z/OS

SecureWay® Security Server DCE Overview

GC24-5921-00

z/OS

SecureWay® Security Server DCE Overview

GC24-5921-00

Note

Before using this information and the product it supports, be sure to read the general information under Appendix A, “Notices” on page 9.

First Edition (March 2001)

This edition, GC24-5921-00, applies to Version 1 Release 1 of z/OS SecureWay Security Server and z/OS DCE Base Services, z/OS DCE user Data Privacy (DES and CDMF), z/OS DCE User Data Privacy (CDMF) (program number 5694-A01), and to all subsequent releases and modifications until otherwise indicated in new editions.

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

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

International Business Machines Corporation
Information Development, Dept. G60
1701 North Street
Endicott, NY 13760-5553
United States of America

FAX (United States & Canada): 1+607+752-2327
FAX (Other Countries):
Your International Access Code +1+607+752-2327

IBMLink™ (United States customers only): GDLVME(PUBRCF)
Internet e-mail: pubrcf@vnet.ibm.com
World Wide Web: http://www.ibm.com/servers/eserver/zseries/zos/

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

Make sure to include the following in your comment or note:

- Title and order number of this book
- Page number or topic related to your comment

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

The following statements are provided by the Open Software Foundation.

Contents

Figures

About This Book

The z/OS SecureWay Security Server includes the following components:

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

For information about the first five components, see the publications related to those components.

This book describes security in the OSF Distributed Computing Environment and provides an overview of the z/OS SecureWay Security Server DCE.

Note: In this book the term “DCE Security Server” refers to the z/OS SecureWay Security Server DCE.

The purpose of this book is to help system managers, system programmers, and system and network administrators understand the DCE Security Server

Who Should Use This Book

This book is intended for system and network administrators who are responsible for defining and administering a DCE Security Server. The reader is assumed to understand the fundamental concepts of a distributed environment. Administrators who have little or no experience with DCE are advised to read *z/OS DCE Introduction*, GC24-5911, before using this book.

How to Use This Book

This book is divided into the following chapters:

- Chapter 1, “DCE Security Server” on page 1 gives an overview of the DCE Security Server and discusses the benefits of having the DCE Security Server on z/OS.
- Chapter 2, “Security in the OSF Distributed Computing Environment” on page 5 gives an overview of security support in the OSF Distributed Computing Environment and how the DCE components work together.

Product Names

The product names, **IBM DCE Base Services** and **DCE** refer to the DCE services in z/OS. These names are used interchangeably in this book.

Conventions Used in This Book

This book uses the following typographic conventions:

Bold	**Bold** words or characters represent system elements that you must enter into the system literally, such as commands, options, or path names.

Where to Find More Information

Where necessary, this book references information in other books using shortened versions of the book title. For complete titles and order numbers of the books for all products that are part of z/OS, see the *z/OS Information Roadmap*, SA22-7500. For complete titles and order numbers of the books for z/OS DCE, refer to the publications listed in the "Bibliography" on page 11.

For information about installing z/OS DCE components, see the *z/OS Program Directory*.

This book can be used with the *z/OS DCE Command Reference*, SC24-5909, which provides the syntax of the DCE administration commands.

Softcopy Publications

The z/OS DCE library is available on a CD-ROM, *z/OS Collection*, SK3T-4269. The CD-ROM online library collection is a set of unlicensed books for z/OS and related products that includes the IBM Library Reader.™ This is a program that enables you to view the BookManager® files. This CD-ROM also contains the Portable Document Format (PDF) files. You can view or print these files with the Adobe Acrobat reader.

Internet Sources

The Softcopy z/OS publications are also available for web-browsing and for viewing or printing PDFs using the following URL:

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

You can also provide comments about this book and any other z/OS documentation by visiting that URL. Your feedback is important in helping to provide the most accurate and high-quality information.

Using LookAt to Look up Message Explanations

LookAt is an online facility that allows you to look up explanations for z/OS messages. You can also use LookAt to look up explanations of system abends.

Using LookAt to find information is faster than a conventional search because LookAt goes directly to the explanation.

LookAt can be accessed from the Internet or from a TSO command line.

You can use LookAt on the Internet at:

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

To use LookAt as a TSO command, LookAt must be installed on your host system. You can obtain the LookAt code for TSO from the LookAt Web site by clicking on the **News and Help** link or from the *z/OS Collection*, SK3T-4269.

To find a message explanation from a TSO command line, simply enter: **lookat** *message-id* as in the following:

```
lookat iec192i
```

This results in direct access to the message explanation for message IEC192I.

To find a message explanation from the LookAt Web site, simply enter the message ID and select the release with which you are working.

Note: Some messages have information in more than one book. For example, IEC192I has routing and descriptor codes listed in *z/OS MVS Routing and Descriptor Codes*, SA22-7624. For such messages, LookAt prompts you to choose which book to open.

Accessing Licensed Books on the Web

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

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

Licensed books are available only to customers with a z/OS license. Access to these books requires an IBM Resource Link user ID, password, and z/OS licensed book key code. The z/OS order that you received provides a memo that includes your key code.

To obtain your IBM Resource Link user ID and password, logon to:

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

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

1. Logon to Resource Link using your Resource Link user ID and password.
2. Select **User Profiles** located on the left-hand navigation bar.
3. Select **Access Profile**.
4. Select **Request Access to Licensed books**.
5. Supply your key code where requested and select the **Submit** button.

If you supplied the correct key code you will receive confirmation that your request is being processed.

After your request is processed you will receive an e-mail confirmation.

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

To access the licensed books:

1. Logon to Resource Link using your Resource Link user ID and password.
2. Select **Library**.
3. Select **zSeries**.
4. Select **Software**.
5. Select **z/OS**.
6. Access the licensed book by selecting the appropriate element.

Chapter 1. DCE Security Server

One of the major challenges that face the business is enterprise of wide security, especially in a heterogeneous environment.

The DCE Security Server provides a fully functional OSF DCE 1.1 level security server that runs on z/OS. You can configure your DCE cell with a security server on the mainframe, the central z/OS enterprise server. Availability of this critical DCE technology component on z/OS provides the following benefits:

- You can keep servers and data on your z/OS systems safe from accidental or malicious loss, and secure from outside attack (disclosure or corruption).
- System/390® and **z**Series 900 are scalable and many z/OS systems are large. You can build DCE cells that are able to handle large numbers of accounts.
- z/OS is more reliable than any other system currently offering DCE. Therefore, a security server on z/OS is more reliable and available than on any other DCE system, giving you the reliability you need to run mission-critical applications in a DCE environment.

Security Service

The DCE Security Service provides trustworthy identification and certification of principals (users, clients, servers, and systems), offers integrity and privacy of communications, and enables controlled access to resources. It controls the interaction between clients and servers.

Today, most systems provide one way authentication, where the client proves its identity to the server. Server identity is rarely verified. In a distributed environment, this trust of servers may be lessened, leading to a requirement for two-way authentication.

In two-way authentication, each server must be able to verify the identity of each client and each client must be confident that it is communicating with a secure server. Clients and servers use trusted keys to request and provide services. Each server must maintain trusted key information for each client that it can serve, and every client must know a trusted key for each server it might use. Two-way authentication is difficult to administer. Every time a server's information changes, all its clients must be updated.

DCE simplifies administration and adds security by implementing a trusted-third-party or a Kerberos approach. The DCE Security Server, acting as a trusted third party, maintains the trusted key information. Clients and servers no longer need to store this information. The DCE Security Server identifies and certifies principals (authentication) and provides information on the privileges associated with each principal. Privileges enable servers to perform selected operations (authorization) for authenticated principals.

Exploring the z/OS DCE Security Service

The z/OS DCE Security Service enables clients and servers to prove their identities to each other. It offers integrity and privacy of communications and supports controlled access to resources. It acts on behalf of principals. In DCE, principals are represented as entries in the DCE Security Service's database, called the registry. These entries include users, servers, and machines.

The DCE Security Service provides tools to help you administer Security on both the local machine and the cell.

Managing the local machine includes running commands that add, delete, or list the key table entries used by non-interactive users, such as machines and server processes.

Cell administration includes managing the DCE Security Server and creating and maintaining information kept in the registry using a Registry Editor. The registry contains information on principals, groups, organizations, accounts, and administrative policies. Each cell has one registry database. It can also have replicas known as slaves.

You can use **dcecp** to set up accounts for foreign cells in your cell's registry, indicating that you trust the Authentication Service in the foreign cell to correctly authenticate its users.

The DCE Security Service consists of several cooperating services and facilities. One of these services is the Registry Service which helps you manage user, group, and account information. In addition to the Registry Service, the DCE Security Service includes the following services and facilities that require very little or no system administration:

- The Authentication Service

  Provides trustworthy identification of principals involved in network operations. A principal gains access to DCE by means of an account, which consists, in part, of the principal name and a secret key (password) that the principal shares with the Authentication Service.

- The Privilege Service

  Certifies a principal's identity and group membership. A principal's identity and group membership, also known as privilege attributes can be used by an Access Control List (ACL) (see below) to determine a principal's access permissions to objects. The Privilege Service provides the privilege attributes that can be used to determine if a principal has the right to do what it wants to do.

- The DCE ACL Facility

  Determines a principal's access to an object by comparing entries in the object's ACL to the identity and group membership of the principal. The **dcecp acl** command is the administrative tool used to create, change, and delete ACL entries. Other DCE components use the ACL model provided by the DCE Security Service through their individual ACL Managers.

- The DCE Login Facility

  Initializes a user's DCE Security environment. It also authenticates the user to the Security Service by means of the user's password, thereby establishing an authenticated network identity.

- The Alternative DB2® Based Security Registry

  DB2 for MVS/ESA™ is available as an alternative database repository for the security registry.

  It is selected by a parameter on the **sec_create_db** command. You can specify the type of database to be created when configuring DCE/MVS from the **dceconf** command menu.

  The **sec_export_db** command and the **sec_import_db** command allow you to preserve security registry entries across a cell reconfigure. They also allow you to switch from one database repository to another without having to reconfigure the cell.

- The Local Services

  Provides Program Call (PC) interfaces, in addition to the normal Remote Procedure Call (RPC) interfaces. The S/390® and **z**Series 900 PC and PR instructions are used to provide a direct linkage between the client application and the DCE Security Server

  These local services are not intended for use by DCE applications. Instead, they are used by system functions which are shipped as part of z/OS. In most cases, they replace existing RPC functions provided by the DCE Security Server.

RACF Interoperability and Single Sign-on

z/OS DCE provides interoperability between RACF, a component of the SecureWay Security Server for z/OS, and z/OS DCE. This security interoperability allows a DCE client to access a DCE-enabled server on a z/OS system and allows the DCE server to acquire corresponding local security credentials for a DCE client to access z/OS resources. The interoperability function allows:

- Appropriately authorized DCE servers to acquire corresponding z/OS security credentials for the DCE client and to use the DCE client's corresponding z/OS user ID for access to RACF-authorized resources.
- A z/OS user to be transparently logged into DCE when necessary, without prompting for a DCE user ID or password. With this single sign-on feature, a z/OS user authenticates to z/OS and can start a DCE program without re-authenticating to DCE.

z/OS DCE also provides administration utilities to implement the interoperability. These incorporate the information into RACF that associates a z/OS user ID with a DCE principal's identifying information and the DCE principal's UUID with the corresponding z/OS user ID. This is called cross-linking information and it is what allows interoperability and single sign-on to work.

The cross-linking information must be set up before interoperability functions can be used. To do this, DCE provides two utilities, **mvsimpt** and **mvsexpt**, for creating the initial cross-linking between the two registries. This cross-linking can be done from either the RACF database or the DCE registry, but **mvsimpt** and **mvsexpt** must be started from the z/OS system where the RACF database whose users are to be cross-linked resides.

z/OS DCE also provides application programming interfaces (APIs) to the System Authorization Facility (SAF) so that you can write your own server programs to take advantage of RACF interoperability.

Chapter 2. Security in the OSF Distributed Computing Environment

The OSF Distributed Computing Environment (OSF DCE) architecture defines a set of services layered between the operating system and network and the distributed applications. It provides the services that enable a distributed application to interact with a collection of either heterogeneous or homogeneous computers, operating systems, and networks as if it was a single system.

Figure 1 shows the DCE architecture and its technology components, along with their relationship to applications, underlying system support, and placeholders for future technologies.

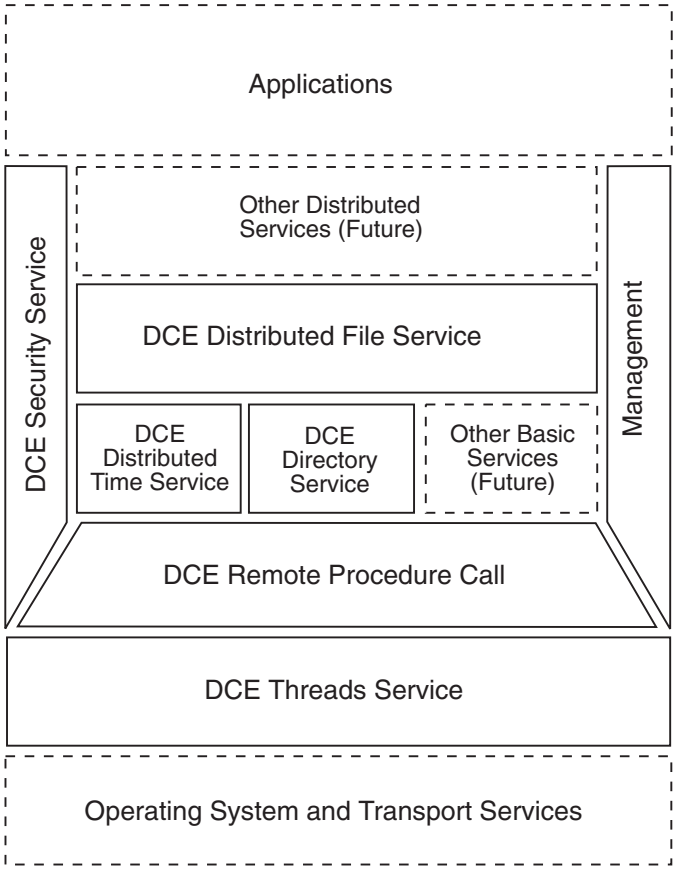

Figure 1. The OSF DCE Architecture

The technologies fall into two general categories: programming services and distributed services.

The DCE Threads Service and DCE Remote Procedure Call (RPC) are programming services. They include libraries that implement application program interfaces (APIs) and program development tools.

The remaining technologies, including the DCE Security Service, are distributed services. Each consists of a daemon, or server process, that runs continuously on a machine and responds to requests sent over the network. These services have administrative components to manage the service, and have APIs and Program Call instructions that programmers can use to access these components.

Application programmers deal mostly with the programming services. Although the distributed services are accessed through APIs, the programmer usually uses them only indirectly through RPC, which in turn uses the APIs of the distributed services. With Local Services, the direct program call is used in place of

a RPC for the DCE login functions. This occurs only if the DCE Security Server is running on the same system as the application. Administrators, on the other hand, deal mostly with the distributed services.

The administration of the OSF DCE components can itself be distributed, allowing distributed management of the distributed computing environment. The need for a centralized authority is alleviated making the distributed environment more flexible, scalable, and allowing for redundancy. You can maintain a central authority, distribute authority, or implement a combination of both.

For more detailed information about the DCE architecture and its components, refer to the *z/OS DCE Introduction*.

How the DCE Components Work Together

Although DCE consists of distinct components, these components are integrated and interrelated. This section summarizes the relationships between components that have associated system administration tasks.

Most DCE components rely on RPC, the DCE Directory Service, the Distributed Time Service (DTS), and the DCE Security Service. The interaction is often reciprocal. For example, RPC uses the DCE Security Service's Authentication Service to get tickets and keys, and the Privilege Service to securely associate clients with their identities. The DCE Security Service, in turn, uses RPC for its communications.

The Cell Directory Service (CDS) component of the DCE Directory Service, DTS, and the DCE Security Service, along with RPC, are the components that every DCE cell requires.

The Global Directory Agent (GDA) and Global Directory Service (GDS) components of the DCE Directory Service and Distributed File Service (DFS) are not required for a minimum DCE configuration. If these services are part of your cell, they rely on some or all of the services mentioned in the previous paragraph.

Remote Procedure Call

An RPC server can store information about itself in CDS. An RPC client can look up location information about RPC servers in CDS when it wants to make a call to a particular server. CDS returns information that RPC libraries interpret as binding information and turn into a binding handle. The binding handle identifies the RPC server so the RPC client can make its RPC call.

RPC uses the DCE Security Service for authenticated RPC, the process by which RPC clients and servers are identified to one another, and by which privacy and integrity of communications are maintained. To use authenticated RPC, clients and servers must be running as principals, have accounts, and have performed login operations.

Each RPC program is likely to require some administration of CDS namespace entries and directories, as well as some server-specific file administration.

Directory Service

CDS servers and CDS clients use RPC and the DCE Security Service's Authentication Service to communicate with each another. CDS can also store information about the location of the RPC servers and interfaces that the RPC servers support.

CDS uses the Access Control List (ACL) model provided by the DCE Security Service to ensure

authorized access to directory data in CDS. To authenticate CDS interactions, CDS uses authenticated RPC provided through the DCE Security Service.

When you create entries in the CDS namespace, a timestamp accompanies the entry. The timestamp is used for propagation to replicas and the expiration of temporary entries. CDS relies on DTS to maintain clock synchronization in the network so that the timestamps are accurate.

CDS uses GDS to find names outside of a cell by means of the GDA. Other DCE components interact with CDS for directory service (global and local), but only CDS and application programs access GDS directly.

Unlike CDS and other DCE components, GDS does not use RPC for its communications. GDS has its own security implementation and does not depend on the DCE Security Service. GDS conforms to the international standard X.500 protocols.

Distributed Time Service

Like CDS, DTS uses RPC to handle communications between DTS servers and DTS clerks.

DTS registers the servers that synchronize system clocks in the network with CDS and also uses CDS to find DTS servers and their locations.

To authenticate DTS interactions, DTS uses authenticated RPC provided through the DCE Security Service. DTS also uses DCE ACLs to control which users can run certain **dcecp** commands. The permissions required to run these commands are discussed in *z/OS DCE Command Reference*.

Security Service

The DCE Security Service uses RPC for its communications. The DCE Security Service registers the location of its Security servers (**secd** daemons) with CDS. Other servers in the network can use CDS to locate the Security servers. You manage the name space entries using the CDS Control Program.

The DCE Security Service relies on DTS to maintain synchronized clocks so that passwords and tickets (used for obtaining network services) are properly time stamped and their expiration is enforced.

The DCE Security Service provides an ACL model for controlling access to objects that are managed by the DCE services. Based on this ACL model, objects and the ACLs on objects are controlled and managed by the DCE service that owns the object. You can use **dcecp** to manage access to principals, groups, and organizations that are registered in the CDS namespace.

The RACF interoperability and single sign-on functions of the Security Service make use of the other DCE services in the same way as the rest of the Security functions. Specifically, for MVS users on a system that is protected by RACF, single sign-on allows a user who was authenticated to RACF to start a DCE program without re-authenticating to DCE. This is done using RPC and is transparent to the user.

Integrating the DCE Components

Figure 2 on page 8 shows how the DCE components work together in a distributed environment.

1. Distributed Time Service (DTS) keeps the clocks on the different machines synchronized.
2. Each server is registered with the Directory Service. The server processes (Procedure X and Procedure Y) advertise their locations (host address and network identification) in the Directory.
3. The client's RPC queries the Directory for a server offering Procedure X, which is required or called in Application 1.

4. The Security Service verifies the identity and authority of both the client and server.
5. The client (Application 1) makes a remote procedure call to the server for Procedure X.
6. The server checks the client's security credentials.
7. The server performs Procedure X.
8. The server returns the results to the client application.

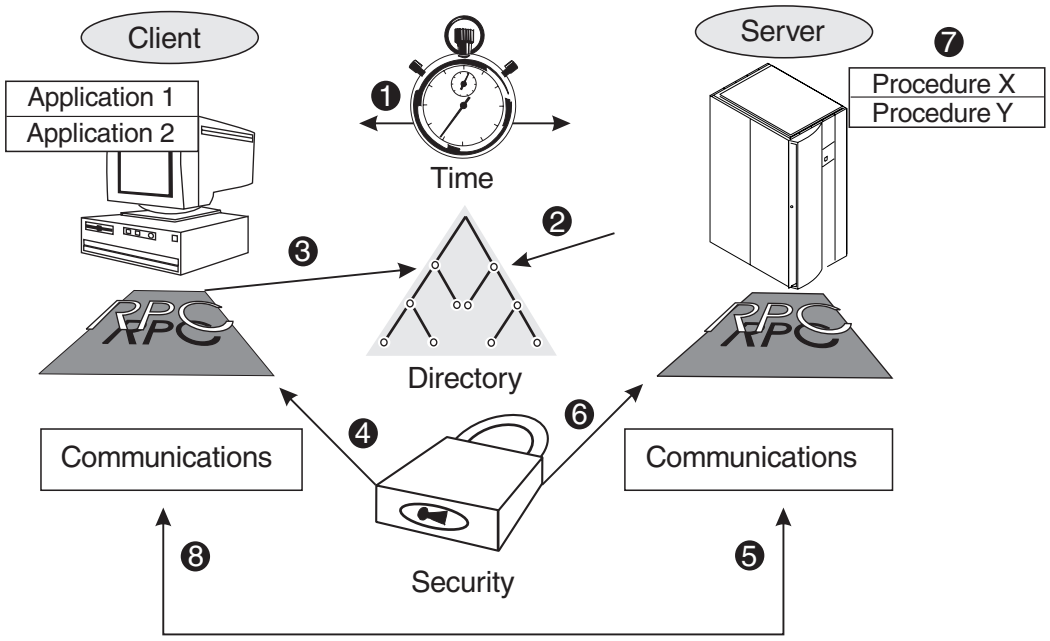

Figure 2. DCE's Integrated Components

The DCE components, although running in different locations, are so well integrated that users do not know or need to know if the applications are running locally (on their machine) or remotely.

This integration also hides the details of security and directory from the application programmers using them. Applications written on one machine can run on other machines, the location of required or called procedures is handled by the directory. The portability of the code, the hidden details of security and the directory, and the transparency of the communications interface ensures ease and flexibility for programmers who are creating distributed application programs.

Appendix A. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Mail Station P300
522 South Road
Poughkeepsie, NY 12601-5400
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

BookManager	CICS	DB2
IBM	IBMLink	IMS
Library Reader	MVS/ESA	RACF
Resource Link	S/390	SecureWay
System/390	z/OS	zSeries

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

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

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

Bibliography

This bibliography is a list of publications for z/OS DCE and other products. The complete title, order number, and a brief description is given for each publication.

z/OS DCE Publications

This section lists and provides a brief description of each publication in the z/OS DCE library.

Overview

- *z/OS DCE Introduction*, GC24-5911

  This book introduces z/OS DCE. Whether you are a system manager, technical planner, z/OS system programmer, or application programmer, it will help you understand DCE and evaluate the uses and benefits of including z/OS DCE as part of your information processing environment.

Planning

- *z/OS DCE Planning*, GC24-5913

  This book helps you plan for the organization and installation of z/OS DCE. It discusses the benefits of distributed computing in general and describes how to develop plans for a distributed system in a z/OS environment.

Administration

- *z/OS DCE Configuring and Getting Started*, SC24-5910

  This book helps system and network administrators configure z/OS DCE.

- *z/OS DCE Administration Guide*, SC24-5904

  This book helps system and network administrators understand z/OS DCE and tells how to administer it from the batch, TSO, and shell environments.

- *z/OS DCE Command Reference*, SC24-5909

  This book provides reference information for the commands that system and network administrators use to work with z/OS DCE.

- *z/OS DCE User's Guide*, SC24-5914

  This book describes how to use z/OS DCE to work with your user account, use the directory service, work with namespaces, and change access to objects that you own.

Application Development

- *z/OS DCE Application Development Guide: Introduction and Style*, SC24-5907

  This book assists you in designing, writing, compiling, linking, and running distributed applications in z/OS DCE.

- *z/OS DCE Application Development Guide: Core Components*, SC24-5905

  This book assists programmers in developing applications using application facilities, threads, remote procedure calls, distributed time service, and security service.

- *z/OS DCE Application Development Guide: Directory Services*, SC24-5906

  This book describes the z/OS DCE directory service and assists programmers in developing applications for the cell directory service and the global directory service.

- *z/OS DCE Application Development Reference*, SC24-5908

  This book explains the DCE Application Program Interfaces (APIs) that you can use to write distributed applications on z/OS DCE.

Reference

- *z/OS DCE Messages and Codes*, SC24-5912

  This book provides detailed explanations and recovery actions for the messages, status codes, and exception codes issued by z/OS DCE.

z/OS SecureWay® Security Server Publications

This section lists and provides a brief description of books in the z/OS SecureWay Security Server library that may be needed for z/OS SecureWay Security Server DCE and for RACF® interoperability.

- *z/OS SecureWay Security Server DCE Overview*, GC24-5921

  This book describes the z/OS SecureWay Security Server DCE and provides z/OS SecureWay Security Server DCE information about the z/OS DCE library.

- *z/OS SecureWay Security Server LDAP Client Programming*, SC24-5924

  This book describes the Lightweight Directory Access Protocol (LDAP) client APIs that you can use to write distributed applications on z/OS DCE and gives you information on how to develop LDAP applications.

- *z/OS SecureWay Security Server RACF Security Administrator's Guide*, SA22-7683.

  This book explains RACF concepts and describes how to plan for and implement RACF.

- *z/OS SecureWay Security Server LDAP Server Administration and Use*, SC24-5923

  This book describes how to install, configure, and run the LDAP server. It is intended for administrators who will maintain the server and database.

- *z/OS SecureWay Security Server Firewall Technologies*, SC24-5922

  This book provides the configuration, commands, messages, examples and problem determination for the z/OS Firewall Technologies. It is intended for network or system security administrators who install, administer and use the z/OS Firewall Technologies.

Tool Control Language Publication

- *Tcl and the Tk Toolkit*, John K. Osterhout, (c)1994, Addison—Wesley Publishing Company.

  This non-IBM book on the Tool Control Language is useful for application developers, DCECP script writers, and end users.

IBM C/C++ Language Publication

- *z/OS C/C++ Programming Guide*, SC09-4765

  This book describes how to develop applications in the C/C++ language in z/OS.

z/OS DCE Application Support Publications

This section lists and provides a brief description of each publication in the z/OS DCE Application Support library.

- *z/OS DCE Application Support Configuration and Administration Guide*, SC24-5903

  This book helps system and network administrators understand and administer Application Support.

- *z/OS DCE Application Support Programming Guide*, SC24-5902

  This book provides information on using Application Support to develop applications that can access CICS® and IMS™ transactions.

Encina Publications

- *z/OS Encina Toolkit Executive Guide and Reference*, SC24-5919

  This book discusses writing Encina applications for z/OS.

- *z/OS Encina Transactional RPC Support for IMS*, SC24-5920

  This book is to help software designers and programmers extend their IMS transaction applications to participate in a distributed, transactional client/server application.

Readers' Comments

z/OS
SecureWay® Security Server
DCE Overview

Publication No. GC24-5921-00

You may use this form to report errors, to suggest improvements, or to express your opinion on the appearance, organization, or completeness of this book.

Date: _____

IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Note

Report system problems to your IBM representative or the IBM branch office serving you.
U.S. customers can order publications by calling the IBM Software Manufacturing Solutions at **1-800-879-2755**.

In addition to using this postage-paid form, you may send your comments by:

FAX	1-607-752-2327	Internet	pubrcf@vnet.ibm.com
IBMLink	GDLVME(PUBRCF)		

Would you like a reply? ___YES ___ NO If yes, please tell us the type of response you prefer.

___ Electronic address: _____

___ FAX number: _____

___ Mail: (Please fill in your name and address below.)

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments
GC24-5921-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Department G60
International Business Machines Corporation
Information Development
1701 North Street
ENDICOTT NY 13760-5553

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Program Number: 5694-A01

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC24-5921-00

Spine information:

z/OS DCE SecureWay Security Server DCE Overview