VisualAge Pacbase 2.5

SECURITY SYSTEMS INTERFACE REFERENCE MANUAL

DDSEC000151A

Note

Before using this document, read the general information under "Notices" on the next page.

According to your license agreement, you may consult or download the complete up-to-date collection of the VisualAge Pacbase documentation from the VisualAge Pacbase Support Center at:
http://www.software.ibm.com/ad/vapacbase/support.htm

Consult the Catalog section in the Documentation home page to make sure you have the most recent edition of this document.

First Edition (May 1996)

This edition applies to the following licensed programs:

- VisualAge Pacbase Version 2.0
- VisualAge Pacbase Version 2.5

Comments on publications (including document reference number) should be sent electronically through the Support Center Web site at:
http://www.software.ibm.com/ad/vapacbase/support.htm
or to the following postal address:
IBM Paris Laboratory
VisualAge Pacbase Support
30, rue du Château des Rentiers
75640 PARIS Cedex 13
FRANCE

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

NOTICES

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 that IBM product, program, or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

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:

Intellectual Property and Licensing
International Business Machines Corporation
North Castle Drive, Armonk, New-York 10504-1785
USA

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 information which has been exchanged, should contact:

IBM Paris Laboratory
SMC Department
30, rue du Château des Rentiers
75640 PARIS Cedex 13
FRANCE

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

IBM may change this publication, the product described herein, or both.

TRADEMARKS

IBM is a trademark of International Business Machines Corporation, Inc.
AIX, AS/400, CICS, CICS/MVS, CICS/VSE, COBOL/2, DB2, IMS, MQSeries, OS/2, PACBASE, RACF, RS/6000, SQL/DS, TeamConnection, and VisualAge are trademarks of International Business Machines Corporation, Inc. in the United States and/or other countries.

Java and all Java-based trademarks and logos are 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.
UNIX is a registered trademark in the United States and/or other countries licensed exclusively through X/Open Company Limited.

All other company, product, and service names may be trademarks of their respective owners.

TABLE OF CONTENTS

1. PACBASE - RACF OR TOPSECRET INTERFACE

1.1. INTRODUCTION

INTRODUCTION

Security systems provide a mechanism for data access control. They perform user identification and verification, and they check resource access authorizations.

These systems control security over the whole data processing installation and, as such, operate independently from the PACBASE system. The Interface is designed to ensure control communication between the security systems and PACBASE.

In connection with PACBASE and the Transaction for managing parameters and turnover to production (xxEE), the Security Interface performs the following tasks:

- On-line: automatic retrieval of the CICS or IMS SIGN-ON USERID, which is displayed on the log-on screen for PACBASE or the xxEE transaction.

- Library access control: performed by PACBASE instead of the security system.

- In batch: for PACBASE procedures including user input ('*' line) that are executed under TSO, it will be possible to leave the user code and the password blank.

In order to ensure compatibility with all security systems, the PACBASE system is not directly connected with the security system, but with SAF (System Authorization Facility) via the RACROUTE macro-instructions for RACF or the TSS macro-instructions for TOPSECRET.

1.2. INSTALLATION

INSTALLATION

INSTALLATION AT THE PACBASE LEVEL

PACBASE-RACF or TOPSECRET INTERFACE being an extension of PACBASE, its installation implies that the PACBASE system access key must be changed.

This access key is supplied with the product along with the PACBASE-RACF or TOPSECRET Interface.

The second operation is to define, in PACBASE, the type of security system used (RACF or TOPSECRET), as well as the class in which PACBASE logical resources will be defined.

You can perform both operations:

. in on-line mode, by accessing the 'Access Keys Updating' PK screen, via the xxEE transaction (xx being the root of the Database). For a complete description of this screen, refer to the PACBASE User's Reference Manual, Chapter 'Database Management', Subchapter 'Access Keys Updating'.

. in batch mode, via the PARM procedure. In the execution JCL, you must code an 'NK' line to change the access key, and an 'NS' line to define the security system and the class. For a complete description of the 'NK' and 'NS' lines, refer to the PACBASE Operations Manual, Chapter 'PARM: Updating User Parameters', Subchapter 'Recommendations-Results'.

INSTALLATION AT THE SECURITY SYSTEM LEVEL

1. Creation of a RACF Class or a TOPSECRET Resource Class

A class name or a resource class name is coded on four characters and must be identical in PACBASE and in the security system.

Creation of a RACF Class

Each PACBASE Database must be identifiable to the RACF system. As a result, each database corresponds to a class. A class must be created within the PACBASE system via the 'PK' screen or the PARM batch procedure, and within the RACF system via the RACF 'ICHERCDE' macro. This macro generates an entity located in the ICHRRCDE member found in SYS1.LINKLIB.

A resource must be coded with four characters (one for the access authorization code and three for the library).

The PACBASE system is not directly connected with the security system, but with SAF (System Authorization Facility) via the RACROUTE macro-instructions.

RACROUTE macro-instructions are taken into account when the class is coded via the ICHRFRTB macro-instruction, which generates an entry in the 'RACF ROUTER' table (member ICHRFR01 in SYS1.LINKLIB).

Creation of a TOPSECRET Resource Class

In order for TOPSECRET to work properly, all the PACBASE logical resources are asssociated with a TOPSECRET resource class, defined in PACBASE via the 'PK' screen or the PARM batch procedure, and in TOPSECRET via the command:

```
TSS ADD(RDT) RESCLASS(cccc) RESCODE(xx), with

cccc: resource class
xx  : hexadecimal code which indicates the resource type.
```

2. Creation of resources

A class includes all the logical resources of a PACBASE Database, i.e., all possible access authorizations for each library presented as couples (authorization/library).

For RACF:

Resources are created by the 'RDEFINE' procedure.

For TOPSECRET:

Resources are created by the command

```
TSS ADD(dept-name) cccc(nlib) cccc(nlib)..., with

 dept-name = department name,
 cccc = resource class,
 n = authorization level,
 lib = PACBASE Library code.
```

EXAMPLE:

A PACBASE Database is made up of two libraries: LI1 and LI2. The class for this database is defined as follows:

4LI1 3LI1 2LI1 1LI1 0LI1 4LI2 3LI2 2LI2 1LI2 0LI2

Note: there is no distinction between the global authorization and the Database authorization, since this latter does not exist in the Security Systems Interface.

When the PACBASE-SECURITY SYSTEM Interface is being installed, a special$$') must be created for each
database and will support the general access authorization:

$$ 3$$$ 2$$$ 1$$$ 0$$$

Since '*' is the generic character for the security system, the 'Inter-Library '***' mode must be coded as '£££' (if the '£' key is not available, the British Pound symbol can be used).

There are three other special Library codes:

. $B for an access to the batch procedures,

. $E for an authorization to the Dictionary Extensibility function,

. $P for an authorization to the PARM procedure.

3. Defining users

Granting resource access authorizations to individual end users is done:

```
For RACF via the 'PERMIT' procedure.

For TOPSECRET via the command:
  TSS PERMIT(user-code) cccc(lib) cccc(lib) ...
```

Resources and user codes not declared to the security system are consequently prohibited under PACBASE.

INVOLVED PROGRAMS

Once the PACBASE-RACF or TOPSECRET Interface is installed, new programs or load-modules are available.

ASSEMBLER program

For RACF:

PACSECU8: batch & on-line.

This program is linked with the RENT and REUS parameters and must be stored in an authorized library. It must be inserted in the LNKLSTxx member in SYS1.PARMLIB so as to avoid the concatenation of this library in JCL STEPLIBs.

This program must also be declared to the RACF system in the ICHAUTAB table in SYS1.LPALIB, with the authority of RACLIST SVC and RACFINIT SVC.

For TOPSECRET:

PACTSS: batch under MVS/CICS; batch and on-line under MVS/IMS.
PACTSSC: on-line under MVS/CICS.

COBOL programs

PACSECB: Batch operations under MVS-CICS. Batch and on-line operations under MVS-IMS-DB/DC

xxSECT : On-line operations under MVS-CICS. This program must be inserted in the CICS PPT.

1.3. OPERATING MODE

OPERATING MODE

The interface performs verification based on three indicators specified in the PARM procedure:

- Security system use indicator

- User authorization indicator:

  For RACF, it indicates whether the user logged on under CICS or IMS for on-line, or TSO for batch, is entitled to log on to PACBASE with a user code other than his/her own. This indicator is valid only if the security system is used.

  For TOPSECRET, this indicator is forced: it is impossible to log on with a user code other than his/her own.

- Resource indicator (library access) managed by PACBASE or by the security system. This indicator is valid only if the security system is used.

These indicators are used to distinguish the following methods of management: total and strict management under a security system, total and flexible management under a security system and resource management under PACBASE.

TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM

Verification of users and library access is managed by the security interface, and a user can log on only with his/her own code. PARM

1. Logging on for on-line processing: the PACBASE or SIGN-ON screen is initialized with the code under which the user logged on to CICS or IMS. This code is retrieved in the IO-PCB under IMS and by an EXEC CICS ASSIGN USERID command under CICS (valid only from CICS release 1.7 on). Changing the user code is prohibited.

2. GP screen (RACF only) : since RACF does not carry over the user code and the CICS or IMS password, you have to insert them on the JOB card. Since the system does not pass on the password, the user has to enter it on the GP screen (a masked field) the first time he/she does a SUB or a JOB.

   A warning message is displayed if the field has not already been filled in.
   Starting with release 1.9, the password no longer needs to be filled in since a user can submit a job for another ('surrogate') user.

3. Batch procedures that include a '*' line: the user code and password are no longer required since the system automatically takes the code under which the user signed on to TSO.

   As a result, the PASSWORD is no longer present in the temporary files found in batch jobstreams, including GPRT, since the security system ensures the propagation of the USER code and the PASSWORD for compile jobs submitted via this procedure.
   Another consequence is that jobstreams including steps with a '*' line can be linked together without manual intervention so that the password can be specified.
   For RACF, this process implies a restriction: the user cannot code several '*' lines with user codes other than his/her own for procedures which would normally allow the user to do so.
   For TOPSECRET, the user can never enter user codes other than his/her own.

4. The password field is locked and cannot be filled in. The cursor is positioned on the library code.

TOTAL AND FLEXIBLE MANAGEMENT UNDER A SECURITY SYSTEM

This management is possible under RACF only.

Verification of users and library access is managed by the security interface, but the user can log on with a code other than his/her own.

1. Logging on for on-line processing: identical to number 1 under 'TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM' above, but the field including the USER code is an input field, as is the PASSWORD field. The user can change these two fields; the password is required. In the case of a change, the interface performs a test to validate the USER code, and the security system performs a test to validate the password.

2. GP screen: identical to number 2 under 'TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM' above. If the user entered the password on the logon screen, it doesn't have to be entered again.

3. Batch procedures that include a '*' line: just as in the case of on-line processing when the user code is different from the one under TSO, the password has to be filled in.

   This makes it possible to submit jobs with several '*' lines having different user codes.
   In the case of different USER codes, jobs submitted by GPRT will include the USER and PASSWORD parameters.
   Even in this case, temporary files will not include the password, which means that it is not possible to link together steps having a '*' line. The password has to be entered every time.
   Of course, if the USER code is identical to the one under TSO, verification of users and library access is managed as described in number 3 under 'TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM' above.

RESOURCE MANAGEMENT UNDER PACBASE

User verification is performed according to one of the two preceding methods for RACF or always according to the 'TOTAL AND STRICT MANAGEMENT' method for TOPSECRET, but library access verification is managed by PACBASE. Library access authorizations must be entered under PACBASE, on the PU screen, and the password field is not an input field.

NOTE: The following three functionalities are not available with the security interface:

- The +AG command for the GPRT procedure,
- Copying JCL from the GP screen to another user.
- Password modification on the logon screen.

1.4. ERROR MANAGEMENT (RACF ONLY)

RACF ERROR MANAGEMENT

If the RACF system detects an error when a user logs on, a PACBASE error message is displayed. This message is completed by a return code that includes a RACF return code and the error type.

The security administrator should be informed of the general return code so that the problem can be resolved accordingly.

There are five error types:

'I': Error on user code

REQUEST=VERIFY RACROUTE macro-instruction (checks the user code with password).

'L': Unauthorized library access

REQUEST=LIST, ENVIR=CREATE RACROUTE macro-instruction (used to create a back-up copy of all resource profiles for the class in question).

'C': Unauthorized library access

REQUEST=FASTAUTH RACROUTE macro-instruction (checks the access authorization in relation to a given resource).

'D': Unauthorized library access

REQUEST=LIST, ENVIR=DELETE RACROUTE macro-instruction (used to delete the back-up copy created by ENVIR=CREATE).

'P': Blank password.

2. PACTABLE - RACF OR TOPSECRET INTERFACE

2.1. INTRODUCTION

INTRODUCTION

Security systems provide a mechanism for data access control. They perform user identification and verification, and they check resource access authorizations.

These systems control security over the whole data processing installation and, as such, operate independently from the PACTABLE system. The Interface is designed to ensure control communication between the security systems and PACTABLE.

In connection with PACTABLE and the Transaction for managing parameters and turnover to production (xxEE), the Security Interface performs the following tasks:

- On-line: automatic retrieval of the CICS or IMS SIGN-ON USERID, which is displayed on the log-on screen for PACTABLE or the xxEE transaction.

- Library access control: performed by PACTABLE instead of the security system.

- In batch: for PACTABLE procedures including user input ('*' line) that are executed under TSO, it will be possible to leave the user code and the password blank.

In order to ensure compatibility with all security systems, PACTABLE is not directly connected with the security system, but with SAF (System Authorization Facility) via the RACROUTE macro-instructions for RACF or the TSS macro-instructions for TOPSECRET.

2.2. INSTALLATION

INSTALLATION

1. Class creation

Each PACTABLE Database must be identifiable to the security system. As a result, each database corresponds to a class. A class must be created within the PACTABLE function by the PACTABLE manager using the XX90 transaction, and:

. under RACF via the 'ICHERCDE' RACF macro.

. under TOPSECRET via the command:

```
TSS RESCLASS(cccc) RESCODE(xx), with
  cccc = resource class,
  xx = hexadecimal code which identifies the resource.
```

A class name is coded on four characters and must be identical in the security system and in PACTABLE.

2. Resource creation

The creation of resources is necessary only when these are going to be checked by the security system.

A class includes all the logical resources of a PACTABLE Database, i.e., all possible access authorizations for each table (down to the sub-schema, sub-system levels). These authorizations include the following data:

AUTHORIZATION + SUB-SCHEMA + SUB-SYSTEM + TABLE NUMBER

The authorization search is processed according to the order of these elements. If there are no sub-schema, sub-system and table number, blanks are replaced by '$' signs. When a table is not assigned a specific authorization, the general access authorization is taken into account.

For RACF:

Resources are created via the 'RDEFINE' procedure.

For TOPSECRET, resources are created via the command:

```
TSS ADD (dept-name) cccc(nstable) cccc(nstable)... with

  dept-name = department name,
  n = sub-schema number,
  s = sub-system number,
  table = table code.
```

EXAMPLE:

The PACTABLE manager wishes to check all table authorizations on a given table:

```
SUB-SCHEMA NUMBER      SUB-SYSTEM NUMBER        TABLE NUMBER

      1                       3                    TABLE

The search is performed in the following order:

  1   1    3      TABLE
  2   $    3      TABLE
  3   1    $      TABLE
  4   $    $      TABLE
  5   $    $      $$$$$$
```

Under RACF or TOPSECRET, the asterisk is a generic character. As a result, on the sites controlled by a security system, the PACTABLE manager's$$$$$$$'.

3. Defining users

Resource access authorizations are granted to individual end users :

. under RACF via the 'PERMIT' procedure.

. under TOPSECRET via the command:

```
     TSS PERMIT (user-code) cccc(nstable), with
       cccc = resource class,
       n = sub-schema number,
       s = sub-system  number,
       table = table code.
```

Resources and user codes not declared to the security system are consequently prohibited in PACTABLE operations.

INVOLVED PROGRAMS

Once the PACTABLE-RACF or TOPSECRET Interface is installed, new programs or load-modules are available.

ASSEMBLER program

For RACF:

PACSECU8: batch & on-line.

This program is linked with the RENT and REUS parameters and must be stored in an authorized library. It must be inserted in the LNKLSTxx member in SYS1.PARMLIB so as to avoid the concatenation of this library in JCL STEPLIBs.

This program must also be declared to the RACF system in the ICHAUTAB table in SYS1.LPALIB, with the authority of RACLIST SVC and RACFINIT SVC.

For TOPSECRET:

PACTSS: batch under MVS/CICS; batch and on-line under MVS/IMS.
PACTSSC: on-line under MVS/CICS.

COBOL programs

PACSECB: Batch operations under MVS-CICS. Batch and on-line operations under MVS-IMS-DB/DC

xxSECT : On-line operations under MVS-CICS. This program must be inserted in the CICS PPT.

2.3. OPERATING MODE

OPERATING MODE

The addition of the PACTABLE / RACF or TOPSECRET requires a modification of the database parameters. The 'XX90' transaction where XX is the database root enables the database manager to update these parameters, specifying the security system type ('R' for RACF or 'S' for TOPSECRET), the PACTABLE database identification class, and two indicators:

- User authorization indicator:

  For RACF, it specifies whether the user, connected on CICS or IMS for the on-line mode, or TSO for the batch mode, is allowed a PACTABLE connection under a user code other than his/hers. This indicator applies only when the security system is used.

  For TOPSECRET, this indicator is forced because the user cannot log on with a user code other than his/hers.

- Resource indicator:

  Access through PACTABLE or through the security system. This indicator applies only when the security system is used.

These indicators are used to distinguish the following methods of management: total and strict management or total and flexible management under a security system.

TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM

Verification of users and table access is managed by the security interface, and a user can log on only with his/her own code.

1. Logging on in on-line mode: the PACTABLE SIGN-ON screen is initialized with the code under which the user logged on to CICS or IMS. This code is retrieved in the IO-PCB under IMS and by an EXEC CICS ASSIGN USERID command under CICS (valid only from CICS release 1.7 on). Changing the user code is prohibited.

2. The password field is locked and cannot be filled in. The cursor is positioned on the library code.

3. RACF only: LJ and LE screens: since RACF does not carry over the user code and the CICS or IMS password, they must be inserted on the JOB card. Since the system does not pass on the password, the user must enter this on the LJ or LE screen (masked fields) when first submitting a JOB or SUB action.

   A warning message is displayed if the field has not already been filled in. From release 1.9 of RACF, the password no longer needs to be filled in since a user can submit a job for another ('surrogate') user.

4. Batch procedures that include a '*' line: the user code and password are no longer required since the system automatically takes the code under which the user signed on to TSO. As a result, the PASSWORD is no longer present in the temporary files found in batch jobstreams.

   For RACF only: another consequence is that jobstreams including steps with a '*' line can be linked together without manual intervention so that the password can be specified. This process implies a restriction: the user cannot code several '*' lines with user codes other than his/her own for procedures which would normally allow him/her to do so.
   Note: with TOPSECRET, the user can never enter a code other than his/her own.

TOTAL AND FLEXIBLE MANAGEMENT UNDER A SECURITY SYSTEM

This management is possible with RACF only.

Verification of users and library access is managed by the security interface, but the user can log on with a code other than his/her own.

1. Logging on in on-line mode: identical to number 1 under 'TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM' above, but the field including the USER code is an input field, as is the PASSWORD field. The user can modify these two fields (password is required). In case of modification, the interface performs a test to validate the USER code, and the security system performs a test to validate the password.

2. LJ, LE screens: identical to number 3 under 'TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM' above. If the user entered the password on the logon screen, it does not have to be entered again.

3. Batch procedures that include a '*' line: just as in the case of on-line processing when the user code is different from the one under TSO, the password has to be filled in. This makes it possible to submit jobs with several '*' lines having different user codes.

   Temporary files do not include the password, which means that it is not possible to link together steps having a '*' line. The password has to be entered each time. Nevertheless, if the USER code is identi Nevertheless, if the USER code is identical to the one under TSO, verification of users and library access is managed as described in number 4 under 'TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM' above.

Field TYPE of transaction XX90 has therefore one of two values: "blank" or "P". "P" stands for the resource verification by PACTABLE and not by the security system.

Field BLOC has one of two values: "blank" or "N". "N" specifies that the user cannot use a password other than his/her own.

2.4. ERROR MANAGEMENT (RACF ONLY)

RACF ERROR MANAGEMENT

If the RACF system detects an error when a user logs on, a PACBASE error message is displayed. This message is completed by a return code that includes a RACF return code and the error type.

The security administrator should be informed of the general return code so that the problem can be resolved accordingly.

There are five error types:

'I': Error on user code

REQUEST=VERIFY RACROUTE macro-instruction (checks the user code with password).

'L': Unauthorized library access

REQUEST=LIST, ENVIR=CREATE RACROUTE macro-instruction (used to create a back-up copy of all resource profiles for the class in question).

'C': Unauthorized library access

REQUEST=FASTAUTH RACROUTE macro-instruction (checks the access authorization in relation to a given resource).

'D': Unauthorized library access

REQUEST=LIST, ENVIR=DELETE RACROUTE macro-instruction (used to delete the back-up copy created by ENVIR=CREATE).

'P': Blank password.

3. DSMS - RACF OR TOPSECRET INTERFACE

3.1. INTRODUCTION

INTRODUCTION

Security systems provide a mechanism for data access control. They perform user identification and verification.

These systems control security over the whole data processing installation and, as such, operate independently from the DSMS system. The Interface is designed to ensure control communication between the security systems and DSMS.

In connection with DSMS, the Security Interface performs the following tasks:

- On-line: automatic retrieval of the CICS or IMS SIGN-ON USERID, which is displayed on the log-on screen.

- In batch: for DSMS procedures including user input ('*' line) that are executed under TSO, it will be possible to leave the user code and the password blank.

In order to ensure compatibility with all security systems, DSMS is not directly connected with the security system, but with SAF (System Authorization Facility) via the RACROUTE macro-instructions for RACF or the TSS macro-instructions for TOPSECRET.

3.2. INSTALLATION

INSTALLATION

INVOLVED PROGRAMS

Once the DSMS-RACF or TOPSECRET Interface is installed, new programs or load-modules are available.

ASSEMBLER program

For RACF:

PACSECU8: batch & on-line.

This program is linked with the RENT and REUS parameters and must be stored in an authorized library. It must be inserted in the LNKLSTxx member in SYS1.PARMLIB so as to avoid the concatenation of this library in JCL STEPLIBs.

This program must also be declared to the RACF system in the ICHAUTAB table in SYS1.LPALIB, with the authority of RACLIST SVC and RACFINIT SVC.

For TOPSECRET:

PACTSS: batch under MVS/CICS; batch and on-line under MVS/IMS.
PACTSSC: on-line under MVS/CICS.

COBOL programs

PACSECB: Batch operations under MVS-CICS. Batch and on-line operations under MVS-IMS-DB/DC

xxSECT : On-line operations under MVS-CICS. This program must be inserted in the CICS PPT.

3.3. OPERATING MODE

OPERATING MODE

The interface performs verification based on the indicators specified in the DRST procedure:

- Security system use indicator

- User authorization indicator:

  For RACF, it indicates whether the user logged on under CICS or IMS for on-line, or TSO for batch, is entitled to log on to DSMS with a user code other than his/her own. This indicator is valid only if the security system is used.

  For TOPSECRET, this indicator is forced: it is impossible to log on with a user code other than his/her own.

These indicators are used to distinguish the following methods of management: total and strict management under a security system, total and flexible management under a security system and resource management under DSMS.

TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM

Verification of users and library access is managed by the security interface, and a user can log on only with his/her own code.

1. Logging on for on-line processing: the DSMS SIGN-ON screen is initialized with the code under which the user logged on to CICS or IMS. This code is retrieved in the IO-PCB under IMS and by an EXEC CICS ASSIGN USERID command under CICS (valid only from CICS release 1.7 on). Changing the user code is prohibited.

2. LVQ screen (RACF only): since RACF does not carry over the user code and the CICS or IMS password, you have to insert them on the JOB card. Since DSMS reads the password in the TUD table, the password must be identical to that declared in CICS or iMS.

3. Batch procedures that include a '*' line: the user code and password are no longer required since the system automatically takes the code under which the user signed on to TSO.

   As a result, the PASSWORD is no longer present in the temporary files found in batch jobstreams, including DPRT, since the security system ensures the propagation of the USER code and the PASSWORD.
   Another consequence is that jobstreams including steps with a '*' line can be linked together without manual intervention so that the password can be specified.
   For RACF, this process implies a restriction: the user cannot code several '*' lines with user codes other than his/her own for procedures which would normally allow the user to do so.
   For TOPSECRET, the user can never enter user codes other than his/her own.

4. The password field is locked and cannot be filled in. The cursor is positioned on the library code.

TOTAL AND FLEXIBLE MANAGEMENT UNDER A SECURITY SYSTEM

This management is possible under RACF only.

Verification of users and library access is managed by the security interface, but the user can log on with a code other than his/her own.

1. Logging on for on-line processing: identical to number 1 under 'TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM' above, but the field including the USER code is an input field, as is the PASSWORD field. The user can change these two fields; the password is required. In the case of a change, the interface performs a test to validate the USER code, and the security system performs a test to validate the password.

2. LVQ screen: identical to number 2 under 'TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM' above.

3. Batch procedures that include a '*' line: just as in the case of on-line processing when the user code is different from the one under TSO, the password has to be filled in. This makes it possible to submit jobs with several '*' lines having different user codes. In the case of different USER codes, jobs submitted by DPRT will include the USER and PASSWORD parameters. Even in this case, temporary files will not include the password, which means that it isn't possible to link together steps having a '*' line. The password has to be entered every time. Of course, if the USER code is identical to the one under TSO, verification of users and library access is managed as described in number 3 under 'TOTAL AND STRICT MANAGEMENT UNDER A SECURITY SYSTEM' above.

3.4. ERROR MANAGEMENT (RACF ONLY)

RACF ERROR MANAGEMENT

If the RACF system detects an error when a user logs on, a DSMS error message is displayed. This message is completed by a return code that includes a RACF return code and the error type.

The security administrator should be informed of the general return code so that the problem can be resolved accordingly.

There are two error types:

'I': Error on user code

REQUEST=VERIFY RACROUTE macro-instruction (checks the user code with password).

'P': Blank password.