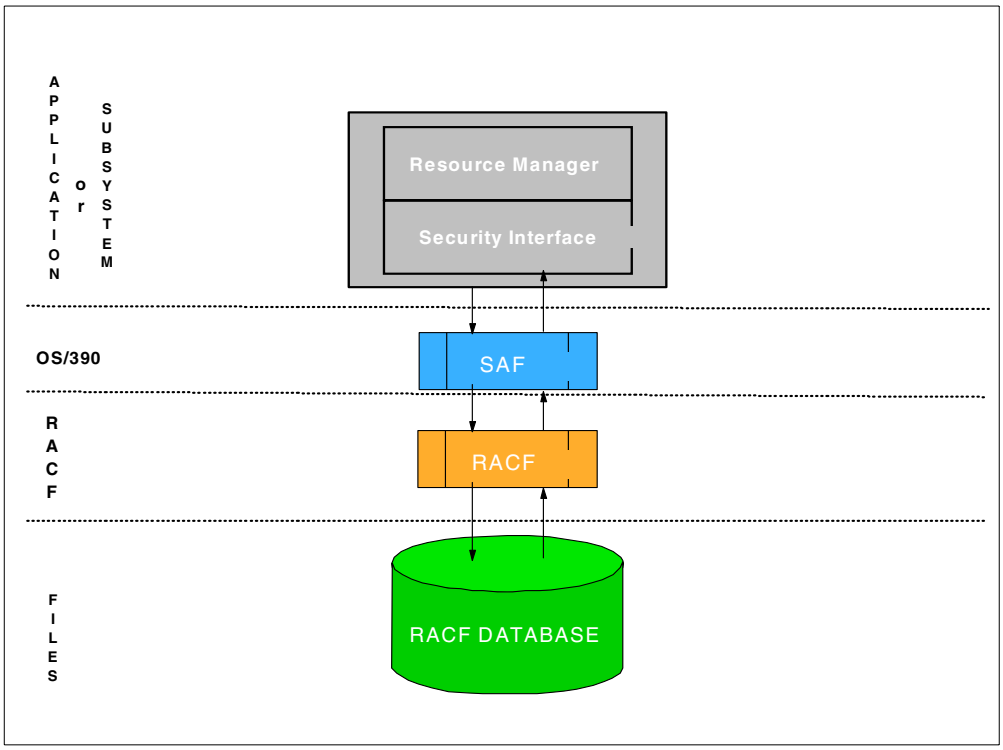


*Figure 11. Information flow for RACF*

The application directs a request to RACF. Depending on the type of request, information is passed along with the request; for example:

Example 1

```
Request to RACF       : Verify user identity

Information passed    : USERID and PASSWORD
```

Example 2

```
Request to RACF       : Check user access to a resource

Information passed    : USERID
                        Resource name and type
                        User intent
```

The security interface formats the information gathered by the application to be used by the security monitor (here RACF) and passes it to the System Authorization Facility (SAF).

SAF determines what actions are required to process the request and may forward the request to RACF if needed. If requested, RACF then performs the check by verification against data retrieved from the RACF database. Although Figure 1 may indicate an input operation is performed, RACF data is often retrieved from areas in storage and no input operation takes place.

RACF always returns a return code as a response to a request. A reason code may also be returned. For list-type requests, RACF also returns the requested data.

A return code of zero (0) indicates a valid request. A non-zero return code indicates a request failure. This return code is passed to the resource manager that issued the request. It is up to the resource manager to take appropriate action.

The logical functions of each component are as follows:

- Interface role
  - Receive and format information from the application.
  - Route information to the SAF facility.
  - Receive a return code from RACF and return it to the caller.
- SAF role
  - Route the request to the security monitor.
  - Route the response to the proper requestor.
- RACF role
  - Send back a return code and reason code as a response to a security request.
  - Add, modify, or delete profiles in the database as required by RACF commands executed by an authorized user.
  - Set global option values as directed by authorized users.
  - Return requested information from the database in response to a list-type command.

### 3.1.1 Authorization flow

For all resources, security authorization is processed through the system as summarized in Figure 2. For more information on authorization flow, see *OS/390 Security Server* (*RACF) Security Administrator's Guide*.

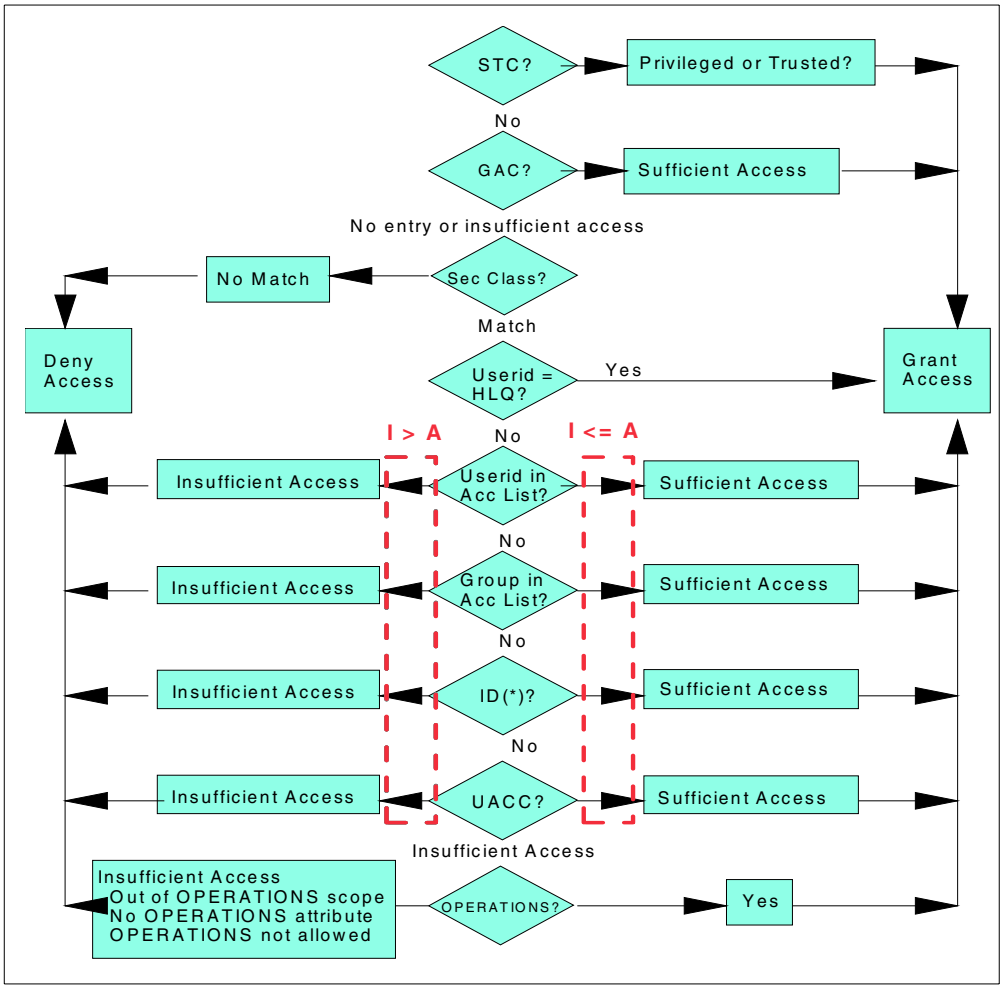


*Figure 12. Authorization flow for RACF*

## 3.2 Vocabulary

This section defines terms used in RACF.

### 3.2.1 RACF user

A RACF user is always defined as a member of a RACF group. This group is called its *default group*. An entry in the RACF database describing a user is called a *user profile*.

A user profile describes the user by name (user ID), password, default group, the times that user can use the computing system, and statistics on a prior logon by the user. It also describes other groups the user may belong to. A user must be a member of at least one group (the default group), and potentially of other groups (connect groups).

User profiles may also contain *user attributes*. These attributes describe the privileges and restrictions that the user has when using the system. Attributes are classified as either user-level or group-level attributes. When attributes are assigned at the user level, the scope of the attributes are at the system level and

privileges granted are across the entire system. When attributes are assigned at the group level, the corresponding privileges are restricted to a group or the scope of the group in which attributes are assigned. Related product data may also be recorded in user profiles. The set of data for a specific product is called a *segment*. At the user level, there may be segments for:

- CICS
- DCE
- DFP
- LANGUAGE
- LNOTES
- NDS
- NETVIEW
- OMVS
- OPERPARMS (for MCS extended console sessions)
- OVM
- TSO
- WORKATTR (for APPC/MVS processing)

For more information on each segment's content, see the corresponding topic in this book, or in *OS/390 Security Server (RACF) Command Language Reference*.

The ability to define attributes at the system or group level is used to build the correct administrative structure for RACF. The `SPECIAL` and `AUDITOR` attributes, defined at the appropriate level, are used to achieve centralized or decentralized security administration.

For conversion purposes, users are often classified as:

- TSO users
- STC (or started task users)
- Others

In the RACF database, there is no special definition for a TSO user, an STC user, or other users. All are RACF users. The default group, attributes, and other values in the profiles make the difference. It should be noted that a RACF user ID can range from one to eight characters in length, but a RACF user ID used for TSO LOGON must not be longer than seven characters.

### 3.2.2 RACF group

A RACF group consists of all the users that have similar requirements for access to the system's resources. Each group, with the exception of the highest group (SYS1), has a superior group. A RACF group is identified by its name. The name of a group is one to eight alphameric characters, the first being alphabetic or special characters.

An entry in the RACF database describing a group is called a *group profile*. A group profile contains the group name, the superior group, the owner name (if not

the superior group), a list of all RACF groups that have the described group as its superior group, and a list of user IDs that are members of the group.

The *scope* of a group is confined to all resources and users within that group and those of all groups that are subordinate to that group.

Related product data may also be recorded in group profiles. The set of data for a specific product is called a *segment*. At the group level, there may be segments for:

- DFP
- OMVS
- OVM
- TME

### 3.2.3 Owner

Each entry (or profile) in the RACF database has an *owner*. The owner must be a RACF-defined USER or GROUP. For ease of administration, group ownership is preferred. The RACF owner of a profile has full administrative authority over the profile. If the profile is a user or a group profile that is in turn designated as the owner of other profiles, the RACF owner of the top profile has full administrative authority over the other profiles.

### 3.2.4 RACF protected resources

RACF resources are all the components of a computing complex required by a job or a task. RACF resources include input/output devices, processing units, data sets, job output, nodes, programs, and other items that must be kept secure for normal business operations.

RACF protected resources can be divided into two categories:

- Data sets
- General resources

Both are described by *resource profiles*. RACF subdivides resource profiles into two types: discrete profiles and generic profiles.

A *discrete profile* protects a single resource that has unique requirements. This profile contains a description of the resource, including the authorized users, the access authority of each user, and in the case of data sets, the volume of the data set.

A *generic profile* protects several resources that have a similar naming structure and security requirements. This profile contains a description of the resources, including the authorized users and the access authority of each user. For more information on discrete and generic profiles, see *OS/390 Security Server (RACF) Security Administrator's Guide*.

#### 3.2.4.1 Data sets

Data-set resources include both DASD and tape data sets, and are described in the RACF database using *data set profiles*. A data set profile contains information about the data set profile owner, universal access, and other optional information, such as the device volume serial number and data set security classification.

Before a data set profile can be created in the RACF database, a group profile or user profile having the data set high-level qualifier (HLQ) as the group or user name must be defined. This group or user is used in the RACF database as an anchor point for all profiles having the same HLQ.

Therefore, protection for a data set always includes at least two entries (but optionally more) in the RACF database:

- A group profile or user profile (with same name as data set HLQ)
- One or more data set profiles (either discrete or generic)

When a data set can be protected by several different profiles, RACF searches for the best-fitting profile. The search is made from the most specific profile to the least specific. Access is then granted or denied according to the security classification associated with the data set and the user requesting access, the access lists contained in the selected resource profile, and user attributes.

#### 3.2.4.2 General resources

A *general resource* is any resource other than a data set. For example, transactions, TSO logon procedures and job SYSOUT are general resources. RACF defines the set of general resources in a Class Descriptor Table (CDT), which identifies a RACF class of entities by the resource class name. This table includes the resource class name, all syntax rules, and auditing and statistical control.

A standard IBM-supplied CDT is installed with RACF at initialization time. You can append your unique class names to the standard CDT to represent your installation's requirements outside of those identified by RACF. For more information on the Class Descriptor Table and on how to add new resource classes, see *OS/390 Security Server (RACF) System Programming Library:*

A conversion to RACF may require you to add installation-defined classes to the standard CDT.

Protection of a general resource can be achieve through use of one or several profiles, either specific or generic. Note that:

- No anchor point is needed for general resource profiles (unlike data-set profiles).
- Authorization is the same as for data sets.

For most of the general resource classes, a relationship exists between a class called a *member* class and another class called a *grouping* class.

The class TCICSTRN, for example, is a standard RACF resource class in which one can create profiles to protect one or several similarly named CICS transactions.

For example:

- A transaction named TRN1 can have a profile in the TCICTRN class with a resource name of TRN1.
- All transactions whose names begin with TRN can have a profile in the TCICSTRN class with a resource name of TRN*.

But we may wish to define transactions TRN5, TRTA, and XYZ as having the same protection and authorization requirements.

We can then use the CICS grouping resource class name of GCICSTRN. Our grouping transaction profile can then be defined in the GCICSTRN class with a name of MYOWNAME and members TRN5, TRTA, and XYZ. This profile will then control access to all the member transactions. MYOWNAME is an arbitrary unique name within the GCICSTRN class. This name is assigned by the installation to be a meaningful mnemonic. Grouping classes should be considered when converting protection rules from another security system.

### 3.2.5 RACF system-wide options

RACF system-wide options are used to customize RACF for installation-specific security. Mainly, these options deal with:

- Auditing
- Statistics
- Activation of classes
- Use of generics
- In-storage profiles
- JES job verification
- Default JES user IDs
- Data set protection and access
- Password rules
- SECLABELS
- Default language

Setting appropriate values for all general options in order to provide equivalent RACF functions when converting from another security product is part of the conversion project. When needed, changes to these values are mentioned in the appropriate chapters. For a complete description of RACF options, see *OS/390 Security Server (RACF) Command Language Reference* and OS/390 Security Server (*RACF) Security Administrator's Guide*.

### 3.2.6 The RACF database

There is only one RACF database, which holds the following:

- System options
- User profiles
- Group profiles
- Data set profiles
- General resource profiles

For performance purposes, this database can be broken into several files spread across system DASD volumes.

For recovery purposes, this base can be *mirrored* onto another database. The main database is referred to as the *primary database*. The mirror database is referred to as the *secondary database*.

Modifications to the primary database are reflected in the secondary base at the time they occur. RACF database definitions allow flexibility in the information to be mirrored, providing the secondary database is online and active.

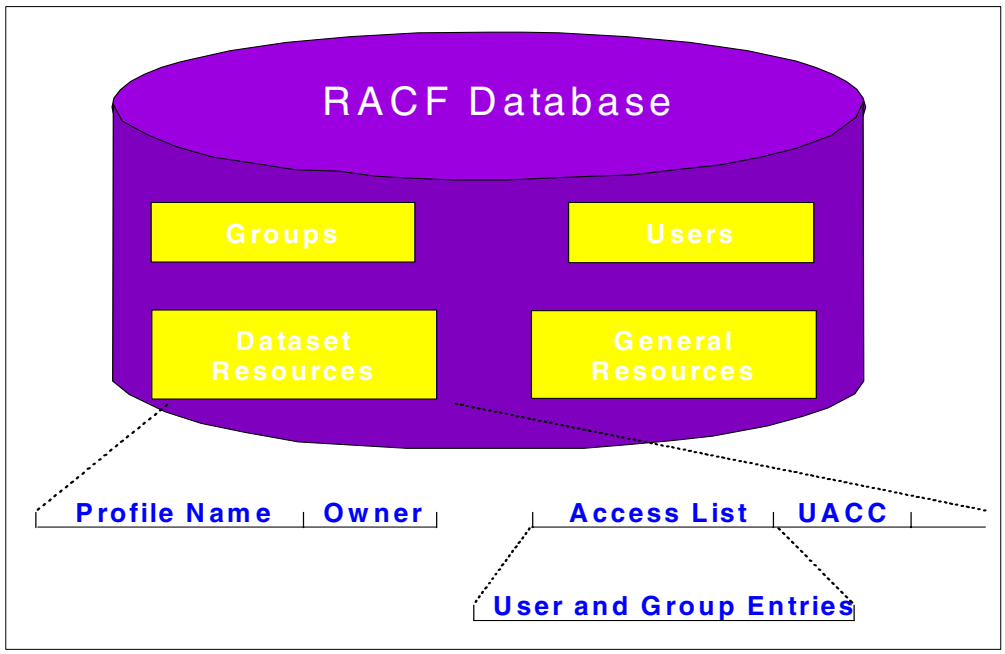


*Figure 13. Database structure for RACF*

### 3.2.7 RACF commands

RACF commands are TSO/E commands that may be executed either online from a TSO terminal or as a part of a batch TMP job. RACF panels and REXX procedures are both available in addition to the online commands.

In following chapters we will see that one of the main tasks in a conversion process is the generation of many RACF commands. These typically will be used as input to several batch TMP jobs to load the RACF database with security information. Creation, review, edit, and execution of such files is an iterative process during the conversion. Following is a brief review of the main commands:

- Commands directed to user profiles:

  `ADDUSER (AU)` Add User Profile

  `ALTUSER (ALU)` Alter User Profile

  `DELUSER (DU)` Delete User Profile

  `LISTUSER (LU)` List User Profile

  `PASSWORD (PW)` Specify User Password

  `CONNECT (CO)` Connect User to Group

**REMOVE (RE)** Remove User from Group

**SEARCH (SR)** Search for User Profiles

- Commands directed to group profiles:

  **ADDGROUP (AG)** Add Group Profile

  **ALTGROUP (ALG)** Alter Group Profile

  **DELGROUP (DG)** Delete Group Profile

  **LISTGRP (LG)** List Group Profile

  **SEARCH (SR)** Search for Group Profiles

- Commands directed to data-set profiles:

  **ADDSD (AD)** Add Data Set Profile

  **ALTDSD (ALD)** Alter Data Set Profile

  **DELDSD (DD)** Delete Data Set Profile

  **LISTDSD (LD)** List Data Set Profile

  **PERMIT (PE)** Maintain Data Set Access List

  **SEARCH (SR)** Search for Data Set Profiles

- Commands directed to general-resource profiles:

  **RDEFINE (RDEF)** Define General Resource Profile

  **RALTER (RALT)** Alter General Resource Profile

  **RDELETE (RDEL)** Delete General Resource Profile

  **RLIST (RL)** List General Resource Profile

  **PERMIT (PE)** Maintain General Resource Access List

  **SEARCH (SR)** Search for General Resource Profiles

- Others (RRSF, System, etc..):

  **DISPLAY** Display Sign-On-From List

  **HELP (H)** Obtain RACF Help

  **RACDCERT** RACF Digital Certificate

  **RACLINK** Administer User ID Associations

  **RESTART** Restart RRSF Functions

  **RVARY** Change Status of RACF Database

  **SET** Set RRSF Operational Characteristics

  **SETROPTS (SETR)** Set RACF Options

  **SIGNOFF** Sign Off Session

  **STOP** Shutdown RRSF

  **TARGET** Define RRSF Nodes

Figure 14 on page 30 shows an overview of all RACF commands.

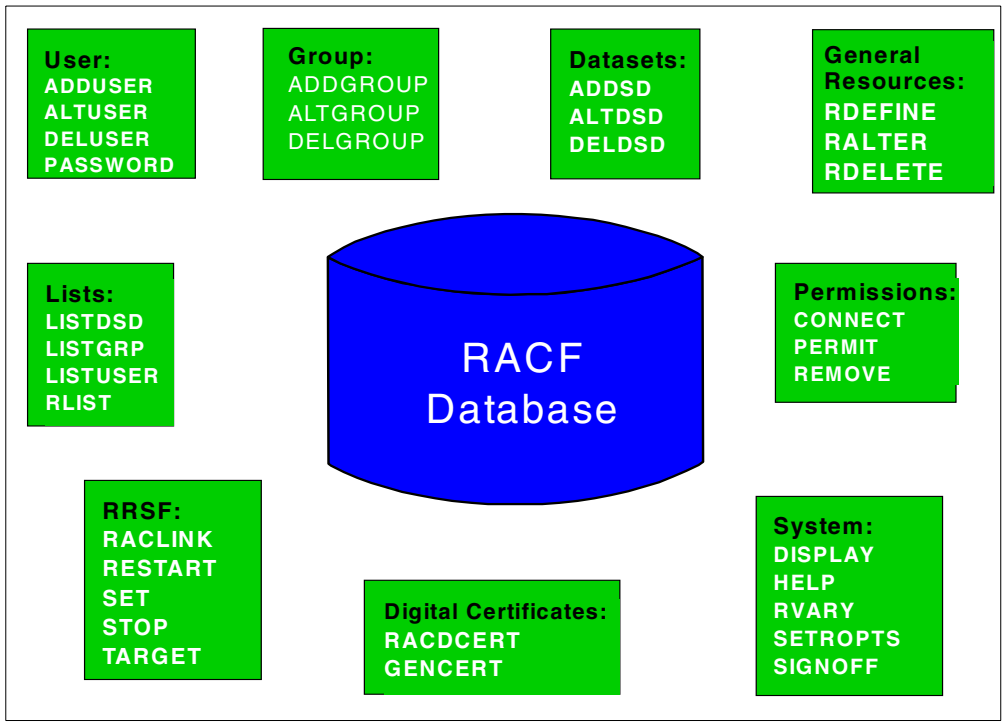


*Figure 14. Commands for RACF*

Complete details about each command can be found in *SecureWay Security Server RACF Command Language Reference,* SC28-1919.

## 3.3 Interfaces

This section describes the interfaces to RACF.

### 3.3.1 Product interfaces

Products may or may not have security interfaces to RACF. RACF product or application interfaces fall into three categories:

- Implicit

  A product interface to RACF is *implicit* when no parameter value settings are needed in the product to enable it to use RACF for security controls. For example, products such as JES2 or TSO/E have implicit interfaces.

- Explicit

  A product interface to RACF is *explicit* when parameter value settings are needed in the product to enable it to use RACF for security controls. For example, products such as CICS and IMS have explicit interfaces.

- Exit Driven

  If neither an implicit nor an explicit interface to RACF exists for a product, the installation can create the interface by using standard API. The security requests are called from standard product exits. This approach can also be used to create interfaces to RACF from within applications.

One of the major problems in converting from another security system to a RACF security system is the inventory of all interfaces used by the non-RACF security product. We may discover that an exit interface has been used by the non-RACF security product in order to bypass a standard implicit interface to RACF, or parameter values to activate RACF from an explicit interface have not been set.

Re-establishing use of standard interfaces is one part of the conversion task.

### 3.3.2 The SAF interface

The System Authorization Facility (SAF) is a part of OS/390 and is always active. Any security product can use the SAF interface. The main purpose of SAF is to route requests from applications or subsystems to the proper security component for processing. This routing uses the SAF Router Table. Depending on the type of request SAF may, or may not, invoke RACF services.

For a description of SAF and how to add entries in the SAF Router Table, see *SecureWay Security Server RACF System Programmer's Guide,* SC28-1913.

### 3.3.3 RACF exits

RACF provides exit points that can be used for additional levels of protection. Figure 15 shows all the exits that RACF currently supports. Most installations will not need to code these exits. Where possible, standard RACF functions should be used.

The following section gives a brief description of some of the more common exits and their possible uses. You can verify which exits are active by reviewing the RACF DSMON report. Some exits can do both pre- and post-processing. Normal RACF usage does not require the use of any exits. The exits provide interfaces for changing normal RACF processing.

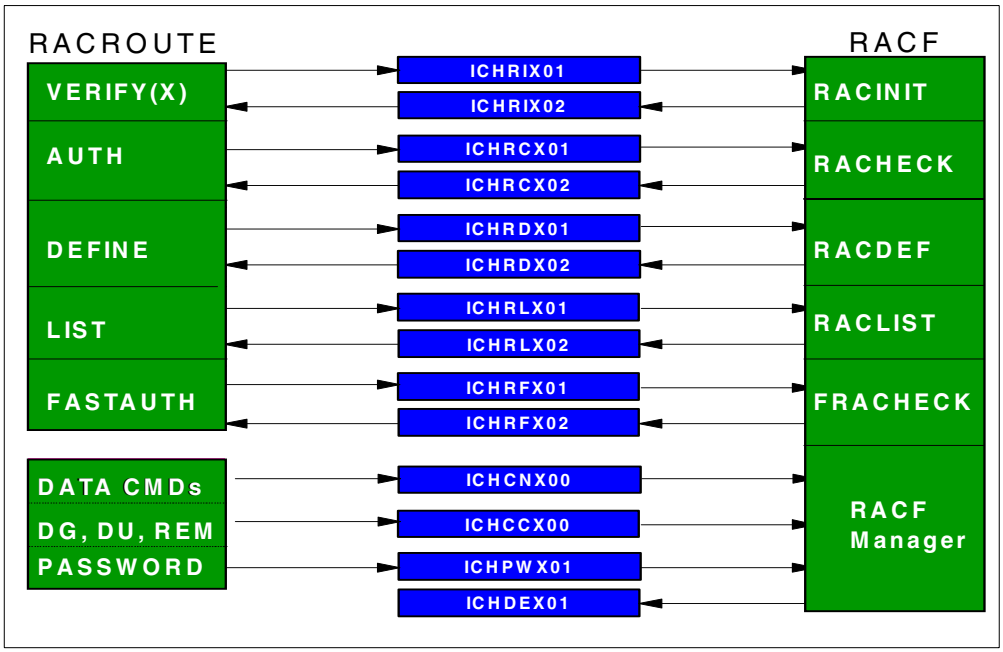


*Figure 15. RACF exits*

#### 3.3.3.1 Command exits - ICHCNX00/ICHCCX00

These exit routines allow the installation to associate additional security checking, or processing, with certain RACF commands, or to bypass checking altogether.

#### 3.3.3.2 Authorization exits - ICHRCX01/ICHRCX02

The `RACROUTE REQUEST=AUTH` exits can alter the decision-making process that determines if a user should have access to a resource.

#### 3.3.3.3 Define exits - ICHRDX01/ICHRDX02

The `RACROUTE REQUEST=DEFINE` exits can alter the creation (or deletion) of profiles. These might be used to enforce local standards.

#### 3.3.3.4 Verify exits - ICHRIX01/ICHRIX02

The `RACROUTE REQUEST=VERIFY(X)` exits can alter the authentication processing for a user.

#### 3.3.3.5 Password encryption - ICHDEX01

This exit can be used to alter the form in which passwords are stored.

#### 3.3.3.6 Password checking exit - ICHPWX01

This exit can be used to check for trivial passwords and enforce local password rules in addition to normal RACF password rules.

#### 3.3.3.7 Data set naming convention table - ICHNCV00

This table allows the installation to set up and enforce data set naming conventions that are different from standard RACF naming conventions. For example, you may need to perform RACF checking on the second-level qualifier of a data set and not the first, which is the way RACF normally works.

# Chapter 4. CA-ACF2 overview

This chapter briefly describes the Computer Associates Access Control Facility, CA-ACF2.

## 4.1 CA-ACF2 security philosophy

CA-ACF2 is designed to authenticate users and to protect a variety of OS/390 resources. Users must have a valid CA-ACF2 Logon ID (LID) and must know the current password in order to enter a CA-ACF2 protected OS/390 system. Resources consist of data sets and other resources as determined by individual resource managers. For instance, the resource manager CICS calls the External Security Manager (in this case CA-ACF2) for authorization on CICS transactions, commands, files, and other CICS-related activity.

Security definitions in CA-ACF2 are called *rule sets*. Resources other than data sets are called *generalized resources* (GRS) and may also be protected by rule sets. The name of the GRS is limited to a 3 character type.

A rule set protects a resource or a set of resources by defining the environment, the access levels, and user authorizations.

If no rules apply, access is denied by default. The MODE setting at a system-wide level may alter this default.

If several rules apply, normal search order is from the most specific rule to the least specific rule, as in RACF. A $NOSORT parameter indicates that rules are to be searched in the exact sequence of entry in the rule set, rather than allowing the rules to be sorted during rule compilation. Difficulties in the conversion process may arise if the $NOSORT parameter is set for some rules.

Authorization is allowed or prevented (denied) to a user by a rule if there is a match between a character string (UID string) in the rule and the UID string identifying the requesting user. The user UID value is assigned at the time a user is defined to CA-ACF2.

Authorization to access a resource is explicitly granted or denied by a *rule*, but implicit authorizations may also be granted by *privilege* values in the CA-ACF2 user description (also called Logon ID (LID)), or other fields in the same LID record. Privilege values include:

**ACCOUNT** A privilege that grants administrative access to LIDs in the CA-ACF2 data base.

**SECURITY** A privilege that grants access to all resources with logging. Security also grants the LID administrative privileges over other parts of the CA-ACF2 data base.

**NON-CNCL** A privilege that grants access to all resources, regardless of what the associated rule set allows. Though access will be granted to all resources, access is logged when the LID is not on the access list at the requested level. This provides an audit trail of NON-CNCL accesses.

**MAINT** A privilege that grants access to all resources when using a maintenance program from a given library. Program and library

names are recorded as part of the privilege. There is no logging of accesses when the MAINT privilege is in effect.

**READALL** A privilege where only READ access is granted to all data sets, regardless of what the associated rule set allows.

**PREFIX** A parameter in a LOGONID section. Access is granted to all data sets whose high-level qualifier (HQL) is equal to the PREFIX value.

### 4.1.1 CA-ACF2 information flow

The flow of information in CA-ACF2 is similar to that of RACF. One difference is CA-ACF2 requires non-standard SAF modules for its interface with any Resource Manager. Additionally, CA-ACF2 honors standard RACROUTE macro interfaces; however, since CA-ACF2 modifies SAF, not all RACROUTE macros will behave the same as in a standard RACF/SAF environment. Also, some resource managers have CA-ACF2 intercepts created for their use with CA-ACF2. The most commonly used Resource Manager modification occurs within CICS.

To summarize, CA-ACF2 modifies some resource managers and modifies SAF. See the following diagram for an example of the CA-ACF2 information flow:

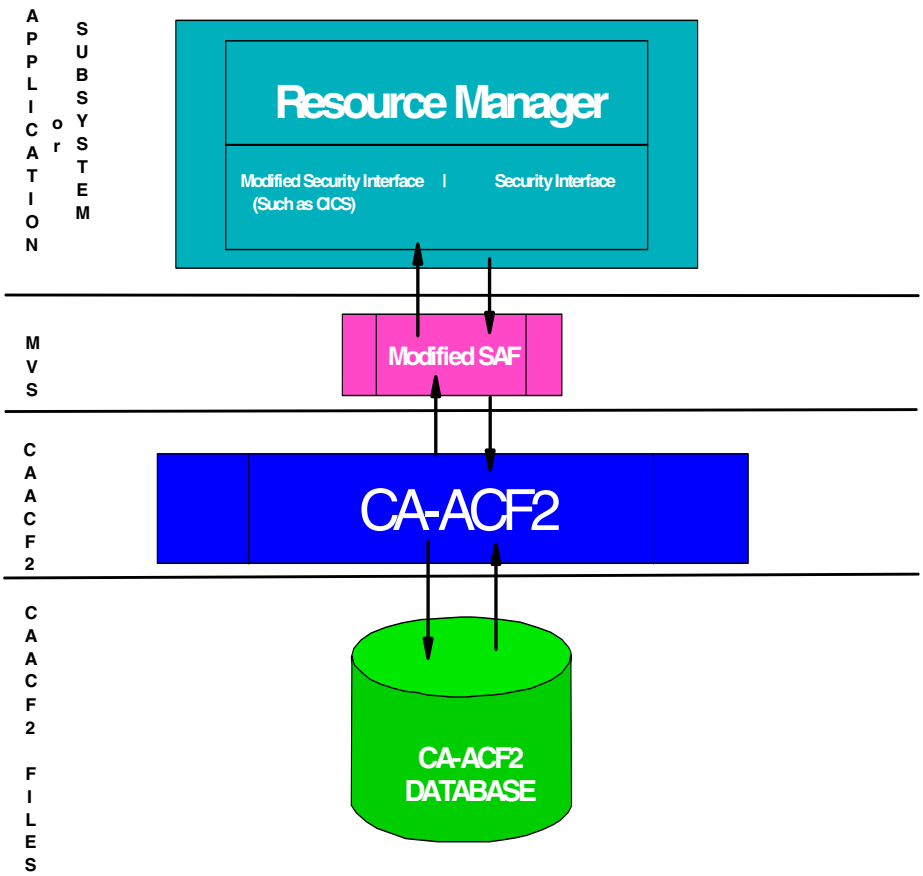


*Figure 16. CA-ACF2 information flow*

The CA-ACF2 subsystem executes in its own address space. CA-ACF2 execution is stopped by entering a STOP (P) command (with the proper procedure name) on

an OS/390 console. RACF cannot be stopped or removed from an operating system after the IPL.

### 4.1.2 CA-ACF2 access flow

CA-ACF2 uses different access flow logic when compared to RACF. In general, RACF honors the access list rather than any special privileges. Compare the CA-ACF2 access flow, shown in Figure 17, against the RACFauthorization flow, shown in Figure 12 on page 23**.**

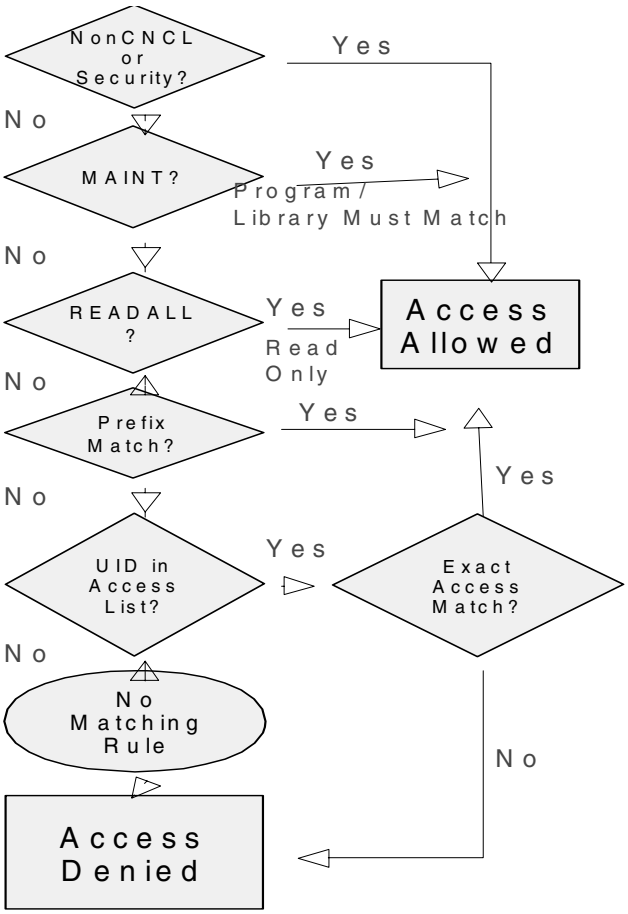


*Figure 17. CA-ACF2 Access Flow*

All CA-ACF2 data is stored in the CA-ACF2 database in a “compiled” format from a “source” format created by administrators having the appropriate authority. When converting, consider the use of a “de-compiled” listing of the database to be certain to get the current CA-ACF2 rule sets.

### 4.1.3 Interfaces to CA-ACF2

From a logical point of view, it may be convenient to consider that applications and subsystems pass data and requests to CA-ACF2 by means of an interface specific to each subsystem or application. Since CA-ACF2 modifies SAF and some resource managers, CA-ACF2 behaves differently than the 100% SAF-compliant RACF. Furthermore, due to architectural differences, the type of data passed as part of the CA-ACF2 request will differ from RACF.

For these reasons, most of the interfaces from an IBM subsystem to the CA-ACF2 security system use CA-ACF2 modules executed from standard exit points or CA-ACF2 *intercepts*. The best example of standard exit points creating an interface to CA-ACF2 is the JES subsystem. Both JES2 and JES3 on a CA-ACF2 system require several CA-ACF2 specific JES exits.

However, modules within an application may issue security requests through standard SAF macros such as `RACROUTE`. This means applications can issue SAF-compliant, or subsystem-related security commands without using CA-ACF2 proprietary calls.

When converting CA-ACF2 interfaces to standard RACF interfaces, do not forget to remove all CA-ACF2 modules from your libraries. Using the JES example, you need to check the JES initialization parameters for calls to the CA-ACF2 exits. To get a picture of the active CA-ACF2 exits, or intercepts, issue the following command (with the proper authority) from a TSO `READY` prompt:

```
ACF
SHOW All
END
```

You may wish to use the preceding command in a batch environment to produce a listing to edit. Use the `ACFBATCH` program as documented by the vendor.

**Note:** This does not show CA-ACF2 enabled interfaces within subsystems like JES or CICS.

## 4.2 CA-ACF2 environment

The CA-ACF2 environment is described in this section.

### 4.2.1 Global system options

Global system options (GSOs) are defined in GSO Records. Records are identified by a record identification or *recid*. GSO records contain exit names, performance options, system-wide default values, functional choices made by the installation, exceptions to standard processing, and so on. Some recids and their contents are:

| | |
|---|---|
| **`OPTS`** | for global values |
| **`PSWD`** | for password rules |
| **`TSO`** | for TSO LOGON default values |
| **`NJE`** | for job propagation and control between systems |
| **`BACKUP`** | time of day the database is to be backed up to a sequential file |

For more details on GSO options and how to list them refer to the vendor documentation.

## 4.2.2 Personnel

CA-ACF2 security administrators are needed to obtain information on how CA-ACF2 security is implemented in the installation that is to be converted. The following sections describe the personnel involved in the conversion project.

### 4.2.2.1 Security administrators

Authority to administer, update, delete, and add information to the CA-ACF2 database is given to a user by values set in the *privilege* section of the CA-ACF2 description (LOGONID record) of the user. The following administrative authorities must be considered in your conversion:

- SECURITY
- ACCOUNT
- AUDIT
- LEADER
- CONSULT

Authority granted to a user in the privilege section of the LOGONID record can be limited to a subset of users or resources. The SCPLIST parameter in the LOGONID record of the user points to the name of a CA-ACF2 SCOPE RECORD. This record contains a description of masks that limit privileged access to rules or records, as follows:

- DSN - a mask to restrict DATA SET RULE access
- LID - a mask to restrict LOGONID record access
- UID - a mask to restrict LOGONID record access
- INF - a mask to restrict administrative CA-ACF2 certain resource Types

These values (PRIVILEGE and SCOPE) are a part of the user description and must be considered as part of the migration project.

#### *CA-ACF2 security officer*

The security officer with the ACCOUNT and SECURITY privileges will be able to give you most of the information you need to convert the CA-ACF2 database into RACF commands.

#### *CA-ACF2 security auditor*

The auditor has the same duties in both the CA-ACF2 and RACF environments. The CA-ACF2 auditor can give you information on CA-ACF2 database contents and also on the reporting and auditing level needed.

### 4.2.2.2 OS/390 system programmers

These programmers will be responsible for all MVS/JES/TSO exits and user modifications. They are needed for maintaining libraries, modules, procedures, and parameters.

### 4.2.2.3 Storage administrators

Storage administrators frequently have unique privileges within an OS/390 environment. Frequently they have the Administrator authority within DFDSS.

Check for any unique privileges or LIDWORDS associated with the storage administrators.

#### 4.2.2.4 Product system programmers

These programmers will be responsible for converting and updating all product interfaces to CA-ACF2.

### 4.2.3 Rules

In CA-ACF2, a resource protection definition is called a *rule*. There are rules for data sets and rules for general resources.

An example of a data set rule is shown in the following figure.

```
ACF75052 ACCESS RULE INST STORED BY YAB ON 92/02/15-13:28
   $KEY(INST)
   $MODE(ABORT)
    PDF.MPANELS UID(WTSC) READ(A)
    PDF.MPANELS UID(WTSCS1) READ(A) WRITE(A) ALLOC(A) EXEC(A)
    PDF.MPANELS UID(*)
    - UID(WTSCS1S) READ(A) WRITE(A) ALLOC(A) EXEC(A)
    - UID(*)
```

*Figure 18. A CA-ACF2 data set rule*

Rule INST protects all data sets beginning with an HLQ of INST.

- Data set INST.PDF.MPANELS can be read by all LOGONIDs beginning with WTSC. READ(A) means read allowed. The 'A' could have been 'P' (PREVENT) or 'L' (LOG).
- Data set INST.PDF.MPANELS can be accessed without restrictions by all LOGONIDs beginning with WTSCS1.
- Data set INST.PDF.MPANELS cannot be accessed by any other users, no matter what the intended access is.
- The following "-" rules cover all other data sets which start with INST. The first "-" indicates WTSCS1S prefixed UIDs can access without restriction other INST data sets. The last "catch-all" rule prevents access to all other Logon IDs.

A general-resource rule is characterized by a rule TYPE code. For example:

```
$KEY(CTR1) TYPE(CKC)
 UID(WTSC) ALLOW
```

In this example, a resource named CTR1 is described. The resource TYPE code is CKC. This is the CA-ACF2 provided default value for CICS transaction resources. All users with UIDs beginning with WTSC can access transaction CTR1.

In the following example, a resource named IKJACCNT is protected. The resource type is TPR. This is the CA-ACF2 provided default value for TSO LOGON procedures. All users with UID strings beginning with WTSC can access LOGON procedure IKJACCNT. No other users can access IKJACCNT.

```
$KEY(IKJACCNT) TYPE(TPR)
 UID(WTSC) ALLOW
 UID(*) PREVENT
```

### 4.2.4 CA-ACF2 databases

The CA-ACF2 database consists of three separate databases.

- LOGONID record database

  This database consists of one entry, or LOGONID record, per user. Each LOGONID record includes various fields that define users. The main sections and their contents are:

  - IDENTIFICATION section

    This section contains the user's name and phone number. A field named *uid*, for User IDentification, is also in this section. The UID string provides a mask to use for authorization checking when accessing resources.

  - PRIVILEGES section

    This section describes authorization to access TSO and subsystems, as well as administrative or operative authorities. Also included are attributes for “reserved” users.

  - PASSWORD section

    Password usage statistics and password rules are mixed in this section.

  - TSO section

    This section provides information for LOGON default values, and therefore is useful for initializing the TSO Segment in the RACF database.

  - SUBSYSTEM sections

    These sections supply data for CICS, IMS, or IDMS

- ACCESS RULE database

  This database contains definitions (or access rule sets) for data set protection and access. One rule set exists for all data sets beginning with the same data set name. The data set name high-level qualifier often is used as the KEY of the rule set. The important parameters, or control word values, to consider during the conversion include:

  - $KEY

    This parameter defines an HLQ for all following rules. For example:

    ```
    $KEY(SYS1) ..........
    ```

    is the first parameter of the description of protection for all data sets whose names begin with SYS1.

  - Rule entries

    These define access to a particular set of data sets. For example:

    ```
    $KEY(SYS1)
     PROCLIB UID(WTSC) READ(A)
    ```

    Users like those described in matching the UID string “WTSC” will be allowed to access the SYS1.PROCLIB data set with read authority.

- INFOSTORAGE database

  This database contains definitions for all general resources other than data sets. Following is a table containing some common predefined CA-ACF2 general resource types.

*Table 1. CA-ACF2 predefined general resources*

| Resource type | Protected resource |
|---|---|
| CFC | CICS Files |
| CKC | CICS Transactions |
| CPC | CICS Programs |
| CTD | CICS Transient Data |
| CTS | CICS Temporary Storage |
| DAT | CA-IDMS Areas |
| IAG | IMS Application Group names |
| ITR | IMS Transactions |
| PSB | CICS DL/I PSBs |
| SSC | CA-IDMS Subschemas |
| TAC | Logon Account number (TSO) |
| TPR | Logon Procedure |

`TYPE` values given are those provided as default by CA-ACF2. Except for `TAC` and `TPR TYPE` values, an installation may change these values, or add new values. You should have an inventory of all `TYPEs` used in your installation.

### 4.2.5 Commands

For the conversion process, some subcommands of the CA-ACF2 ACF command are described below. They display information needed in the conversion to RACF. Commands and subcommands listed here are online commands from TSO READY. All the subcommands must be preceded by the ACF command, followed by the `SET` command, as follows:

```
ACF
SET fieldname
```

- Displaying LOGONIDs

```
SET LID
LIST logonid
LIST LIKE(-)
```

- Displaying data set rules information

```
SET RULE
LIST LIKE(-)
```

- Displaying resource rules information

```
SET RESOURCE(typ)
LIST LIKE(-)
```

## 4.3 CA-ACF2 subsystem interfaces

The interfaces discussed in this section provide CA-ACF2 access to OS/390 subsystems.

### 4.3.1 System Authorization Facility (SAF)

CA-ACF2 currently installs a CA-ACF2 modified front-end to the SAF interface. This is installed when the CA-ACF2 subsystem is initialized. Additionally, prior to IPL there are CA-ACF2 specific SAF modules installed in LPA that replace part of the standard SAF interface.

### 4.3.2 TSO logon

CA-ACF2 implements a logon interface for TSO through the logon pre-prompt exit, `IKJEFLD`. The CA-ACF2 logon interface will change the appearance and sequence of the TSO logon.

### 4.3.3 CICS

There is a separate CA-ACF2 product for CICS which must be installed and maintained. CA-ACF2 for CICS heavily modifies CICS and changes the CICS external security calls. Additionally, such controls as using CICS privileges to determine who can sign on to a particular CICS region are translated to RACF APPL resources. Since CA-ACF2 has heavily modified the standard CICS interface, obtaining the services of someone who is experienced in CICS, CA-ACF2 and RACF is prudent for a successful migration project.

### 4.3.4 IMS

Just as with CICS, CA-ACF2 has modified the standard IMS security interface. CA-ACF2 for IMS is a separate product which must be installed and maintained. A variety of IMS resources protecting transactions and commands need to be converted to applicable RACF resources. Additionally, the RACF APPL class will be the resource class used to protect access to the IMS region(s). In ACF2 this is the IMS privilege bit on the LID.

### 4.3.5 DB2

CA-ACF2/DB2 is a separate CA-ACF2 product which must be installed and maintained. The standard DB2 external security module has a standard interface to RACF which replaces the need for the separate security product.

### 4.3.6 JES

Both JES2 and JES3 have a number of CA-ACF2 centric exits which are delivered with the CA-ACF2 product. This results in differences within RJE, NJE and unique JCL cards such as //*LOGONID cards.

# Chapter 5. RACF migration project overview

This chapter is intended as a project management guide for a CA-ACF2 to RACF conversion. It was written to give you a starting point from which to create a security migration project plan that is appropriate for your environment.

The information presented here was gathered from several CA-ACF2 to RACF conversions. The project examples represent a typical, generic migration project converting only one CA-ACF2 database to RACF, with expected completion within three to six months. The actual time it will take you to complete your migration will probably differ, depending on the nature and complexity of your project.

There is no guarantee that, for any particular conversion, the information contained in this manual is either complete, accurate, or even appropriate. Any individual security migration usually has tasks associated with it that are unique and specific to that particular migration. However, there are also many tasks that are common to all security migrations. The purpose of this document is to describe those tasks, and let you decide whether the task is appropriate for your particular migration.

Some of the tasks in a security migration project involve determining how other products, such as CICS, IMS and DB2, interface with RACF or CA-ACF2. Whenever those tasks are discussed in this book, you are usually referred to the documentation of the other product. It would be difficult, if not impossible, to accurately maintain that kind of information in a manual of this type. Instead, this book concentrates on providing information not readily found in other sources, such as creating a security migration plan and giving you some practical guidelines for converting your CA-ACF2 database to an equivalent RACF database.

This chapter describes how to prepare for the migration project, build the project plan, and schedule the necessary resources. The need for assessing the current environment and suggested personnel skills are also discussed.

## 5.1 Preparing for the migration project plan

In order to build a good plan, you will have to review your CA-ACF2 database and supporting system environment for any security-related impacts. What you find will determine the number and types of people you need to find for the migration team. In addition, you must consider what type of education is needed, who would need it, and when it should be completed.

Your overall goal is to build as complete a migration plan as possible, using information from this book or other sources. The plan should identify all required tasks, who will do them, and when the tasks should be completed.

### 5.1.1 Review the current CA-ACF2 environment

The first step is to look at what security functions are implemented using the CA-ACF2 database. You will also need to decide how to convert the CA-ACF2 database, determine any impacts on the supporting system environment, and identify applications with security interfaces.

#### 5.1.1.1 Assess the current CA-ACF2 database

Some features in CA-ACF2 do not convert easily or on a one-to-one correspondence to RACF. This is due to the fact that CA-ACF2 and RACF are two separate, individual products.

Typically, this means you have to examine each vendor product (for example, OEM) implemented in your environment and determine what has to be done, if anything, for each product to work with RACF. In most cases, each vendor's product documentation will have published RACF installation instructions and these should be reviewed. Identify all vendor product features you are using that RACF does not have an equivalent function for, then determine alternative ways of providing the same protection using RACF functions. Also, you have to check your OS/390 base product code for any security-related usermods, accounting exits, JES2 exits, and so forth.

As you assess the CA-ACF2 database and uncover potential issues, ask whether a current business need still exists which caused the original implementation of the security feature. If a need still exists, a solution should be found for converting the feature to the RACF environment. Many solutions can be found using either procedural controls or automated solutions.

#### 5.1.1.2 Decide on how to convert the security database

You will have to create a RACF database that matches, as much as possible, your CA-ACF2 database. As part of this task, you have to write or obtain automated programs that can assist in converting the rules and parameters contained in the CA-ACF2 database to the appropriate RACF commands.

You have several choices here:

- You can buy or lease an existing product to assist with the migration.
- You can write your own conversion routines.
- You can "start from scratch", that is, instead of converting your current CA-ACF2 database, you build the RACF database with new definitions.

If you choose to convert your CA-ACF2 database, most likely you will have to write or obtain automated programs that can assist in database conversion. Typically, these programs or "tools" use the information in the CA-ACF2 database to create RACF commands. When these RACF commands execute, they load the appropriate security information into an empty RACF database.

Because of differences between the way CA-ACF2 and RACF protect resources, any database conversion will probably not be completely transparent. Therefore, it is very important that you ensure the RACF commands will implement the same, or better, access control integrity than the CA-ACF2 environment.

If you choose to write your own conversion programs, be aware that the programs may take several months to write. Keep in mind that they need to be ready before

the start of unit testing. In addition, you should do several RACF database loads during the development phase in order to ensure an adequate amount of testing.

If you choose to obtain the conversion programs from other sources, ensure that you will be able to customize these programs to fit your individual needs.

**Note:** It is very important that you understand the amount of work involved in converting your CA-ACF2 database. Several chapters of this book are devoted to this topic. You should review them thoroughly before making your decision.

#### 5.1.1.3 Analyze the current system environment

You will need to complete a comprehensive, detailed review of any products, programs, or interfaces that perform security functions. Depending on what is being done, you may have to modify program code or write program code or exits which would perform the function on behalf of a user's request.

To analyze your current system environment, start by listing all hardware and software products you have installed. Identify which ones have security interfaces, or may otherwise be affected by this conversion. (This research is similar to what you might do in preparation for a systems software upgrade, such as a ServerPac installation.)

For each product that has a security interface, determine how RACF can provide the same protection. Also determine the amount of work required to have the product work with RACF, instead of CA-ACF2.

#### 5.1.1.4 Preparing the RACF test system

A test system, similar in size and nature to one that might be used for an OS/390 software upgrade, has to be available for the migration project.

You need the RACF test system on a "dedicated" basis for about two to three months to complete this project in a timely and efficient manner. By a "dedicated" test system, we mean one that is available during the normal working day so that the project team can work on the environment during their normal day-to-day work schedule.

Typical test system requirements include:

- A SYSRES volume to install RACF
- DASD space for the RACF database
- DASD space for the applications to be tested under RACF

In some cases, because of system constraints, the only test system you can dedicate to the project may not be large enough to handle the testing of more than one application at a time. While this will allow you to do much RACF testing, you will eventually have to test RACF using a second, more comprehensive test system. You will probably not be able to dedicate this second test system to the project.

You have to install RACF typically on a test system that is separate from the CA-ACF2 production system. You will most likely not have to upgrade or install any product for the sole purpose of using RACF. However, some of the advanced functions of RACF may work only with the higher release levels of some products.

### 5.1.2 Personnel

A typical security migration project involves people with the following generic job descriptions. Most people working on migrations usually perform multiple duties throughout the project. As you determine which tasks need to be done, also determine how many people are needed to perform the tasks, in order to ensure a successful migration.

Figure 19 describes the organization that should be implemented prior to the beginning of a migration.

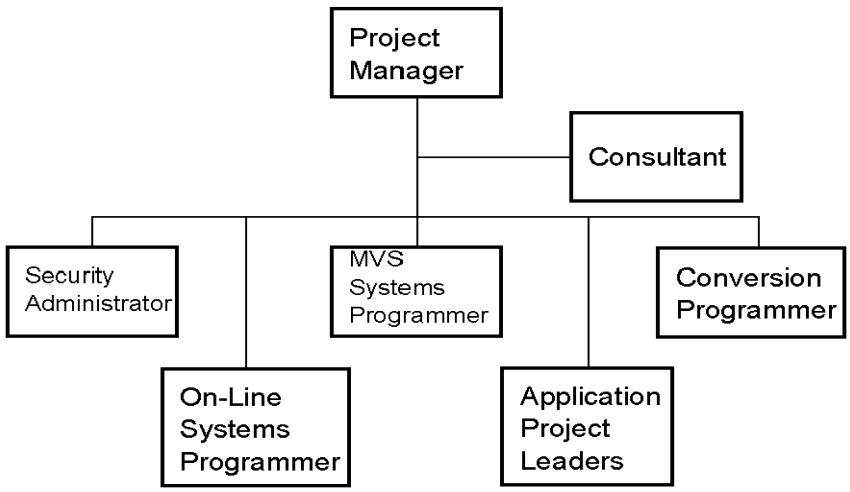


*Figure 19. Sample migration project organization*

#### 5.1.2.1 The security administrator

The security administrator is usually the most important and busiest person in a security migration. This person is the focal point for all questions related to what protection is currently in effect and why it was originally implemented. The administrator also determines the methodology and customization of the conversion programs that convert the CA-ACF2 database to RACF.

Frequently the administrator is also responsible for coordinating all testing, updating all security procedures, and educating end users in RACF. Because of the many responsibilities the administrator has regarding technical issues, this person is usually too busy to be the project manager.

A key factor to the success of any migration project is having a security administrator on the team who knows why past decisions were made and can provide guidance on whether current business needs exist for carrying functions into the RACF environment.

#### 5.1.2.2 The project manager

The project manager is primarily responsible for creating the migration plan, with the assistance of the migration team, and for monitoring the progress of the project. Since the migration team usually consists of people from several

departments, the project manager has to make sure everyone is committed to performing and completing the tasks he or she is responsible for throughout the project. This person is responsible for acquiring any additional personnel or systems support necessary to keep the project on schedule. The project manager may also assist the security administrator in his tasks.

#### 5.1.2.3 The conversion programmer

The conversion programmer is responsible for configuring the options of the conversion programs. This programmer coordinates resolution of database conversion issues and configures the conversion programs to properly represent the desired RACF result.

#### 5.1.2.4 The OS/390 systems programmer

The main responsibilities of the OS/390 systems programmer are to install and customize RACF, to create and maintain the test system to be used throughout the conversion, and to assist in the testing of RACF.

In some cases, the OS/390 systems programmer also installs and customizes the company's use of vendor (OEM) program products which use security interfaces. Vendor product documentation usually contains specific instructions on how to set up their product to use RACF.

#### 5.1.2.5 The online systems programmers

Online systems programmers are responsible for performing whatever work is necessary so that their subsystems work properly when RACF is installed. This typically means analyzing their current subsystem for interfaces to CA-ACF2, preparing the appropriate code and JCL to accomplish the same protection under RACF, and assisting in the RACF testing. Some examples of subsystems are TSO, IMS, CICS, DB2 or VTAM.

#### 5.1.2.6 The application project leaders

Application project leaders are responsible for verifying that they are the true owners of any resources (usually data sets) as identified through the CA-ACF2 database, and ensuring adequate testing of their applications. During the testing phase, they are responsible for determining that the security protection for their resources under RACF is acceptable, and that their applications function as well or better than they did with CA-ACF2.

### 5.1.3 Education

You need to determine who must receive RACF education before the project starts, when the education should be completed, and which classes should be attended. This education could include formal IBM-taught classes, self-study courses, or classes you may develop in-house for help desk or end-user training. You should schedule and attend RACF education for performing day-to-day administration prior to starting the migration project.

## 5.2 Building the migration project plan

This task simply means documenting all the tasks that have been identified, who is to do them, and when they are to be done. Once you have decided you *want* to convert to RACF, you then have to determine what methodologies to use in converting to RACF. You need to develop a detailed migration plan which identifies the tasks to be performed, who are the most qualified to complete the task, and a projected time frame. Remember to include items that are not pure tasks, such as educational needs and test system availability.

To create accurate estimates for the work involved in some of the migration tasks, analyze what it will take to complete that particular task. Remember, there can be multiple items to perform in order to finished the project tasks. Ask the same questions for any other significant software installed on the CA-ACF2 system. Following is an example of a potential project task.

You, as project manager, review the list of software installed on your system and see that CICS is one of the products installed. You ask the CICS systems programmer the following questions:

1. Are there any “non-standard” uses of security that would interfere with a migration to RACF?
2. How much work would be involved in converting the security for the CICS regions to RACF?

If the answer to the first question is yes, then that is identified as a potential migration issue. Also, the amount of overall work involved in converting CICS security to RACF, and who will do that work, is identified in the plan. You will not begin that work until you have determined that the issue identified in the first question will not cause a delay in the overall project.

In all cases, determine whether a current business need exists for the project task. If something was done in CA-ACF2 which does not need to be carried forward into the RACF environment, then this item does not need to be addressed.

Figure 20 on page 49 shows a typical migration project plan by phase lasting over 14 weeks. There are seven major phases to the migration project: assessment, education, project planning, development, unit testing, integration testing and production cutover.

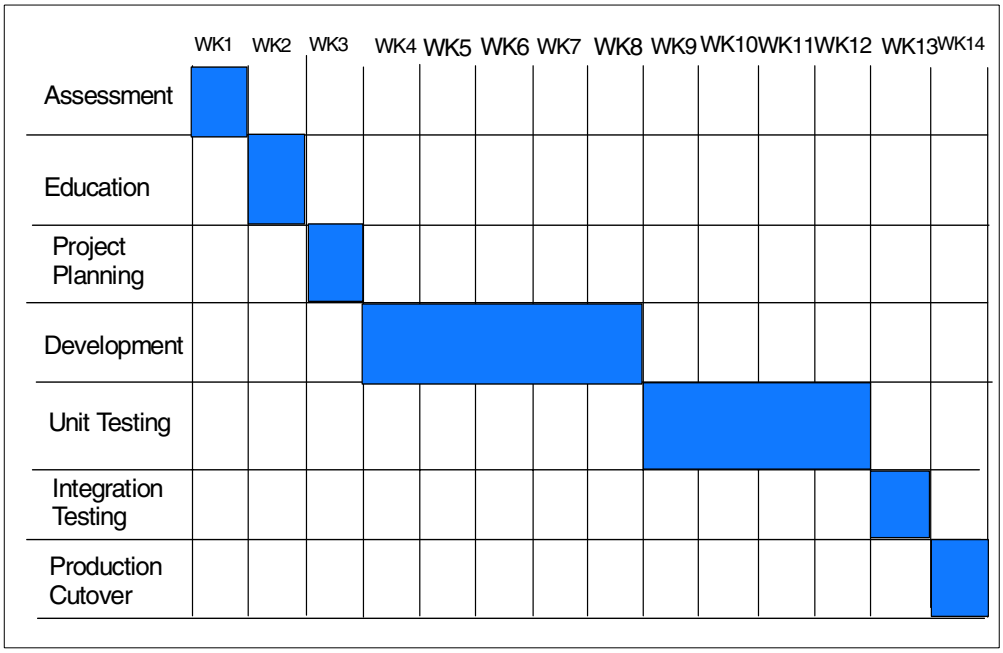


*Figure 20. Project planning phase items*

## 5.2.1 Significant project tasks

The following project tasks will be involved.

### 5.2.1.1 Analyze the current security environment

Examine the security database and system environment to identify which technical issues need to be addressed. This includes database features which do not have a direct RACF functional equivalent and any system exits or product interfaces which perform security functions. Review all issues against whether a current business need exists.

### 5.2.1.2 Project management

Throughout the project, you have to monitor and adjust the plan you created at the beginning of the project.

### 5.2.1.3 Planning

In this phase, a detailed project plan is developed for the remainder of the project. It lists who is to be involved, what other resources are needed, all the security interfaces currently in effect, and any issues that have to be resolved before proceeding to the next phase. Typical significant checkpoints would be the initial load of the RACF database, testing and migration cutover.

### 5.2.1.4 Identify project team

Identify the people who will complete the migration tasks identified in the project plan.

### 5.2.1.5 Identify major concerns or system changes

Review all conditions or situations that were identified as potential migration issues. Determine whether any of them are serious enough to warrant delaying the project until the condition or situation in question is resolved. Also, make sure

you coordinate with other projects in the company, such as software upgrades or hardware installations, that could interfere with the schedule for this project.

You have to identify anything that could be interpreted as a significant technical project issue. You need to identify any issue which would adversely affect the project timeframe. You want to avoid putting a lot of effort into the migration if a condition exists that will cause you to delay the project anyway. For example, if the necessary test system is not going to be available for several months, there is no need to have the online systems programmers preparing their products for RACF.

In many cases, you will need the support and approval of the end-user community before beginning this project. Often, the information from this phase is used to help obtain that support and approval.

#### 5.2.1.6 Install and customize RACF

You have to install RACF, typically on a test system apart from the production system that contains CA-ACF2. You also have to review the customizing options available, and determine what would be appropriate for your environment.

#### 5.2.1.7 Prepare the RACF test environment

In this phase, you prepare a RACF test environment that emulates the CA-ACF2 environment. All the security interfaces that exist in the current system are identified. Any code that has to be prepared to accomplish the same protection under RACF is prepared in this step.

#### 5.2.1.8 Install Conversion Programs

In this phase, install the conversion programs to be used to convert the CA-ACF2 to RACF. These programs should be customized based on your specific requirements.

#### 5.2.1.9 Review naming conventions

Naming conventions are important, because high-level qualifiers of data sets play a more important role in RACF than they do in CA-ACF2. RACF assigns ownership of data sets according to a high-level qualifier. Only one RACF group can “own” a high-level qualifier at any one time. For example, CA-ACF2 allows the use of generic characters for masking of high-level qualifiers, while RACF does not.

#### 5.2.1.10 Review security procedures

Identify all procedures that will change due to the migration to RACF. Typical procedures of this type include how help-desk personnel are to change passwords, or how operators and software automation products interact with RACF and OS/390 operations.

#### 5.2.1.11 RACF group structure planning

This is a very important part of the database conversion. You want to build a RACF group structure which is manageable, well-designed, and meets your specific needs. For example, there are certain CA-ACF2 logonid fields which provide security administrative functions and the migration team needs to decide how to provide similar functionality to the RACF community through centralized or distributed security administration procedures. Figure 21 on page 51 shows a sample RACF group structure.

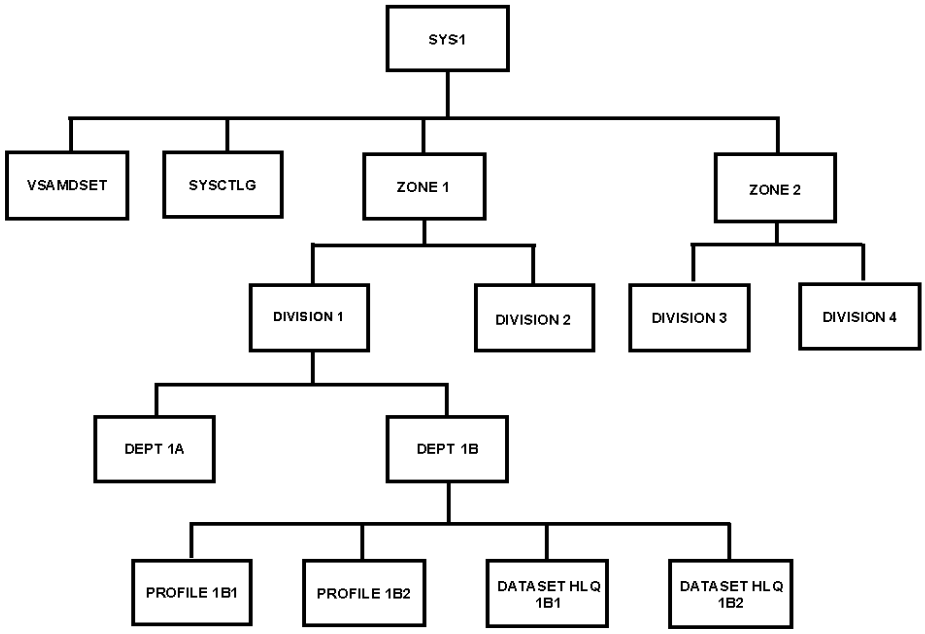


*Figure 21. Sample RACF group structure*

#### 5.2.1.12 Convert the security database

In this phase, you run your conversion programs to convert the CA-ACF2 database to RACF commands. Through repetitive executions of the tool against the CA-ACF2 database, you should be able to build a functionally equivalent RACF database. Final testing should verify the integrity of the user ID and resource profile definitions.

#### 5.2.1.13 Testing

A typical RACF testing sequence, or “cycle”, might be:

- Create a RACF database to match the CA-ACF2 database.
- IPL the test system with RACF.
- Execute the test plans.
- Review the results.
- Make any corrections to the conversion programs.
- Retest the system.

Several testing cycles are usually needed before your RACF environment is ready for testing against the full production system. This usually takes several weeks of effort.

***Unit testing***

Unit testing tasks concentrate on verifying the initial RACF database, system environment and selected important applications. You identify any differences between the old and new security environments, make any necessary corrections, and retest until you’re satisfied.

***Integration testing***
In this phase, you test your RACF environment against the full production system. You also target major applications within the company to verify their current functionality has not been adversely impacted. This is usually done on weekend "graveyard" shifts. If there are no major problems during this phase, you are ready to convert to RACF.

#### 5.2.1.14 Develop a backout plan

It would be prudent to develop a backout plan in case you need to back out RACF and return to the CA-ACF2 environment. The backout plan typically identifies all exits and interfaces that were replaced, how to reinstall them if necessary, and relinking to the CA-ACF2 databases. Each project team member responsible for implementing changes for the RACF migration needs to provide input into the overall backout plan.

Another option is to publish a set of items, or expectations, which would potentially trigger a backout. Some examples include inadequate testing of security functions and applications not converted to use RACF. These expectations should be communicated to all affected users prior to the cutover date.

#### 5.2.1.15 Preserve the CA-ACF2 databases

Prior to the cutover date, make copies of the CA-ACF2 security databases. Problem resolution will be critical during the days immediately following the cutover, and access to the previous security environment could help resolve user and system issues.

Once the migration to RACF has been completed, you may need to check user access problems against what the access was in CA-ACF2. Since you may not have the ability to log on to CA-ACF2, you must have the LIST(ACID) reports for all ACIDs available, or any other report used to diagnose and solve user access problems. These files and/or reports can be written to DASD files as part of the cutover process for easy accessibility.

You could also migrate CA-ACF2 to your test environment concurrent with the RACF production environment cutover. Then you could log on to CA-ACF2 to quickly resolve problems.

#### 5.2.1.16 Production Cutover

Before migrating RACF to production, you probably want to test RACF with the full production system, similar to the way you might test an OS/390 software upgrade before putting it into production.

Successful migrations freeze all changes to CA-ACF2 shortly before the cutover weekend. The conversion tool is run one last time and a final RACF database is built. All modified exits and interfaces are installed and passwords are synchronized.

## 5.3 Resource scheduling

You need to decide how and when to allocate your project team skills across the entire migration project. Table 2 on page 53 is a representative sample of the

typical resources needed by project phase and the level of effort required. Each of the six project skills has responsibilities in each project phase.

In this table, the Full-time or Part-time designation represents the allocation of time on the migration project *in relation to their overall job responsibilities.* For example, if the teammate can work 20 hours per week on the migration project, then a Full designation would mean 20 hours of migration level-of-effort.

*Table 2. Scheduling graph*

| Resource type | Assessment | Education | Planning | Development | Unit Testing | Integration Testing | Production Cut-over |
|---|---|---|---|---|---|---|---|
| Project manager | Full | Full | Full | Part | Part | Full | Full |
| Security administrator | Full | Full | Full | Part | Part | Full | Full |
| OS/390 systems programmer | Full | Full | Part | Full | Part | Full | Full |
| Conversion programmer | Full | Full | Part | Full | Part | Part | Part |
| Online systems programmer | Full | Part | Part | Full | Part | Full | Full |
| Application project leaders | Full | Part | Part | Part | Part | Full | Full |

## 5.4 Summary

In summary, the success of the migration project will depend on the quality of the project plan and the deployment of the right migration project team members with the right skill level at the right time. Here are some additional considerations.

***Management Involvement***
You need strong management commitment to undertake a major migration of any kind. Owners or managers of production applications, in particular, must be involved in testing phases. This is an additional task for these people, and there must be sufficient management commitment to force testing compliance on a reasonable schedule.

***Test System***
It is not practical to run both CA-ACF2 and RACF on the same OS/390 system. Likewise, it is not practical to undertake a migration to RACF without having a RACF system available for testing. In this case “testing” means a large range of testing, and this is not practical on any production system. Therefore, you need a RACF OS/390 system to use solely for test purposes.

In practice the test system is most likely to be a Logical Partition (LPAR) on a larger processor. With some care, the test OS/390 can share DASD with your production data, making testing much easier. Whether you clone your production OS/390 (removing CA-ACF2 and installing RACF), or install a new OS/390 (with RACF already integrated) is your choice. In either case, systems programming time is needed to install, make ready, and maintain the test OS/390 system.

### *Education*

You can obtain a reasonable overview and understanding of RACF by reading the RACF manuals. This is sufficient for many purposes. However, if you are the project manager, or intend to be the primary RACF specialist in the organization, you should arrange for formal RACF education.

### *Application Involvement*

A major goal of the migration project is to avoid disruption of production applications, and this can be accomplished only with sufficient testing. Major applications can be complex, with many jobs, files, procedures, and programs involved. Specific job and application knowledge is usually required to test these applications, and this means involvement by the application groups. They must help you test their applications in the new RACF environment.

### *Manpower and timing considerations*

For a security subsystem to be effective, it must be very tightly tied into the heart of the operating system. Given this, it is quite difficult to make a major change in the security subsystem without impacting system production. A large, production OS/390 installation has many complex jobs. Some of these are rarely used, such as year-end jobs or obscure recovery jobs.

The bulk migration of basic CA-ACF2 user records and resource rule records can be automated. However, testing the results of this conversion, and discovering/migrating all the special cases that exist, *without disrupting production*, is another matter altogether. Nevertheless, this is the requirement for almost all CA-ACF2 to RACF migrations. It is these practical considerations that dictate the timeframe and manpower needed for migration.

No single plan can apply to all situations. However, a timeframe of three to six months, with one full-time person and several part-time people working on the project, is typical.

# Chapter 6. Database migration

This chapter describes the process of the actual database migration of CA-ACF2 to IBM's RACF. It provides guidance on how to convert a certain CA-ACF2 function to the equivalent function in ACF.

## 6.1 Conversion methodology

This chapter discusses some of the issues and approaches that can be used when converting your CA-ACF2 database to RACF. RACF, like CA-ACF2, offers a number of ways to implement security policies and procedures. Experience has shown that some approaches work better than others. This chapter provides a number of recommendations for designing and implementing a conversion methodology from CA-ACF2 to RACF.

### 6.1.1 Migration considerations

The migration from CA-ACF2 to RACF involves more than a conversion of database records. Some of the key elements are discussed in this chapter. We must first note that this is an excellent time (just before your migration) to review, rethink, and polish your security policy. A clear vision of what you want to produce will help the migration work, and provide better results. Some of the key elements to a migration project are discussed in Chapter 5., "RACF migration project overview" on page 43. Before you begin the conversion, you must have a plan that includes:

- Management involvement
- Test system
- Education
- Application involvement
- Manpower and timing

One of the lasting aphorisms of the data processing business is "Garbage In -Garbage Out," commonly known as GIGO. While it is a complex, one-time activity, migrating a security database from one product to another is a data processing function, especially when an automated tool is used to help perform part of the work. A fairly clean input database at the beginning of the migration will help produce a higher quality result. There is no magic in the migration process or tools that will automatically clean up substantial problems in the initial database.

Unless meticulously maintained, a security database tends to accumulate a certain amount of unwanted or erroneous entries over time. There are a number of causes: changing security administrators, changing philosophy of security management, former users who still own resources, and so forth. You have several choices for handling these problems:

- Make a reasonable effort to clean up your original database, before starting the migration process.
- Migrate whatever is in your original database, and clean up the resulting RACF database.

- Ignore the problems, and accept whatever appears in the final RACF database.

The first choice is usually the best one. You understand your CA-ACF2 database, and have the skill to review it. While reviewing and correcting a large security database is not an enjoyable task, it will certainly reduce future problems. Some migration tools may help you clean up your database; see Appendix A, “IBM migration services” on page 113 for an example.

Schedule pressures may push you toward the second choice. The problem with this approach, cleanup after migration, is that the migration process may amplify the problems in the original database. The conversion of a CA-ACF2 database to a RACF database is not a simple, one-to-one process. Small anomalies in the input, easily corrected there if someone would take the time to do it, might create large unwanted structures in the output.

A pre-migration review process should consider (and correct) obvious errors in the database. It should also consider design and philosophical changes that will produce a better database after migration. Again, small changes here may make the migration much easier, and produce a better result. Examples of such changes are the elimination of global flags that are not really needed, or removing SCOPE controls that are outdated.

In practice, of course, you are likely to use all three choices: some clean up of the original database, some clean up of the RACF database, and then go into production with the resulting database.

## 6.2 Converting users

This section details the conversion of CA-ACF2 Logon IDs to RACF User IDs.

### 6.2.1 CA-ACF2 user migration considerations

Migrating the basic user from CA-ACF2 to RACF isn't necessarily a complex task. What may become more complicated is the migration of some user privilege attributes. Some of these privileges can be carried across into RACF while there are a few that will require careful planning and possibly an exit. We have tried to keep this section focused on some fairly common areas. We have noted where RACF does not have a native corresponding function.

An essential piece of the conversion process is the selection of a RACF administrative group structure based on the UID string from the CA-ACF2 database. This RACF structure should allow for user administration and user access authorization.

The conversion process is shown pictorially in Figure 22.

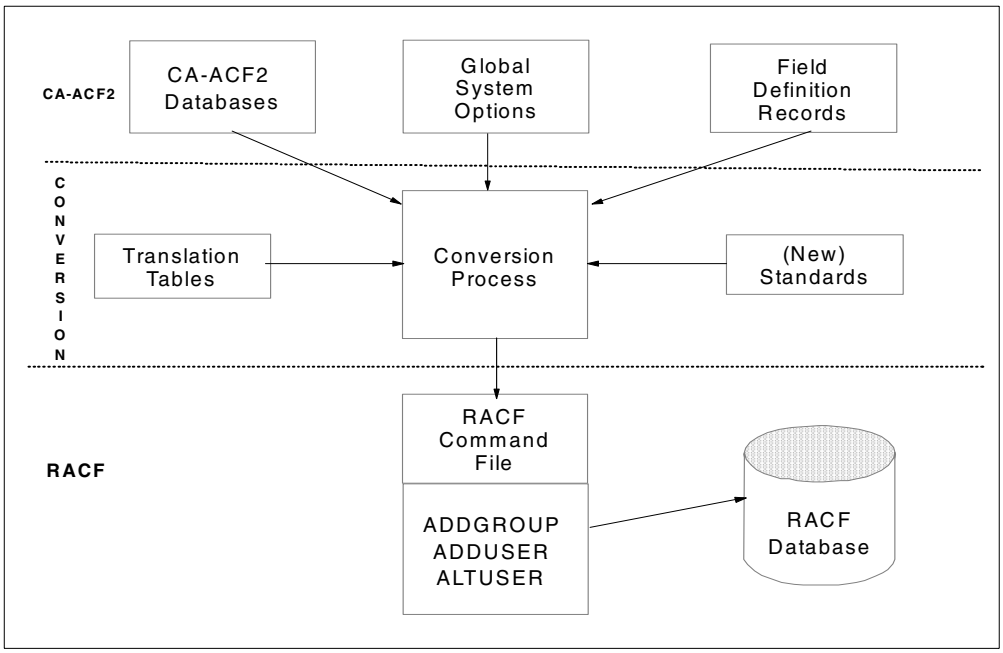


*Figure 22. Security database conversion process*

The flow of user conversion may be:

1. Design and define a set of new naming standards for the RACF database.
2. Design and define the RACF group structure.
3. Run a CA-ACF2 Report against the Logon ID (LID) database, which lists all Logon IDs into a data set.
4. Use the output from the report as an input to the conversion process.
5. Output from the conversion process is a set of RACF commands written to a data set. These commands define group profiles and user profiles, as well as user-to-group connections.

### 6.2.2 Translation of CA-ACF2 UIDs

Each user is defined to CA-ACF2 by a unique Logon ID and Logon ID record. This Logon ID (LID) record is used for user verification and resource access validation. A password is often used to verify the authenticity of the user.

Figure 23 is an example of a Logon ID record.

```
C046870              B05D12F1C046870    JOE USER 555-888-8034
                     BRANCH(B05) FUNCTION(F1) DEPARMENT(D12)
 PRIVILEGES          CICS CICSPRD JOB TSO
 ACCESS              ACC-CNT(159) ACC-DATE(05/31/00) ACC-SRCE(LUTERM01)
                     ACC-TIME(11:03)
 PASSWORD            MAXDAYS(30) MINDAYS(7) PSWD-DAT(00/00/00) PSWD-INV(3)
                     PSWD-TOD(05/19/00-04:56) PSWD-VIO(0) PSWD-DAT(08/25/99)
                     PSWD-INV(3) PSWD-SRC(LUTERM01) PSWD-TIM(08:33)
 TSO                 DFT-PFX(C046870) DFT-SOUT(X) INTERCOM JCL LGN-ACCT
                     LGN-MSG LGN-PROC LGN-RCVR MAIL NOTICES PROMPT
                     TSOACCT(ACCT#33) TSOFSCRN TSOPROC(@TSOPROD)
                     TSOSIZE(4,096) TSOUNIT(SYSDA) WTP TSORBA(000072)
 STATISTICS          SEC-VIO(0) UPD-TOD(05/31/00-00:33)
 CICS                CICSCL(000001) CICSID(HWQ) CICSKEY(000007) CICSPRI(1)
                     IDLE(30)
 RESTRICTIONS        PREFIX(C046870)
```

*Figure 23. Logon ID record content*

The CA-ACF2 Logon ID record fields are installation-defined by the CA-ACF2 Field Definition Record (FDR). These fields define:

- The Logon ID (LID)
- The user name
- User privileges
- User system access history
- Other product-related (i.e. CICS, IMS, TSO and vendor) information (optional)
- Other CA-ACF2 system related information
- Other user-defined information (optional)

The user identification (UID) used by CA-ACF2 is a 1 to 24 byte character string made from some of the above selected fields. Field selection and the order of concatenation are determined by the CA-ACF2 FDR.

The UID contains more than a user ID. For example, in Figure 24 on page 59, we can see how a very basic UID could be expanded into a RACF user ID with equivalent RACF GROUP connections.

- BRANCH is the first UID field; length is three characters
- DEPARTMENT is the second UID field; length is three characters
- FUNCTION is the third UID field; length is two characters
- Logon ID is the fourth UID field; length is one to eight characters

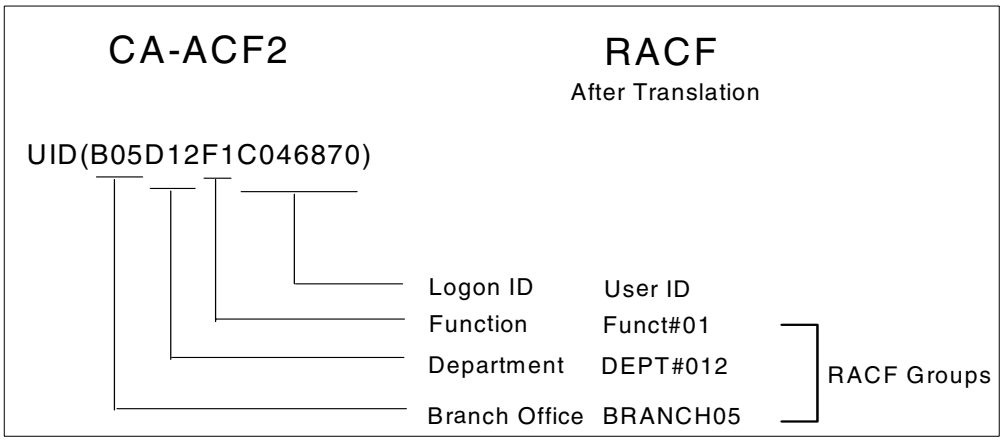


*Figure 24. Possible CA-ACF2 Logon ID Conversion to Groups and User ID*

A sequence of activities for the first stage of the conversion process is:

1. Create a central RACF group for administration, and optional groups for decentralized user administration.
2. For each existing combination of unique CA-ACF2 UID field values, define corresponding RACF group names.
3. For each RACF group name, generate an `ADDGROUP` command.
4. For each Logon ID having the same UID field values, generate a RACF `ADDUSER` command defining the user, with one of the groups just created as the default and owning group.
5. If the user needs access to resources based on the Branch Office and Function, create the appropriate groups and connect the user to them.

For example:

1. Assume the translation rules developed for CA-ACF2 UID to a RACF grouping conversion have users being defined to RACF groups by Branch and Department.
2. Therefore, a possible RACF group name from the UID string `B05D12` from the previous example is `DEPT#012`. The `ADDGROUP` command is:

   ```
   ADDGROUP DEPT#012 SUPGROUP(USERADM) OWNER(USERADM)
   ```

3. The CA-ACF2 Logon ID from our previous example is `C046870`. The `ADDUSER` command is:

   ```
   ADDUSER C046870 DFLTGRP(DEPT#012) OWNER(DEPT#012).....
   ```

4. Connect the user to the groups it needs access to. The example commands below assume the groups have been previously created.

   ```
   CONNECT (C046870 ) GROUP(BRANCH05) OWNER(BRANCH05)
   CONNECT (C046870 ) GROUP(FUNCT#01) OWNER(FUNCT#01)
   ```

To provide a complete translation of CA-ACF2 UIDs into RACF group names, translation rules must accommodate:

- Blank fields within UID strings.
- Fields within the UID string that are to be part of the RACF group name must contain the letters (A-Z), numbers (0-9), or # (X'7B'), $ (X'5B'), or @ (X'7C').

- No two groups can have the same name. No group name can be the same as a user ID.

Other suggestions for user conversion include:

- Make the rules for translating CA-ACF2 UID strings to RACF group names meaningful to your site's naming conventions and standards.
- Do not be esoteric!
- Have consistent, easy-to-read, RACF group names that one can easily understand.

### 6.2.3 Adding additional fields in the RACF user profile

We now consider other fields in the CA-ACF2 Logon ID record that can be converted into the RACF user profile either with an ADDUSER command, or, after the ADDUSER command has been executed, by an ALTUSER command for the same user. Some of these additional fields are:

- NAME and PHONE

  The NAME field of the CA-ACF2 Logon ID record contains the name of the user. The PHONE field contains the telephone number of the user. As RACF provides a NAME parameter in the ADDUSER command, the conversion process can translate the name value from CA-ACF2 to RACF. The CA-ACF2 PHONE field may be entered using the DATA parameter of the ADDUSER command. Some examples are shown below:

  CA-ACF2 Logon ID record information:

  ```
  A70665D         B07D10 A70665D      W.R.SOMEBODY (914) 432-4142
  ```

  RACF ADDUSER command:

  ```
  ADDUSER A70665D DFLTGRP(DEPT#010) NAME('W.R.SOMEBODY')
  ```

  CA-ACF2 Logon ID record information:

  ```
  A70665D         B07D10 A70665D      WILLIAM SOMEBODY  (914) 432-4142
  ```

  RACF ADDUSER command:

  ```
  ADDUSER A70665D DFLTGRP(DEPT#010) NAME('WILLIAM SOMEBODY') -
                 DATA('(914) 432-4142')
  ```

- CANCEL or SUSPEND

  The CANCEL or SUSPEND attribute indicates a Logon ID that cannot be used to access the system. The RACF attribute REVOKE (without date) should be the translation used for the CANCEL/SUSPEND attributes. Early in the conversion process, begin the search for cancelled or suspended users. Evaluation of the status of the user in question should be made by looking at the CA-ACF2 CSDATE value. For example:

  ```
  A0018               B04D44F5A0018     SOMEBODY
  CANCEL/SUSPEND      CSDATE(10/17/88) ......... SUSPEND  .....
     .......          ............................
  RESTRICTIONS        PREFIX(A0018)
  ```

  User A0018 has been suspended since October 17th, 1988. Review why such Logon IDs have been cancelled or suspended to determine whether these IDs should be converted to RACF.

- SHIFT

The SHIFT record defines the allowable system access periods for this specific CA-ACF2 Logon ID. A translation of this field can be made with the RACF user profile WHEN field. An ALTUSER command is used to implement this translation. For example, for CA-ACF2 Logon ID record information:

```
A70665D B06D45F8A70665D      W.R.SOMEBODY        4142
  .......          ..................
RESTRICTIONS    PREFIX(A70665D) SHIFT(HH2)
```

and HH2 SHIFT record information:

```
 SHIFT HH2 .......
  DAYS(MO,TU,WE,TH,FR) TIME(0830-1730) .......
```

the corresponding RACF ALTUSER command would be:

```
ALTUSER A70665D  WHEN(DAYS(WEEKDAYS) TIME(0830:1730))
```

- PASSWORD

  CA-ACF2 user passwords are encrypted and stored in the CA-ACF2 data base. The encryption algorithm has been DES since CA-ACF2 Release 5. For the conversion process, you may implement one of the following:

  - A routine that assigns each user a unique and randomized password. You then have to communicate that password to the proper user and include it in the proper ADDUSER or ALTUSER command.
  - A set of routines to extract passwords from the CA-ACF2 database and to transfer them to the RACF database. This can be difficult, but it eliminates the need to communicate new passwords to users.

  If transparency to end users is a key point in the conversion project, the second option should be considered.

- STATISTICS and HISTORY

  In the conversion process, you may want to keep track of previous facts recorded for a user in the CA-ACF2 Logon ID record. The RACF DATA field, whose length is up to 255 characters, can contain a copy of selected fields from CA-ACF2. Creation date of the Logon ID record or any other requested data can be copied.

### 6.2.4 Converting CA-ACF2 user privileges

In a sense, CA-ACF2 has two sets of privilege groups: those that operate on records within the CA-ACF2 database and are subject to SCOPE records, and those that grant operational accesses not related to changing database records and are not subject to SCOPE records.

RACF privileges are easy to identify, understand, and administer, but they are not as granular as CA-ACF2 privileges. Conversely, the CA-ACF2 privileges allow more granular control of authority, but have more complex interactions and may require more administrative effort. This section discusses the privileges we consider most important for user conversion.

CA-ACF2 user privileges can be classified as:

- Privileges similar to some RACF attributes at the system or group level (for example, NON-CNCL, SECURITY).
- Application access authorizations (for example: CICSPRD and TSO in Figure 23 on page 58).

- Resource access authorization (for example: BLP).
- Others (for example: DUMPAUTH, JOB).

#### 6.2.4.1 Scoped CA-ACF2 privileges

There are many CA-ACF2 user privileges that can be assigned to users; where possible, we have tried to simplify them and break them down into a RACF function. This section discusses the privileges we consider most important for user conversion.

In CA-ACF2 you can restrict user privileges by using SCOPE records. This is similar to RACF group-related user attributes.

In RACF, users who have the group-SPECIAL, group-AUDITOR, or group-OPERATIONS attributes are restricted to only profiles that are within the scope of their groups. Table 3 lists the RACF translations of CA-ACF2 privileges that can be scoped. (This table does not imply that the listed CA-ACF2 and RACF privileges are one-to-one translations to each other. They are not, but with the proper creation of the RACF Group Tree, and if the appropriate RACF attributes are given to administrators, they will allow the same functional administration in RACF.)

*Table 3.* CA-ACF2 user privileges

| CA-ACF2 | RACF | RACF Description |
|---|---|---|
| ACCOUNT and SECURITY | SPECIAL OPERATIONS | Full control over ALL of the RACF database and access to most resources. |
| ACCOUNT | group-SPECIAL or SPECIAL | Allows a user to list, alter, and define other user profiles in that group structure. |
| SECURITY | group-SPECIAL or SPECIAL and /or group-OPERATIONS or OPERATIONS | Allows a user to list, alter and define other user profiles in that group structure. Operations will allow access to data sets. |
| CONSULT | AUDITOR at a group level | A RACF user may display his user profile. He is not allowed to modify or delete it unless he is the owner. |
| AUDIT | AUDITOR | AUDITOR allows display of all RACF profiles and monitoring of all RACF related activities. |

Table 4 is a summary of the scoped Logon ID privileges which can be mapped into RACF user and group attributes.

*Table 4.* CA-ACF2 scope records mapping to RACF attributes table

| Scope field | Security | Account | Audit |
|---|---|---|---|
| LID and UID | group-SPECIAL and/or group-OPERATIONS | group-SPECIAL | group-AUDITOR |
| DSN | group-SPECIAL group-OPERATIONS | group-SPECIAL | group-AUDITOR |

The SECURITY- or ACCOUNT-privileged Logon IDs will receive more authority after the SCOPE record migration is completed according to Table 4. An ACCOUNT-privileged Logon ID receives extended authority for data set management, even though it previously had authority only to create matching Logon IDs in the CA-ACF2 environment. The same is true for a user with the SECURITY privilege with “LID()” or “UID()” specified. This will allow the user to manage any data sets owned by the groups that the user is connected to.

#### 6.2.4.2 Non-scoped CA-ACF2 privileges

The following privileges are not covered by SCOPE but can be compared to RACF functions.

***RESTRICT privilege***

A CA-ACF2 Logon ID with the RESTRICT privilege may be specified on a JCL JOB statement as a value for the keyword USER without specifying a PASSWORD. The CA-ACF2 Logon ID with the RESTRICT privilege cannot be used for LOGON or SIGNON purpose.

A CA-ACF2 Logon ID with the RESTRICT privilege can be specified in JCL as an extended JCL statement (beginning columns are //* or /*). CA-ACF2 provides JES exits to handle this JCL statement.

To convert the CA-ACF2 Logon ID RESTRICT privilege to the RACF equivalent, you might:

- Disallow terminal access for the user ID, and/or limit logon by making the ID a RACF protected user ID.
- Allow SURROGATE job submission for the user ID.

Access to resources for CA-ACF2 Logon IDs with the RESTRICT privilege is given at the user level rather than the group level. An inventory of all users or applications authorized to use CA-ACF2 Logon IDs with the RESTRICT privilege should be made, and these users or applications can be authorized to use the proper RACF protected user IDs.

***NON-CNCL privilege***
CA-ACF2 Logon IDs with the NON-CNCL privilege have full access to all data sets and resources, but are logged if they are not on the access list. No access restrictions can be assigned to this user.

For data set access in RACF this could translate to a RACF user ID with the OPERATIONS attribute. Access to resources allowed with the OPERATIONS attribute should be logged.

### 6.2.5 Other CA-ACF2 LID fields

The previous conversion methodologies for fields within the CA-ACF2 LID record are some of the major methodologies one needs to consider for each of the fields in use in the CA-ACF2 LID database. Additional information that is needed from the CA-ACF2 LID records will need a conversion methodology designed to convert those CA-ACF2 LID fields and user-defined LID fields to RACF where applicable.

## 6.3 Converting data set protection

Data set protection, along with user authentication, is the most basic function of RACF and CA-ACF2. Data set protection is usually the primary reason for implementing an OS/390 security product, and most if not all installations protect data sets before using other CA-ACF2 or RACF functions.

The quality of protection that is achievable depends on product functions as well as on installation-specific parameters such as naming standards. In our assessment, the data set protection functions of CA-ACF2 and RACF are largely equivalent, and we believe that the installation standards are the key factors determining the resulting protection of data sets. Access rules in CA-ACF2 and access lists in RACF can become long and complex unless well-defined naming conventions for users, groups, and data sets are established, and group structures are clearly defined.

### 6.3.1 Goals

The goal of any implementation or conversion should be default protection, appropriately restricted public access, and specific access defined according to the principle of least necessary privilege. In addition, the administration of access authorities should be easy and create little overhead. Access should be given to groups, and not specific users, whenever feasible and practical.

### 6.3.2 Control issues

Key control issues for data set protection are:

- The security system may not be called to control access to data sets due to privileges set for started procedures or the PPT NOPASS privilege allowed to some programs.
- Unprotected data sets may exist. Access to unprotected data sets is prevented only if default protection is implemented ($MODE ABORT in CA-ACF2 and PROTECTALL FAIL in RACF).
- Public access may be inadequate. A temptation exists in all security environments to grant high levels of public access to data sets in order to

"simplify" administration. This is done in CA-ACF2 rules through UID(*) entries and in RACF through UACC or ID(*) specifications.

- Excessive user privileges may bypass many rules. All security systems offer user privileges that bypass normal rule checking. The CA-ACF2 NONCNCL and READALL privileges and the RACF OPERATIONS attribute fall into this category.
- Specific access may not be in line with policy. Access rules may not exactly reflect policy for two main reasons: policy may require a more granular control than technically possible, or policy may change over time while access rules do not.
- Data set protection rules may be difficult to understand or audit. This is often the case in CA-ACF2 when the $NOSORT option is used; in RACF an incorrect use of Global Access Table entries may contribute to such confusion.
- Application integrity may require program pathing. The nature of an application such as payroll may require a need for eliminating access to files through other than certified application programs; for example, TSO EDIT access may not be acceptable.

While all these issues exist in both environments, a migration from CA-ACF2 to RACF is probably a good time to revise some of these controls.

### 6.3.3 Security interface

CA-ACF2 can set intercept points (modifications) in key OS/390 routines, or use the SAF interface. The general use of SAF is a fairly recent CA-ACF2 feature, and many CA-ACF2 installations use the intercept implementation. In this case, when CA-ACF2 is installed, intercept points are inserted in all the DADSM functions, so that CA-ACF2 will be called each time a data set is accessed.

When SAF is used, the ALWAYS CALL function of DFP will cause a RACROUTE call when a data set is accessed, except for programs that have the PPT NOPASS privilege.

### 6.3.4 Protection modes

Both products can be set to enforce default data set protection, meaning denial of access to data sets not covered by a CA-ACF2 rule or a RACF profile. When no CA-ACF2 rule is found for a data set, the GSO MODE option or the RULE $MODE option will decide what will happen. If the $MODE is set to ABORT, the data set must have a matching rule set, otherwise access is denied. If the global RACF option PROTECTALL(FAILURES) is set, RACF will require a matching profile for all accessed data sets. Without a profile match, access will be denied. So CA-ACF2's $MODE=ABORT and RACF's PROTECTALL(FAILURES) will both require all data sets to be protected.

CA-ACF2's $MODE can have these setting: QUIET, LOG, WARN, RULE and ABORT. RACF PROTECTALL can have these settings: not specified, WARNING and FAILURES.

- Not specified can be compared to RULE mode. If a profile exists, grant access accordingly. In RACF, if no profile is found, the data set is *unprotected*.
- WARNING or WARN has approximately the same function in both products. Check access rules, but always grant access and report any violations to SMF.
- FAILURES is the same as ABORT.

- CA-ACF2' s QUIET is the same as having no profiles defined and all data sets are UNPROTECTED.
- The CA-ACF2 LOG mode could, theoretically, be replaced by RACF AUDIT(ALL), but this may not be a practical solution.

***RACF profiles***

Consider the following CA-ACF2 access rule set:

```
$KEY(SYS2)
$MODE(ABORT)
PARM***.PARMS UID(ITSO) READ(A) EXEC(A)
PARMLIB.- UID(ITSOKM1234) READ(A) WRITE(L) ALLOC(L) EXEC(A)
IMS.RESLIB UID(*) READ(A) EXEC(A)
- UID(*)
```

For RACF this could be converted as follows:

1. SYS2 would most likely be a group ID. It is also a high level qualifier for data sets. SYS2 should also be the OWNER of all SYS2.something data sets.
2. The CA-ACF2 generic data set name PARM***.PARMS would convert to a RACF generic profile of SYS2.PARM*.PARMS. In CA-ACF2, "UID(ITSO-) READ(A))" permits all users whose UID begins with the characters "ITSO" to have READ access to the indicated data sets. In RACF, we would create a group that is given READ access to the profile for these data sets, and then connect all appropriate users to this group.
3. PARMLIB.- would be SYS2.PARMLIB.** with ID(KM1234) ACCESS(ALTER) AUDIT(SUCCESS(UPDATE)) OWNER(SYS2) GENERIC
4. IMS.RESLIB would be SYS2.IMS.RESLIB with ID(*) ACCESS(READ) OWNER(SYS2) GENERIC. A fully qualified generic profile.

   It could have been a discrete profile if generic was not specified. Discrete means it covers only this specific data set on this specific volume/unit combination and the DSCB protect flag is set. Creating discrete profiles is not recommended since most sites use SMS and coding specific volumes is not a recommended implementation when using SMS.
5. - UID(*) would be SYS2.** UACC(NONE) OWNER(SYS2) which allows no further access to data sets under SYS2.

### 6.3.5 Protection by volume

Through the GSO option SECVOLS, users in CA-ACF2 can be granted access to data sets at the volume level. The access specified for the volume applies to all the data sets it contains. There is no equivalent facility in RACF, so these CA-ACF2 rules must be converted to regular RACF data set profiles[1]. A common misunderstanding exists with regard to the RACF DASDVOL class. Although the name may suggest it, this class does not provide general volume level access nor allocation control. The RACF DASDVOL class is only used by programs that perform DASD management functions, like DF/DSS.

### 6.3.6 Program Pathing

Both products can control access to data sets through *program pathing* (CA-ACF2) or *Program Access to Data Sets* - PADS (RACF). CA-ACF2 does it through the data set rule by using the LIB and PGM control options.

[1] By using exit programming, RACF can provide access control at the volume level.

RACF uses the PROGRAM class to define the controlled programs and libraries. On the data set profile the additional statement `WHEN(PROGRAM(xxx))` results in a Conditional Access List which is used to restrict access only through this program.

The following must be observed:

- In the PROGRAM class, both the library name and program name need to be specified.
- Any aliases of the program being defined must also be included in the PROGRAM class profile.
- In addition, the PROGRAM class profile can specify `PADCHK` or `NOPADCHK` (`PADCHK` is the default). `PADCHK` adds the following additional requirements:
  - all programs represented by the opening task's PRBs, and
  - all programs that link to, load or call the program that opens the data set must be controlled in class PROGRAM.
- `PADCHK` may be difficult to establish and maintain and is therefore rarely used.

### 6.3.7 Erase-On-Scratch (EOS)

Erase-On-Scratch (EOS) should be used for confidential data to ensure that residual data cannot be accessed after deletion. Residual data is a potential security exposure for confidential data. In CA-ACF2 it is done on a volume level based on the `GSO AUTOERAS` option. In RACF it can be done on a data set level and as such can be very selective, and used without causing potential performance problems.

### 6.3.8 data set conversion methodology

The conversion methodology for data sets is:

- Start with `PROTECTALL(WARNING)` mode to enable corrections in the setup and adjustments in the access lists, but always target `PROTECTALL(FAILURES)` as the option for the production cut-over to RACF. It only affects data set protection on DASD (and TAPE data sets if the `TAPEDSN` option is active). Other resource classes are not impacted.
- Use group IDs as data set high-level qualifiers as much as possible, except for typical TSO user data sets.
- Establish `UACC(NONE)` as a basic rule for all profiles, but allow for exceptions when and where necessary.
- Use group IDs as the owners of user ID profiles whenever possible.

To simplify administration, use generic profiles whenever reasonable. When one generic profile can cover many data sets, this will also improve system performance. However, using too many *fully-qualified* generic profiles can hurt both performance and administration.

- Try to stay with group IDs for access administration, to keep access lists shorter and easier to handle. User IDs on the access list should be an exception.

### 6.3.9 Converting CA-ACF2 data set access rules

The following sections discuss the use of CA-ACF2 access rules and how to convert these to RACF data set profiles. Figure 25 shows the syntax of a typical CA-ACF2 Access Ruleset Entry (ARE).

```
$KEY( )
$MODE( )
$PREFIX()
$USERDATA( )
dsn-mask
UID( )
READ( ) WRITE( ) ALLOC( ) EXEC( ) DATA( )
UNTIL( )/FOR( )
PGM/PROG( ) LIB( )
VOL( )
DDN( ) SOURCE( ) SHIFT( )
NEXTKEY( )
```

*Figure 25. CA-ACF2 rule set*

### 6.3.10 Converting CA-ACF2 data set $KEY and $PREFIX values

The $KEY control card supplies the high-level index of the data set name that this rule is to protect.

During access validation, the $KEY value is used as the prefix unless the $PREFIX control card is specified in the rule set. The $PREFIX control card shows the value that overrides the rule set's $KEY as a prefix to all data set names in the rule set.

Table 5 provides a comparison of the $KEY and $PREFIX control cards used in CA-ACF2 rule sets and their equivalent functions in RACF data set profiles. It is assumed that the RACF EGN option is in effect.

*Table 5. CA-ACF2 $KEY and $PREFIX control cards with RACF equivalents*

| CA-ACF2 $KEY and $PREFIX control cards | RACF data set profile name |
|---|---|
| $KEY(SYS1)<br>PROCLIB | SYS1.PROCLIB (discrete or generic) |
| $KEY(SYS1)<br>- | SYS1.** |
| $KEY(SYS1)<br>****LIB- | SYS1.%%%%LIB.** |
| $KEY(NKEY#01)<br>$PREFIX(USER01)<br>- | USER01.** |

### 6.3.11 Converting the CA-ACF2 data set $MODE control card

CA-ACF2 provides a RULE transition mode. The $MODE control card is effective only if the system option of RULE mode has been selected. Table 6 on page 69 has suggested translation rules for converting the CA-ACF2 $MODE keywords. The

recommended conversion technique is to use the ABORT keyword for converting all of the CA-ACF2 resource protections to RACF.

*Table 6. CA-ACF2 $MODE control card with RACF equivalents*

| CA-ACF2 Rule Mode | RACF Equivalent | Description |
|---|---|---|
| QUIET | AUDIT(NONE)<br>UACCs of ALTER | Only user ID validation, no access control. |
| LOG | AUDIT(ALL)<br>UACCs of ALTER | Grant all access requests and log violations. |
| WARN | AUDIT(FAILURES)<br>UACCs of NONE<br>Profiles with WARNING | Grant all access requests and log violations, send warning messages to user. |
| ABORT | AUDIT(xxxx)<br>UACCs xxxx | Normal RACF access checking, xxxx means the converted access value. |

### 6.3.12 Converting the CA-ACF2 data set $USERDATA control card

Many installations use the $USERDATA control card for documentation. When converting your access rules, this descriptive data can be reinstalled in the DATA parameter of the RACF ADDSD command. For example, if the CA-ACF2 rule set is:

```
$KEY(TEST)
$PREFIX(TESTA)
$MODE(LOG)
$USERDATA(THIS IS FOR TESTING ON SYSTEM A)
```

Then the RACF command is:

```
ADDSD TESTA.** DATA('THIS IS FOR TESTING ON SYSTEM A')
   AUDIT(ALL) UACC(ALTER)
```

### 6.3.13 Converting CA-ACF2 data set rule entries

To complete the conversion of CA-ACF2 rule sets, you must convert the individual rule entries that follow the control cards. This section describes the major components of the rule entries and how to convert these to the RACF equivalents.

The syntax of the data set rule entry is:

```
dsn-mask
UID( )
READ( ) WRITE( ) ALLOC( ) EXEC( )
DATA( )
UNTIL( )/FOR( )
PGM/PROG( ) LIB( )
VOL( )
DDN( ) SOURCE( ) SHIFT( )
NEXTKEY( )
```

The description and suggested conversion of these parameters is discussed next.

#### 6.3.13.1 Dsn-mask

This is the name of the data set(s) that the CA-ACF2 rule set describes. The high-level qualifier does not appear since it is in the $KEY( ) control card.

The combination of the $KEY/$PREFIX control card and dsn-mask result in the profile-name parameter of the ADDSD command. Refer to 6.3.10, “Converting CA-ACF2 data set $KEY and $PREFIX values” on page 68 for a description.

#### 6.3.13.2 UID

This identifies which users this rule set applies to.

Use the RACF PERMIT command to set up an access control list for all groups and users that have been translated from the CA-ACF2 UID string value.

#### 6.3.13.3 READ, WRITE, ALLOC, EXEC

You can permit RACF-defined users and groups to access a RACF-protected data set by adding them to the access list of the data set profile. Table 7 shows the CA-ACF2 access permission and the equivalent RACF access levels. To best match the access in CA-ACF2 you have to also specify the audit level for the RACF data set profile.

*Table 7. CA-ACF2 and RACF access level equivalents*

| CA-ACF2 access permission | RACF access level | RACF description |
|---|---|---|
| ALLOCate | ALTER | Resource can be read, updated, created and deleted |
| WRITE | UPDATE or CONTROL (for some VSAM) | Resource can be read and updated. |
| READ | READ | Resource can be read and executed. |
| EXECUTE | EXECUTE | Program maybe executed |
| Allow | RACF Permission | Granting the RACF permission allows the access |
| Log | RACF Permission and the appropriate AUIDT() value. | Granting the RACF permission allows the access and the appropriate AUDIT will need to be set. |
| Prevent | NONE | Resource cannot be accessed |

#### 6.3.13.4 UNTIL/FOR

This parameter specifies the days or the date for which this rule set is valid.

These parameters can be converted by implementing the RESUME and REVOKE parameters of the RACF CONNECT command by creating a holding group for the resource being protected, connecting the users matching the UID string to this holding group, and specifying the RESUME and REVOKE parameters to cover the period indicated by the UNTIL/FOR parameters.

#### 6.3.13.5 PGM/PROG and LIB

The name of a program and the library from which it must be executed.

The CA-ACF2 access rule stipulates that access to a data set can be conditional based on the program in use through the LIB and PGM/PROG parameters.

An example of the CA-ACF2 access rule set with LIB/PGM rule entries is:

```
$KEY(TECH3)
  ABC.FILE UID(B05D12F1) LIB(PGM.LIB) PROGRAM(TECHPGM)
  READ(A) WRITE(A) ALLOC(A) EXEC(A)
```

The example above results in the following RACF commands:

1. Translate all the user that match the UID string to the RACF group TECHGRP
2. Define the program TECHPGM in library 'TECH3.PGM.LIB' to the PROGRAM class:

   ```
   RDEFINE PROGRAM TECHPGM UACC(NONE) OWNER(RACFADM) -
     ADDMEM('TECH3.PGM.LIB'//NOPADCHK) UACC(NONE)
   ```

3. Permit the TECHGRP group access to the TECHPGM program:

   ```
   PERMIT TECHPGM CLASS(PROGRAM) ID(TECHGRP) ACCESS(READ)
   ```

4. Permit group B05D12F1 to ALTER access to data set 'TECH3.ABC.FILE' when executing program TECHPGM from library 'TECH3.PGM.LIB':

   ```
   PERMIT 'TECH3.ABC.FILE' ID(TECHGRP) ACCESS(ALTER) WHEN(PROGRAM(TECHPGM))
   ```

#### 6.3.13.6 VOL

This parameter specifies the volume or volumes on which this data set must reside in order for the rule set to apply.

This parameter can be converted into the VOLUME and UNIT parameters of the RACF ADDSD command.

#### 6.3.13.7 DDN, SOURCE, SHIFT

These paarameters do not have a direct conversion to RACF. However, you can use a combination of JES and RACF exits to provide these functions. The parameters are defined as follows:

- DDN - The DDNAME(s) that must be used in reference to this data set in order for this rule set to apply.
- SOURCE - Indicates the valid input source to which this rule applies. The SOURCE parameter does not convert to RACF on a one-to-one basis. Input sources in RACF are handled in several areas and will need to be addressed during the conversion.
- SHIFT - Specifies the name of the SHIFT record for this rule set. Consider implementing these controls in the system access control provided in the RACF user profile.

#### 6.3.13.8 DATA

This parameter can also be specified in the RACF ADDSD command in the same manner that the $USERDATA control card information is converted. RACF does not support user data based on access levels. If this information is significant to some applications, it will need to be evaluated and an appropriate conversion methodology will need to be developed.

#### 6.3.13.9 NEXTKEY

Shows the alternate $KEY to be checked if access is not allowed in this rule set.

The NEXTKEY points to an access rule set, and the $PREFIX control card of the pointed-to access rule set replaces the value in its $KEY control card. The conversion program used will need to enable this sometimes complex algorithm to ensure the correct conversion of data set access rules.

### 6.3.14 Converting data set masking

CA-ACF2 data set masking rules are quite similar to RACF data set masking rules, when the RACF system-wide option of Enhanced Generic Naming (EGN) is in effect, with the following exceptions:

- In data set rules with more than one dash level, each interior dash level can be converted to a single RACF asterisk. (In other words, a single RACF asterisk represents one level.)
- In data set rules with multiple dash levels where one of them is the last level, the last level can be converted to a RACF double asterisk and all interior level dashes can be converted to RACF single asterisks.
- Data set rules with multiple asterisks within a qualifier can be converted to the RACF masking character of (%) for each CA-ACF2 (*). When the asterisks are at the end of a qualifier, they can be converted to multiple RACF data set profiles, one for each asterisk and a profile to cover the case where the asterisk represents zero characters.

For more information on the use of RACF generic characters, refer to *SecureWay Security Server (RACF) Security Administrator's Guide*, SC28-1915.

### 6.3.15 Data set conversion summary

Each CA-ACF2 rule set must be analyzed for features used. Most of them can be directly translated to RACF profiles and Access Control Lists (ACL), but some will have to be either converted, removed, or even converted into exit code, which should be the last option considered.

The rule options that cannot be converted directly to RACF without some planning are:

- %CHANGE or %RCHANGE used to specify additional users with authority to change this rule set besides OWNER and SECURITY.
- DDN used to limit this rule set to be used only when referred to by the DDNAME mentioned.
- SOURCE used to control input sources. RACF's TERMINAL and JESINPUT conditional access lists can be used for part of this function.
- SHIFT used to control access to resources based on a time period.
- The DATA option does not have a direct translation to RACF. You need to review any applications or administration options that are using this field. This may require changes to the programs using this information.

## 6.4 General resource protection

General resources (GRS) are physical or logical objects, other than data sets, that can be protected through RACF. For example, general resources can include CICS and IMS transactions, DASD and tape volume resources, load modules

(programs), terminals, DB2 external security and application-specific resources, just to name a few of the general resources that can be protected using RACF.

### 6.4.1 Definition

RACF-protected resources can be divided into two categories: data sets and general resources. General resource classes and their properties are defined in the RACF Class Descriptor Table (CDT). Note that the SAF router table (which is part of OS/390) must contain corresponding entries.

The RACF CDT initially contains general resource classes defined by IBM; it is designed to accommodate additional installation-defined classes. Such classes are often used to provide protection for critical add-on products such as performance monitors, job schedulers, tape management systems, and the like. The installation procedures for some products may require that you create a new class in RACF. Sometimes the FACILITY class is used for a limited number of profiles as an alternative to creating a new class.

RACF general resource classes can also be used to implement application security by placing `RACROUTE` calls in applications and maintaining rules in RACF.

### 6.4.2 General resource considerations

Except for the class FACILITY, which is designed to control various resource types (through a limited number of profiles), general resource classes are typically used for one specific resource type. The length and syntax of resource names depend on the type of the protected resource and are defined in the CDT. As an example, the resource name in class TERMINAL is the 8 character terminal name, while the name field in class JESSPOOL is composed as follows:

```
localnodeid.user ID.jobname.jobid.dsnumber.name
```

It follows that, for existing general resource classes, you must use the exact syntax as defined in the CDT and described in the RACF documentation. For installation-defined resource classes, the resource name can be chosen as required by the resource type. General resource classes can be defined in pairs of member and group classes, or can occur as single classes. In still another case, single non-grouping, non-member classes can be used. In some cases both parts are used, e.g., for CICS transactions where the standard member class is called TCICSTRN and the group class is GCICSTRN. In other cases only the grouping class is used, for example, class PROGRAM.

The basic concept is that the name of a profile is the resource name. Generic profile names can be used to protect several resources with similar names and identical protection requirements through a single profile. When the resource has both grouping and member classes, the generic entries should normally be created in the member class.

To protect multiple resources with identical protection requirements but unlike names through one profile, group profiles (in resource group classes) can be used. Resource group profiles contain the names of protected resources in their member lists.

It is important to understand the use of access authorities in general resource classes. The RACF access authorities of `READ`, `UPDATE`, `CONTROL` and `ALTER` were developed for data set access where they are truly meaningful. They are also

used for general resources, and the original meaning may not apply, depending on the resource. In many resource classes the meaning is reduced to a simple yes/no logic; NONE is interpreted as “no” and any access of READ or more as “yes.” Several exceptions exist to this general rule; for example, in the NODES class the different access authorities do have very specific meanings. The resource manager making the RACROUTE calls and interpreting the return codes can actually define the meaning of an access level, and the security administrator must understand its use by the resource manager.

Default protection depends primarily on the resource manager’s interpretation of a “profile not found” condition (RC=4). Different resource managers handle this condition differently; for example, IMS will grant access to transactions for which a RACF profile is not found, while CICS will deny access. You have two ways to enforce default protection:

1. By modifying the CDT entry (for installation-defined classes) to change RC=4 to RC=8
2. By defining ‘catch-all’ profiles (* with UACC=NONE) where appropriate

In most instances the second solution is the most feasible.

### 6.4.3 Converting CA-ACF2 GRS rule sets

The following sections discuss the use of CA-ACF2 GRS access rules and how to convert these to RACF GRS profiles. Figure 26 shows the syntax of a typical CA-ACF2 general resource Access Ruleset Entry (ARE).

```
$KEY( ) TYPE()
$PREFIX()
$USERDATA( )
grs-mask UID( )
ALLOW/LOG/PREVENT
SERVICE()
UNTIL( )/FOR( )
SHIFT( ) SOURCE( )
DATA( )
NEXTKEY( )
```

*Figure 26. CA-ACF2 general resource rule set fields*

### 6.4.4 Converting CA-ACF2 GRS types

Some types are used by CA-ACF2 for its own internal resource checking and most probably will not need to be converted to RACF. All other user-defined or OEM product-defined CA-ACF2 general resource types will need to be evaluated. The appropriate conversion methodology will need to be developed for each CA-ACF2 general resource type.

For each CA-ACF2 general resource type planned for conversion, a Class Descriptor Table (CDT) and SAF router table entries will need to be created. The programs that use the resource type will need to be evaluated for how the call is being made and what return codes are expected. Some applications may need to be modified to make the appropriate RACF calls.

### 6.4.5 Converting CA-ACF2 GRS $KEY and $PREFIX values

The $KEY control card supplies one of the following:

- The full name of the object being protected up to 40 characters
- The beginning value that will be prefixed to the grs-masks in the ruleset
- The name of a Nextkey

The $PREFIX control card shows the value that overrides the GRS rule set $KEY as a beginning value to all grs-masks in the rule set.

### 6.4.6 Converting the CA-ACF2 GRS $USERDATA control card

Many installations use the $USERDATA control card for documentation. When converting your GRS access rules, this descriptive data can be reinstalled in the DATA parameter of the RACF RDEFINE command. For example, if the CA-ACF2 GRS rule set is:

```
$KEY(CEDA) TYPE(CKC)
$USERDATA(CICS TRANSACTION)
```

then the RACF command is:

```
RDEF TCICSTRN CEDA UACC(NONE) OWNER(RACFADM) DATA('CICS TRANSACTION')
```

### 6.4.7 Converting CA-ACF2 general resource rule entries

To complete the conversion of CA-ACF2 GRS rule sets, you must convert the individual rule entries that follow the control cards. This section describes the major components of the GRS rule entries and how to convert them to the RACF equivalents.

Figure 27 shows the syntax of the GRS rule entry.

```
grs-mask
UID( )
ALLOW LOG PREVENT
SERVICE()
UNTIL( )/FOR( )
SOURCE( ) SHIFT( )
DATA( )
NEXTKEY( )
```

*Figure 27. GRS rule entry syntax*

The description and suggested conversion of these parameters is discussed next.

#### 6.4.7.1 grs-mask

This is the name of the object being protected. The beginning of the object's name does not appear since it is in the $KEY( ) control card.

The combination of the $KEY or $PREFIX control card and grs-mask result in the profile name that needs to be created by the RACF RDEFINE command.

#### 6.4.7.2 UID

The UID identifies which users this rule set applies to.

Use the RACF PERMIT command to set up an access control list for all groups and users that have been translated from the CA-ACF2 UID string value.

#### 6.4.7.3 ALLOW, LOG and PREVENT

These parameters can be converted as follows:

ALLOW A RACF access level of READ will allow access to the resource or a higher level of access may need to be given depending upon what CA-ACF2 service options are defined for the resource.

LOG The same method as used for ALLOW, along with the appropriate auditing for the RACF general resource profile.

PREVENT A RACF access level of NONE.

#### 6.4.7.4 Converting CA-ACF2 service keywords

You can permit RACF-defined users and groups to access a RACF-protected resource by adding them to the access list of the RACF general resource profile. RACF supports the access hierarchy of NONE, READ, UPDATE, CONTROL, ALTER and EXECUTE. For example, if a user has update access to a resource, the user also has read access to the resource.

Table 8 shows the CA-ACF2 service keywords and the equivalent RACF access levels for a CA-ACF2 permission of *Allow*. If the CA-ACF2 permission is PREVENT then the RACF access Authority for all the CA-ACF2 Service Keywords would be NONE.

The translation of the CA-ACF2 SERVICE option depends on the resource manager's or the application's implementation of the options.

*Table 8. CA-ACF2 service keyword translation to RACF access levels*

| CA-ACF2 service keyword | RACF access authorities for GRS |
|---|---|
| READ | READ |
| UPDATE | UPDATE |
| DELETE | UPDATE |
| ADD | UPDATE |
| EXECUTE | EXECUTE |
| ALL | ALTER |

#### 6.4.7.5 UNTIL/FOR

Specifies the days for which this rule set is valid.

These parameters can be converted by implementing the RESUME and REVOKE parameters of the RACF CONNECT command by creating a holding group for the resource being protected, connecting the users matching the UID string to this holding group, and specifying the RESUME and REVOKE parameters to cover the period indicated by the UNTIL/FOR parameters.

#### 6.4.7.6 SOURCE, SHIFT

These parameters do not have a direct conversion to RACF. However, you can use a combination of RACF and/or application exits to provide these functions. The parameters are defined as follows:

- SOURCE - Indicates the valid input source which this GRS rule applies to. The SOURCE parameter does not convert to RACF on a one-to-one basis. Input sources in RACF are handled in several areas and will need to be addressed during the conversion.
- SHIFT - Specifies the name of the SHIFT record for this rule set. Consider implementing these controls in the system access control provided in the RACF user profile.

#### 6.4.7.7 DATA

This parameter can also be specified in the RACF RDEFINE command in the same manner as the $USERDATA control card information is converted. RACF does not support user data based on access levels. If this information is significant to some applications, it will need to be evaluated and an appropriate conversion methodology will need to be developed.

#### 6.4.7.8 NEXTKEY

This parameter shows the alternate $KEY to be checked if access is not allowed in this rule set.

The NEXTKEY points to an access rule set, and the $PREFIX control card of the pointed-to access rule set replaces the value in its $KEY control card. The conversion program used will need to enable this sometimes complex algorithm to ensure the correct conversion of GRS access rules.

### 6.4.8 General resource conversion summary

Each CA-ACF2 GRS type must be analyzed for features used. Most of them can be directly translated to RACF general resource profiles and access control lists, but some will have to be either converted, removed, or even converted into exit or application code, which should be the last options considered.

The CA-ACF2 GRS rule options that do not convert to directly to RACF without some planning are:

- %CHANGE or %RCHANGE used to specify additional users with authority to administer the GRS rule set.
- The SOURCE option used to control input sources. RACF's TERMINAL and JESINPUT conditional access lists can be used for part of this function.
- The SERVICE() option does not have a direct translation to RACF. You need to review the RACF classes that you are planning to use and then select the authority you need. For each RACF class you can have a specific meaning of security levels: READ, UPDATE, CONTROL and ALTER.
- The DATA option does not have a direct translation to RACF. You need to review any applications or administration options that are using this field. This may require changes to the programs using this information.
- SHIFT used to control access to resources based on a time period.

Most general resources supported under CA-ACF2 can be converted to RACF, typically by creating a class in the CDT and the router table. An evaluation of the programs and applications making calls to RACF may be necessary.

## 6.5 Other conversion considerations

This section details other important considerations when converting CA-ACF2 definitions.

### 6.5.1 Started task protection

The security issue regarding started procedures is that it is necessary to associate a started procedure with a user ID (and optionally a group name) to properly control the resources accessed by the procedure. CA-ACF2 and RACF use rather different techniques for this process. CA-ACF2 provides the capability to define logon IDs equal to the procedure name with a privilege that these IDs can only be used for started procedures.

RACF supports two methods for protecting started procedures:

- Using profile definitions in the RACF STARTED Class
- Using the RACF Started Procedure Table (module `ICHRIN03`)

With the STARTED class, you don't need to change code or re-IPL the system in order to add or modify RACF identities for started procedures.

**Note:** You must have a started procedure table (module ICHRIN03), even if your installation uses the STARTED class. RACF does not initialize if `ICHRIN03` is not present. However, the table can be empty, as it is when delivered with RACF. It is recommended that you use the STARTED class, and also create a Started Procedure Table (`ICHRIN03`), in case, for example, someone unintentionally deactivates the STARTED class. For more information, see *SecureWay Security Server (RACF) System Programmer's Guide,* SC28-1913.

Below is an example of some of the commands to set up the STARTED class:

```
SETROPTS GENERIC(STARTED)
RDEFINE STARTED JES2.* STDATA(USER(JES2) GROUP(STCGROUP) TRUSTED(YES))
RDEFINE STARTED ** STDATA(USER(=MEMBER) GROUP(STCGROUP) TRACE(YES))
SETROPTS CLASSACT(STARTED)
SETROPTS RACLIST(STARTED)
```

The ** entry has the effect that all procedures not defined in the preceding profile definitions will use a user ID equal to their procedure name. The security administrator should define a user ID for each new procedure and connect it to the designated group. "`STCGROUP`" in the examples above is the name of a group for started procedures.

With this information, normal access checking is performed for all started procedures using the associated RACF user ID and group name. You can indicate that selected started procedures are to be considered as `PRIVILEGED` or `TRUSTED`, such as JES2 in the example above, which means that most RACF authorization checks are accepted unconditionally. `TRUSTED` is the recommended choice because it provides the ability to turn on logging.

#### 6.5.1.1 Migration considerations

The following are considerations when migrating started task definitions:

- A CA-ACF2 Logon ID with the `STC` privilege can be used only by a started procedure, and is not allowed to log on with this user ID. It is recommended

that you make these IDs protected user IDs in RACF so they cannot be used to enter the system by any means that require a password to be specified, such as TSO logon, CICS sign-on, or batch jobs that specify a password on the JOB statement.

- It is recommended that you do not assign user attributes such as SPECIAL and OPERATIONS to any ID assigned to a started procedure.
- It is also recommended that you assign the TRUSTED attribute to system procedures as recommended in the appropriate documentation to avoid problems in starting up your system, but do not assign the PRIVILEGED or TRUSTED attribute to any other procedures, and certainly not to the generic catch-all entry in your Started Class definitions.

## 6.5.2 Batch job submission protection

In commercial mainframe environments, batch jobs are an important part of day to day production. They are used in support of online systems as well as pure batch applications, and operating systems without batch job capabilities have limitations in satisfying commercial application needs.

### 6.5.2.1 Goals

Good batch job management has operational goals as well as control aspects. Operational goals include the timely and successful execution of jobs in a predetermined order; these goals are usually met through the use of job scheduling software such as OPC/ESA. The control aspects include:

- Secure submission of user-owned jobs, mostly test jobs
- Control over the submission of production batch jobs
- Control over access to job output
- The ID under which a job executes and its data set access authority
- Potentially, control over production job names

### 6.5.2.2 Control issues

Key control issues with batch job submission are:

- Passwords may be exposed in the submission process. Whether they are stored in files or added unencrypted during submission time, all techniques violate the principle that no clear passwords should be stored.
- Jobs with unknown user IDs may be executed, but their access to resources is limited to UACC-level access.
- Production jobs may have excessive privileges (meaning the power to access any data set across all applications, a violation of the least necessary privilege and granularity of controls principles).

#### 6.5.2.3 Terminology and differences

Jobs submitted from user address spaces (via TSO or batch INTRDR) are treated similarly in CA-ACF2 and RACF; the authority of the submitting environment is passed on to spawned jobs without user intervention. This concept is called inheritance in CA-ACF2 and propagation in RACF.

The approaches to controlling production batch jobs in CA-ACF2 and RACF differ in more than just terminology. Specifically, the differences are:

- The CA-ACF2 command ACFSUB (for TSO) and utility JOBCOPY (for batch or STC) enables authorized users to submit a job with a different jobname. In RACF more specific controls are available through surrogate user support without special commands or utilities. Surrogate user support uses the SURROGAT resource class to define batch user IDs which can be submitted by surrogate users and, for each ID, which users or groups are authorized to submit (or cancel) jobs.
- The CA-ACF2 JCL statements //*LOGONID and //*PASSWORD are ignored in a RACF environment since JES will treat the cards as comments. RACF user IDs and/or passwords must be provided on the job statement or via propagation.

#### 6.5.2.4 The RACF approach

Many different approaches to job submission have been developed over time; some involve TSO submit exits, router exits, scheduler exits, JES exits, and so forth. The following, recommended approach is an effective and easy way to manage jobs in a RACF environment without exits.

***Controlled job submission***

Except for jobs submitted via RJE and NJE, passwords should not be specified on job statements:

- To submit a job under the same user ID (to have the authority of the current address space propagated), neither user ID nor password should be specified on the job statement. This is the recommended technique for user-owned jobs and does not require additional setup.
- To submit jobs to be executed under a different (production) user ID, that user ID (and no password) should be coded on the job statement. This technique invokes surrogate user support and requires that the submitting user ID is properly authorized to the submitted user ID in class SURROGAT. This is the recommended technique for enabling job scheduler software to submit production jobs.

***Required controls***

The surrogate user support in RACF is only a technique to control job submission; to achieve adequate controls, it must be used appropriately by:

- Specifying the SETROPTS option BATCHALLRACF to enforce that all batch jobs have a valid user ID.
- Defining and assigning appropriate user IDs for batch production (that is, individual IDs by application or processing type).
- Defining specific access authorities to these IDs according to the principle of “least necessary privilege.”
- Authorizing only the job scheduler to submit production jobs.

- Establishing change control over production JCL and protecting job libraries adequately.

***Other controls***

If production job names have operational or control significance, their use can be controlled by profiles in the RACF JESJOBS class. Profiles in this class control which users or groups of users can submit jobs with production job names. If it is important to establish control over the job origin (CA-ACF2 source, RACF port of entry), profiles in the RACF classes TERMINAL and JESINPUT can be used to authorize users accordingly.

Control over spooled job input and output files can be achieved in RACF through profiles in the JESSPOOL class.

#### 6.5.2.5 Summary

Batch controls in RACF are effective and easy to implement through user ID propagation for user-owned jobs and through surrogate user support for production jobs. No major problems are expected in migrating batch jobs from CA-ACF2 to RACF.

### 6.5.3 NJE and RJE protection

RACF can implement network protection at a variety of different levels. A migration plan must determine which of these functions, using CA-ACF2, are currently in use and need to be migrated to RACF.

#### 6.5.3.1 NJE security overview

NJE security provides the installation with control over data entering and leaving a node. There are subtle differences in some of the ways in which CA-ACF2 and RACF implement NJE protection. This section describes the way in which RACF employs its protection.

The requirements are to preserve the security of the system so it is not compromised by NJE functions or jobs, and to enhance the overall security of the network. NJE security, with JES and RACF, does the following:

- Controls who can send jobs and data to another node on the basis of destination node and sending user ID.
- Controls owner and level of jobs and data entering a node on the basis of origin node, user ID and group.
- Propagates user validation across the network, so passwords do not have to be sent with the job. (When passwords are required, provides a means of encrypting them.)
- Permits different user IDs or GROUPs on different nodes and provides a means for translating them to locally-defined values under installation control.
- Permits surrogate job submission across NJE nodes.
- Can define a default user ID under certain conditions.

These controls are exercised primarily on the origin and destination nodes, not on store-and-forward nodes. It is assumed that all the nodes and links in the network are trusted to the extent that they will not make unauthorized changes to security fields in the NJE headers. Centralized SAF/RACF management allows mixed

levels of nodes in a network, including previous levels of JES2 and RACF as well as JES3 and VM.

If the NJE network is not defined to RACF through the NODES profiles, then existing JES security controls are used.

RACF does not require any modifications to the NJE headers.

#### 6.5.3.2 NJE levels of trust

The level of RACF verification is determined by the level of trust, as defined in the RACF NODES class profiles. Each access level corresponds to one of the levels of trust.

**Levels of trust:** Jobs coming from other nodes are validated during input service processing in the receiving node. The NODES class is used to verify whether the transmitting node and its user ID or group is trusted, semi-trusted, or un-trusted. Userids may be translated only from trusted nodes, but groupids may be translated from trusted or semi-trusted nodes.

**Trusted** The node and user IDs are accepted as validated without a password. The trusted attribute is defined by `UACC(UPDATE)` in the NODES profile definition.

**Semi-Trusted** The node is trusted enough to ensure that NJE headers are valid, but the user must supply a password (which can be encrypted). The semi-trusted attribute is defined by `UACC(READ)` in the NODES profile definition.

**Untrusted** The node is not trusted, and any jobs received from this node will be purged, with a message sent to the submitting user. This is defined to RACF as `UACC(NONE)`.

**Local** Local nodes are treated as Trusted nodes if they are defined in the RACF `&RACLNDE RACVARS` profile. It is assumed that all users and groups are defined identically on all local nodes, and share either the same or a compatible RACF database.

Trust should usually be assigned at the node level. In other words, you either trust all users on a given node to have verified headers, or you trust no users of that node.

#### 6.5.3.3 RACF NODES class

RACF profiles in the NODES class contain the names of all networking nodes that are controlled on this system. There are four levels of access available for this class:

**NONE** Allows no work from the specified node to be entered into this system.

**READ** Allows work from the specified node to be entered into this system if a user ID and password are given.

**UPDATE** Allows work from the specified node to be entered into this system because the node is trusted and no additional verification is required; however, the user ID and group that was assigned must exist in the receiving system.

**CONTROL** Allows work from default or down-level nodes to have the trusted attribute, which allows the user to be validated.

The Universal Access field (UACC) controls jobs on a node-by-node basis. Individual users can also be permitted to the NODES class profile with the required authority. Any user that requires verification on the current node must be defined to RACF on this node.

You can also use a generic access profile to cover all work from any nodes entering this system.

An installation can choose to protect either inbound work, outbound work, or both. For inbound jobs and SYSOUT, you can decide whether to protect jobs, SYSOUT, or both. You can also determine which users or group of users are allowed to enter NJE jobs or SYSOUT.

#### 6.5.3.4 NJE migration considerations

The migration of NJE security from CA-ACF2 to RACF is not a complex task. The following details should be considered if CA-ACF2 and RACF are to be implemented in the same NJE environment:

- The user's current-connect group is defined in both products.
- The nodes should be Trusted.
- The appropriate NODES profiles should be defined to RACF.

#### 6.5.3.5 RJE signon (JES2)

RJE passwords for signon/logon are checked by JES2. These passwords are specified in JES2 initialization parameters. With RACF and JES, sign-on processing can be verified by RACF provided that:

- RACF is active
- FACILITY resource class is active
- "RJE.rmt-name" profile is defined in FACILITY class
- RJE remote name is defined as a user to RACF through ADDUSER command.

The user ID that represents the remote name, password, and new password are passed to SAF/RACF. After this check, the remote name is recognized as a user ID by RACF. Security checking for commands coming from remote terminals is also done by RACF. Instead of the remote terminal password, you can use the line password for signon/logon commands. The line passwords are still checked by JES2.

JES2 checks the password if no decision is made by RACF, indicating that the FACILITY class profile was not found.

#### 6.5.3.6 RJP signon (JES3)

The protection of RJP workstations is based on JES3 verification of the workstation passwords. JES3 initialization parameters or operator commands are used to update the passwords.

The protection of RJP workstations can be controlled by RACF. To activate the RACF protection, you must define the RJP workstation to the FACILITY class and also define a RACF user ID with the workstation name.

Additionally, controls can be placed on remote printers or punches. Furthermore, operator commands that are allowed from the workstation can also be controlled by RACF.

If the workstation is not defined to RACF, then existing JES3 verification is used.

### 6.5.4 Other network controls

RACF can control network resources at a variety of different levels. Few installations use all the possible controls, and frequently use none of them directly. A migration plan must determine which of these functions, using CA-ACF2, are currently in use and need to be migrated to RACF. This is a good time to determine if changes are needed in this area, since perceptions and accepted methods for network controls have changed considerably during the last few years.

#### 6.5.4.1 VTAM ACBs

VTAM ACBs are controlled through the RACF VTAMAPPL class for non-APF authorized programs. VTAM does a `RACHECK` against the class to verify that the user is allowed to open the specified `ACB(APPLID)` name. CA-ACF2 provides a similar check, and migration should be straightforward.

#### 6.5.4.2 APPC

APPC usage can be complex because application programming is involved. Both RACF and CA-ACF2 have resource classes used to protect the basic elements of the APPC environment. APPC applications may be multi-user applications, possibly running in an authorized state. This implies that the applications may be responsible for fine-grain security, and this requires application code. The application designer has many options for handling his security requirements, under either CA-ACF2 or RACF. Migration may involve inspecting each APPC application. If most of the applications are written to a common pattern, as often happens, this inspection and migration should be straightforward.

#### 6.5.4.3 Terminal

Terminal usage can be restricted in both products. In RACF it is not often used for standard VTAM-connected terminals. Most installations rely on user, application, and data set protection for basic security. Security controls that attempt to manage which users can use which terminals tend to have unusually high manpower requirements for administration. Also, terminal pass-through connections (through SNA, from another host, or through connections such as telnet) can make terminal-related security management very difficult to administer and sometimes pointless. Migration of terminal controls to RACF may not be difficult, but we suggest you review the need for these controls first.

#### 6.5.4.4 Netview

Netview uses standard SAF functions for user authentication. Both RACF and CA-ACF2 support this interface, and there should be few, if any, migration issues.

#### 6.5.4.5 Netview Access Services

Netview Access Services (NVAS) uses predefined resource classes in RACF. NVAS installations using CA-ACF2 should have defined several resources and rules for use with NVAS. Migration of these functions to RACF should be straightforward.

#### 6.5.4.6 General VTAM applications

General VTAM Applications that do user authentication typically use `RACROUTE VERIFY` processing. This implies that CA-ACF2 is set up for `RACROUTE VERIFY`, and migration to RACF should be straightforward.

### 6.5.5 CICS protection

Prior to CICS 3.2.1, security could be accomplished by CICS internal security, an External Security Manager (ESM), or a combination of both. Starting with CICS 3.2.1, all CICS security must be implemented through an ESM.

CICS uses SAF to communicate with RACF for all security calls and CA-ACF2 implements its CICS security through the CA-ACF2/CICS subsystem interface. The following section describes, at a high level, the differences and conversion approaches that can be used to migrated your CICS security to RACF.

#### 6.5.5.1 CICS users

CA-ACF2 allows or denies access to an application through entries in the `PRIVILEGES` section of Logon ID records. Your installation may have several CICS regions executing at the same time and users allowed to log on to more then one region.

With RACF and CICS, authorization checking can be made against a resource class called APPL. For each CICS region requiring logon control, you must have a corresponding profile in the RACF APPL class. CICS users can then be connected to an access group which in turn is given access to the APPL profile. This way the APPL profile remains static, and users are connected and removed from the access group as required.

***CICS user session parameters***

In CICS 3.2.1, support for CICS internal security was dropped and customers could only use an ESM to provide CICS security. In CA-ACF2 this support is provided in the Logon ID record. With RACF the support is included in the CICS segment of the RACF user profile.

#### 6.5.5.2 CICS resources

The CA-ACF2 TYPEs of all rules that apply to protected resources in a CICS environment are specified by parameter values in the CA-ACF2/CICS `ACF2PARM` options data set. Default values for CA-ACF2 and corresponding RACF default class names are given in Table 9.

*Table 9. CICS default resources*

| CA-ACF2 default TYPE | RACF default class | Resource description |
|---|---|---|
| CKC | TCICSTRN/GCICSTRN | Transactions |
| CTD | DCICSDCT/ECICSDCT | Destination Control Table |
| CFC | FCICSFCT/HCICSFCT | File Control |
| CPC | MCICSPPT/NCICSPPT | Processing Program Table |
| PSB | PCICSPSB/QCICSPSB | Program Specification Blocks |
| CTS | SCICSTST/UCICSTST | Temporary Storage Table |

| CA-ACF2 default TYPE | RACF default class | Resource description |
|---|---|---|
| XCD | CCICSCMD/VCICSCMD | CICS System Programming Commands |
| | ACICSPCT/BCICSPCT | Program Control Table |
| CMR | Not Needed | MRO in/outbound |

### *ACF2 user resources*

In a multiple CICS address space environment, a CA-ACF2 installation may define other rule TYPEs besides those provided by default. This allows unique resource authorizations to be defined for each CICS region. The TYPEs that apply to a specific CICS region are given by the keyword CICSKEY in the CA-ACF2/CICS ACF2PARM data set. Figure 28 shows some examples of how CA-ACF2 TYPES are mapped to CICS resources.

```
CICSKEY ...,TYPE=KC1,RESOURCE=TRANS,...
CICSKEY ...,TYPE=FC1,RESOURCE=FILE ,...
CICSKEY ...,TYPE=PC1,RESOURCE=PROGRAM,...
CICSKEY ...,TYPE=TS1,RESOURCE=TEMPSTRG,...
CICSKEY ...,TYPE=PS1,RESOURCE=PSB,...
```

*Figure 28. CA-ACF2 CICSKEY example*

The rule TYPEs that are defined in Figure 28 for our CICS region are KC1, FC1, PC1, TS1, and PS1. For a transaction, CA-ACF2 checks the KC1 GRS rule TYPE for user authorization.

### *RACF user resources*

As displayed in Table 9, a set of default RACF resource classes is provided by RACF at installation time. In a multiple CICS region environment, it may be preferable to define the same resources with different access lists; for example, test and production. The CEMT transaction, for instance, may be allowed to a substantial number of people in a CICS test region and reserved to very few people in a CICS production region.

There are two RACF methods available to differentiate authorizations by CICS region. They are:

- Prefixing of resource names
- User-defined resource class names

### *Prefixes*

If this option is chosen, CICS will use only those profiles that are prefixed with the user ID associated with this CICS region. This user ID comes from either the job statement, started task identifier, or user ID propagated by JES if CICS is started by a submitted job without a USER on the job statement. You need to plan whether to use prefixing or not. There are administrative and run-time considerations that vary with the release of CICS being used.

***User resource classes***
It is recommended that you define unique classes for all your CICS regions. The class names specified in the CICS `DFHSIT` are the class names that will be checked by RACF for authorization to the various resources.

Table 10 may be used to translate the CA-ACF2 rule `TYPEs` to RACF classes from our example in Figure 28 on page 86.

*Table 10.* Example of CA-ACF2 CICS TYPE translation to RACFclasses

| Resource | CA-ACF2 TYPE | DFHSIT Parameter | RACF Classes |
|---|---|---|---|
| Transaction | KC1 | $PRDTRN | T$PRDTRN/G$PRDTRN |
| File | FC1 | $PRDFCT | F$PRDFCT/H$PRDFCT |
| Program | PC1 | $PRDPCT | M$PRDPCT/N$PRDPCT |
| Temporary Storage | TS1 | $PRDTST | S$PRDTST/U$PRDTST |
| Program Specification Blocks | PS1 | PRDPSB | P$PRDPSB/Q$PRDPSB |

It is recommended that you include a national or numeric character in your user class name. In the examples, we used the “$” character. IBM has stated that any new IBM-defined RACF resource class will never include a national or numeric character.

### 6.5.5.3 CICS application security
There may be some CICS applications that make security calls to CA-ACF2 from within the application. If this is the case, provided that they are written in CICS Command Level language, you can use an equivalent function with RACF. The `CICS QUERY SECURITY` command can be issued from your program against a user-defined RACF resource CLASS. RACF then returns to your program the access level for you to make a decision.

### 6.5.5.4 Migration considerations
The migration of security from CICS/CA-ACF2 to CICS-RACF is not always a trivial task. If an installation is running several non-connected CICS regions and only protecting CICS transactions, a migration will be reasonably straightforward. When CICS is operating using connected CICS regions, you should review the *CICS RACF Security Guide*, SC33-1701 for implementation using RACF, since CA-ACF2 uses it own CA-ACF2/CICS subsystem interface (`MROIN` and `MROOUT` Types) for its implementation, and there is no direct translation of these two methodologies.

Applications that make security calls directly to CA-ACF2 will present the greatest challenge, especially on versions prior to CICS 3.1. In this case exits may have to be written.

Some installations will administer CA-ACF2 from within CICS. While RACF itself does not offer this function, there are two alternatives.

1. Purchase a vendor product that allows this; there are several to choose from.
2. Write an application using APPC. You will need to code APPC Allocate, Send, Receive and Free calls in your CICS transaction and initiate an APPC/MVS

transaction that runs TSO, with RACF TSO commands to perform the desired administration functions.

## 6.5.6 IMS protection

CA-ACF2 and RACF can basically control the same resources for IMS. One exception is that CA-ACF2 has special code that can be installed for DL/1 batch processing for the protection of database segments.

### 6.5.6.1 Terminology and differences

CA-ACF2/IMS security is provided by a separate CA-ACF2 IMS subsystem which has its own GSO records defining the options used. For example: CA-ACF2 for OS/390 can be in ABORT mode, while CA-ACF2 for IMS is in LOG mode. This is based on specifications in the different CA-ACF2/IMS records.

The CA-ACF2 /ACF SHOW STATE command in IMS will display all the IMS records and their settings.

CA-ACF2/IMS calls CA-ACF2/OS/390 to perform the actual user identification and access checking.

CA-ACF2/IMS provides an IMS transaction (ACF) that can be used to maintain Logon ID records for IMS users directly from IMS.

There are no subsystems to activate IMS controls in RACF. Just activate the IMS resource classes APPL, TIMS, and GIMS; and specify in the IMS CNTRL and SECURITY macros used to control/generate IMS that RACF is to be used for logon and transaction control. If the class is active, IMS will perform an authorization check. If the resource is defined in the class, IMS will verify access according to rules (UACC and/or access list). If the transaction is not defined or the class is not active, the transaction will be regarded as unprotected and access will be granted. This is opposite to CA-ACF2 IMS, which by default regards all resources as protected. A generic ** profile with UACC(NONE) is an easy way to implement default protection for IMS transactions under RACF.

### 6.5.6.2 RACF approach

This section details the RACF security approach for IMS:

- Specify your security requirements in the IMSCTRL and SECURITY IMS definition macros. Use SECURITY TYPE=(TRANAUTH,SIGNAUTH) and SECLVL=(FORCSIGN) to implement transaction security and RACF user authentication, and don't allow the MTO operator to override any of the security settings at IMS start/restart.
- If you are to control dependent regions' access to resources through the Application Group Name (AGN) function, specify these names and run Security Maintenance Utility (SMU) to define these resource names to IMS.
- Define all IMS subsystems in the RACF APPL class with UACC(NONE) and permit users and groups read access.
- Define transactions in the TIMS or GIMS classes with UACC(NONE) and give users and groups read access.
- If AGN is used, define the applications in the AIMS class with UACC(NONE) and give the IDs for the dependent regions read access to the AGN group they need.
- To implement default protection, add ** profiles with UACC(NONE).

- Remember to protect all libraries, data sets and databases.

#### 6.5.6.3 Goals

The basic goals for both products are to:

- Authenticate users
- Control user access to IMS systems
- Control user access to transactions
- Record attempted violations

#### 6.5.6.4 Summary

RACF-IMS is a structured and well-defined interface. No IMS code changes or exit codes are needed. There are few differences in the way resources are protected, and migrating from CA-ACF2 to RACF should be fairly straightforward.

### 6.5.7 TSO protection

The privilege for a user to start a TSO session is maintained—together with certain session parameters, limitations, and functional privileges— either in the TSO User Attributes data set `SYS1.UADS` or within the security software. Both products, CA-ACF2 and RACF, provide the option to maintain this information in `SYS1.UADS` or in their respective databases. RACF stores TSO information in an optional TSO segment of the user profile and uses general resource classes to control user access to account numbers, logon procedures, and TSO privileges.

#### 6.5.7.1 TSO segment

A TSO segment in the RACF user profile supplies default information to TSO during logon processing. You can specify the following fields in the TSO segment of a user's profile:

| | |
|---|---|
| `ACCTNUM` | User's default TSO account number when logging on through the TSO/E logon panel |
| `JOBCLASS` | User's default job class |
| `MSGCLASS` | User's default message class |
| `HOLDCLASS` | Uuser's default hold class |
| `SYSOUTCLASS` | User's default sysout class |
| `DEST` | Default destination to which the system will route dynamically-allocated sysout data set |
| `PROC` | Name of the user's default logon procedure when logging on through the TSO/E panel |
| `MAXSIZE` | Maximum region size the user can request at logon |
| `SIZE` | Minimum region size if the user does not request a region size at logon |
| `SECLABEL` | User's security label if one was entered on the TSO LOGON panel |
| `UNIT` | Default name of a device or group of devices that a procedure uses for allocations |
| `USERDATA` | Optional installation data defined for the user |

If a user logs on to TSO and you haven't defined a TSO segment for that user, TSO checks the SYS1.UADS data set for information it needs to build a session. If TSO does not find an entry for the user in SYS1.UADS, the logon attempt is terminated.

When a user logs on, if using the TSO segment in RACF, TSO checks the authority to use certain TSO resources such as account numbers (class ACCTNUM) and logon procedures (class TSOPROC). If the user is authorized to use a resource such as an account number, TSO continues building a session for the user. Otherwise TSO prompts the user for a valid account number or logon procedure.

You can move TSO user attribute information from SYS1.UADS to the RACF database. When you do this, RACF stores this information in the TSO segment of the user's profile. You must maintain an entry in SYS1.UADS for certain users, such as IBMUSER and/or one or more system programmers. They are used if you need to deactivate RACF for an emergency repair.

Other information that you may need to supply is profiles in TSOAUTH class. This class controls TSO authorities, like MOUNT, JCL, CONSOLE, TESTAUTH and so forth.

#### 6.5.7.2 Migrations considerations

If you are using SYS1.UADS in your current CA-ACF2 environment, you can continue to do so when migrating to RACF. We recommend, however, using TSO segments and suggest the RACONVERT command for a conversion from UADS to RACF segments. Other conversion considerations are:

- Conversion of logon ID accounting and TSO procedure privileges
- Conversion of other CA-ACF2 TSO privileges that convert to TSO profile attributes; for example, MAIL, PREFIX, and NOTICES
- Conversion of CA-ACF2 TSO GRS Types of TAC and TPR to the appropriate RACF classes

### 6.5.8 DB2 protection

There are three areas in which control of DB2 resources can be protected. These controls can be implemented in both CA-ACF2 and RACF and are:

- Control of access to DB2 subsystems
- Control of access to DB2 Secondary Authorization IDs
- Control of access to DB2 objects through the use of external security

#### 6.5.8.1 Access to DB2 subsystems

Controlling access to the DB2 subsystem from different environments (such as TSO, BATCH, CICS, or IMS), is accomplished by DB2 issuing a SAF call to see if the user is allowed access to the subsystem using a specific environment. Since this DB2 control is using SAF, conversion from CA-ACF2 is rather straightforward. The general resource that is used in RACF for this control is the DSNR class and the appropriate CA-ACF2 GRS Type can be mapped to this class in order to convert the definitions.

#### 6.5.8.2 DB2 Secondary Authorization IDs

If your implementation to control access to DB2 objects utilizes DB2 Secondary Authorization IDs, which is just a group of users, then the conversion of the

records in the CA-ACF2 Source Group definitions from the Information Storage database that are used for CA-ACF2 DB2 Secondary Authorization is straightforward. These CA-ACF2 Source group records will convert to RACF groups with the appropriate users connected to those groups.

#### 6.5.8.3 Controlling access to DB2 objects

A user can have access to DB2 objects, such as tables and plans. DB2 has it own access control mechanism to control these objects, maintained through DB2 administration. Control of these objects can also be implemented by using DB2 external security. CA-ACF2 has a CA-ACF2/DB2 subsystem feature to accomplish this; RACF provides this access control through the RACF/DB2 External Security Module.

Controlling access to DB2 objects using external security and it's implementation is different in CA-ACF2 and RACF. Some of the DB2 privileges in CA-ACF2/DB2's external security subsystem do not directly translate to the same "Type-Class translations" for general resource definitions. Conversion and careful attention to this will be needed to ensure these privileges get mapped to the correct RACF classes.

#### 6.5.8.4 Migration considerations

The migration considerations for DB2 are:

- Review which CA-ACF2 functions are used to control users in DB2.
- RACF can control user or group access to the different DB2 subsystems and resource objects. It is highly recommended to use RACF groups for access to DB2 objects within DB2, to reduce administration overhead, and to reduce the number of access rules that will need to be maintained.
- In CA-ACF2, a logon ID can be the same name as a DB2 Secondary Authorization ID. However, in RACF, since DB2 Secondary Authorization IDs are groups and not user IDs, and you can not have a group name that is the same as a user ID, you may have to rename some of the DB2 Secondary Authorization IDs or user IDs as part of the conversion effort.
- If the CA-ACF2/DB2 external security subsystem is in use, the RACF External Security Module will need to be implemented and the CA-ACF2 DB2/GRS definitions will need to be converted to the correct RACF/DB2 GRS profiles.
- DB2's own security features can be used to control internal tables and plans in DB2, but the preferred method of using the RACF/DB2 External Security Module should be implemented. If there is no CA-ACF2 external security information to be converted to RACF, there are methodologies and tools available to assist in converting DB2's internal security to DB2 external security using RACF.

### 6.5.9 OS390 UNIX protection

This section describes using RACF with OS/390 UNIX and the conversion of CA-ACF2 UNIX users definitions to RACF. The OS/390 UNIX security functions provided by RACF include user validation, file access checking, privileged user checking, and user limit checking. RACF can be used to manage system and data security in an OS/390 UNIX environment by:

- Identifying and authenticating a user

- Verifying that a user can access the following:
  - OS/390 UNIX processes
  - OS/390 UNIX files
  - Other OS/390 UNIX resources

#### 6.5.9.1 OS/390 UNIX users

OS/390 UNIX users are defined with RACF commands. When a job starts or a user logs on, the user ID and password are verified by RACF. When an address space requests an OS/390 UNIX function for the first time, RACF does the following:

1. Verifies that the user is defined as an OS/390 UNIX user.
2. Verifies that the user's current-connect group is defined as an OS/390 UNIX group.
3. Initializes the control blocks needed for subsequent security checks.

OS/390 UNIX information about a user is stored in an OMVS segment in the RACF user profile. OS/390 UNIX information about a RACF group is stored in the OMVS segment in the RACF group profile.

A user is identified by an OMVS user ID (UID), which is kept in the RACF user profile, and one or more OMVS group IDs (GIDs), which are kept in RACF group profiles.

The system verifies the user IDs and passwords of the users when they enter the system using a TSO/E, rlogin, telnet, or when a job starts. When a user attempts to initiate an interactive session that invokes the shell, RACF verifies that the interactive user is defined to OS/390 UNIX before the system initializes the shell. When a program requests a service from OS/390 UNIX for the first time, RACF verifies that the user running the program is defined to OS/390 UNIX before the system provides the service.

To authorize a RACF user to access OS/390 UNIX resources, you must add a UID to the RACF user profile for an existing or new user and connect each user to a RACF group that has a GID. You also have to add a GID to a RACF group profile for an existing or new RACF group. The UID and GID number value can be between 0 and 214783647.

When a user is logged on to OS/390 UNIX, the UID from the user's RACF user profile becomes the effective UID of his process. This effective UID is used to check the user's UNIX authorization to access OS/390 UNIX resources.

When a user is initialized as an OS/390 UNIX user, the GID from his current-connect group becomes the effective GID of the user's process. The user can access OS/390 UNIX resources available to members of the user's effective GID.

When RACF list-of-group checking is active, a user can access an OS/390 UNIX resource if it is available to members of any group the user is connected to that has a GID in its RACF profile. These additional groups are called supplemental groups.

#### 6.5.9.2 OMVS segment

An OMVS segment in the RACF user profile supplies the OS390 UNIX information during system entry validation processing. You can specify the following fields in the OMVS segment of a user's profile:

**HOME** Hierarchical file system (HFS) initial directory pathname

**PROGRAM** Program and pathname (shell program)

**UID** User identifier

**ASSIZEMAX** Maximum RLIMIT_AS resource value that a user's processes can receive.

**CPUTIMEMAX** Maximum RLIMIT_CPU resource value that a user's OS/390 UNIX System Services processes can receive

**FILEPROCMAX** Maximum number of files a user is allowed to have concurrently active or open

**MMAPAREAMAX** Maximum amount of data space storage, in pages, that can be allocated by a user for memory

**PROCUSERMAX** Maximum number of processes a user is allowed to have active at the same time

**THREADSMAX** Maximum number of threads that a user can have concurrently active

#### 6.5.9.3 Migration considerations

The CA-ACF2 OMVS UNIX user and group information convert directly to RACF's User OMVS segment and Group OMVS segment with no issues. The areas that may need some attention are:

- Ensuring that the user's default group has a GID assigned to it. This will alleviate the need for users to change their current-connect group at sign-on to a group that has a GID assigned to it.
- Ensuring that all the groups with valid GID values that a user had access to in CA-ACF2 by means of the TYPE TGR rules are translated to a connection to a RACF group.

### 6.5.10 Program control

Both products can control the execution of programs. This involves two steps, the protection of load libraries and the protection of specific programs in those libraries:

- Load libraries in OS/390 are regular data sets, and are protected like other data sets through CA-ACF2 rules or RACF profiles. To allow the execution of programs in a library, but prevent users from copying them, EXECUTE access can be used in both environments.
- Programs and TSO commands (considered programs in this context) are protected in slightly different ways.
- In CA-ACF2, there are few different options. The GRS Type PGM is available and can be used to control programs. Specific programs can also be defined in the PPGM and LOGPGM GSO options.

  In RACF, programs are protected through profiles in the RACF class PROGRAM; program definitions are very specific and can consist of three

parts: the program name, the library name, and an optional volser of the DASD volume containing the library.

When protecting programs, it is important to note that for programs with alias names, all aliases must be protected. For example, to effectively protect the superzap program, both commonly used names, AMASPZAP and IMASPZAP, as well as a number of less commonly known names, must be defined in class PROGRAM.

Program protection is not a prerequisite for CA-ACF2 Program Pathing controls, although RACF program protection is a prerequisite for RACF PADS, a technique to restrict data access through a specific program. This approach can improve application integrity by enforcing access through certified application programs and eliminating other access (such as editors and other tools). See 6.3.6, “Program Pathing” on page 66 for more details.

### 6.5.11 Tape protection

Although tape is typically not the primary storage medium for production data, tape silos and traditional storage facilities are found in most mainframe shops. The primary uses of tape are for data backup, archiving, and data exchange.

#### 6.5.11.1 Goals

Information on tape should be protected as securely and effectively as data on DASD, preferably by the same rules. Due to the differences in the architecture of disk and tape controllers, and the nature of tape media, some limitations exist.

#### 6.5.11.2 Issues

When securing data on tape, it must be noted that:

- Multiple data sets on tapes cannot be secured separately. Therefore, protection must be limited to the volume level, or a user must implement procedures not to store information with different protection requirements on the same tape.
- Tape labels contain only the last 17 characters of the 44 character data set name. The full data set name for security checking must therefore be obtained from other sources, such as a tape management system.
- There is often a need to process *foreign* tapes, that is, tapes received from other organizations containing unknown data set names. They are typically used in “bypass label processing” (BLP) mode.
- Tapes are likely to be shipped or stored outside the physically secured computing facility, and CA-ACF2 or RACF protection is not effective. Data encryption is often used to protect such information.

#### 6.5.11.3 Terminology

CA-ACF2 and RACF use slightly different approaches to protecting tape and to granting privileges to bypass tape protection:

- TAPE-BLP attribute in the CA-ACF2 logon ID record grants full BLP processing. The RACF equivalent is a user's access authority on the access list of the ICHBLP profile in class FACILITY. READ access provides the ability to read a tape in BLP mode, UPDATE access permits reading and writing to it.
- TAPE-LBL is a similar attribute that grants limited BLP privileges; there is no direct RACF equivalent.
- TAPEDSN is the name of similar options in CA-ACF2 and RACF. It activates access checking for tape at the data set level.
- SECVOLS in CA-ACF2 defines a limited list of volumes (disk and tape) for which access control is performed at the volume rather than the data set level. The RACF equivalent for tape volumes is profiles in the TAPEVOL resource class.

#### 6.5.11.4 RACF tape protection concepts

This section describes the recommended approach to protecting tape data under RACF.

***Tape data set protection***

The RACF option SETROPTS TAPEDSN activates tape protection at the data set level through profiles in the DATASET class. This is the recommended standard for all local tape data.

***Tape volume protection***

The activation of RACF class TAPEVOL and the definition of profiles enables access control at the volume level. Tape volume checking is done first and therefore overrides data set level checking. This is helpful when dealing with tapes for which data set names are not defined or not known. You can apply tape volume controls to foreign tapes if your tape management product does not handle this function.

***Maintaining full data set names***

As mentioned earlier, the data set name field in standard tape labels contains only the right most, least significant 17 characters of an OS/390 data set name, which can be up to 44 characters long. There are two potential solutions available:

- Maintaining the full name in a tape management system which makes OS/390 SAF calls to RACF
- In the absence of tape management software, maintaining the full name in a TVTOC, an extension of a TAPEVOL profile

If a tape management system was used with CA-ACF2, its interface issuing OS/390 SAF calls should also work with RACF.

***Archiving on tape***

The use of HSM for automated archiving on tape is a specialized area of tape usage. Provided you establish clear goals for protection of data sets automatically retrieved from tape storage, RACF setup can be fairly straightforward. The issue here is often the handling of retrieved data sets for which the owner is no longer present in the current RACF database.

#### 6.5.11.5 Summary

In summary, the conversion of tape protection should be simple and straightforward. The protection at the data set level should be addressed by the standard rule conversion for DASD, volume level protection should translate easily, and existing tape management systems should interface in a compatible way with RACF.

## 6.6 Converting system-wide security options

This section describes some of the system-wide security options for both CA-ACF2 and RACF. These options determine how the security product is protecting your system. The best conversion solution is presented for the system options of CA-ACF2 and how to implement these with RACF security. A table is included to show the most direct mapping of some of the CA-ACF2 global system options to RACF's system-wide options.

### 6.6.1 Common system-wide security options

Table 11 displays the system-wide options common to both CA-ACF2 and RACF.

*Table 11. System-wide options common to RACF and CA-ACF2*

| CA-ACF2 GSO RECID | Description | Equivalent RACF implementation |
|---|---|---|
| AUTHEXIT | Provides for extended user authentication | RACINIT pre-processing exit |
| AUTOERAS | Indicates the physical erasure of the DASD data set when deleted. | SETROPTS ERASE and data set ERASE flag |
| BLPPGM | Specifies programs authorized to use tape Bypass Label Processing. | ICHBLP profile in FACILITY Class |
| EXITS | Specifies names of installation written exits. | Exits found during RACF start-up are activated. |
| LOGPGM | Specifies programs for which all data set accesses are logged. | AUDIT() operand of ADDSD and LOGOPTIONS |
| NJE DFTLID() | Specifies the default ID for jobs coming into a system. | SETROPTS JES (UNDEFINEDUSER()) or NODES class profiles |
| NJE INHERIT/ VALIN()/ VALOUT | A job sent to a node inherits the submitting Logon ID. | JESINPUT, JESJOBS, and NODES class profiles |
| OPTS DFTLID() | Specify default user ID is assigned to batch jobs that enter the system and do not have a execution user ID assigned. | NODES class profile ADDMEM(user ID) |
| OPTS DFTSTC() | Specify default STC ID. | Started class profiles or ICHRIN03 |

| CA-ACF2 GSO RECID | Description | Equivalent RACF implementation |
|---|---|---|
| OPTS MODE() | Specify what actions to take when a violation occurs. | SETROPTS PROTECTALL() and LOGOPTIONS() |
| OPTS TAPEDSN | Tape data set protection. | SETROPTS TAPEDSN and TAPEVOL class |
| OPTS UADS | Specifies if UADS is being used. | The RACF TSO SEGMENT is checked first, then UADS. |
| OPTS XBM | Specifies if JES Execution Batch Monitor support is active. | SETROPTS JES XBMALLRACF |
| PSWD | Defines password controls and options. | SETROPTS PASSWORD() |
| TSO | Defines global TSO usage and system options for TSO logon. | RACF TSO SEGMENT of user ID and TSO/E resource protection |

### 6.6.2 Command Propagation Facility (CPF)

CA-ACF2's Command Propagation Facility implementation and functionality is quite different than RACF's Remote Sharing Facility (RRSF) and cannot be directly converted to RACF. RRSF allows you to administer and synchronize multiple RACF databases in the same location or in a remote environment. RRSF can be as global or as granular as your installation requires without the need for any exits. For instance, you can synchronize some or all commands and/or user passwords automatically or you can specify what commands and/or user passwords are to be propagated to what databases. For more detailed information on RRSF refer to *SecureWay Security Server (RACF) Security Administrator's Guide,* SC28-1915.

### 6.6.3 CA-ACF2 global system options

Some of the CA-ACF2 `GSO` options not listed in Table 11, but which also have to be analyzed, are listed below. Suggestions on how to convert these are offered where possible.

- `BACKUP` - Defines the automatic backup procedures for the CA-ACF2 databases.

  RACF automatically maintains backup copies of profiles in a live secondary (backup) database as defined in the RACF Data Set Name Table (`ICHRDSNT`). You can direct RACF to maintain the backup at a different site.

  For this reason, RACF does not have to perform automatic physical database backups.

- `LNKLST` - Defines libraries that are considered part of the system linklist. This is used with the CA-ACF2 program protection facility. Analyze and document the use of the libraries identified in this record. If the use of these libraries is still valid, consider using PROGRAM control in RACF.

- `OPTS STC` - Validates data set accesses by Started Task Control (STC). The STC user IDs, groups, and privileges are defined in the STARTED class or in Started Procedures Table (`ICHRIN03`).

- PPGM - Defines which users can execute specified programs. To restrict access to programs do the following:
  - Activate the PROGRAM class in RACF.
  - Define a data set profile to protect the library.
  - Define a profile in the PROGRAM class to protect the program.

### 6.6.4 RACF options

This section describes some additional RACF options that are highly recommended when defining system-wide protection for your installation. The following example specifies that all the current RACF options be displayed.

```
SETROPTS LIST
```

Additional RACF SETROPTS parameters can include:

- NOADDCREATOR - Specifies that if a user defines any new DATASET or general resource profile, RACF does not place the profile creator's user ID on the profile's access control list.
- NOADSP - Disallows the automatic creation of RACF discrete profiles. This parameter is strongly recommended.
- EGN - Activates enhanced generic naming (EGN). This option allows you to specify the generic character ** (in addition to the generic characters * and %).
- GENCMD(*) - Activates generic profile command processing for all classes and needs to be re-issued each time a new class is added.
- GENERIC(*) - Activates generic profile checking for all classes except grouping classes, and needs to be re-issued each time a new class is added.
- GRPLIST - Specifies that authorization checking processing is to perform list-of-groups access checking for all system users. When you specify GRPLIST, a user's authority to access or define a resource is not based only on the authority of the user's current-connect group; access is based on the authority of any group that the user is a member of.
- JES(BATCHALLRACF) - specifies that JES is to test for the presence of a user ID and password on the job statement or for propagated RACF identification information for all batch jobs. If the test fails, JES is to fail the job.
- PASSWORD() - Specifies the monitoring and checking of passwords by indicating the following sub-operands. The use of the operands may replace CA-ACF2 logon and password exits:
  - HISTORY() - Specifies that 1 to 32 previous passwords are saved and compared to a new password if specified.
  - INTERVAL() - Indicates the number of days that the current password is valid (1 to 254). This value is used as a default for new users added with the ADDUSER command and is also used as the upper limit for the INTERVAL operand of the PASSWORD command.
  - REVOKE() - Indicates the number of invalid passwords that can be entered before RACF revokes the user ID.
  - RULEn() - Specifies 1 to 8 individual password syntax rules. The rule contains a length attribute and content keywords describing valid passwords. For example:

```
RULE1(LENGTH(8) ALPHA(1:3) CONSONANT(4,8) NUMERIC(5:7))
```

You can use the ICHPWX01 exit to perform additional checks for password rules, such as: the password cannot be equal to the user ID.

- PREFIX() - Enables protection of data sets with a single-qualifier data set name and specifies an HLQ to be prefixed to these data set names during RACF authorization processing. The prefix should be a defined group name and not an existing HLQ.
- PROTECTALL() - Enables protect-all processing. All data sets that do not have a RACF profile cannot be accessed, including data sets on DASD, GDG, and catalogs. Tape data sets are also included if TAPEDSN is active. NOPROTECTALL specifies that a user can create or access a data set that is not protected by a profile.

  The two operands used with PROTECTALL are:

  - FAILURES - Causes RACF to deny access to all data sets that are not protected with a RACF profile. This is the recommended option for production cut-over and should be set as soon as possible during the migration to ensure adequate testing is performed in this mode of operation.
  - WARNING - Causes RACF to allow access to data sets that are not protected by a RACF profile and issue a warning to the user and security administrator. This option should only be used during initial conversion testing to assist in setting up data set security protection.

  The PROTECTALL parameter pertains only to data set protection. General resources are covered only by their existing resource profiles with specified access levels and an optional WARNING parameter. Note that default protection of general resources can be controlled by “catch-all” profiles, such as a profile definition of ‘**’ with UACC=NONE.

For more detailed information on RACF’s system-wide options refer to *SecureWay Security Server RACF Command Language Reference,* SC28-1919.

# Chapter 7. Administration and maintenance

The administration of the security subsystem is an important factor when selecting the subsystem, or when migrating to another one. In general, normal OS/390 users see only the effects of the security system, and very seldom issue commands directly to it. Security administrators, however, frequently issue commands to the security subsystem, and the structure (and convenience) of this process is important to them.

## 7.1 The administrative interface

RACF administration consists of several different categories of tasks:

1. Routine, day-to-day functions, such as adding users, resetting passwords, adding resource protection profiles, and so forth.
2. Higher-level administration, such as adding new `SPECIAL`, `GROUP SPECIAL`, `OPERATIONS` users, setting `AUDIT` controls, and so forth.
3. Setting global RACF controls.
4. Maintaining the database, in the sense of purging unwanted entries, detecting unwanted situations, monitoring the correctness of the security policy reflected by the database, and so forth.
5. Monitoring the audit records written by RACF.
6. Maintaining the database, in the sense of backups and reorganization, monitoring performance, and so forth.

RACF commands are normally used for the first three tasks in this list. There are a number of ways to enter RACF commands, and these are discussed in the following sections.

There are many ways to address the fourth task, database quality maintenance. Using the RACF `SEARCH` command or the `IRRRID00` utility is a starting point, and may be all that is required. In more demanding cases, you might need to write or obtain an application to address this area.

The fifth task, monitoring audit records, involves listing selected SMF records. The RACF report writer (no longer actively maintained by IBM) is an easy starting point. There are many SMF reporting programs, including the SMF Unload utility that is part of RACF, which can be used with DB2 or DFSORT's `ICETOOL`.

The sixth task, physical care of the database, involves several utilities supplied with RACF, and also involves normal OS/390 tuning activities.

## 7.2 Commands

CA-Top Secret and RACF both have their own command sets. In each case, ISPF panels are available to ease the use of the commands, but the underlying line commands are central to understanding the use of the product. Both products have extensive documentation. Refer to *SecureWay Security Server RACF Command Language Reference*, SC28-1919, for an explanation of all RACF commands and syntax.

RACF commands may be entered in a number of ways:

- RACF commands from the TSO command line
- ISPF panels (provided with RACF)
- Batch jobs (which issue the same commands as under TSO)
- Application programs (or third-party products) that issue RACF commands
- RACF commands from OS/390 operator consoles

Most commonly, TSO line commands and the ISPF panels are used for day-to-day administration, and batch jobs are useful for bulk updates.

RACF commands issued from an OS/390 operator's console are very useful in critical situations, but are not intended for routine administration. The operator must have performed a logon function (password authentication) before entering RACF commands. (An exception exists for the operator command that switches to the backup RACF database; an operator logon is not needed in order to issue this command.)

Both products have many commands, and many of these are used only by the security administrator or systems programmers. Only a small part of the full command sets is used daily by other administrators, help desk personnel, and end users.

RACF has four general types of database entities (profiles): User, Group, Dataset, and General Resources. Each of these types has associated commands to add, modify, delete, and list profiles. The following table lists the basic commands for these operations. The table shows, for example, that the ALTGROUP command would be used to alter a group profile.

*Table 12. RACF commands to add, modify, delete and list resources*

| | **User** | **Group** | **Dataset** | **General resource** |
|---|---|---|---|---|
| **Add** | ADDUSER | ADDGROUP | ADDSD | RDEFINE |
| **Modify** | ALTUSER | ALTGROUP | ALTDSD | RALTER |
| **Delete** | DELUSER | DELGROUP | DELDSD | RDELETE |
| **List** | LISTUSER | LISTGRP | LISTDSD | RLIST |

This table is quite simplistic and is not intended to convey any of the ramifications of the indicated functions. More detailed information on the functionality of the RACF commands can be found in Chapter 3, "RACF overview" on page 19. For complete definitions and the syntax of the commands, refer to *SecureWay Security Server RACF Command Language Reference,* SC28-1919.

The various privilege levels of RACF commands are described in detail in previous chapters. A very brief summary, related to the use of RACF commands, may be helpful here:

- Someone with the SPECIAL privilege can issue any RACF command, except those restricted to auditors. (A SPECIAL user can grant himself the AUDITOR privilege, and then issue those commands.) This level is usually restricted to a few security administrators. The SPECIAL user typically issues global RACF commands, constructs important generic data set profiles, defines groups, and delegates Group-SPECIAL authority.
- Someone with a Group-SPECIAL privilege can issue RACF commands that affect only a designated group, or its subgroups. A group may own many subgroups, providing many ways to structure and delegate authority. Distributed security administrators typically have Group-SPECIAL authority for their areas. Help desk personnel may have Group-SPECIAL authority.
- The owner of a profile can issue several RACF commands that affect only that profile. In practice, this means that the owner of a data set profile can control which users (and at what level) can access data sets protected by that profile. The primary command involved is PERMIT.

In the PROTECTALL environment, a RACF profile will already exist for a user's HLQ (created when the user ID was added to RACF). A user can grant permission to other users to access his files. The PERMIT command is used for this, and this may be the only RACF command that typical users issue. In a well-designed environment, with appropriate use of generic data set profiles, most users will never need to issue PERMIT commands.

RACF commands can be issued from OS/390 operator consoles. This should not be regarded as a routine interface for RACF administration, but it can be very useful in an emergency situation. A profile class, OPERCMDS, is used to control which operators can issue which RACF commands. Operators are required to log onto the OS/390 operator console before they can issue RACF commands.

Once the basic command structure is understood, using RACF commands instead of CA-Top Secret commands should not present any problems. The more important migration issues are the organizational processes that occur before any commands are issued.

In practice, CA-Top Secret and RACF commands are usually issued from the TSO command line (more experienced administrators) or from ISPF panels. In both cases, a good understanding of the security policy in use, and the use of consistent naming conventions and group conventions, is key to understanding and using the security administrative commands. In both cases, commands can be batched by using the PGM=IKJEFT01 method of running TSO functions in batch jobs.

## 7.3 RACF utilities

Several utilities are provided with RACF. These are normally used in batch jobs, and address some of the tasks previously listed. These utilities are:

**IRRUT100** This program reads the RACF database, and can search for specified entries. While reading, it checks the correctness of internal index records and other pointers.

**IRRUT200** This program will simply copy the RACF database, checking major structural items as it copies. However, it observes all RACF interlocks for update activities that occur while the copy is in progress. This ensures a logically consistent copy. `IEBGENER` can be used to copy a RACF database, but it does not observe such interlocks and, if there are RACF updates during the copy, it may not produce a complete copy.

**IRRUT400** This program also copies the RACF database, but it reorganizes it at the same time. It can split the database into multiple data sets (for performance) or merging multiple data sets back into one. `IRRUT400` can rebuild internal index records, and generally corrects small structural errors.

**IRRADU00** This program unloads the security relevant SMF records into sequential records. It is readable by a person, and can be used as input to external programs.

**IRRDBU00** This program unloads the RACF database into sequential records, with fields specified in EBCDIC characters. It is readable by a person, and can be used as input to external programs. For example, some installations load this data into DB2 and perform what if searches there.

**IRRRID00** This program searches an unloaded RACF database for user IDs and groups that are about to be removed from the installation. You can specify the user ID or group that will replace these departing user IDs and groups.

## 7.4 Security reports

Reports are important for security administration, in order to enable tracking and monitoring of events and status of the security environment established, and to uncover changes that could lower or change the expected security level. The problem is to collect and get the correct data to meet the objectives. Too many organizations collect too much data, without having any plan or strategy for its use.

There are two levels of reporting for OS/390 security subsystems. One level reflects the contents of the security database, and describes what is protected and how it is protected. This is called *status monitoring*. The other level reflects the security events that occurred during a particular period; for example, which users logged onto the system, or what attempted security violations were detected. This is called *event monitoring*.

For both CA-Top Secret and RACF, event monitoring is centered around SMF records. There are many programs and products available for listing SMF records.

The usefulness of event monitoring depends on what is monitored; that is, what causes an SMF record to be written? CA-Top Secret and RACF have options to control which events cause an SMF record to be written. RACF has an orderly structure of auditing controls for this purpose. Controls exist at both individual profile levels and at the global level. Since a profile can be used to protect a single data set, or to protect a large number of data sets (with similar higher-level qualifiers), auditing controls can be selective.

RACF controls can be set to write SMF records on either access failures (where data set access was prevented by RACF), or on access successes (where data set access was permitted by RACF). In general, reporting of successful accesses is not desired, partly because the volume of SMF records would be too large. However, successful access reporting may be appropriate for a carefully selected set of application data sets. Access failure events are typically used to create an SMF record, and a basic part of the security administrator's duties is to review these records.[1]

RACF can also log (to SMF) changes to the RACF database itself, and records are created indicating changes to user profiles with any of the high-level authorities, such as SPECIAL, should always be reviewed. Some of the key global controls of RACF, related to auditing, are:

- SAUDIT is used to log all commands that need a SPECIAL user privilege. This is used to review activities by these privileged users. It can also be used to recreate profiles and commands from SMF data in an emergency.
- OPERAUDIT is used to log all data accesses a user with the OPERATIONS privilege is granted, due to this privilege. Access through normal access rights are not logged.

  Use both SAUDIT and OPERAUDIT to enable auditing of privileged users and their activities.
- CMDVIOL is used to switch on/off RACF command reporting; CMDVIOL will record all attempts to use RACF commands outside a user's authority.
- LOGOPTIONS are used to specify logging options for different resource classes, from no logging to full logging. These can be used to globally force logging of resources in one class to avoid having to specify the AUDIT option on each profile.
- GLOBALAUDIT can be specified by someone with the AUDITOR privilege. This generates audit data without requiring that specific profiles be selected for auditing.

In addition to these global and class options, each resource profile can have its own audit requirements defined through the AUDIT option, from no logging to full logging. This setting will not lower the logging requirement set by the LOGOPTIONS value for that class. All profiles have a default AUDIT setting; for example, for data sets it is AUDIT(FAILURES).

[1] There are many different approaches to this. Some installations want to review every access failure, while others check only for substantial patterns of access failures. An access failure is not a security failure; it is simply an indication that the security subsystem was doing its job. In practice, reviewing every access failure tends to be impractical.

In addition to the various logging options mentioned here, all invalid password attempts are logged by default.

UAUDIT can be set on a user profile to cause all RACF activity for that particular user to be logged. It is an effective way to trace all activities of a user, but must be used with some restraint to avoid writing too many SMF records.

Status monitor involves listing control settings in the security database, and monitoring changes to these controls. SMF records, written by RACF, are useful for detecting changes, while static information must be extracted from the database itself. Several tools are provided by RACF:

- DSMON (Data Security Monitor) is a program for reporting on several security settings, user privileges and protection status of important system data sets. It should be run regularly to monitor any changes to any of these security areas.
- The RACF ISPF panels offer a number of options to display various control settings.
- RACFRW (RACF Report Writer) is an ad hoc reporting program. The Report Writer has been stabilized, so new functions will not be reported. The traditional RACF functions such as data set and resource violations can be reported.
- The IRRDBU00 utility-produced flat file can be used in a number of ways: through locally-written programs, by loading it into DB2 and executing searches there, or by using any standard report-writing software.
- The IRRADU00 utility-produced flat file can be used in a number of ways: through locally-written programs, by loading it into DB2 and executing searches there, or by using any standard report writing software.
- The RACFICE reporting tool utilizes the ICETOOL function of DFSORT to produce various reports using the output of IRRDBU00 or IRRADU00, or both.
- The IBM Performance Reporter product can also be used for RACF reporting and comes with 11 canned reports for RACF.

In summary, log and audit functions are an important part of an organization's security policy. The security policy should clearly define what is expected for logging and audit, and how it will be used. This requires some skill and experience, since a balance is needed between what is practical, the effects on performance, the problems of generating too much data, and so forth.

## 7.5 Availability considerations

CA-Top Secret and RACF, when fully implemented and used, are both functions critical to an OS/390 production environment. Their availability and recoverability must therefore be carefully designed, planned and tested. Due to different technical features and capabilities of the two products, recovery techniques and strategies differ. Approaches to RACF recovery are discussed in the following sections.

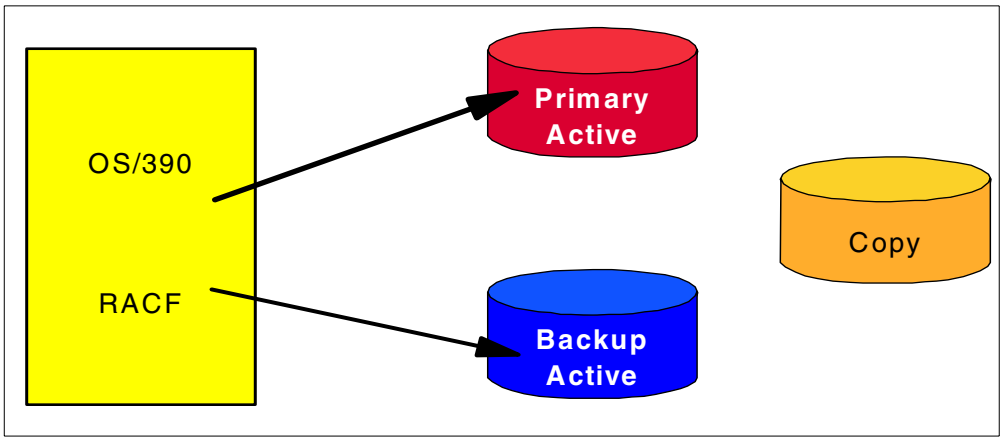


*Figure 29. RACF primary and backup data sets*

### 7.5.1 RACF active backup option

A unique recovery feature in RACF is the active backup data set option, the commonly used option to maintain a software mirror image of the primary RACF database.

While RACF performs all authentication and authorization checking against its primary database, all updates are automatically duplicated onto the active backup database. In case the primary database is lost, a switch to the backup database can be performed without the need for an IPL or other recovery procedures.

#### 7.5.1.1 RACF database backup

The initial setup of the RACF recovery environment requires defining the name of the backup data set in the RACF Dataset Name Table `ICHRDSNT` and making a copy of the primary database (while no updates are taking place). Good recovery strategies also have provisions to periodically take additional backup copies (independent of the active backup). We believe that the best tool to create such copies is the RACF verify utility program `IRRUT200`; this program enqueues on the input database for the duration of the copy process and has the additional advantage that it provides an analysis of the database structure. The `IRRUT200` list output can be used to determine the degree to which the database is full and to identify potential structural problems that need to be addressed.

#### 7.5.1.2 RACF database recovery

When a problem with the primary RACF database is discovered, an `RVARY SWITCH` command is issued on the system console or in a TSO session to initiate a switch to the active backup database. This one now becomes the primary database and the original primary is deactivated. The system continues to run with just a

primary database, and the creation and activation of a new backup database is scheduled for a period of low activity.

To avoid false alarms, this switching capability is secured by a password under the control of the central security administration; this feature can be used to enforce procedures that require the involvement of security management in any RACF status change.

### 7.5.2 Reorganizing the RACF database

Some organizations include periodic reorganizations of their RACF databases in their backup and recovery plans. In a quiesced environment, use the RACF split/merge utility `IRRUT400` to create a “logical” copy of your RACF database (specify one input and one output file). This process eliminates CI-like splits in the database structure and profiles that have been logically deleted (no pointers in the index structure), but may physically still be present.

## 7.6 RACF performance considerations

There can be a conflict between your ideal security policy and the performance practicalities of the security subsystem. Controlling CICS transaction accesses is an example of a function that can be torn between security needs and performance needs. Extracting the best performance from the security subsystem involves these areas:

- Using global options that short-circuit the rest of the security monitor.
- Using some type of cache in main storage.
- Using special coding options in applications that result in an unusually fast response by the security subsystem.
- Using a good design for sharing the database file among multiple systems, since the need for a shared security database is common.
- Using normal DASD tuning techniques to improve I/O response.

Both CA-Top Secret and RACF provide options in all these categories. Some of these are not simply performance options; they affect the policy design of the security database and should be considered part of your high-level design.

Some of the key RACF features in this area include:

- Global Authorization Check (GAC) - RACF uses this in-storage table to make quick decisions about whether further RACF checking is needed.
- RACLIST refers to the process of moving a complete RACF CLASS of profiles into storage, for faster access.
- In-storage buffers refer to the allocation, in main storage, of a given number of buffers that are managed by RACF with a type of Least Recently Used (LRU) purging technique.
- RACF can take advantage of the Coupling Facility to further improve performance

If not deflected by a Trusted or Privileged property, RACF checks the GAC when beginning to process an access request. The GAC is an in-storage table owned by RACF. It is copied into storage when RACF is started, and is static during

operation, unless updated by a security administrator. It is usually a very small table. The most typical use is to grant permission to access (in any manner) a data set with the same HLQ as the caller. That is, a user can work with his own data sets (as identified by a matching HLQ) without any further checking by RACF. The GAC can contain lists of exceptions to the general rules it sets, causing the normal profiles to be checked for these exceptions.

This process can provide excellent performance. The exposure is that no other RACF controls are checked. If, for example, the GAC gives all users `READ` access to all `SYS1` data sets, then no `SYS1` data sets can have a general access level of `NONE` because the profiles that try to establish this condition are not checked. The use of a GAC entry bypassed them. The use of the GAC table is important for performance, but the usage must flow from the overall security policy being defined.

The installation can specify a certain amount of buffer space to be dedicated to a RACF cache, known as *in-storage buffers*. This space is in protected common storage. It is pagable, but for practical purposes can be regarded as fixed because it is referenced frequently. The use of this cache is transparent to policy design, and is a pure tuning function. (The cache is limited to RACF elements that are normally read-only, or write-through cache data. The RACF database, on disk, must always reflect current data to other OS/390 systems sharing the same database.)

RACF can manage a *backup* database, in addition to its primary database. Practically every installation elects to have a backup RACF database. We do not consider deleting this to be a reasonable action. In addition to profile updates, RACF writes statistical data in its database, for example, the date and time of a users most recent TSO logon. There is an option to bypass updating the backup database with statistical data. Many installations select this option. In the rare event of a database failure, requiring use of the backup RACF database, some statistical data will be missing. This is usually considered a reasonable tradeoff.

Customers can make use of OS/390's virtual lookaside facility (VLF) to cache ACEEs and information for OS/390 UNIX. If RACF finds information in VLF, it will avoid I/O to the database.

RACF can use "split databases", meaning the database can be divided into multiple files, on multiple volumes. (The backup database can also be split.) RACF still uses it as a single logical database. By placing parts of the database on different volumes, different control units, and/or different channels, normal DASD data set tuning techniques can be applied.

Splitting the RACF database is transparent to security policy decisions. RACF offers a special high-performance interface, `RACROUTE REQUEST=FASTAUTH`, commonly known as `FASTAUTH`. Programs must be specially coded to use it; it is not used by automatic system calls that go through SAF. CICS is the major example that can use `FASTAUTH`. The `FASTAUTH` function references only in-storage tables (placed in storage by the `RACROUTE REQUEST=LIST` function), providing major performance benefits over standard authorization that involves disk database inquiries.

The `IRRUT400` utility, supplied with RACF, can be used to reorganize the database. Database performance may degrade slightly over time, as updates and changes occur. The effect is usually fairly minor, unless very large databases are involved

or many profiles have been added and deleted. A typical installation might use this utility to reorganize the database every six months.

### 7.6.1 Performance of shared databases

Sharing a database, CA-Top Secret or RACF, among multiple OS/390 images has become common. This has a number of interesting effects on performance design, including:

- The use of cache functions becomes more restricted, since the corresponding disk record could be updated by another system, making the cached data invalid.
- Extensive use of RESERVE and RELEASE functions (disk locking commands) can badly impact the performance of a shared disk.
- The use of a disk API (access method) that is not optimized for shared system usage can badly impact performance.

RACF uses a low-level, proprietary API for disk access. It does not use VSAM. The RACF design is optimized for shared-system use and should automatically provide a major performance boost compared with shared-VSAM usage.

The RACF use of cache (in-storage buffers) is based on a design that avoids cache coherency problems in the presence of shared-system operation.

The elements of RACF operation that affect shared-system performance are all automatic. There is no user tuning involved. The tuning items discussed are effective in both single-system and multi-system environments.

The Coupling Facility allows OS/390 and other software to share data concurrently among multiple systems in the sysplex with the goal of maintaining a single system image. A sysplex with a Coupling Facility significantly changes the way systems can share data. *Data sharing* is the ability of concurrent subsystems or application programs to directly access and change the same data, while maintaining system integrity. RACF can take advantage of the Coupling Facility in the sysplex to provide security for the resources of all systems in a comprehensive and centralized way. RACF allows you to use the Coupling Facility and shared RACF data to help manage the security of resources for all systems in a sysplex.

### 7.6.2 Migration issues

The complete PPT should be reviewed manually, as part of any migration effort. Other performance elements, especially the GAC, should be created manually.

Performance elements that do not interact with policy design, such as in-storage buffers and database splitting, can be managed independently from the migration process itself. If the basic migration process, normally through the use of specialized software tools, provides acceptable performance, then it may be advisable to postpone tuning these elements until the end of the migration project.

A CICS installation would certainly want to enable FASTAUTH checking for its own applications or program products as part of the migration. This should provide a substantial performance improvement, as well as integrate CICS usage into normal RACF operation.

### 7.6.3 Summary

Tuning can make a major difference in security subsystem performance. RACF offers a number of major tuning options. Some of these interact with the security policy goals of the system, and this aspect must be considered in the overall design of the RACF implementation. With reasonable designs, RACF can offer significant performance improvements, especially for key areas such as CICS.

# Appendix A. IBM migration services

IBM offers a number of migration services, including CA-Top Secret to RACF migration assistance. For a migration project of this scope and magnitude, it is advisable to secure the services of someone who has done migration projects before. The skills needed for a migration are unique and probably will not be needed by an organization after completion of the project. IBM's Software Migration Project Office (SMPO) offers migration services which can be tailored to the client's needs. The following is a brief overview of the migration services.

## A.1 Mainframe system software

In the evolving world of client/server computing, many customers are redefining the role of their mainframes, and re-evaluating their mainframe system software. They are choosing products that not only perform well today, but that are capable of participating in the evolving world of open systems and enterprise-wide computing. They are choosing vendors who offer quality products and quality support, and who offer flexible terms and conditions that allow the software to change as the customer's requirements change. Increasingly, customers are choosing IBM software as a base for their enterprise computing needs.

## A.2 Migration services

Choosing the right product is one thing, but changing mission-critical software can be another. To accomplish the migration with the least disruption to their business, many customers seek expert assistance.

IBM's migration services are designed to minimize the time, risk, and total cost of changing critical system software. By assisting many customers with such migrations, IBM has developed skills, tools, and experience which can be used to assure a successful migration. Our approach is to leverage IBM's experience and tools, along with the customer's knowledge of their systems, to create a cost-effective team. This team approach also allows a great deal of skills transfer to take place naturally throughout the migration, so that when the migration is complete, the customer's staff is able to manage the new environment productively.

## A.3 Conversion vs. migration

One important consideration when choosing migration services is the difference between a conversion and a migration. A *conversion* refers to the translation of the operational data from one format to another. A *migration* project is a much broader effort, beginning with project assessment and planning, continuing with installation and testing (including conversion activities and tools), and ending with final cutover. Though the conversion phase is very important, it is only one piece of a full migration project.

## A.4 Migrations - no two are alike

Most customers have had their mainframe system software installed for some time. Over that time, the software has evolved, and each customer has uniquely

customized their software to better fit their needs. While this customization makes the product more valuable, it also makes the migration more complex. Complexity, along with the amount of skill, resource, and focus that each customer is willing to dedicate to a migration effort, makes each migration unique. As such, each customer will require a different amount of assistance, take a different amount of time, and have a different total cost for completing the same product migration.

## A.5 Migration service offerings

IBM's migration service offerings have a flexible, modular structure to allow each customer to choose the type and amount of service that is needed to meet that customer's needs. While the details regarding specific product migrations differ slightly, the general structure of IBM's migration service offerings is as described in the following sections.

### A.5.1 Migration assessment service

Performed by a migration specialist, this service assists the customer to assess the time, effort, skill requirements, and feasibility of migrating from their current environment. By analyzing reports and extracted data and by interviewing technical staff and management, the migration specialist can create a documented assessment report and review it with the client.

### A.5.2 Database conversion service

IBM can bring customized conversion tools to bear on many of the product migrations. Fixed priced offerings include the customization, usage, and support of the conversion tools.

### A.5.3 Migration consulting services

Migration specialists, experienced from other, similar migrations, are available to provide guidance with a wide variety of migration activities. Typical uses of migration consulting are:

- Migration planning - leading a customer/IBM team to create a documented migration plan, including detailed task list, target dates and people assignments.
- Technical analysis - analyzing the current implementation of the installed product and offer alternative ways of implementing functions using the new product.

Consulting services are typically billed on an hourly basis.

### A.5.4 Migration perform services

IBM Global Services are available to perform many of the tasks required to complete the migration.

Some of the services available are:

- Product installation and customization
- Implementation of new function
- Exit design and/or coding

- Testing, test planning, and validation
- Operations skills transfer
- Project management

Perform services are typically billed on an hourly basis.

### A.5.5 Learning Services

Through IBM Learning Services, a variety of education alternatives are offered. Product classes, as well as migration classes, are available. Classes are available through a per seat, or onsite private class arrangement.

## A.6 Product migrations

IBM can assist in a wide variety of product migrations. IBM's Software Migration Project Office specializes in MVS system software migrations including:

- CA-ACF2 to RACF
- CA-Top Secret to RACF
- CA-7 and CA-11 to OPC/ESA
- Control-M and Control-R to OPC/ESA
- Jobtrac and Runtrac to OPC/ESA
- Zeke and Zebb to OPC/ESA
- CA-Scheduler to OPC/ESA
- CA-Manager to OPC/ESA
- CA-1 to DFSMSrmm
- CA-DYNAM/TLMS to DFSMSrmm
- CONTROL-T to DFSMSrmm
- ZARA to DFSMSrmm
- MVS (OS) Catalog to DFSMSrmm
- CA-IDMS to DB2 Family
- Adabas to DB2 Family
- CA-DATACOM to DB2 Family
- TOTAL to DB2 Family
- Model204 to DB2 Family
- VSAM to DB2 Family
- CA-LIBRARIAN to ISPF/PDF SCLM
- Panvalet to ISPF/PDF SCLM
- CA-OPS/MVS II System Automation for OS/390 (SA OS/390)
- Boole & Baggage Auto Operator to SA OS/390
- Candle's AF/Operator to SA OS/390
- NetMaster to Tivoli NetView for OS/390
- CA-Opera to SA OS/390
- CA-Zak to SA OS/390
- CA-Netman to Tivoli Service Desk for OS/390
- Remedy to Tivoli Service Desk for OS/390
- Peregrine to Tivoli Service Desk for OS/390
- Heat to Tivoli Service Desk for OS/390
- SLR to Tivoli Decision Support for OS/390
- CA-MICS to Tivoli Decision Support for OS/390
- IT/Service Vision to Tivoli Decision Support for OS/390
- MXG to Tivoli Decision Support for OS/390
- CA-JARS to Tivoli Decision Support for OS/390
- Komand to Tivoli Decision Support for OS/390

- CIMS to Tivoli Decision Support for OS/390
- CA-NetSpy to NPM (NetView Performance Monitor)
- CA-TPX to NVAS (NetView Access Services)
- CA-MAI to NVAS (NetView Access Services)
- CMF to RMF (Resource Measurement Facility)
- Connect Direct to TDE (Tivoli Data Exchange)
- CA-Sterling Netmaster TCP/IP (Manage) to NPM/IP (NetView PerformanceMonitor for IP)
- CA-DISPATCH to OnDemand
- CA-VIEW/DELIVER to OnDemand
- INFOPAK to OnDemand

## A.7 Getting started

All security projects are high-risk, high-visibility projects. Managing and controlling the levels of risk are integral parts of project planning, project management, and testing methodologies. Good project planning insures that all tasks, problems, and issues are documented and tracked to solution. Good testing not only ensures that individual problems and issues are tested, it also ensures the total environment is tested. Good project management ensures the project plans and testing is adhered to. Without these elements, the risks are high; with them, the risks can be controlled to acceptable levels.

For additional information, or to discuss how IBM's migration service offerings can be tailored to fit your needs, contact your IBM Client Representative.

# Appendix B. Security policy considerations

Various aspects of security policies have been addressed throughout this document in the context of specific technical discussions. This appendix is intended to consistently summarize policy implementation and enforcement in RACF.

We address general policies such as complete RACF control over users and resources, naming conventions and resource ownership; we also include discussions of effective and efficient security administration policies and RACF resource utilization.

We do not address mandatory access control policies because we have not observed implementations of these policies in commercial environments.

## B.1 User identification

The recommended policy requires that, except for an initial migration, all users must be identified and verified by RACF; in other words, undefined users are not permitted. RACF principally allows for undefined users for two reasons:

- To support an initial migration to a secured environment, and
- To ensure uninterrupted system availability

Techniques to prohibit undefined user IDs vary with the processing environments, as outlined in the following sections.

### B.1.1 Batch

`SETROPTS BATCHALLRACF` is a global RACF option that enforces the requirements for all batch jobs to have a valid RACF user ID, either through coding USER=user ID on the job statement or through propagation (inheritance).

### B.1.2 TSO

To prohibit undefined TSO users, all user IDs defined in SYS1.UADS must also be defined to RACF. The recommended implementation is to use RACF TSO segments for all TSO users and to keep only a few emergency user IDs in SYS1.UADS. In any case, procedures must be implemented to ensure that the RACF database and whatever entries remain in SYS1.UADS are synchronized, and that user IDs deleted from RACF are also removed from the SYS1.UADS data set.

### B.1.3 Started procedures (STC)

Started procedures are considered part of the computing environment that is essential to the availability and functionality of the MVS system. IBM has therefore implemented RACF STC support with focus on availability, i.e., with the goal to allow rather than disrupt the start of procedures. Procedures will start with an undefined user ID under the following conditions:

- The STC user ID (either assigned specifically or through the generic entry in the STC table) is not a RACF-defined user ID, or
- The user ID is not connected to the group specified in the table

Undefined user IDs for started procedures can be prohibited by coding a generic entry containing a default ID such as */STCDEF/STCGRP and by ensuring that all entries in the table are error-free.

User IDs that are assigned to started procedures should have the PROTECTED attribute. Protected user IDs are user IDs that have both the NOPASSWORD and NOOIDCARD attribute. Protected user IDs cannot be used to logon to the system, and are protected from being revoked through incorrect password attempts.

A started procedure can gain access to RACF-protected resources in the following ways;

- By the user ID or group name assigned, as for any other user of the system.
- By having the privileged attribute, which allows the started procedure to pass all authorization checking. No installation exits are called, no SMF records are generated, and no statistics are updated. Use this option with extreme caution.
- By having the trusted attribute, which mean the same as privileged, except that you can request an audit using the `SETROPTS LOGOPTIONS` command.

Policy enforcement for all environments can be complemented by monitoring SMF audit trails and, if required, by coding a RACINIT exit terminating all requests for establishing a RACF environment for the default user ID.

## B.2 Resource protection

The recommended policy requires default protection; that is, the prohibition of access to unprotected (undefined) resources. The techniques used in RACF to implement such policy vary with the type of resource, as described in the following sections.

### B.2.1 Data sets

Default protection for data sets can be activated through `SETROPTS PROTECTALL(FAIL)`. When turned on, unprotected data sets can only be accessed by system-level SPECIAL users. WARN mode is available to ease migration.

### B.2.2 Transactions and other resources

Default protection over general resources can be achieved through a variety of controls:

- Program logic in resource managers calling RACF
- Settings in the RACF CDT
- Catch-all profiles with UACC=NONE and restrictive specific access

We recommend catch-all profiles because the logic applied by resource managers may not always be known, and changing CDT entries for existing resource classes may not be desirable.

## B.3 Authentication

Policy to establish personal accountability must address user behavior as well as strong technical authentication mechanisms. RACF standard user authentication is based on user-selected passwords; another technique supported is RACF passtickets.

### B.3.1 Passwords

Two separate issues must be addressed for RACF passwords, the technique through which passwords are secured when stored in the RACF database and password quality controls.

The recommended standard for password protection is DES encryption. Starting with RACF release 2.1, this is the default. For earlier releases, the RACF exit ICHDEX01 must either be deleted or modified to select DES encryption instead of password hashing.

Password quality controls are `SETROPTS PASSWORD` options, as listed below (together with generally recommended settings):

- rule1(length(6,8) alphanum(1,8) - minimum length 6, alphanumeric with a least one character being numeric
- interval(30) - expiration after 30 days
- history(32) - remember 32 previous passwords
- revoke(3) - revoke ID after 3 invalid password attempts

A related `SETROPTS` option is:

- inactive(30) - revoke user ID after 30 days of inactivity

### B.3.2 Passtickets

RACF offers advanced authentication through passtickets, which are generated by specific products supporting this form of user authentication.

## B.4 Naming conventions

Recommended policy is to establish and enforce adequate naming conventions for all subjects and objects. The RACF support of such policy is discussed in the following sections.

### B.4.1 Data sets

Native RACF strictly enforces data set high-level-qualifier (HLQ) naming conventions; in a `PROTECTALL(FAIL)` environment, only HLQs that match user IDs or group names can be created or accessed. Naming convention tables and exits can be used to transform other naming conventions to the RACF standard.

The enforcement of standards beyond the HLQ is possible but may not always be practical because it limits the use of high-level generic dataset profiles (such as HLQ.**).

### B.4.2 Other resources

The use of catch-all profiles helps enforce naming conventions for general resources; generic profiles, if used, must be designed accordingly.

### B.4.3 Users and groups

User IDs and group names are not controlled by RACF in a way that allows enforcement of local naming standards.

## B.5 Ownership

Recommended policy is to assign resource ownership to business managers responsible for an application or business area. RACF practice suggests group ownership of profiles and offers an approximation to policy, provided the group structure reflects applications and business areas adequately and custodians are properly assigned as group administrators.

## B.6 Security administration

Recommended policy addresses many aspects of security administration; some can be supported by RACF, as discussed in the following sections.

### B.6.1 Structure

Security administration tasks are typically performed within the following structures:

- Central security administration
- Group administration or functional delegation
- Help desk

Mandatory central security administration uses the RACF system-level `SPECIAL` attribute to define or alter all but a few profiles and options in RACF. To set or change some specific audit-related settings requires the system-level `AUDITOR` attribute.

Optional group administration in RACF is based on `group-SPECIAL`, which provides authority within the scope of a group, or on a privilege called class authorization (CLAUTH), or both. Most policy requirements for group administration can be met by assigning `group-SPECIAL` and possibly CLAUTH, and by defining the scope of authority (based on group ownership).

Typical help desk functions such as user ID RESUME and password RESET can be implemented through the RACF FACILITY class, `group-SPECIAL`, or organizations have chosen other (limited) solutions through special programs that run authorized and use authorization schemes other than `group-SPECIAL`.

### B.6.2 Effectiveness

Recommended policy requires security administration to be effective, i.e., to minimize potential risks through errors and omissions, particularly in the area of temporary access and authorization. Typical precautions are automatic expiration dates on user IDs and permissions. RACF provides the direct ability to expire

user IDs automatically through coding `REVOKE(date)` in user definitions; for permissions, expiration dates can be established indirectly through group connections.

### B.6.3 Efficiency

Recommended policy also requires security administration to be efficient, to ensure that administration workload problems do not contribute to risks.

Efficient RACF administration uses two main elements: generic profiles, and group authorization on access lists. The use of generic profiles reduces, in comparison with discrete ones, the number of profiles to be defined and maintained. Using groups instead of user IDs on access lists dramatically simplifies the management of a changing user population.

## B.7 Audit considerations

Recommended policy requires a reasonably complete audit trail and firm procedures to monitor and review security events and status information.

### B.7.1 Logging

RACF provides an audit trail of security-related events through SMF; the nature and amount of information recorded is controlled by RACF options and profile definitions as discussed below:

- `SETROPTS SAUDIT`, `OPERAUDIT CMDVIOL` and `INITSTAT`S are the recommended standard settings, which include privileged user activities.
- `AUDIT(SUCCESS(UPDATE) FAILURE(READ))` is the recommended standard profile option, unless specific reasons exist for different settings.
- The RACF Global Table should not cover any resources for which an audit trail is needed.
- `UAUDIT` should be used rather carefully because, if used generously, it may create a significant amount of noise records.

### B.7.2 Event monitoring

Recommended policy requires regular event monitoring. We recommend putting as much emphasis on success as on detected violations. RACF provides four reporting options:

- Data Security Monitor (DSMON) provides “canned” RACF database and OS/390 auditing reports.
- The RACF report writer allows for ad hoc violation reporting.
- The database unload and SMF unload feature allows you to unload the RACF database and violation records from SMF into flat files.
- The RACFICE reporting tool includes over 30 sample reports, and uses the DF/SORT ICETOOL report generator.

### B.7.3 Status review

Recommended policy requires periodic security status monitoring and full security audits. The RACF DSMON utility provides basic event monitoring capabilities. The RACF data unload utility converts SMF records into a format that can be easily processed by a relational database or other tools. For detailed information on RACF reporting tools, visit the RACF Web site.[1] For more detailed monitoring, or for a full analysis, third-party tools should be considered.

## B.8 Resource utilization

Recommended policy and common sense require that the security monitor's performance impact be minimal.

### B.8.1 Performance options

RACF offers key performance options that should be used in order to comply with policy:

- Resident blocks in the RACF data set name table - recommended value 255
- Global table entries for trivial access in class DATASET - recommended entry &RACUID/ALTER

### B.8.2 Potential performance impact

Performance impacts may be caused by the following RACF practices:

- Extensive use of discrete profiles in class DATASET
- Poor use of generic profiles, such as a huge number of profiles under one HLQ
- No global table in large TSO environments

[1] OS/390 Security Server Audit Tool and Report Application (SG24-4820)

# Appendix C. Frequently asked questions

**Q.** When protecting an HLQ for a production application (when there is no user with a corresponding user ID), when should I use a group name for the HLQ and when should I simply create an artificial user ID? Why?

**A.** Defining a group is the normal approach and this is a normal use for group definitions. We recommend using user IDs only for real users. (Some exceptions exist; artificial user IDs might be used for started task control, for example.) There is no strong technical reason for this recommendation; it is simply that using groupids provides a more orderly way to manage access to application data sets.

**Q.** Can I prevent users from PERMITing access to files they own? How?

**A.** Yes. The most global way to do this is to remove access to the `PERMIT` command. However, we recommend that you do not do this unless there is a particular, pressing need. Experience has shown little need to hide the `PERMIT` command.

**Q.** How can I control the number of PERMITs created by a user? Should I worry about this?

**A.** Again, experience has shown that this is not normally a problem to worry about.

**Q.** Do I need to reorganize the RACF database? Also the backup database? How often?

**A.** The IRRUT400 utility can be used to reorganize the RACF database.

Experience has shown that this does not need to be done frequently. Some installations never reorganize their database. Others do it every month or so. Reorganizing every six months seems to be a medial position. The backup database is subject to the same reorganization process.

**Q.** Can I make simple backups of the RACF database? (Without the complication of using IDCAMS?)

**A.** IDCAMS is never needed with RACF. You can use the IRRUT200 utility provided with RACF. You could use something as simple as IEBGENER, although IEBGENER (or other similar utilities) will not interlock with RACF to provide a self-consistent copy. IRRUT200 provides the proper interlocks (without effectively stopping RACF) so that partly updated profiles will not be copied.

**Q.** Can I administer RACF from CICS?

**A.** This ability is not part of the basic RACF product. There are third-party tools that provide this ability. Some installations have written their own tools, often based on submitting a jobs from CICS (via an internal reader) that executes the appropriate RACF commands. We do not recommend this approach unless you have the skills to assure the security of design. Note that APPC interfaces can also be used to schedule RACF administrative commands.

**Q.** What authority does a help desk need?

**A.** A help desk, especially one that is related to a specific set of departments, is often given access via the RACF Facility class parameter or GROUP SPECIAL authority for those departments. This permits the help desk personnel to make almost any RACF adjustments to users who are members of the groups associated with these departments.

There is considerable debate over what authority is appropriate for help desk operations. The trend is to give them less absolute authority, and more tools to perform specific functions. This debate is more related to appropriate security policy than to specific RACF functions.

**Q.** How do I add a segment to an existing user ID? For example, add CICS to a TSO user?

**A.** The `ALTUSER` command provides this function.

**Q.** What do I need to do to share my RACF database between multiple OS/390 systems?

**A.** Nothing; this function is automatic. You need the appropriate shared-DASD hardware, of course. If sysplex functions are available, a higher-performance mode of sharing can be used.

A major difference between sysplex and a conventional large computer systems is the improved growth potential and level of availability in a sysplex. The Coupling Facility allows OS/390 and other software to share data concurrently among multiple systems in the sysplex, with the goal of maintaining a single system image.

**Q.** Someone gave me some interesting programs that use the RACF `ICHEINTY` set of macros. Should I consider using these?

**A.** The `ICHEINTY` macro is the low-level interface to the RACF database. At this level, RACF does not check updates for consistency. A poorly designed program issuing these macros could destroy your database, or, worse, introduce subtle errors that grow over time. We recommend not using this level of interface unless you really trust the design of the program issuing the commands, or have a very unusual requirement. There are helpful and trustworthy programs that use `ICHEINTY`, but there is no easy way to determine if your programs are in this trustworthy and useful group.

**Q.** I want to see my RACF database contents. The TSO commands and ISPF panels only deal with a small number of elements at one time, and I cannot get an overall picture of what is in the database. How can I do this?

**A.** You can use the RACF database unload utility. With it, you can see every profile in the database, in a printable format. For anything larger than a trivial database, this may not be useful for direct human viewing. It can be used as input to other (locally written) programs, or be used to load DB2 or something similar. The RACF `SEARCH` command can be used to find and display profiles. The RACFICE reporting tool is available, which includes over 30 sample reports, and uses the DF/SORT ICETOOL report generator.

**Q.** Do I need to train all my users for RACF?

**A.** Probably not, especially if you have a well-designed group structure and well-designed generic profiles. A relatively short note might be used to inform users about any changes in logon processing.

Your help desk staff and your group administrators may require more education.

**Q.** Can I list the passwords of my users? I have SPECIAL authority.

**A.** RACF can store passwords in two forms: encrypted and hashed. The encrypted form is the default. The hashed form can be recovered; IBM does not provide details about how to do this, but there are many informal programs that do it. We strongly recommend using the encrypted form. There is no way to list the original passwords, once they have been encrypted.

**Q.** After I install RACF, can I run my OS/390 system without it? What if I make a change that locks out users?

**A.** Once installed, you can run without RACF. This is a very special mode, awkward to use, and suitable for only a single user on the system. In effect, OS/390 issues a console message for every data set allocation, and the OS/390 operator must reply to each message in order for the user to log on and repair the problem. In addition, the user ID used in this situation must be defined in SYS1.UADS. This is so rarely used that many installations and systems programmers have never experienced the situation.

# Appendix D. Special notices

This publication is intended to help system programmers, security administrators, and security officers, who are planning a migration from CA-ACF2 to IBM's SecureWay Security Server for OS/390. The information in this publication is not intended as the specification of any programming interfaces that are provided by SecureWay Security Server for OS/390. See the PUBLICATIONS section of the IBM Programming Announcement for SecureWay Security Server for OS/390 for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

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, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

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

| | |
|---|---|
| IBM ® | AS/400 |
| AT | C/MVS |
| CICS | CT |
| Current | DB2 |
| DFSMSrmm | DFSORT |
| DFTS | Netfinity |
| OS/390 | RACF |
| RMF | RS/6000 |
| S/390 | SecureWay |
| SP | System/390 |
| VTAM | XT |
| 400 | Lotus |
| Approach | Lotus Notes |
| Notes | Redbooks and Redbooks Logo  |

The following terms are trademarks of other companies:

Tivoli, Manage. Anything. Anywhere.,The Power To Manage., Anything. Anywhere.,TME, NetView, Cross-Site, Tivoli Ready, Tivoli Certified, Planet Tivoli, and Tivoli Enterprise are trademarks or registered trademarks of Tivoli Systems Inc., an IBM company, in the United States, other countries, or both. In Denmark, Tivoli is a trademark licensed from Kjøbenhavns Sommer - Tivoli A/S.

C-bus is a trademark of Corollary, Inc. in the United States and/or other countries.

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

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

PC Direct is a trademark of Ziff Communications Company in the United States and/or other countries and is used by IBM Corporation under license.

ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States and/or other countries.

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

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

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

# Appendix E. Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

## E.1 IBM Redbooks collections

Redbooks are also available on the following CD-ROMs. Click the CD-ROMs button at ibm.com/redbooks for information about all the CD-ROMs offered, updates and formats.

| CD-ROM Title | Collection Kit Number |
|---|---|
| IBM System/390 Redbooks Collection | SK2T-2177 |
| IBM Networking Redbooks Collection | SK2T-6022 |
| IBM Transaction Processing and Data Management Redbooks Collection | SK2T-8038 |
| IBM Lotus Redbooks Collection | SK2T-8039 |
| Tivoli Redbooks Collection | SK2T-8044 |
| IBM AS/400 Redbooks Collection | SK2T-2849 |
| IBM Netfinity Hardware and Software Redbooks Collection | SK2T-8046 |
| IBM RS/6000 Redbooks Collection | SK2T-8043 |
| IBM Application Development Redbooks Collection | SK2T-8037 |
| IBM Enterprise Storage and Systems Management Solutions | SK3T-3694 |

## E.2 Other resources

These publications are also relevant as further information sources:

- *SecureWay Security Server RACF System Programmer's Guide,* SC28-1913
- *SecureWay Security Server RACF Security Administrator's Guide,* SC28-1915
- *SecureWay Security Server RACF Security Auditor's Guide,* SC28-1916
- *SecureWay Security Server RACF Command Language Reference,* SC28-1919
- *CICS-RACF Security Guide*, SC33-1701

# How to get IBM Redbooks

This section explains how both customers and IBM employees can find out about IBM Redbooks, redpieces, and CD-ROMs. A form for ordering books and CD-ROMs by fax or e-mail is also provided.

- **Redbooks Web Site** ibm.com/redbooks

  Search for, view, download, or order hardcopy/CD-ROM Redbooks from the Redbooks Web site. Also read redpieces and download additional materials (code samples or diskette/CD-ROM images) from this Redbooks site.

  Redpieces are Redbooks in progress; not all Redbooks become redpieces and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

- **E-mail Orders**

  Send orders by e-mail including information from the IBM Redbooks fax order form to:

| | **e-mail address** |
|---|---|
| In United States or Canada | pubscan@us.ibm.com |
| Outside North America | Contact information is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl |

- **Telephone Orders**

| | |
|---|---|
| United States (toll free) | 1-800-879-2755 |
| Canada (toll free) | 1-800-IBM-4YOU |
| Outside North America | Country coordinator phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl |

- **Fax Orders**

| | |
|---|---|
| United States (toll free) | 1-800-445-9269 |
| Canada | 1-403-267-4455 |
| Outside North America | Fax phone number is in the “How to Order” section at this site: http://www.elink.ibmlink.ibm.com/pbl/pbl |

This information was current at the time of publication, but is continually subject to change. The latest information may be found at the Redbooks Web site.

**IBM Intranet for Employees**

IBM employees may register for information on workshops, residencies, and Redbooks by accessing the IBM Intranet Web site at http://w3.itso.ibm.com/ and clicking the ITSO Mailing List button. Look in the Materials repository for workshops, presentations, papers, and Web pages developed and written by the ITSO technical professionals; click the Additional Materials button. Employees may access MyNews at http://w3.ibm.com/ for redbook, residency, and workshop announcements.

## IBM Redbooks fax order form

**Please send me the following:**

| Title | Order Number | Quantity |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| First name | Last name | |
| Company | | |
| Address | | |
| City | Postal code | Country |
| Telephone number | Telefax number | VAT number |

☐ Invoice to customer number

☐ Credit card number

| | | |
|---|---|---|
| Credit card expiration date | Card issued to | Signature |

**We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.**

## Abbreviations and acronyms

| | |
|---|---|
| ACB | Access Control Block |
| ACEE | ACessor Environment Element |
| APPC | Advanced Program-to-Program Communications |
| API | Application Programming Interface |
| CBIPO | Custom-Built Installation Process Offering |
| CDSA | Common Data Security Architecture |
| CDT | Class Descriptor Table |
| CICS | Customer Information Control System |
| CLAUTH | CLass AUTHorization |
| CLIST | Command List |
| CMDF | Commercial Data Masking Facility |
| CPU | Central Processuing Unit |
| DASD | Data Access Storage Device |
| DB2 | Database/2 |
| DCE | Distributed Computing Environment ,component of SecureWay Security Server for OS/390 |
| DDN | Data Definition Name |
| DES | Data Encryption Standard |
| DFDSS | Data Facility/Data Storage System |
| DFP | Data Facility Product |
| DFSMS | Data Facility/System-Managed Storage |
| DLF | Data Lookaside Facility |
| DNS | Domain Name Services |
| DSMON | Data Security Monitor |
| EOS | Erase On Scratch |
| FDR | Field Definition Record |
| FTP | File Transfer Protocol |
| GAC | Global Access Checking |
| GID | UNIX Group IDentifier |
| GRS | General Resources |
| GSO | Global System Options |
| HFS | Hierarchical File System |
| HLQ | High Level Qualifier |
| ICB | Inventory Control Block |
| IBM | International Business Machines Corporation |
| IMS | Information Management System |
| IPL | Initial Program Load |
| IPSec | Information Protocol Security |
| ISPF/PDF | Interactive System Productivity Facility/Program Development Facility |
| ISV | Independent Software Vendor |
| ITSO | International Technical Support Organization |
| JCL | Job Control Language |
| JES | Job Entry Subsystem |
| LDAP | Lightweight Directory Access Protocol, component of SecureWay Security Server for OS/390 |
| LPA | Link Pack Area |
| LID | Logon ID |
| MVS | Multiple Virtual Storage |
| NAT | Network Address Translation |
| NDS | Novell Directory Services |
| NJE | Network Job Entry |
| OCEP | Open Cryptographic Enhanced Plug-ins, component of SecureWay Security Server for OS/390 |
| OMVS | Open Edition for MVS |
| OVM | Open Edition for VM |
| PADS | Program Access to Data Sets |
| PCICC | PCI Cryptographic Coprocessor |
| PGM | Program |
| PKI | Public Key Infrastructure |
| PL/I | Programming Language/1 |
| RACF | Resource Access Control Facility, component of SecureWay Security Server for OS/390 |
| RJE | Remote Job Entry |

| | |
|---|---|
| RJP | Remote Job Process |
| RRSF | RACF Remote Sharing Facility |
| SA | Security Association |
| SAF | System Authorization Facility |
| SDSF | System Data Spool Facility |
| SMF | System Management Facilities |
| SMPO | Software Migration Project Office |
| SMS | Storage Management Subsystem |
| SNA | Systems Network Architecture |
| SPT | Started Procedures Table |
| STC | Started Task Control |
| SYSRES | System-resident pack |
| TME | Tivoli Management Environment |
| TMP | Terminal Monitor Program |
| TSO | Time Sharing Option |
| UACC | Universal ACCess authority |
| UADS | User Attribute Data Set |
| UID | User IDentifier |
| USS | UNIX System Services |
| VM | Virtual Machinge |
| VOL | Volume |
| VPN | Virtual Private Network |
| VSAM | Virtual System Accessess Method |
| VTAM | Virtual Telecommunications Access Method |

# Index

## Symbols



## A



## B



## C



## D

## E



## F



## G



## H



## I



## K



## L



## M



## N



## O

## P



## R



## S

## T



## U



## V

# IBM Redbooks review

Your feedback is valued by the Redbook authors. In particular we are interested in situations where a Redbook "made the difference" in a task or problem you encountered. Using one of the following methods, **please review the Redbook, addressing value, subject matter, structure, depth and quality as appropriate.**

- Use the online **Contact us** review redbook form found at **ibm.com**/redbooks
- Fax this form to: USA International Access Code + 1 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

| | |
|---|---|
| **Document Number**<br>**Redbook Title** | SG24-5678-00<br>CA-ACF2 to OS/390 Security Server Migration Guide |
| **Review** | |
| **What other subjects would you like to see IBM Redbooks address?** | |
| **Please rate your overall satisfaction:** | O Very Good O Good O Average O Poor |
| **Please identify yourself as belonging to one of the following groups:** | O Customer<br>O Business Partner<br>O Solution Developer<br>O IBM, Lotus or Tivoli Employee<br>O None of the above |
| **Your email address:**<br>The data you provide here may be used to provide you with information from IBM or our business partners about our products, services or activities. | O Please do not use the information collected here for future marketing or promotional contacts or other communications beyond the scope of this transaction. |
| **Questions about IBM's privacy policy?** | The following link explains how we protect your personal information.<br>**ibm.com**/privacy/yourprivacy/ |

(0.2”spine)
0.17”<->0.473”
90<->249 pages

# CA-ACF2 to OS/390 Security Server
## Migration Guide

**Product design similarities and differences**

**Planning the migration**

**Conversion methodologies**

CA-ACF2 and the OS/390 Security Server are both sophisticated products. In some areas their designs are similar, and in other areas the designs are very different. Planning a migration from CA-ACF2 to the RACF element of the OS/390 Security Server, without unduly disrupting an OS/390 production environment, requires considerable planning and understanding. With proper planning, and perhaps with specially skilled people to assist in certain areas, the migration can usually be accomplished in an orderly way.

Understanding the higher-level issues and differences between the two products is an important starting point. This redbook is intended to assist in this area.

**INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION**

**BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:**
**ibm.com**/redbooks

SG24-5678-00 ISBN 0738418927