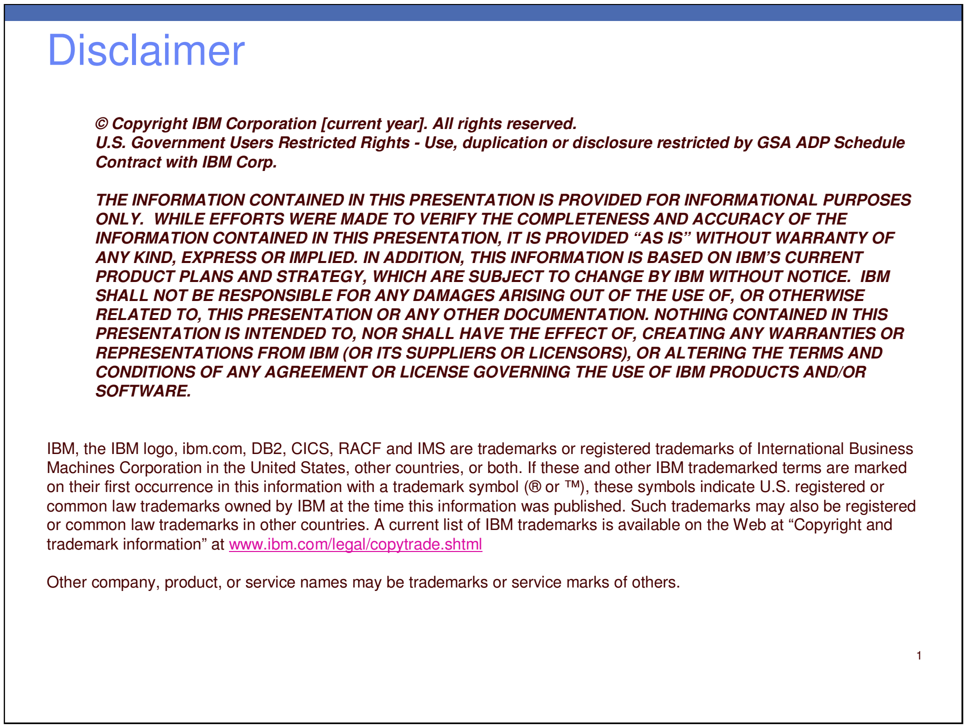
Secrets of IMS Security

Maida Snapper
IBM

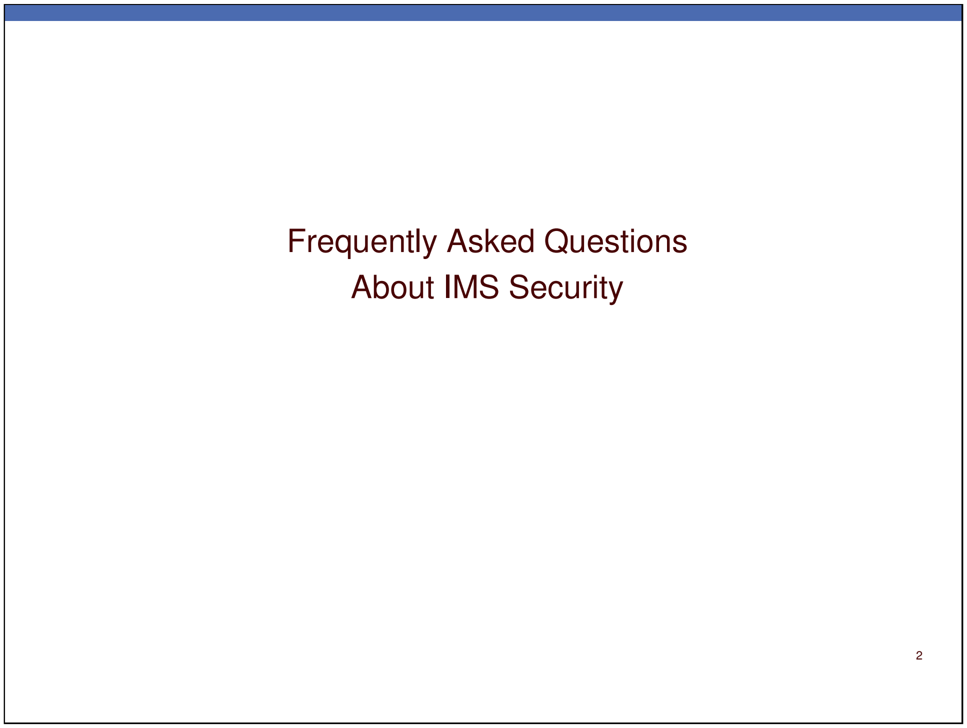
August 5, 2010
Share Session 7862

SHARE in Boston



Disclaimer

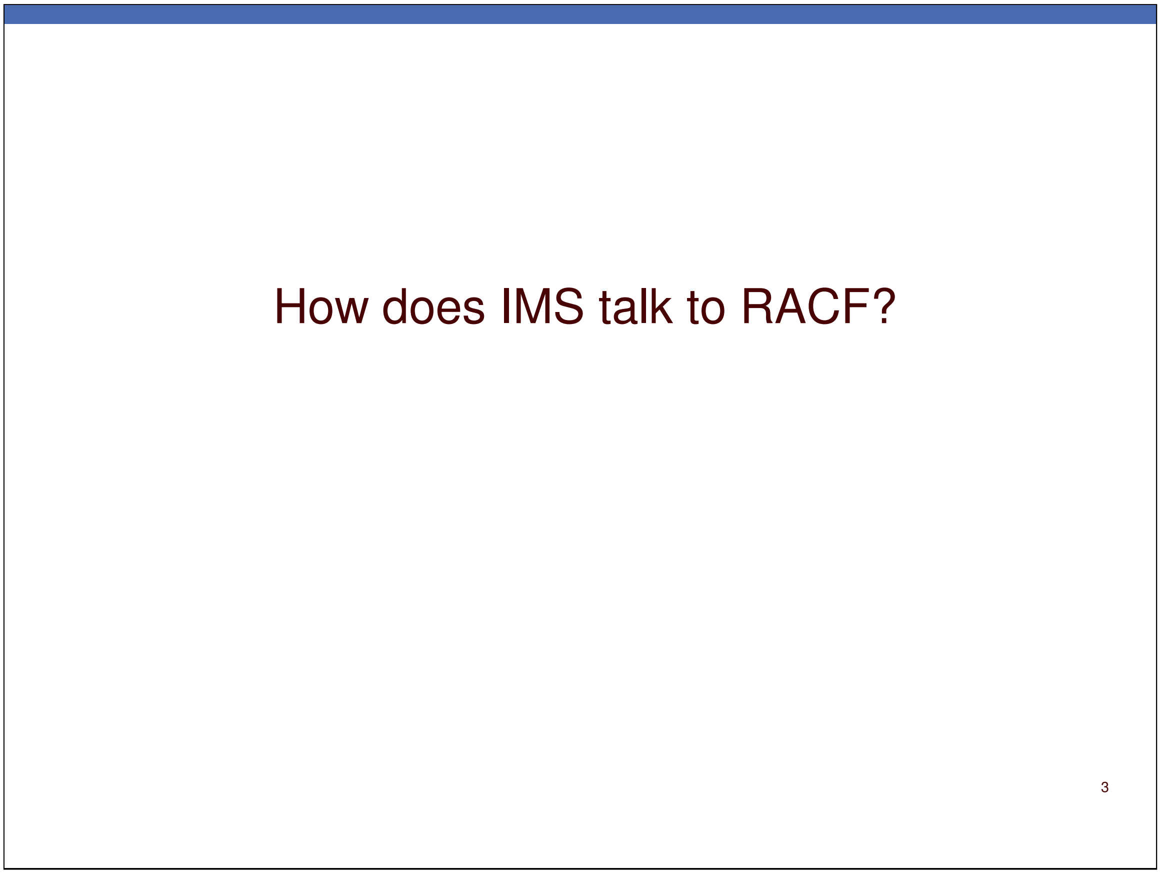
THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS AND/OR SOFTWARE.



Frequently Asked Questions
About IMS Security

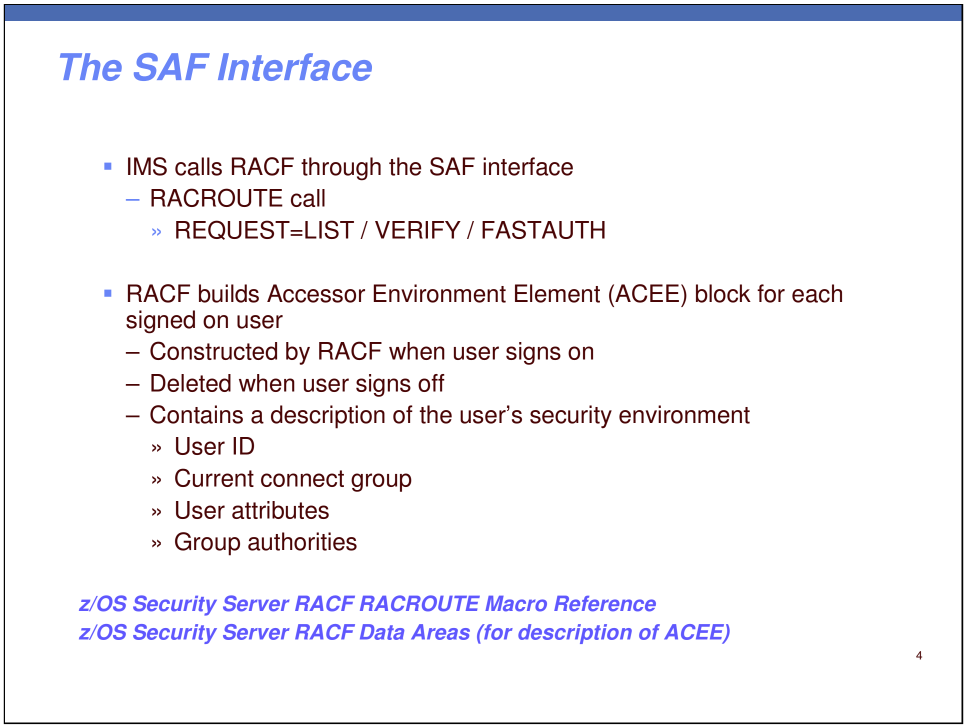
2

At least one form of protection is available for each resource. The protection for each IMS resource may be provided by one or more security facilities, such as RACF and/or user exit routines.



How does IMS talk to RACF?

IMS talks to RACF through the z/OS SAF interface. The security product does not have to be RACF. IMS can talk to any security product that conforms to the rules of the SAF interface including ACF2, Top Secret, or a product you write yourself.



The SAF Interface

- IMS calls RACF through the SAF interface
  - RACROUTE call
    - REQUEST=LIST / VERIFY / FASTAUTH

- RACF builds Accessor Environment Element (ACEE) block for each signed on user
  - Constructed by RACF when user signs on
  - Deleted when user signs off
  - Contains a description of the user’s security environment
    - User ID
    - Current connect group
    - User attributes
    - Group authorities

z/OS Security Server RACF RACROUTE Macro Reference
z/OS Security Server RACF Data Areas (for description of ACEE)

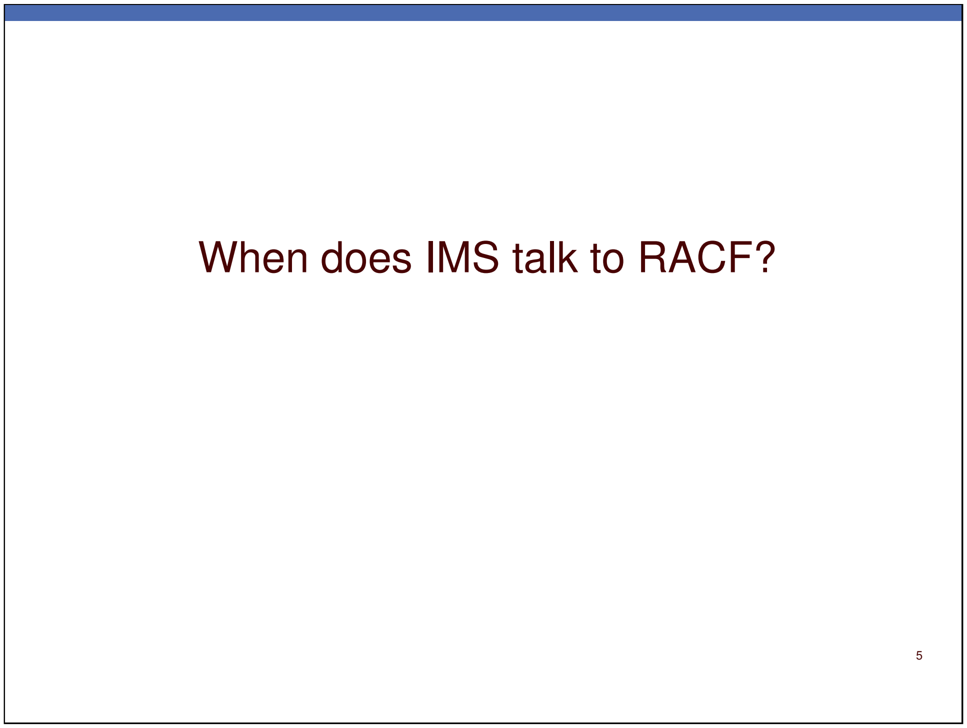
SAF is part of the base z/OS Operating System.

SAF usually works with an External Security Manager (ESM) such as RACF.

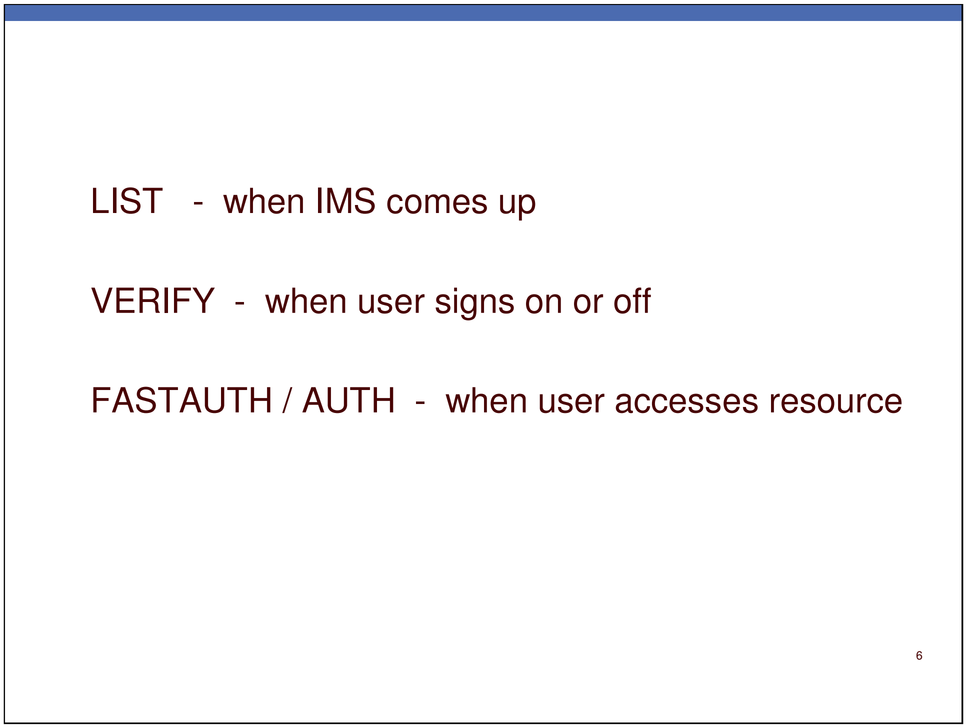
SAF is invoked at many points within the z/OS Operating System where security decisions have to be made.

SAF is invoked to perform Authentication, Resource Access control, and Auditing.

SAF can be invoked by other software



When does IMS talk to RACF?

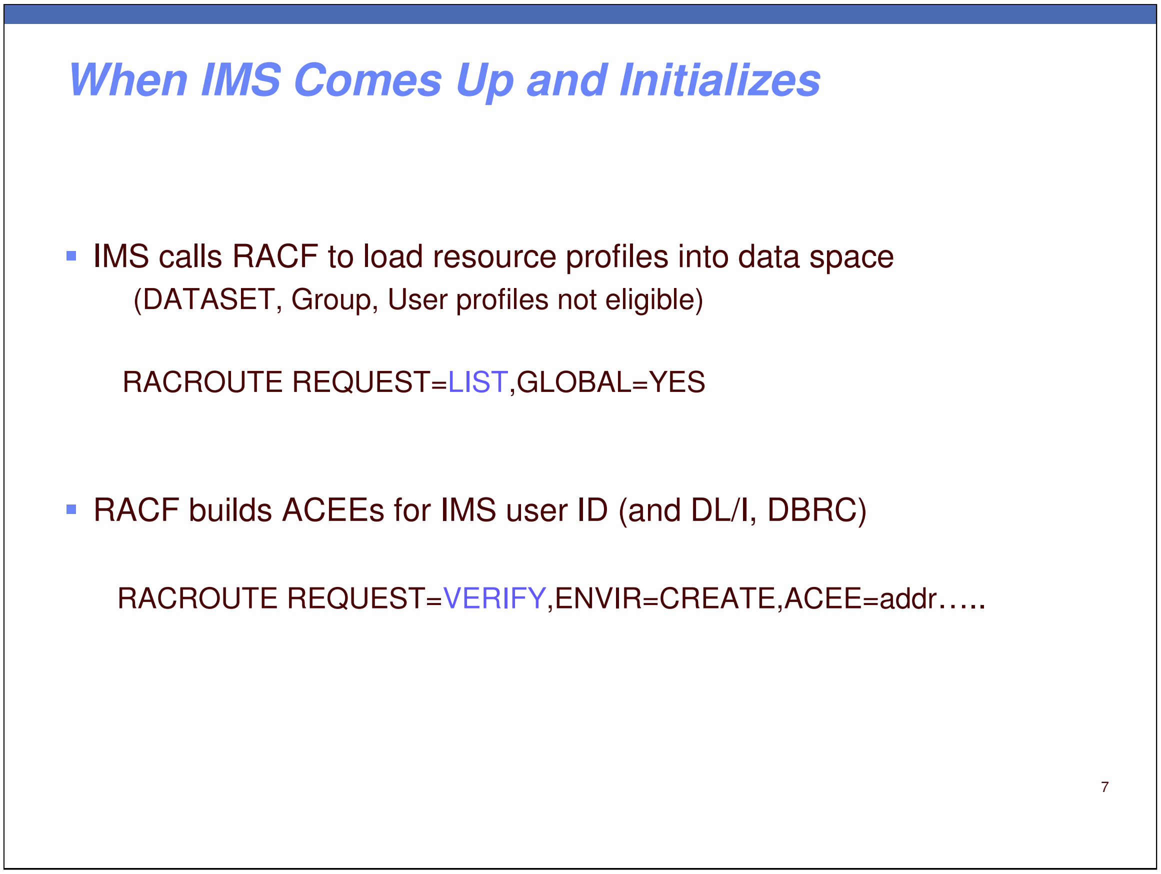


LIST - when IMS comes up

VERIFY - when user signs on or off

FASTAUTH / AUTH - when user accesses resource

6



When IMS Comes Up and Initializes

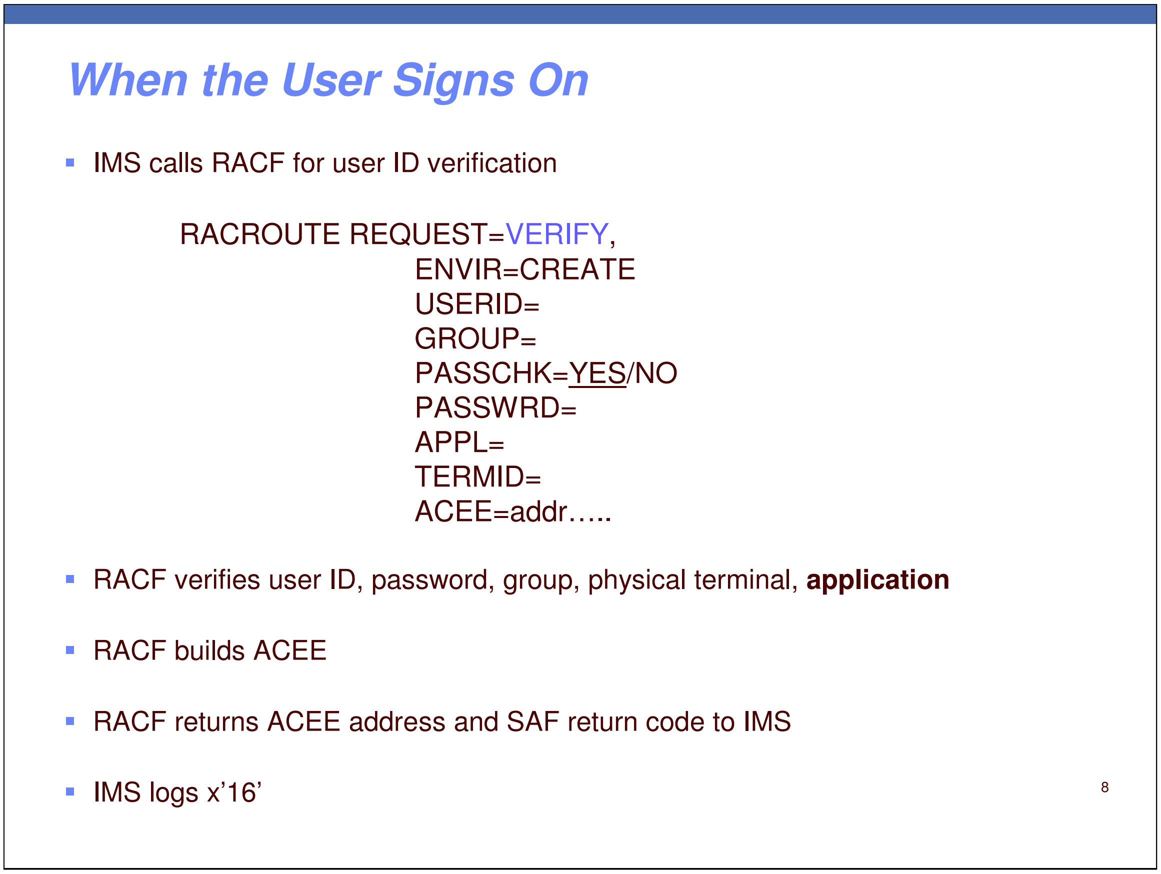
- IMS calls RACF to load resource profiles into data space
  (DATASET, Group, User profiles not eligible)

  RACROUTE REQUEST=LIST,GLOBAL=YES

- RACF builds ACEEs for IMS user ID (and DL/I, DBRC)

  RACROUTE REQUEST=VERIFY,ENVIR=CREATE,ACEE=addr…..

When an application like IMS RACLISTs a class using RACROUTE REQUEST=LIST,GLOBAL=YES, the RACLISTed profiles are stored in a data space. The data space can be shared by many applications. Applications that issue a subsequent RACROUTE REQUEST=LIST,GLOBAL=YES for the same class simply access the data space built by the first application. When all applications have relinquished their access to the data space by issuing a RACROUTE REQUEST=LIST,ENVIR=DELETE request, the data space can be deleted by issuing a SETROPTS NORACLIST(classname) command. The SETROPTS NORACLIST command processes not only the class specified by classname, but also all valid classes that share the same POSIT value as classname. If you issue a SETROPTS RACLIST for that class, RACF rebuilds the data space from the RACF database profiles and replaces the existing data space.



When the User Signs On

- IMS calls RACF for user ID verification

```
          RACROUTE REQUEST=VERIFY,
                          ENVIR=CREATE
                          USERID=
                          GROUP=
                          PASSCHK=YES/NO
                          PASSWRD=
                          APPL=
                          TERMID=
                          ACEE=addr…..
```

- RACF verifies user ID, password, group, physical terminal, **application**
- RACF builds ACEE
- RACF returns ACEE address and SAF return code to IMS
- IMS logs x'16'

z/OS Security Server RACF RACROUTE Macro Reference

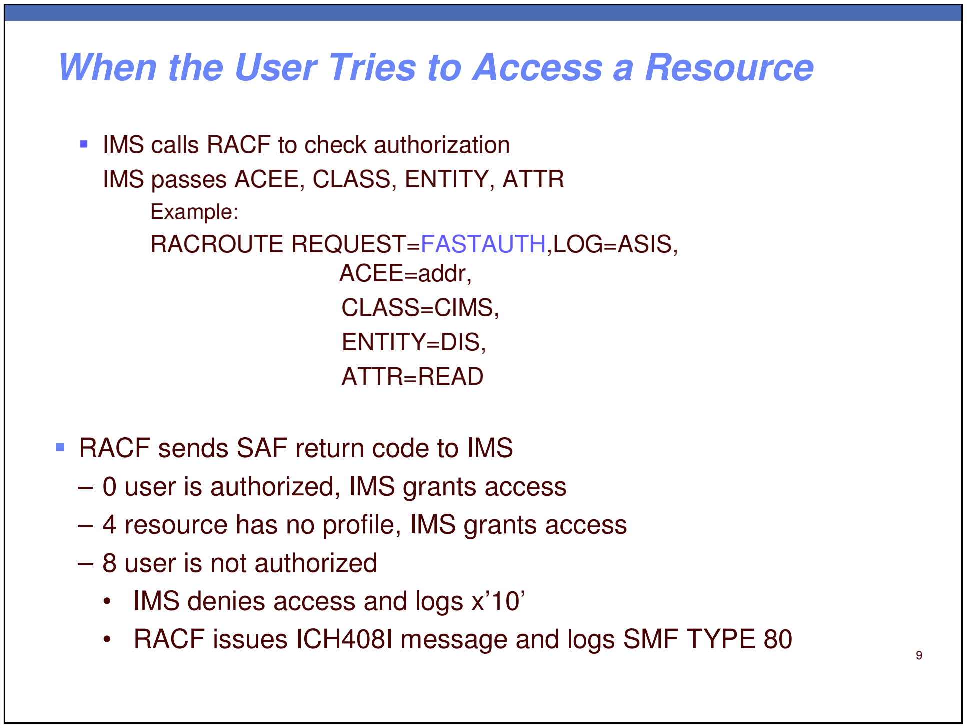
RACF user verification is invoked when an IMS/ESA user enters the /SIGN ON command. RACF verifies:

- *Is this a valid user (defined to RACF)*
- *Is the password correct for this userid (USERID)*
- *Is user authorized to connect to the specified group (GROUP)*
- *Is the user entering a new password (PASSWRD)*
- *Is the user authorized to sign on to this IMS (APPL)*
- *Is the user authorized to use this physical terminal (TERMID)*
- *Is the sign on a being done during the authorized times*

TERMID is the physical terminal being used. If it is protected in the RACF TERMINAL/GTERMNL class, then the user must be authorized in the access list.

APPL is the application the user is accessing. In this case, it is the *imsid*. When applications like IMS, TSO, CICS, etc. are protected in the RACF APPL class, the user must be authorized in the access list.

If IMS RAS security is activated (ISIS=R|A), all dependent region user IDs must also be authorized in the access list of the *imsid* in the APPL class.



When the User Tries to Access a Resource

- IMS calls RACF to check authorization

  IMS passes ACEE, CLASS, ENTITY, ATTR

  Example:

```
RACROUTE REQUEST=FASTAUTH,LOG=ASIS,
                ACEE=addr,
                CLASS=CIMS,
                ENTITY=DIS,
                ATTR=READ
```

- RACF sends SAF return code to IMS
  - 0 user is authorized, IMS grants access
  - 4 resource has no profile, IMS grants access
  - 8 user is not authorized
    - IMS denies access and logs x’10’
    - RACF issues ICH408I message and logs SMF TYPE 80

9

Who is attempting the access?

What is the class of the resource?

What is the name of the resource?

What type of access is being requested (e.g. READ or WRITE)?

Once RACF has completed its actions it passes return code and reason code information back to SAF.

SAF returns control to the Resource Manager, with its own return and reason codes, and with RACF’s return and reason codes.

When RACROUTE passes control back to the resource manager (IMS), the resource manager can examine the Return Code and Reason Code values and can then make a decision on the basis of those codes.

Depending on details about the user, system settings, and resource, logging may take place.

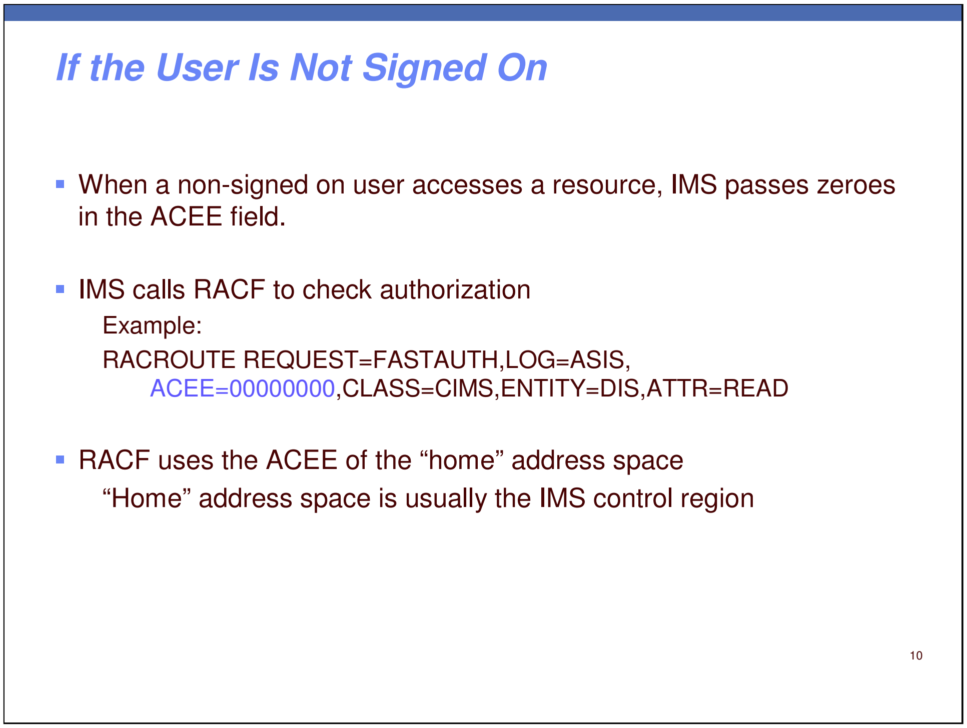
RACF calls SMF to perform the logging. SMF is responsible for placing the log records onto the SMF log datasets.

ASIS RACF records the event in the manner specified in the profile that protects the resource, or by other methods such as a SETROPTS option.

For FASTAUTH, the default is LOG=NONE; IMSV10 specifies LOG=ASIS

IMSV9 does not always specify LOG=ASIS and would have to make a second call to RACF (AUTH) if auditing is required.

For AUTH and VERIFY, default is LOG=ASIS



If the User Is Not Signed On

- When a non-signed on user accesses a resource, IMS passes zeroes in the ACEE field.
- IMS calls RACF to check authorization

  Example:

  ```
  RACROUTE REQUEST=FASTAUTH,LOG=ASIS,
      ACEE=00000000,CLASS=CIMS,ENTITY=DIS,ATTR=READ
  ```

- RACF uses the ACEE of the “home” address space

  “Home” address space is usually the IMS control region

LOG= describes the auditing options

ASIS RACF records the event in the manner specified in the profile that protects the resource, or by other methods such as a SETROPTS option.

For FASTAUTH, the default is LOG=NONE; IMS (as of version 10) always specifies LOG=ASIS

LOG=ASIS ,LOG=NOFAIL ,LOG=NONE specifies the types of access attempts to be audited.

ASIS - RACF performs auditing if its authorization check results in success (RC=0) or failure (RC=8), and determines whether auditing is necessary based on the following conditions:

The user's UAUDIT setting

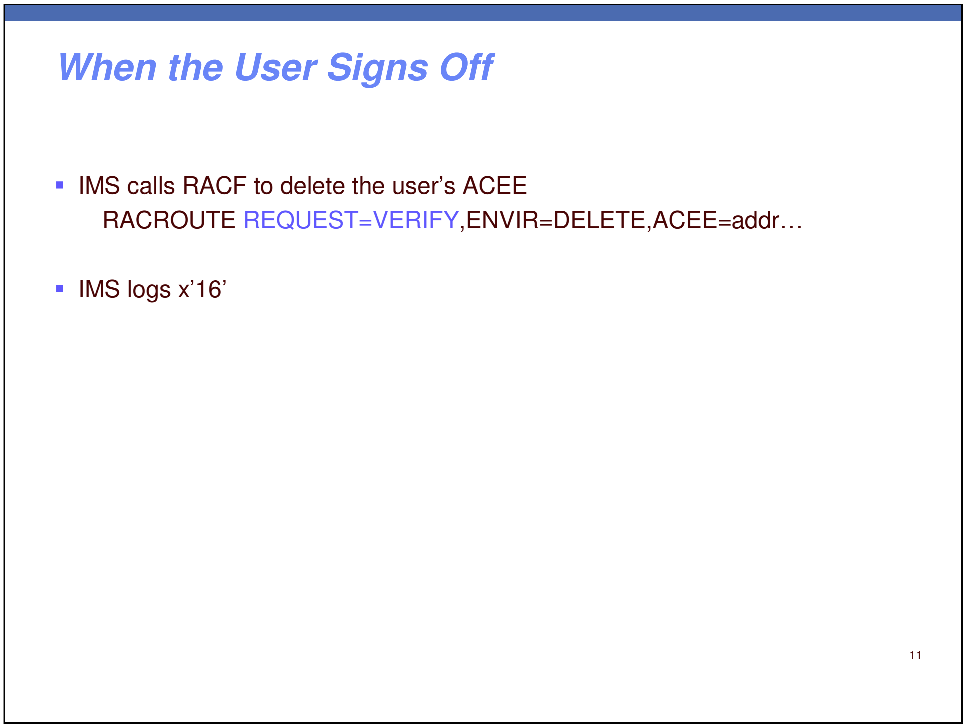
The AUDIT, GLOBALAUDIT, and WARNING options in effect for the resource

If SETR SECLABELAUDIT is in effect, then the AUDIT options in the resource SECLABEL profile

The pre- or postprocessing installation exit's indication of whether or not to do auditing.

NOFAIL - If the authorization check fails, the attempt is not recorded. If the authorization check succeeds, the attempt is recorded as in ASIS.

NONE - The attempt is not recorded. LOG=NONE suppresses both messages

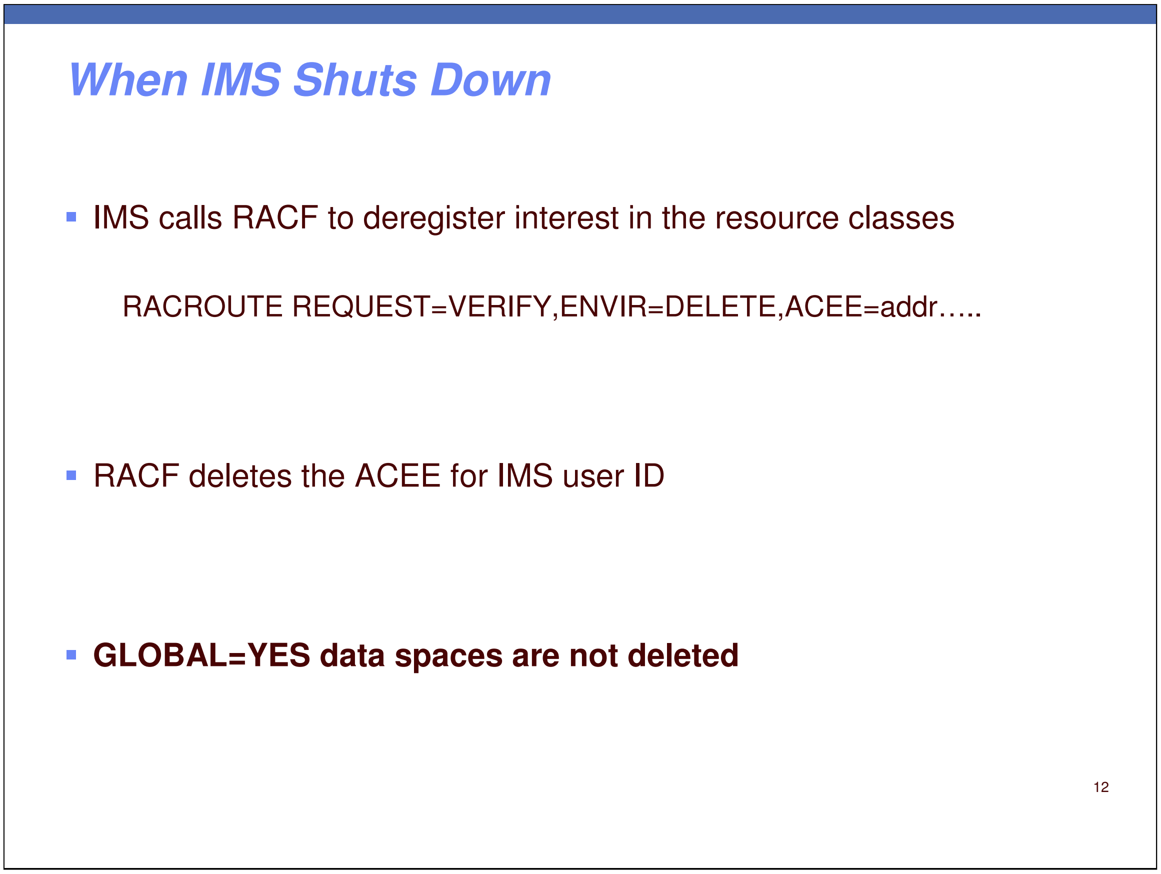


When the User Signs Off

- IMS calls RACF to delete the user’s ACEE

```
RACROUTE REQUEST=VERIFY,ENVIR=DELETE,ACEE=addr…
```

- IMS logs x’16’



When IMS Shuts Down

- IMS calls RACF to deregister interest in the resource classes

  RACROUTE REQUEST=VERIFY,ENVIR=DELETE,ACEE=addr…..

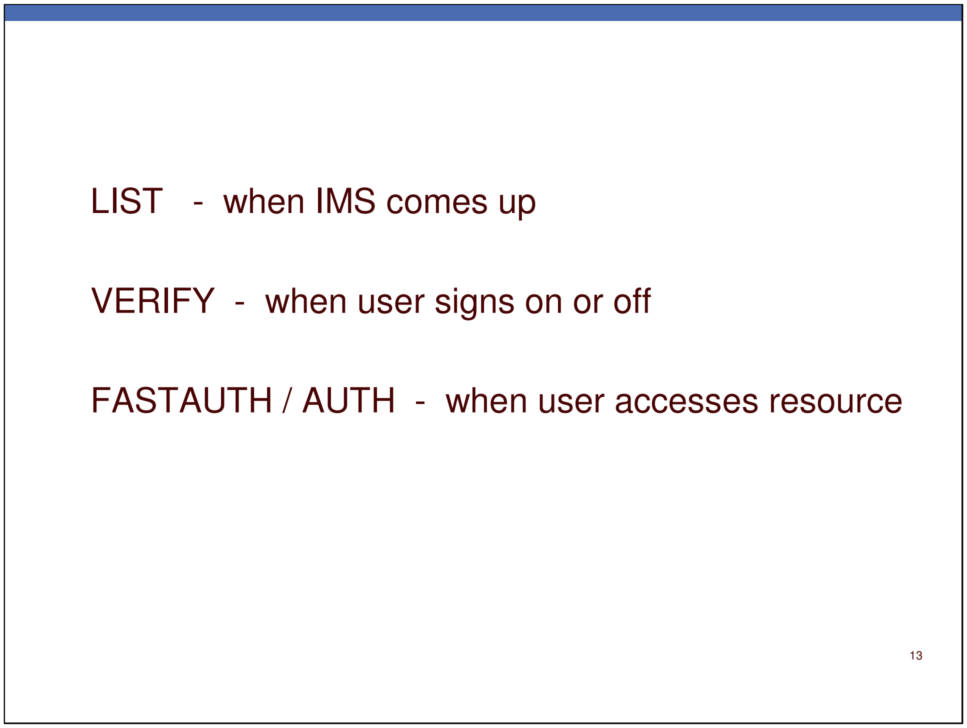
- RACF deletes the ACEE for IMS user ID

- **GLOBAL=YES data spaces are not deleted**

When IMS terminates (and “signs off”), RACF does not delete the data space containing the IMS resource profiles.

When IMS comes up again and issues a RACROUTE REQUEST=LIST,GLOBAL=YES for the same class, RACF will access the data space that is already there. That is why is it necessary to do RACF REFRESH in order for any changes made to the RACF database to take effect in the RACF data space.

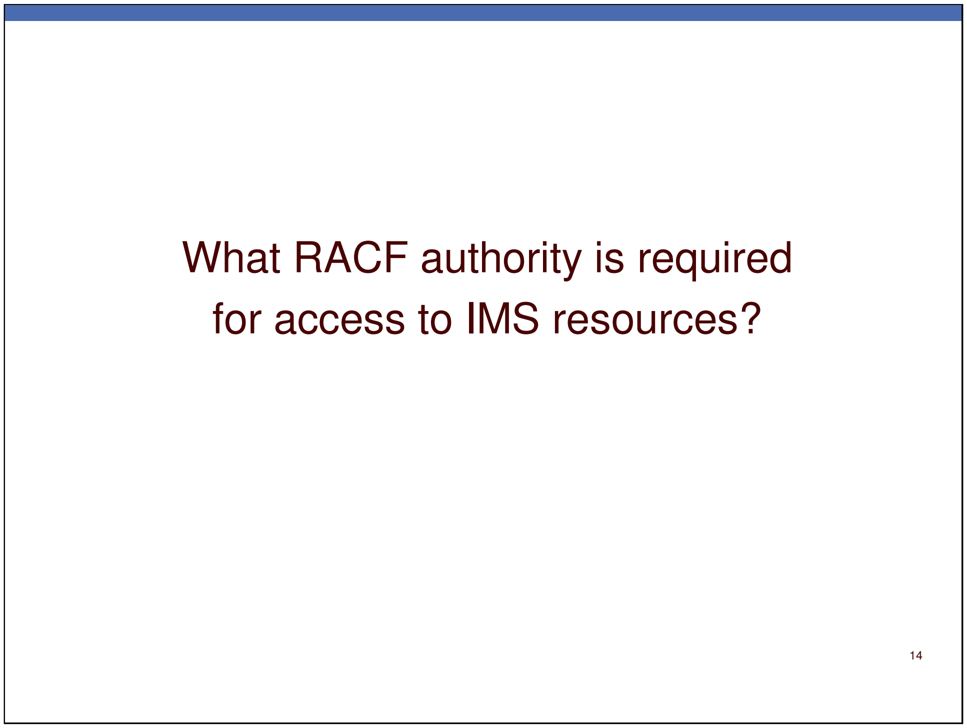
When all applications have relinquished their access to the data space by issuing a RACROUTE REQUEST=LIST,ENVIR=DELETE request, the data space can (optionally) be deleted by issuing a SETROPTS NORACLIST(classname) command.



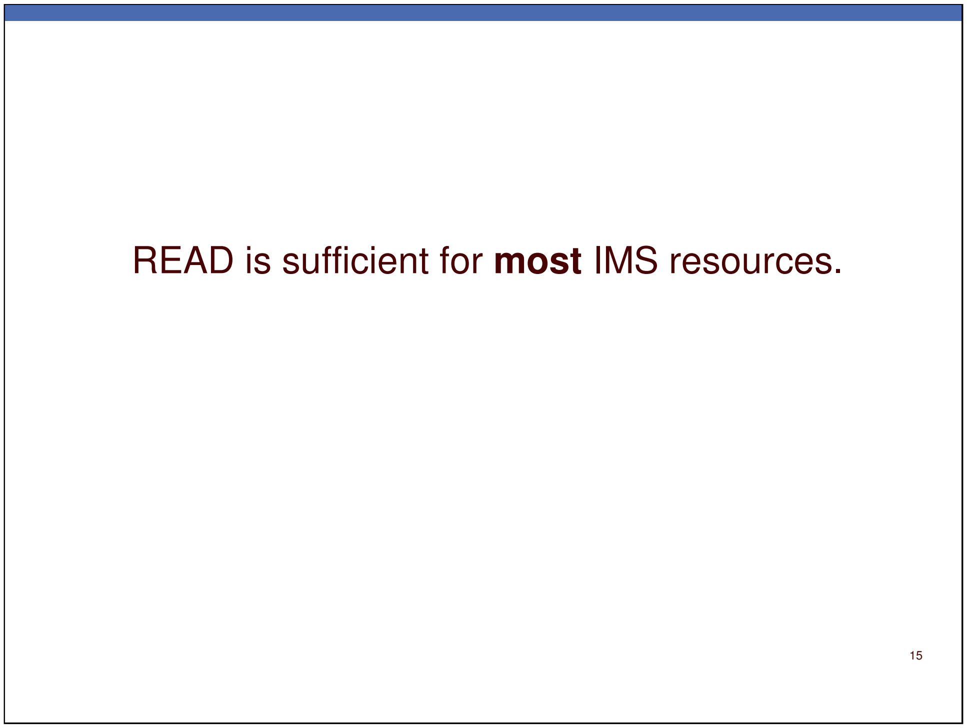
LIST - when IMS comes up

VERIFY - when user signs on or off

FASTAUTH / AUTH - when user accesses resource

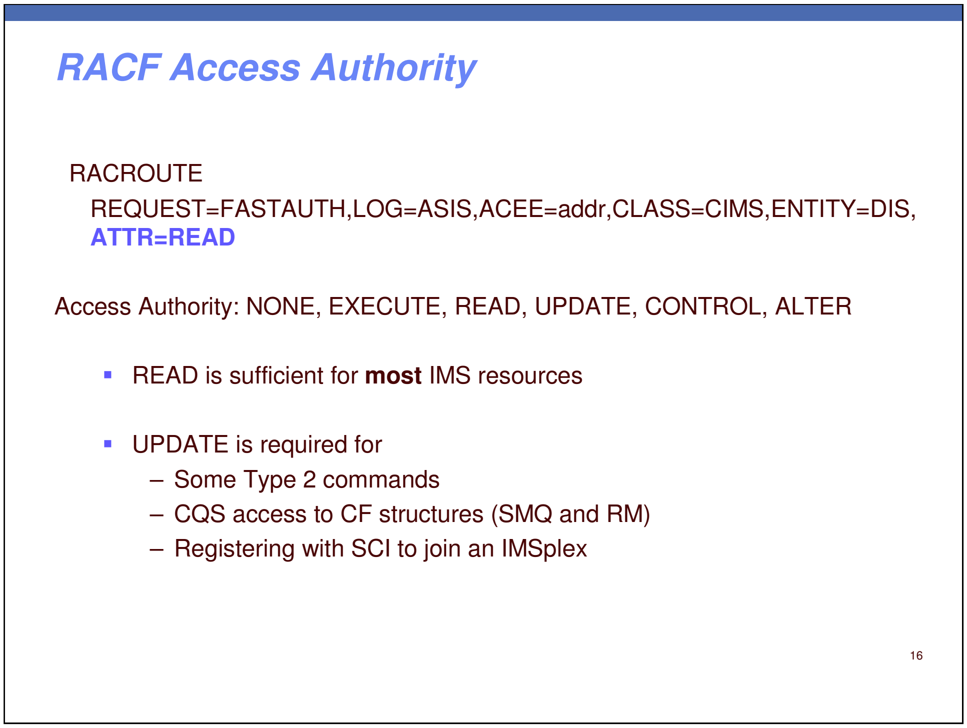


What RACF authority is required for access to IMS resources?



READ is sufficient for **most** IMS resources.

15



RACF Access Authority

```
RACROUTE
  REQUEST=FASTAUTH,LOG=ASIS,ACEE=addr,CLASS=CIMS,ENTITY=DIS,
  ATTR=READ
```

Access Authority: NONE, EXECUTE, READ, UPDATE, CONTROL, ALTER

- READ is sufficient for **most** IMS resources

- UPDATE is required for
  - Some Type 2 commands
  - CQS access to CF structures (SMQ and RM)
  - Registering with SCI to join an IMSplex

Universal access authority (UACC) is the default access authority that applies to a resource if the user or group is not specifically permitted access to the resource. The universal access authority can be any of the access authorities: NONE, READ, EXECUTE, CONTROL, UPDATE, and ALTER.

NONE -Specifies that the user or group not be permitted to access the resource.

READ -Specifies that the user or group be authorized to access the resource for the purpose of reading only. This is the level of access needed to access most IMS resources. In order for users to execute commands and transactions, they need to be permitted with an access level of 'READ'.

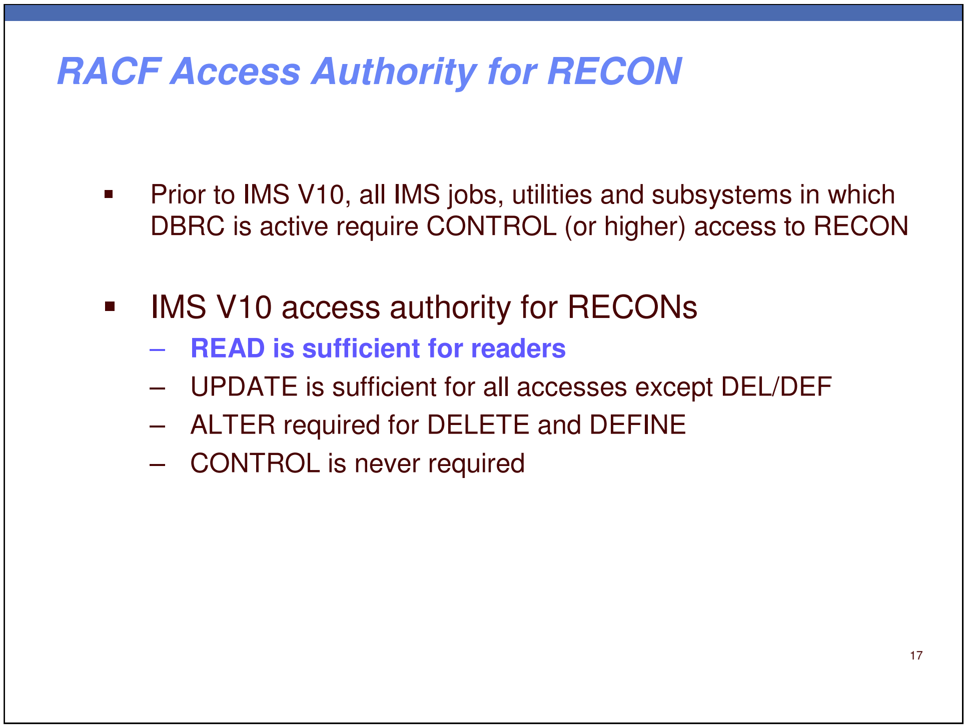
EXECUTE -Specifies that the user or group can run programs but not read or copy them.

UPDATE -Specifies that the user or group be authorized to access the resource for the purpose of reading or writing.

CONTROL -Is used only for VSAM data sets and specifies that the user or group have access authority that is equivalent to the VSAM control password.

ALTER -Specifies that the user or group have full control over the resource.

The other items in the security profile (security classification, auditing options, warning options, and notification options) are not covered in the class. See your RACF security administrator or the RACF manuals for more information on these options.



RACF Access Authority for RECON

- Prior to IMS V10, all IMS jobs, utilities and subsystems in which DBRC is active require CONTROL (or higher) access to RECON

- IMS V10 access authority for RECONs
  - **READ is sufficient for readers**
  - UPDATE is sufficient for all accesses except DEL/DEF
  - ALTER required for DELETE and DEFINE
  - CONTROL is never required

Access authority for data sets Data sets can have one of the following access authorities:

NONE Does not allow users to access the data set.

EXECUTE For a private load library, EXECUTE allows users to load and execute, but not to read or copy, programs (load modules) in the library. In order to specify EXECUTE for a private load library, you must ask for assistance from your RACF security administrator.

Attention Anyone who has READ, UPDATE, CONTROL, or ALTER authority to a protected data set can create a copy of it. As owner of the copied data set, that user has control of the security characteristics of the copied data set, and can change them. For this reason, you should assign a UACC of NONE, and then selectively permit a small number of users to access your data set, as their needs become known.

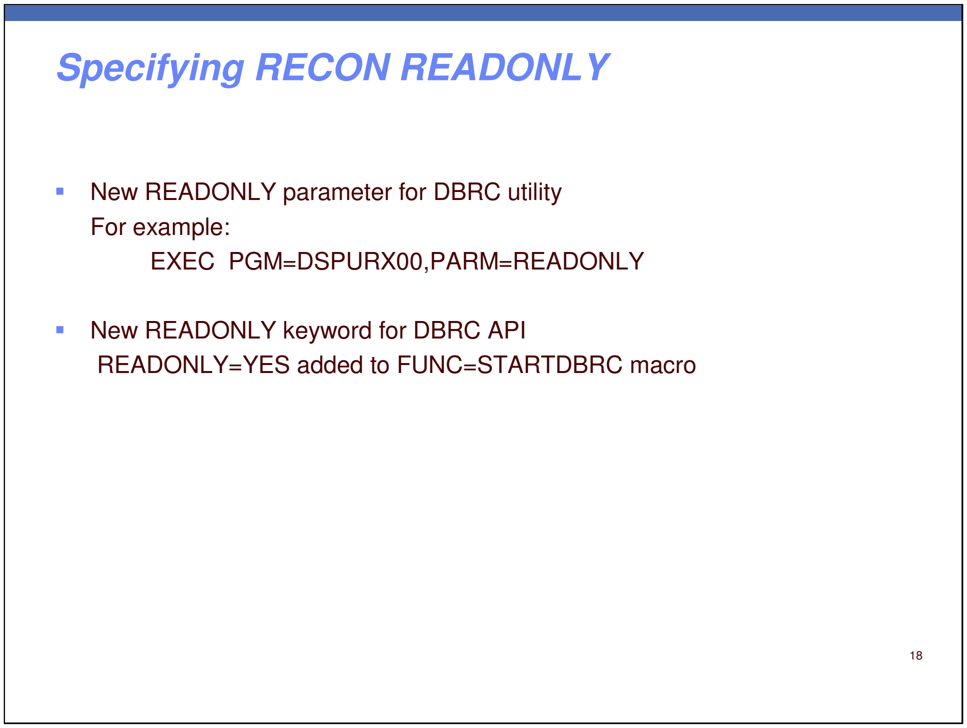
READ Allows users to access the data set for reading only. (Note that users who can read the data set can copy or print it.)

UPDATE Allows users to read from, copy from, or write to the data set. UPDATE does *not* authorize a user to delete, rename, move, or scratch the data set. Allows users to perform normal VSAM I/O (not improved control interval processing) to VSAM data sets.

CONTROL For VSAM data sets, CONTROL is equivalent to the VSAM CONTROL password; that is, it allows users to perform improved control interval processing—CONTROL is control-interval access (access to individual VSAM data blocks), and the ability to retrieve, update, insert, or delete records in the specified data set. For non-VSAM data sets, CONTROL is equivalent to UPDATE.

ALTER ALTER allows users to read, update, delete, rename, move, or scratch the data set.

When specified in a discrete profile, ALTER allows users to read, alter, and delete the profile itself *including the access list*. ALTER does not allow users to change the owner of the profile using the ALTDSD command. However, if a user with ALTER access authority to a discrete data set profile renames the data set, changing the high-level qualifier to his or her own user ID, both the data set and the profile are renamed, *and* the OWNER of the profile is changed to the new user ID. ALTER authority to a generic profile allows users to create new data sets that are covered by that profile, it does not give users authority over the profile itself.



Specifying RECON READONLY

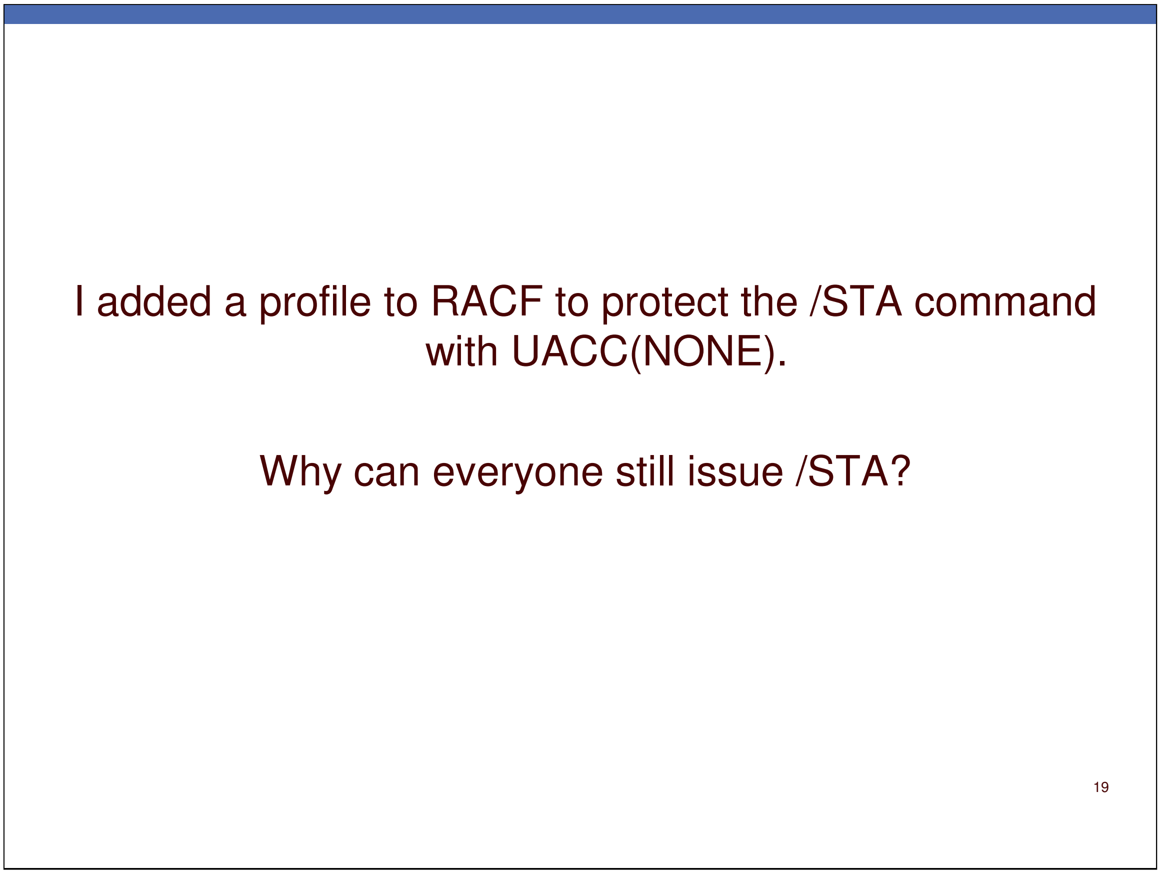
- New READONLY parameter for DBRC utility
  For example:
  ```
  EXEC  PGM=DSPURX00,PARM=READONLY
  ```
- New READONLY keyword for DBRC API
  READONLY=YES added to FUNC=STARTDBRC macro

18

IMS V10 adds READONLY support for the RECONs. This is invoked with PARM(READONLY) on the EXEC statement for the DBRC utility (DSPURX00) or by specifying the new READONLY=YES parameter on the DBRC API FUNC=STARTDBRC macro. When READONLY is specified, the RECONs are opened for read. This means that only READ authority is required in SAF (RACF).

IMS V10 has made another change to open. Due to this change, CONTROL does not have to be specified for users who update the RECONs. Only UPDATE authority is required. Of course, ALTER is still required for users who DELETE and DEFINE the data sets. In previous releases DBRC opened the RECONs with CONTROL specified in the VSAM ACB for the RECONs. This required CONTROL authority for open. In IMS V10 the open has changed. If READONLY is not specified, the open is done for update but CONTROL is not specified in the ACB. This means that only UPDATE authority is required.

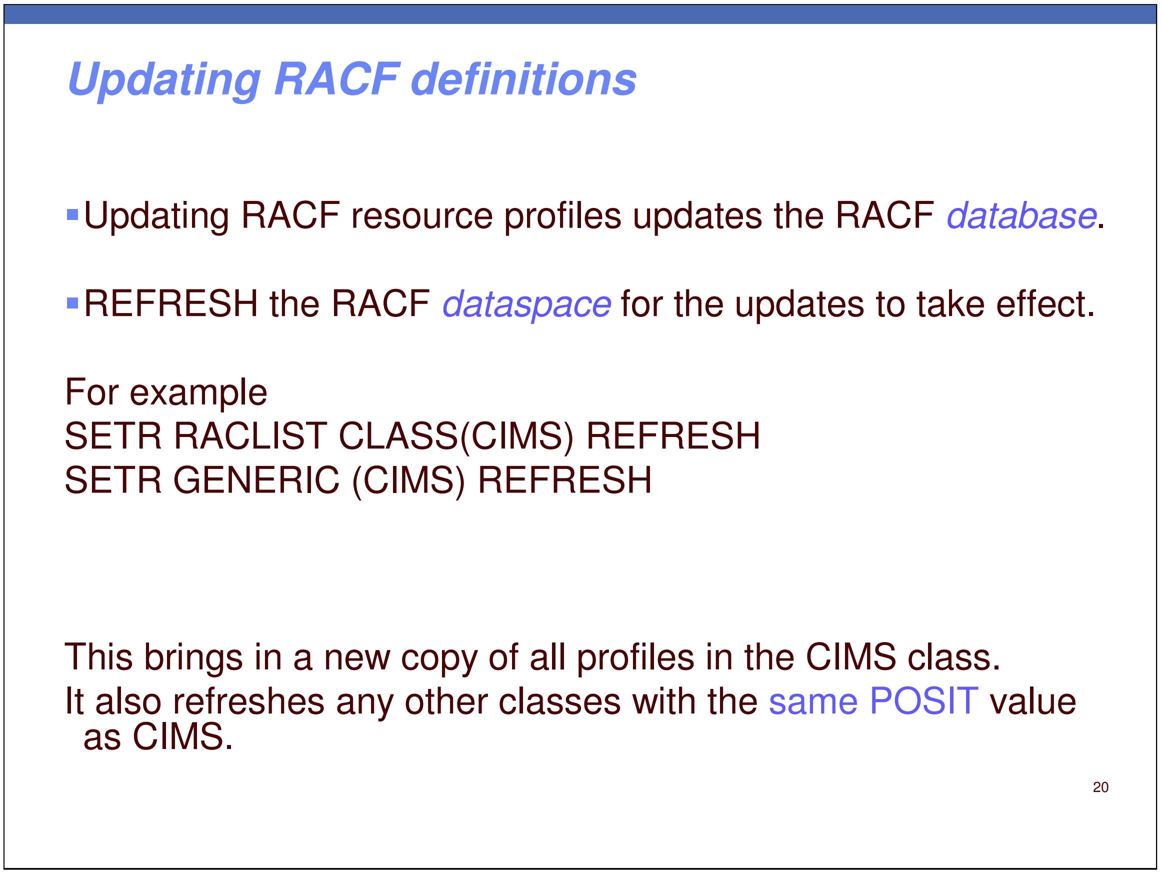
As with previous releases, if you invoke the DBRC utility from your program you may use the DSPURXRT entry point. IMS V10 has added the capability to specify READONLY through a parameter passed to the entry point in the first word of the argument list.



I added a profile to RACF to protect the /STA command with UACC(NONE).

Why can everyone still issue /STA?

Once the security definitions have been created and stored on the RACF database, you will need to refresh the security information in storage to have the new security definitions take effect.



Updating RACF definitions

- Updating RACF resource profiles updates the RACF *database*.
- REFRESH the RACF *dataspace* for the updates to take effect.

For example
SETR RACLIST CLASS(CIMS) REFRESH
SETR GENERIC (CIMS) REFRESH

This brings in a new copy of all profiles in the CIMS class.
It also refreshes any other classes with the same POSIT value as CIMS.

20

SETROPTS RACLIST(classname) REFRESH causes RACF to reload resource profiles from the database into the data space.

The scope of a RACLIST REFRESH command is the class named on the command plus any other classes sharing the same POSIT value. See z/OS Security Server RACF Security Administrator's Guide for further information.

If your installation has two or more systems sharing a RACF database, you must issue the REFRESH on all systems to have the results effective on all systems, unless RACF is enabled for sysplex communication. However, if you do not perform a refresh on a system sharing a RACF database and that system needs to re-IPL, a fresh copy of the RACLISTed profiles is read from the database at IPL time.

When RACF is enabled for sysplex communication, it propagates the REFRESH command to each of the systems in the data sharing group.

SETROPTS GENERIC(classname) REFRESH

When you specify GENERIC and REFRESH, you also specify one or more classes for which you want RACF to refresh in-storage generic profile lists. This causes all of the in-storage generic profiles in the specified general resource class (except those in the global access checking table) to be replaced with new copies from the RACF database.

The following example refreshes in-storage generic profiles for the CIMS and TIMS classes.

```
SETROPTS GENERIC(CIMS TIMS) REFRESH
```

If you specify SETROPTS GENERIC(*) REFRESH, RACF refreshes profile lists for the DATASET class and all active classes except resource grouping classes and classes defined with the GENERIC(DISALLOWED) attribute.

For the DATASET class:

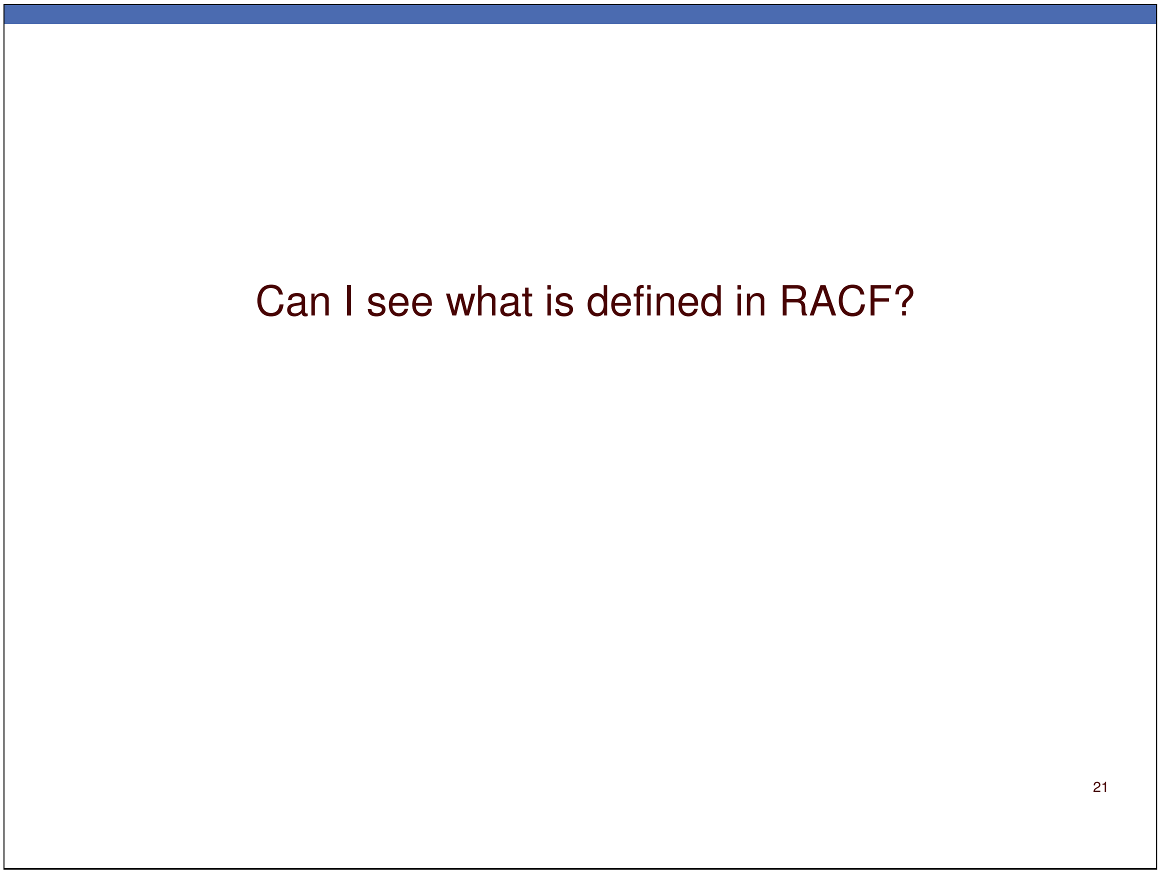
RACF caches a list of generic profiles which begin with the HLQ of a data set for which an authorization check has been done.

For example, if you open ‘IMSP1.RECON1’

RACF loads the names of all the generic profiles which begin with IMSP1

To refresh the list: SETR GENERIC(DATASET) REFRESH

This purges all of the data set profiles that were cached by RACF.

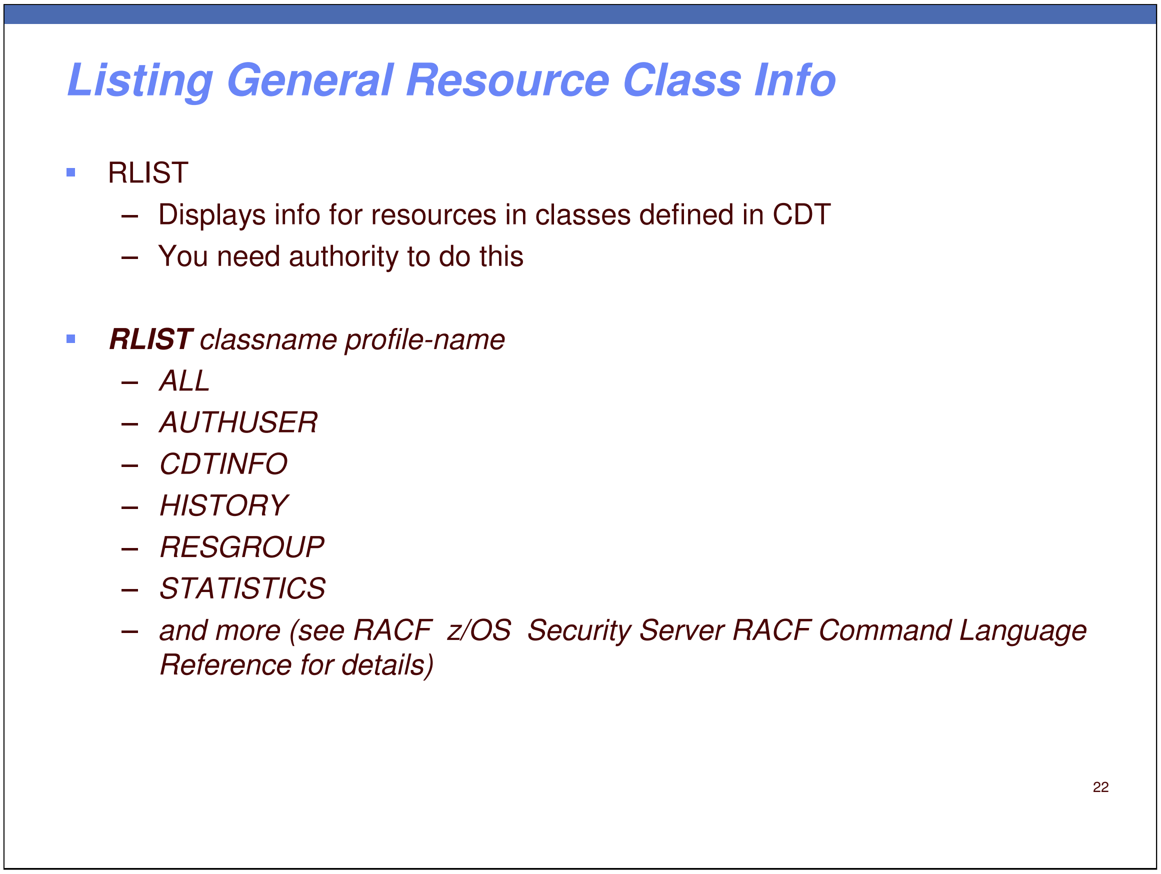


Can I see what is defined in RACF?

21

Use the ***RLIST*** command to display information on resources belonging to classes specified in the class descriptor table. Note that the DATASET, USER, and GROUP classes are not defined in the class descriptor table.

To reduce the impact on the system, use slack times to issue RACF commands that perform large-scale operations against the RACF database. You can also use the database unload utility (IRRDBU00) to obtain information from a copy of the RACF database. For information on IRRDBU00 see *z/OS Security Server RACF Security Administrator's Guide*.



Listing General Resource Class Info

- RLIST
  - Displays info for resources in classes defined in CDT
  - You need authority to do this

- ***RLIST*** *classname profile-name*
  - *ALL*
  - *AUTHUSER*
  - *CDTINFO*
  - *HISTORY*
  - *RESGROUP*
  - *STATISTICS*
  - *and more (see RACF z/OS Security Server RACF Command Language Reference for details)*

Use the ***RLIST*** command to display information on resources belonging to classes specified in the class descriptor table. Note that the DATASET, USER, and GROUP classes are not defined in the class descriptor table.

The ***RLIST*** command lists the contents of general resource profiles in a particular resource class. If you specify a profile that you do not have access to, you might receive an "access violation" message from the ***RLIST*** command.

Note: To see the access list for a resource, you must be the owner of the resource, or have ALTER access to the resource.

AUTHUSER

Displays the standard and conditional access lists for the profile. This is useful information to have before you use the PERMIT command to allow or deny access to the resource.

RESGROUP

Requests a list of all resource groups of which the resource specified by the *profile-name* operand is a member.

I activated RACF (RCF=A).

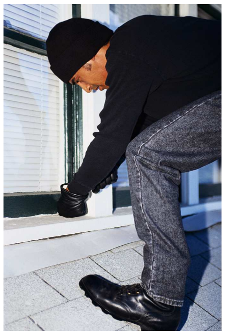
Why isn't RACF protecting everything?

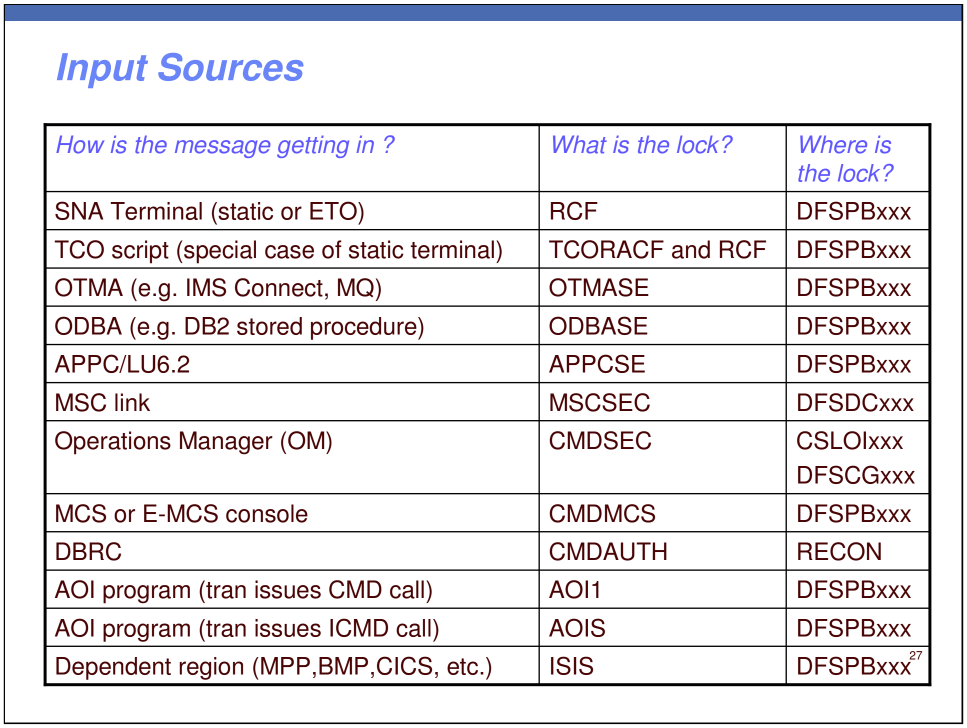
IMS Valuables

- Commands
- Transactions
- Datasets
- Coupling Facility Structures
- Databases
- PSBs
- Terminals

How is the message trying to get in?

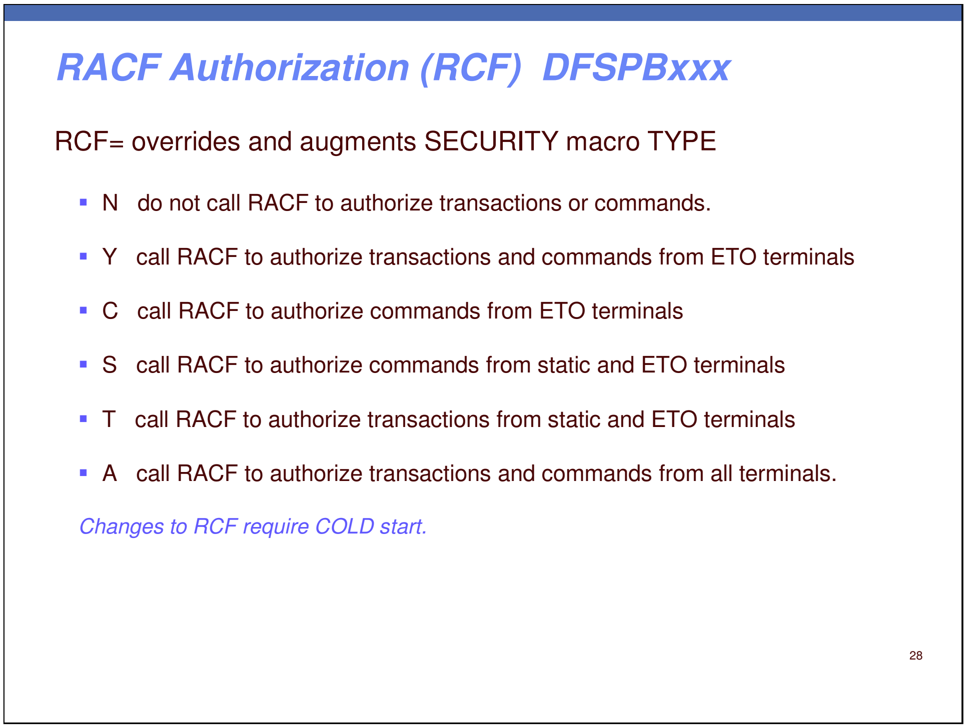
There's a lock for that.





Input Sources

How is the message getting in ?	*What is the lock?*	*Where is the lock?*
SNA Terminal (static or ETO)	RCF	DFSPBxxx
TCO script (special case of static terminal)	TCORACF and RCF	DFSPBxxx
OTMA (e.g. IMS Connect, MQ)	OTMASE	DFSPBxxx
ODBA (e.g. DB2 stored procedure)	ODBASE	DFSPBxxx
APPC/LU6.2	APPCSE	DFSPBxxx
MSC link	MSCSEC	DFSDCxxx
Operations Manager (OM)	CMDSEC	CSLOIxxx DFSCGxxx
MCS or E-MCS console	CMDMCS	DFSPBxxx
DBRC	CMDAUTH	RECON
AOI program (tran issues CMD call)	AOI1	DFSPBxxx
AOI program (tran issues ICMD call)	AOIS	DFSPBxxx
Dependent region (MPP,BMP,CICS, etc.)	ISIS	DFSPBxxx



RACF Authorization (RCF) DFSPBxxx

RCF= overrides and augments SECURITY macro TYPE

- N   do not call RACF to authorize transactions or commands.
- Y   call RACF to authorize transactions and commands from ETO terminals
- C   call RACF to authorize commands from ETO terminals
- S   call RACF to authorize commands from static and ETO terminals
- T   call RACF to authorize transactions from static and ETO terminals
- A   call RACF to authorize transactions and commands from all terminals.

Changes to RCF require COLD start.

28

The RCF parameter determines whether or not RACF is called for:

•Sign on security verification from static and ETO terminals

•Command authorization for commands entered from static and/or ETO terminals

•Transaction authorization

The specification for RCF may be used to override the

SECURITY macro TYPE+ specifications for RACF (RACFAGN, NORACTRM, RACFTERM,

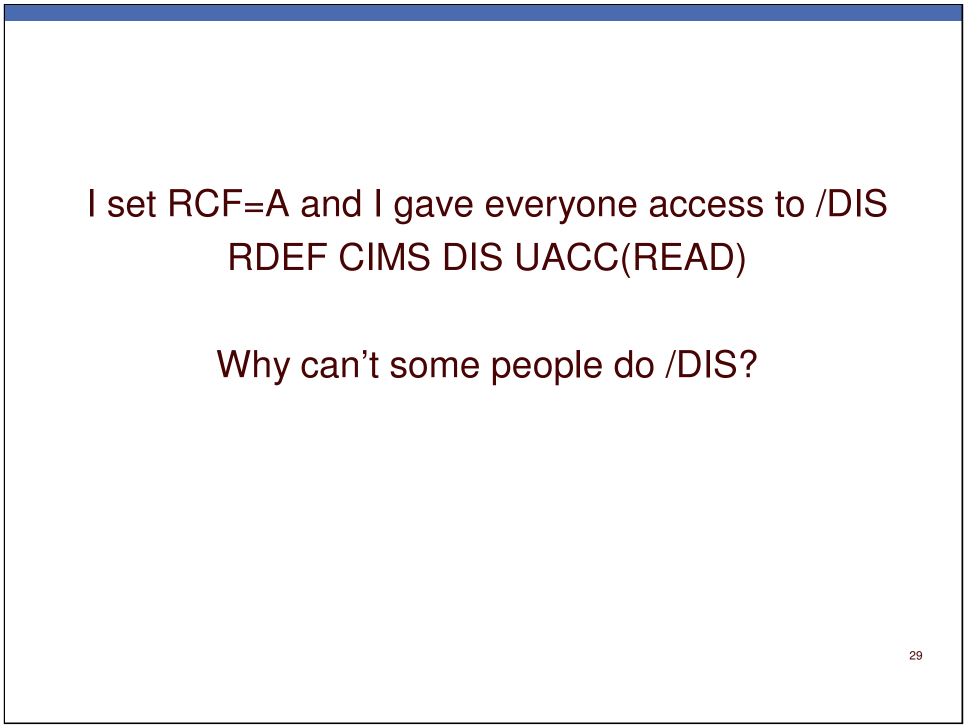
NORACFCM, and/or RACFCOM).

If the RCF parameter is not specified, the defaults used are the values specified (or defaulted to) at

system definition on the SECURITY macro TYPE keyword.

When you change the RCF startup value, a cold start is required to have the new value take effect.

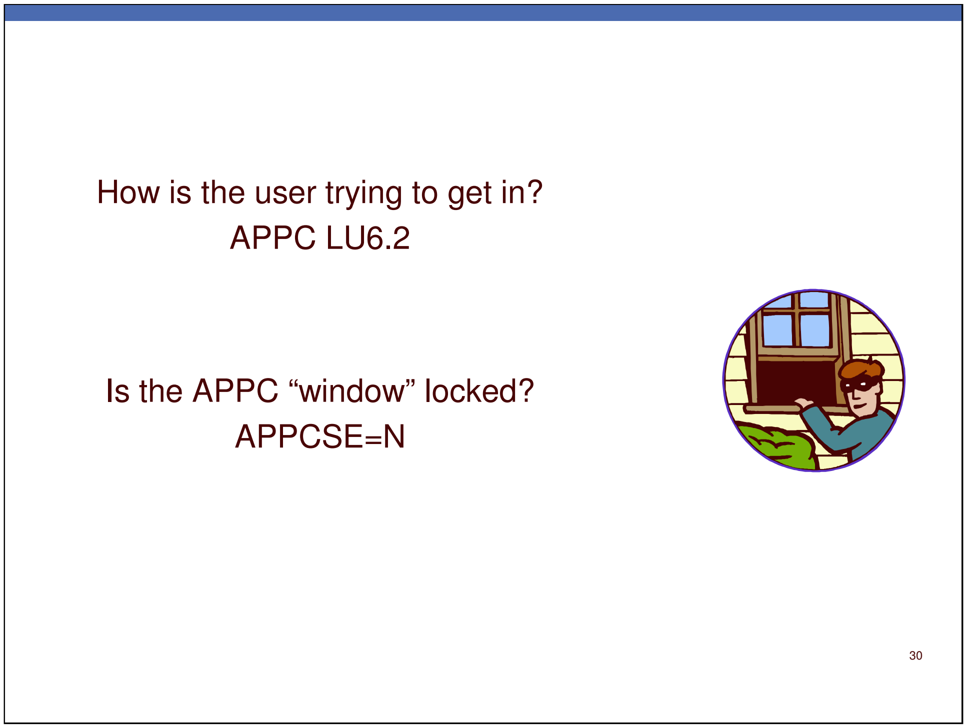
If your installation has more than 65536 terminals, you must use RACF for static terminal security.



I set RCF=A and I gave everyone access to /DIS
RDEF CIMS DIS UACC(READ)

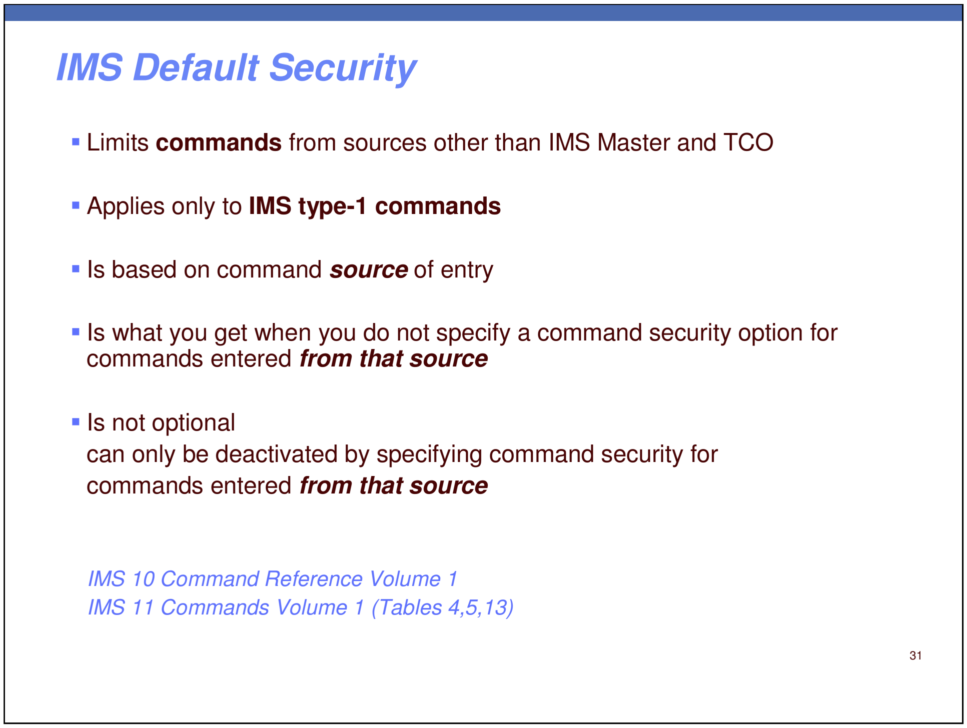
Why can’t some people do /DIS?

29



How is the user trying to get in?
APPC LU6.2

Is the APPC “window” locked?
APPCSE=N



IMS Default Security

- Limits **commands** from sources other than IMS Master and TCO
- Applies only to **IMS type-1 commands**
- Is based on command ***source*** of entry
- Is what you get when you do not specify a command security option for commands entered ***from that source***
- Is not optional
  can only be deactivated by specifying command security for
  commands entered ***from that source***

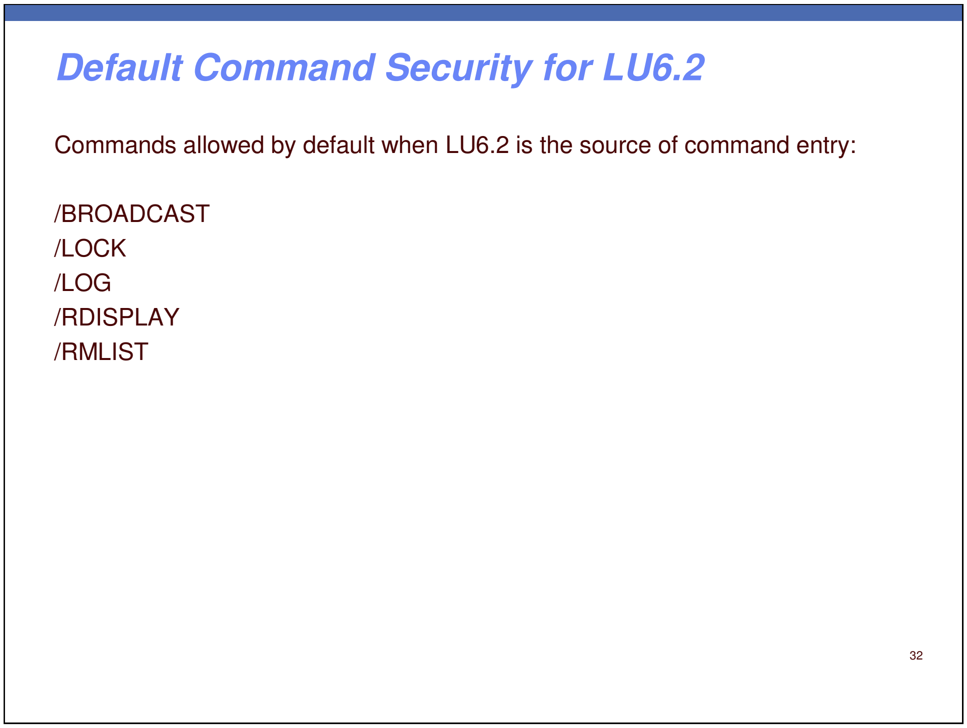
IMS 10 Command Reference Volume 1
IMS 11 Commands Volume 1 (Tables 4,5,13)

Default security is a type of security provided by IMS that only applies to IMS commands. Default security does not affect other IMS resources such as transactions, databases, terminals, programs, and other IMS resources.

Default security allows only a subset of the IMS commands to be entered. The subset of commands allowed when default security is active depends on where the command is entered (the source of entry). For example, the subset of IMS commands that may be entered from a static terminal is different than the subset of IMS commands that may be entered from an APPC device.

When command security is not specified, IMS automatically provides default 'command' security. In this respect, default security is not optional. It may be deactivated by specifying another form of command security.

The default subset of commands allowed for each source is documented in IMS V10 Command Reference Vol 1

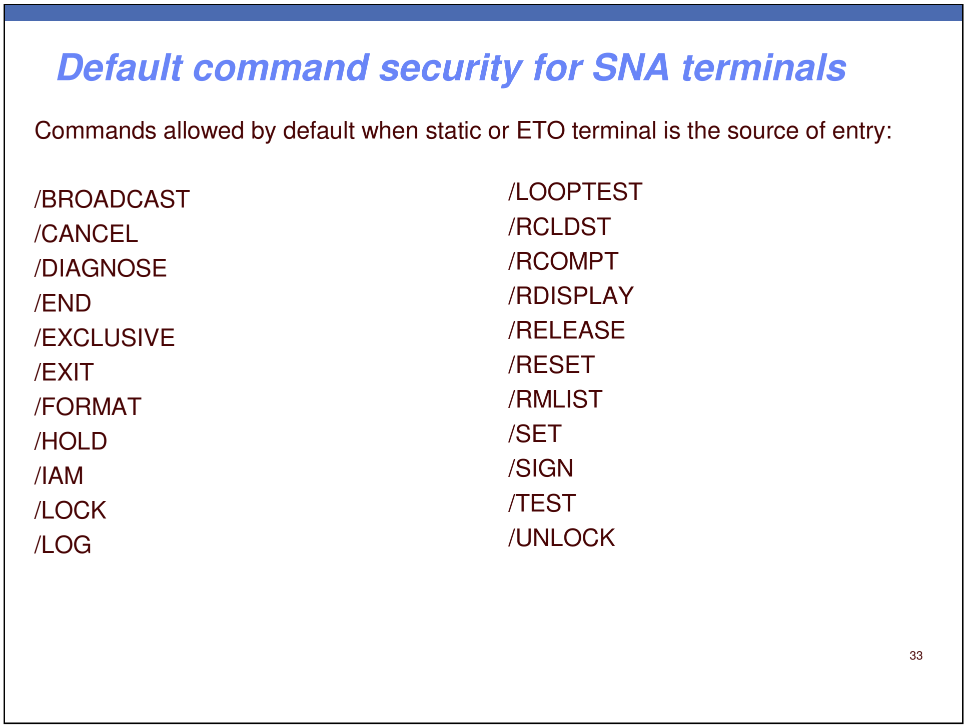


Default Command Security for LU6.2

Commands allowed by default when LU6.2 is the source of command entry:

/BROADCAST
/LOCK
/LOG
/RDISPLAY
/RMLIST

32



Default command security for SNA terminals

Commands allowed by default when static or ETO terminal is the source of entry:

/BROADCAST
/CANCEL
/DIAGNOSE
/END
/EXCLUSIVE
/EXIT
/FORMAT
/HOLD
/IAM
/LOCK
/LOG

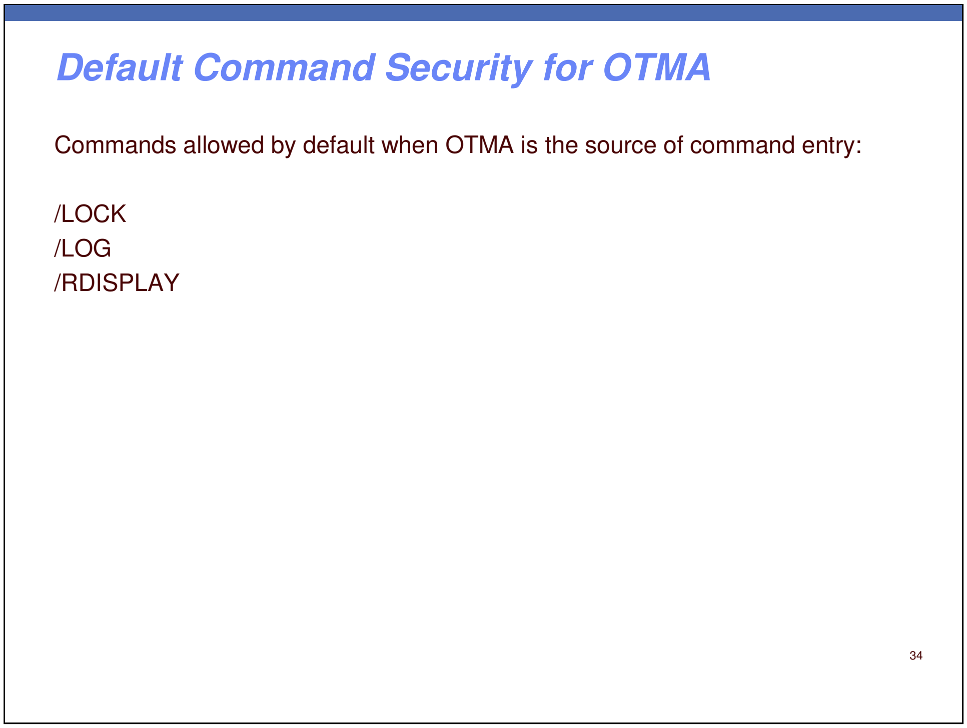
/LOOPTEST
/RCLDST
/RCOMPT
/RDISPLAY
/RELEASE
/RESET
/RMLIST
/SET
/SIGN
/TEST
/UNLOCK

33

Command authorization options for commands entered from static terminals are set by the:

- *TYPE=(RACFCOM) on the SECURITY macro*
- *IMS start up parameter RCF=*
- *CMDAUTH keyword on the /NRE CHECKPOINT 0 or /ERE COLDSYS command used to start the IMS system*
- *Command Authorization Exit Routine (DFSCCMD0).*

The IMS commands that may be issued from a statically defined terminal when default security is active are shown.



Default Command Security for OTMA

Commands allowed by default when OTMA is the source of command entry:

/LOCK
/LOG
/RDISPLAY

34

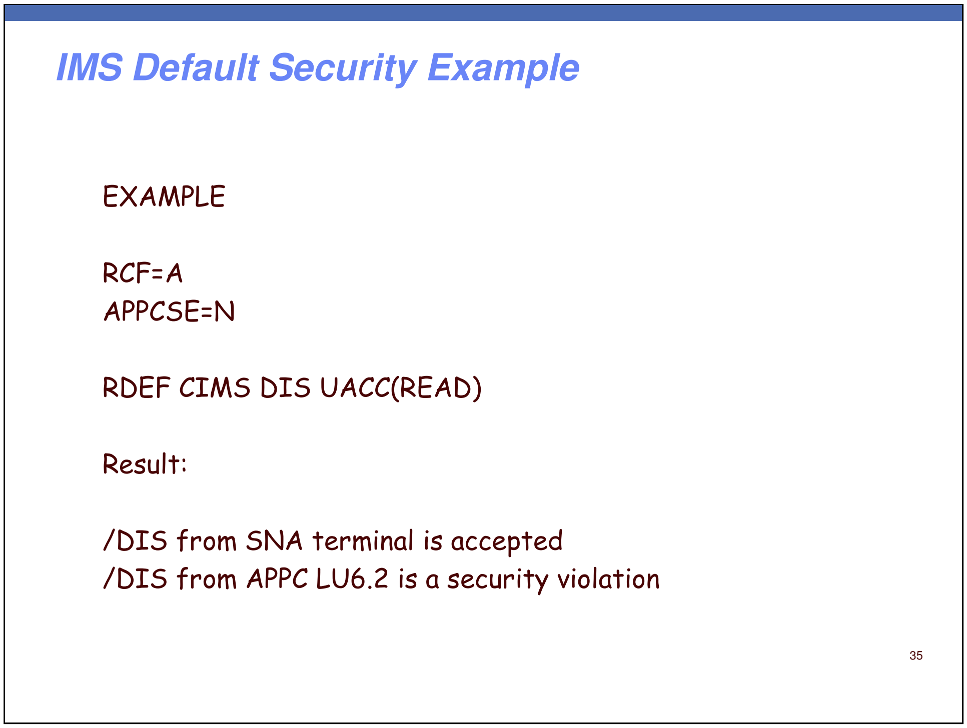
When IMS has been started without command security specified for commands entered from OTMA clients, default security is enforced. In order for default command security to take effect for commands entered from OTMA clients:

- *RACF security checking must be inactive for the OTMA environment and*
- *DFSCCMD0 is omitted from the IMS system; or if included, it is the unmodified sample exit*

RACF security checking is inactive in the OTMA environment when IMS has been started using the IMS start up parameter OTMASE=N or when the /SECURE OTMA NONE command has been issued after IMS start up.

If DFSCCMD0 has been included in the IMS system, it will be used to authorize commands entered from OTMA clients. The unmodified DFSCCMD0 sample exit routine allows only four commands to be entered from OTMA environments when default security is active.

When neither RACF nor DFSCCMD0 is used to authorize commands, default command security is enabled automatically by IMS for commands entered from OTMA clients and only the five commands shown may be entered.



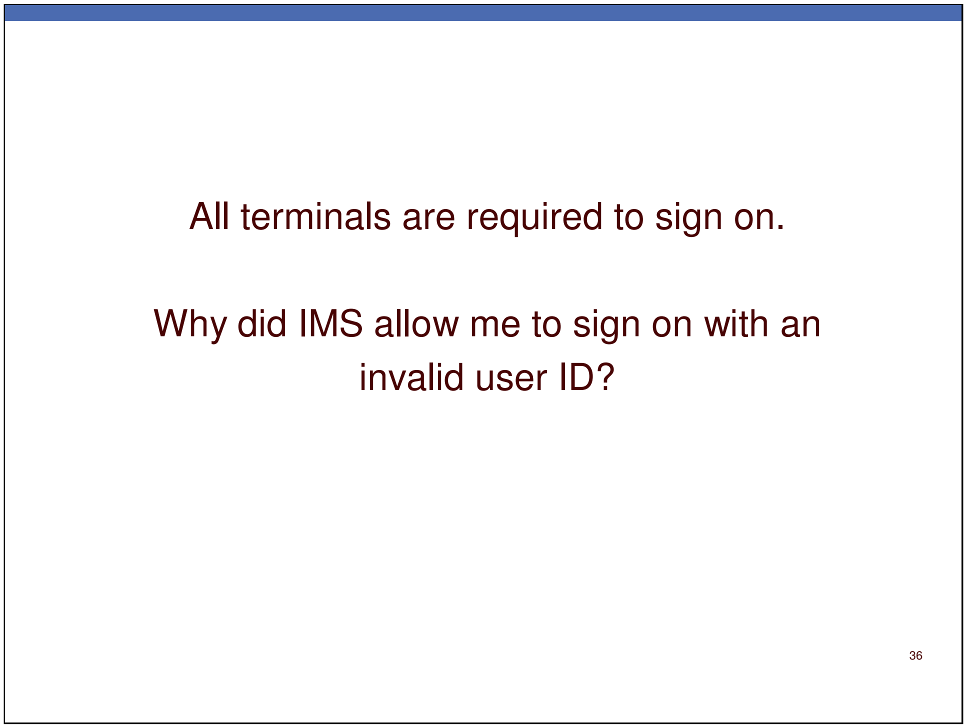
IMS Default Security Example

EXAMPLE

```
RCF=A
APPCSE=N

RDEF CIMS DIS UACC(READ)
```

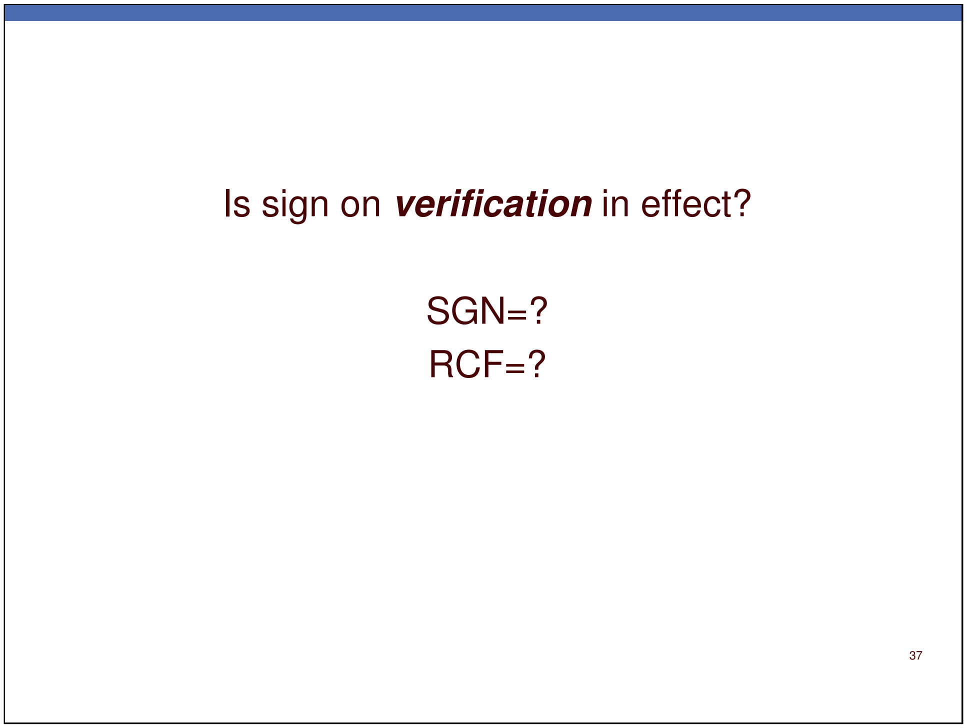
Result:

/DIS from SNA terminal is accepted
/DIS from APPC LU6.2 is a security violation



All terminals are required to sign on.

Why did IMS allow me to sign on with an invalid user ID?

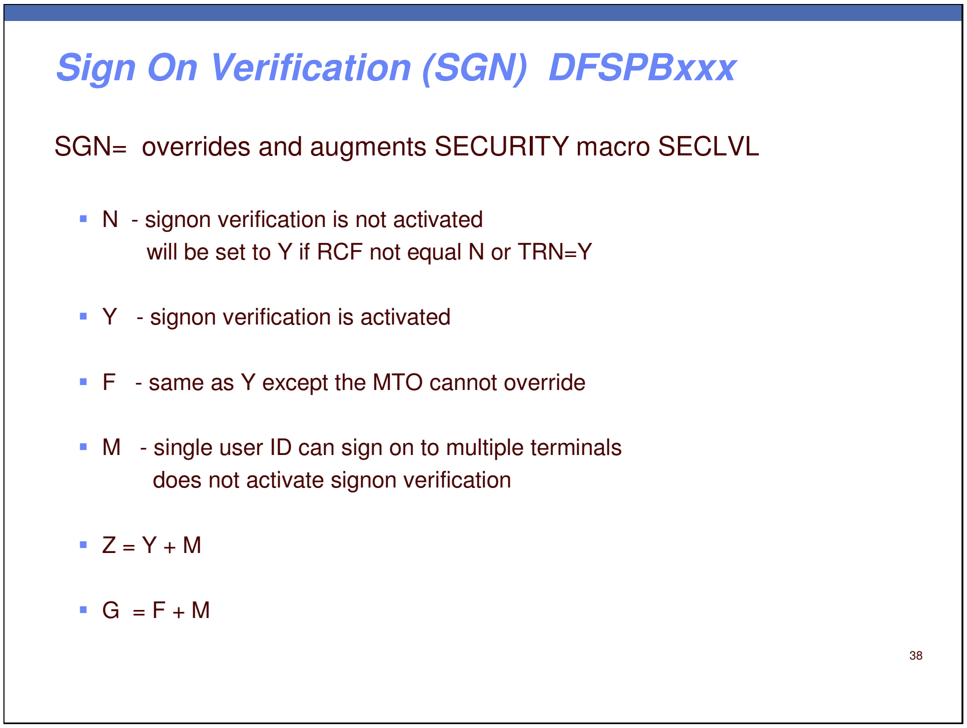


Is sign on ***verification*** in effect?

SGN=?

RCF=?

37



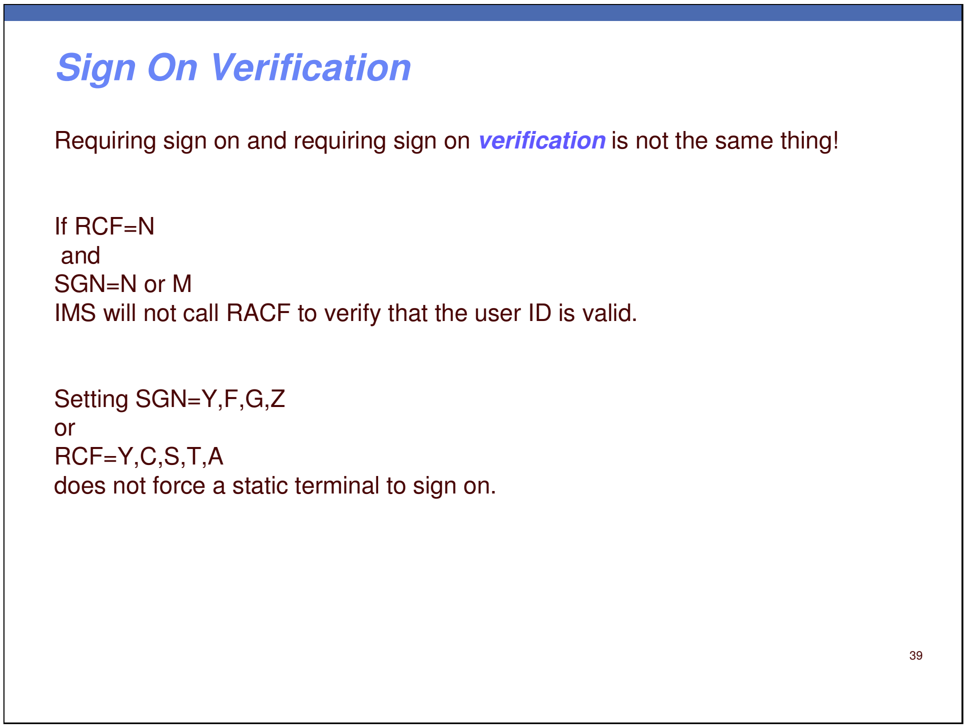
Sign On Verification (SGN) DFSPBxxx

SGN= overrides and augments SECURITY macro SECLVL

- N - signon verification is not activated
  will be set to Y if RCF not equal N or TRN=Y
- Y - signon verification is activated
- F - same as Y except the MTO cannot override
- M - single user ID can sign on to multiple terminals
  does not activate signon verification
- Z = Y + M
- G = F + M

38

The SGN parameter determines whether or not sign on verification will be performed, and whether or not sign on verification can be changed on a /NRE or /ERE COLDSYS restart command.



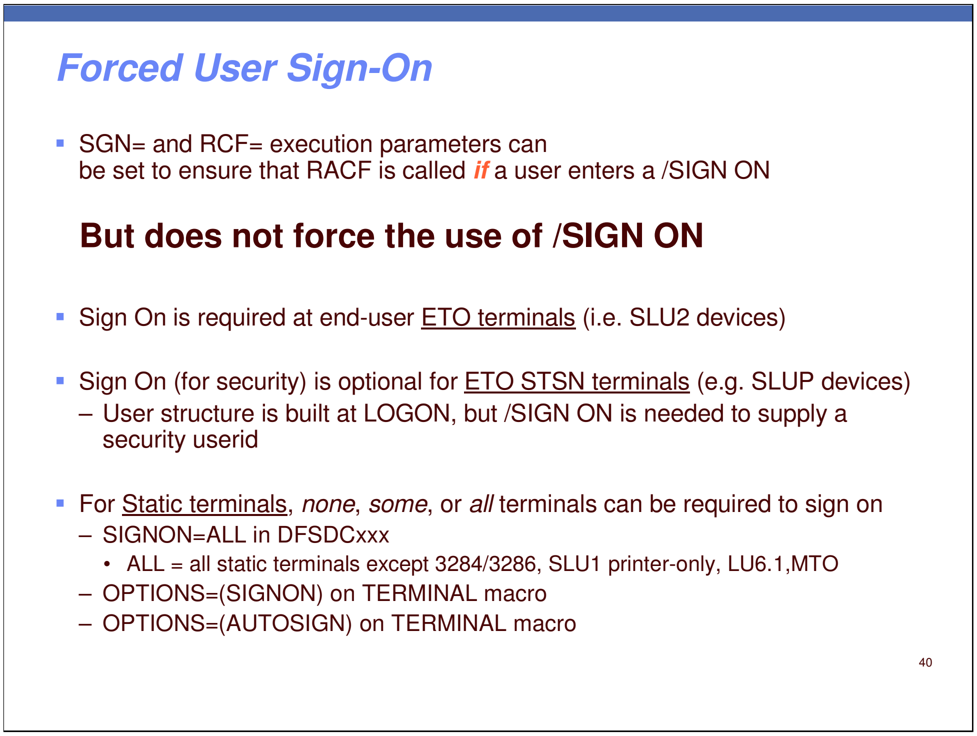
Sign On Verification

Requiring sign on and requiring sign on ***verification*** is not the same thing!

If RCF=N
and
SGN=N or M
IMS will not call RACF to verify that the user ID is valid.

Setting SGN=Y,F,G,Z
or
RCF=Y,C,S,T,A
does not force a static terminal to sign on.

The SGN parameter determines whether or not sign on verification will be performed, and whether or not sign on verification can be changed on a /NRE or /ERE COLDSYS restart command.



Forced User Sign-On

- SGN= and RCF= execution parameters can be set to ensure that RACF is called *if* a user enters a /SIGN ON

But does not force the use of /SIGN ON

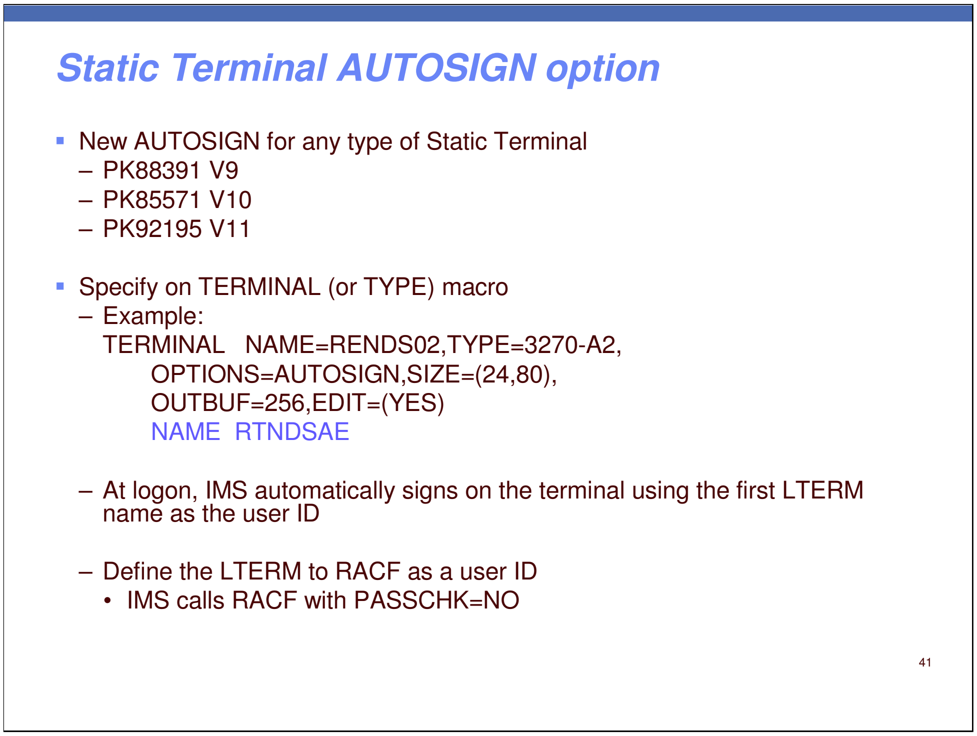
- Sign On is required at end-user ETO terminals (i.e. SLU2 devices)
- Sign On (for security) is optional for ETO STSN terminals (e.g. SLUP devices)
  - User structure is built at LOGON, but /SIGN ON is needed to supply a security userid
- For Static terminals, *none*, *some*, or *all* terminals can be required to sign on
  - SIGNON=ALL in DFSDCxxx
    - ALL = all static terminals except 3284/3286, SLU1 printer-only, LU6.1,MTO
  - OPTIONS=(SIGNON) on TERMINAL macro
  - OPTIONS=(AUTOSIGN) on TERMINAL macro

We've seen that you can specify, on the SECURITY macro, for example, that a security check is to take place if a user SIGNs ON. On this slide, we are discussing forcing a user to SIGN ON.

ETO end-user terminals have no choice – they must SIGN ON. But this is not so for ETO Set-and-Test-Sequence Number (STSN) devices. When a STSN terminal logs on, IMS builds the user structure, but without a security userid. A /SIGN ON command is used to associate a security userid with the User.

But for static terminals – those defined in the IMS GEN with TERMINAL macros – you can specify that none, some, or all require sign on. And this is explained in the lower half of the slide.

Later, we'll look at the security options available when the user is not forced to, and does not sign on.



Static Terminal AUTOSIGN option

- New AUTOSIGN for any type of Static Terminal
  - PK88391 V9
  - PK85571 V10
  - PK92195 V11

- Specify on TERMINAL (or TYPE) macro
  - Example:

```
TERMINAL   NAME=RENDS02,TYPE=3270-A2,
      OPTIONS=AUTOSIGN,SIZE=(24,80),
      OUTBUF=256,EDIT=(YES)
      NAME  RTNDSAE
```

  - At logon, IMS automatically signs on the terminal using the first LTERM name as the user ID

  - Define the LTERM to RACF as a user ID
    - IMS calls RACF with PASSCHK=NO

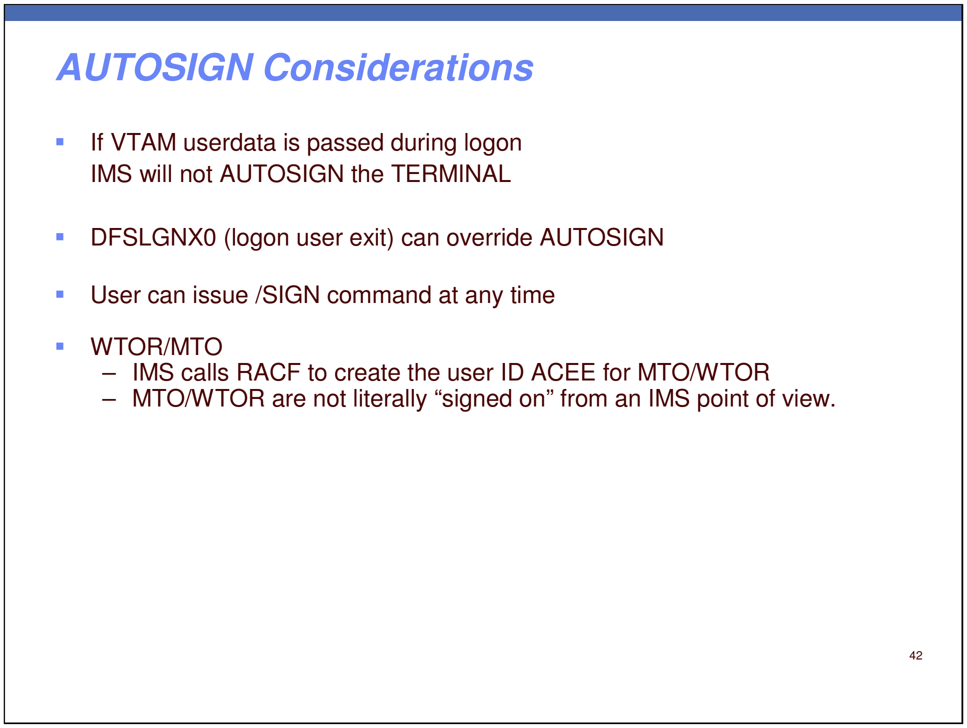
41

The AUTOSIGN function was introduced by maintenance on IMS 9, 10 and 11.

There is a new sub-parameter of the OPTIONS parameter for the TERMINAL or TYPE macro. The default is NOAUTSGN. If AUTOSIGN is specified, the terminal will automatically sign on at logon time, using the LTERM name as the userid. IMS will issue this sign on to RACF with a request to bypass password checking.

The LTERM user IDs can be defined to RACF with the PROTECTED attribute to ensure that end users will not be able to Sign ON using an LTERM userid.

There are two special cases for Static terminals – the Master Terminal and the Console used to reply to the IMS Outstanding WTOR both have unrestricted access to IMS commands. And they are not forced to SIGN ON. However, they can issue transactions and if not signed on, the user ID used for transaction security will be the IMS Control Region’s userid. The maintenance for the AUTOSIGN function also addresses this issue. The DFSDCxxx PROCLIB member can specify the userids to be used for transaction security when transactions are entered at the MTO or via the outstanding WTOR, and the user has not signed on. The DFSDCxxx parameters are MTOUSID and WTORUSID.



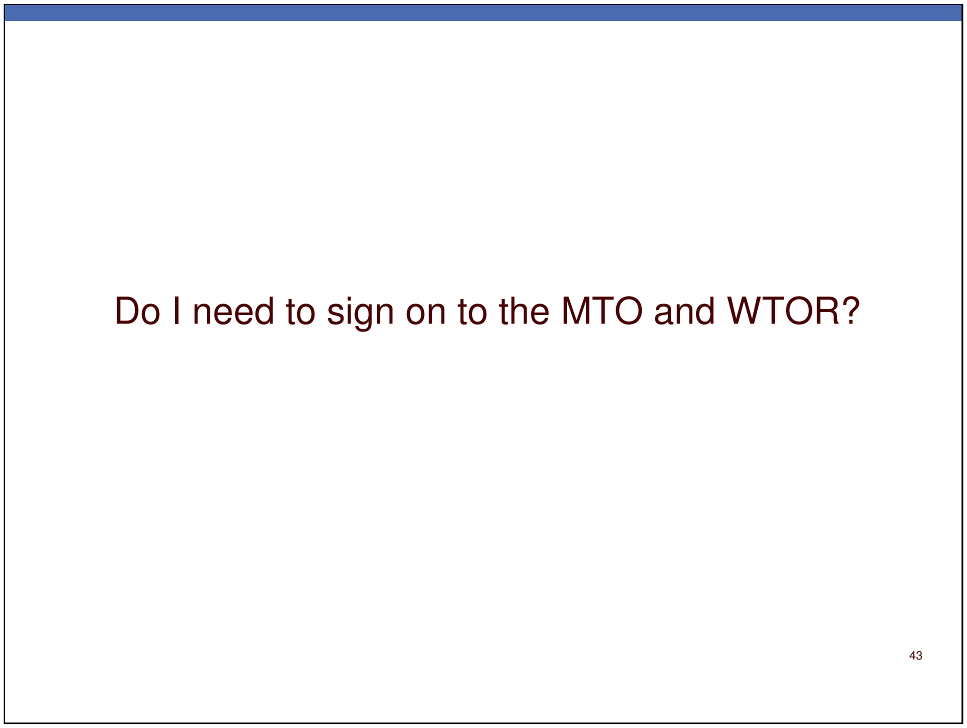
AUTOSIGN Considerations

- If VTAM userdata is passed during logon
  IMS will not AUTOSIGN the TERMINAL

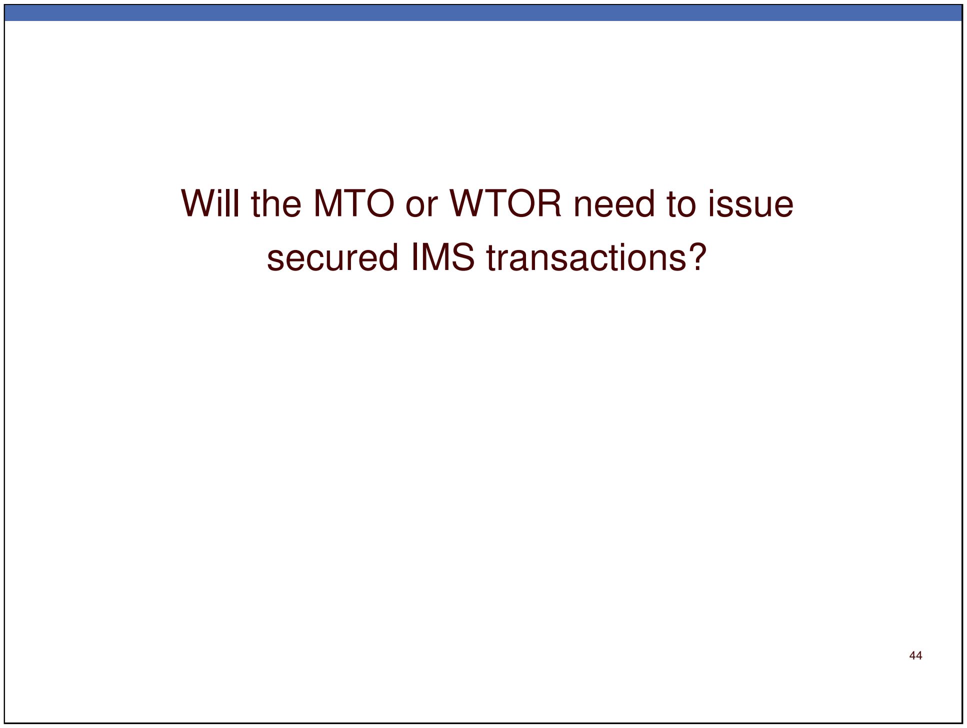
- DFSLGNX0 (logon user exit) can override AUTOSIGN

- User can issue /SIGN command at any time

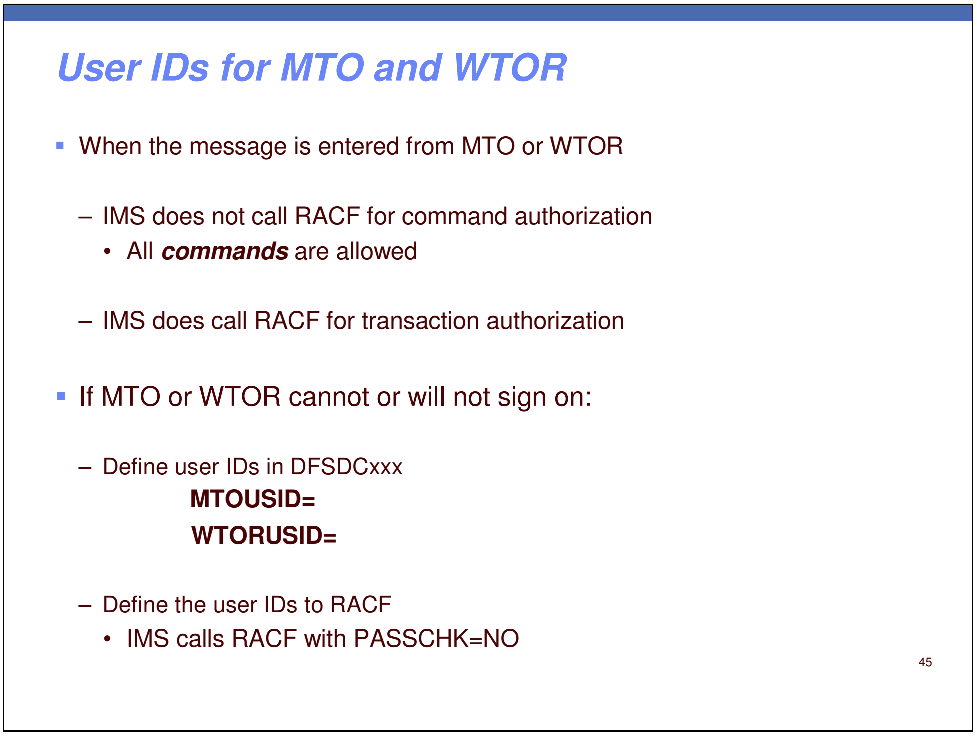
- WTOR/MTO
  - IMS calls RACF to create the user ID ACEE for MTO/WTOR
  - MTO/WTOR are not literally “signed on” from an IMS point of view.



Do I need to sign on to the MTO and WTOR?



Will the MTO or WTOR need to issue secured IMS transactions?



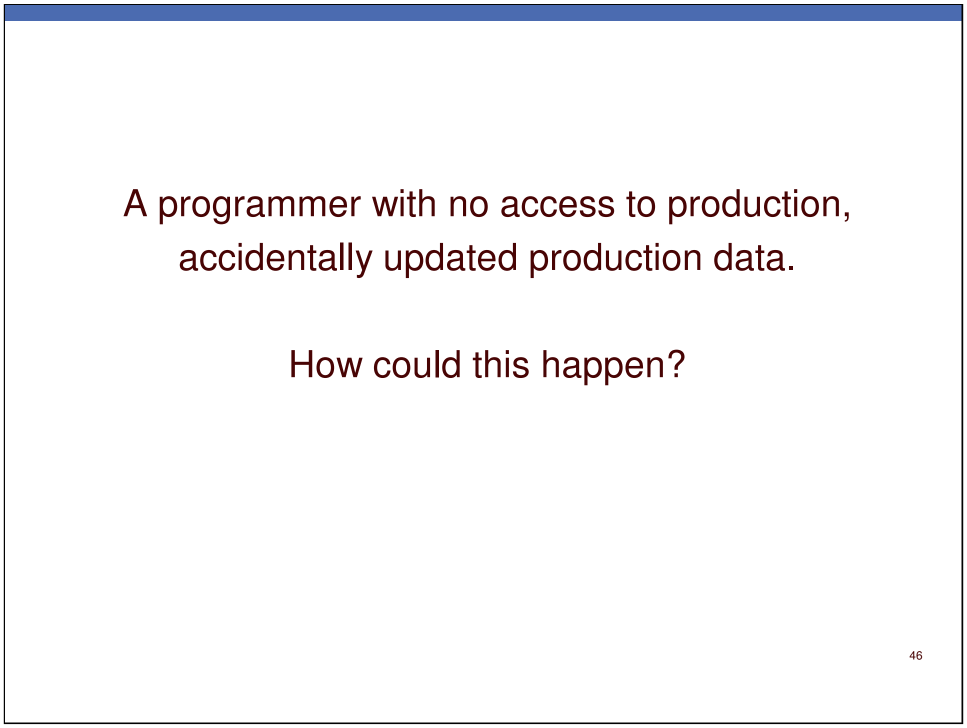
User IDs for MTO and WTOR

- When the message is entered from MTO or WTOR
  - IMS does not call RACF for command authorization
    - All ***commands*** are allowed
  - IMS does call RACF for transaction authorization
- If MTO or WTOR cannot or will not sign on:
  - Define user IDs in DFSDCxxx

    MTOUSID=

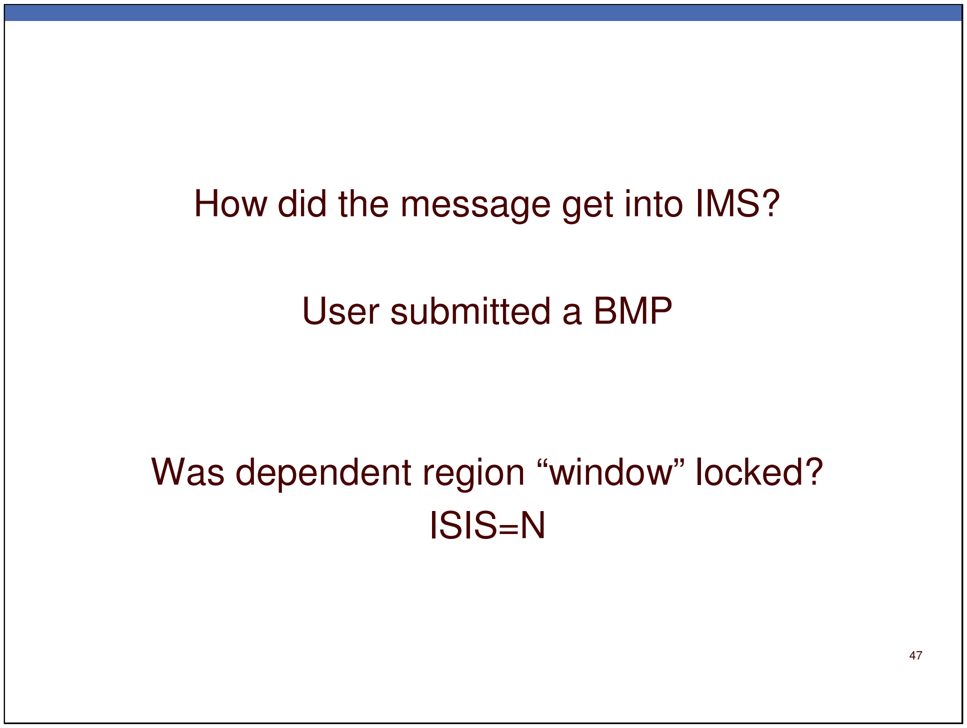
    WTORUSID=
  - Define the user IDs to RACF
    - IMS calls RACF with PASSCHK=NO

Can’t use AUTOSIGN for MTO and WTOR



A programmer with no access to production, accidentally updated production data.

How could this happen?

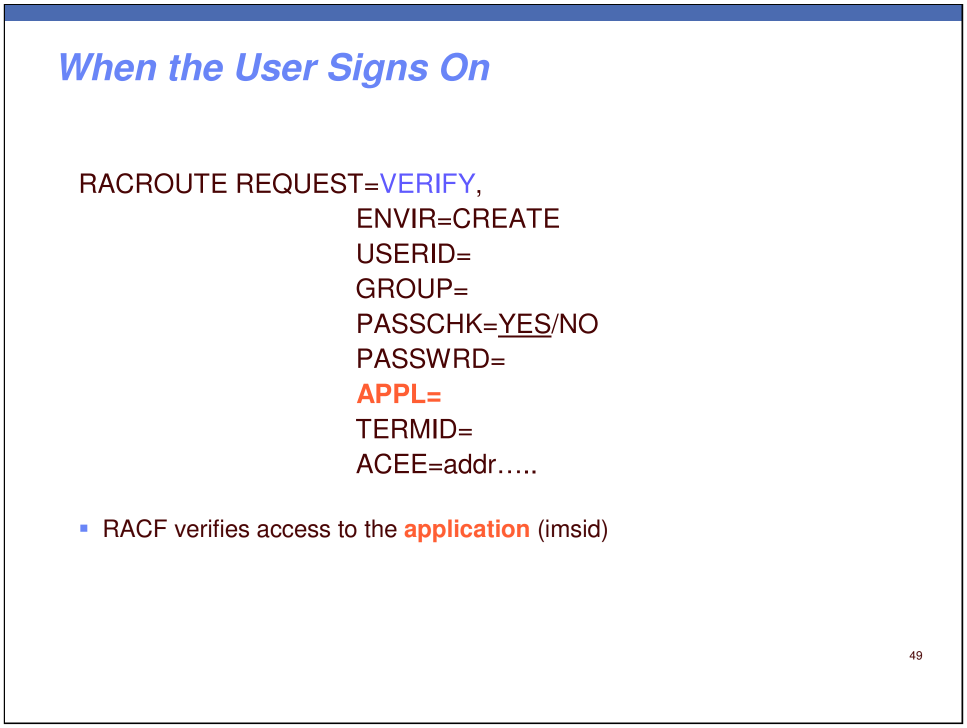


How did the message get into IMS?

User submitted a BMP

Was dependent region “window” locked?
ISIS=N

The APPL Gate

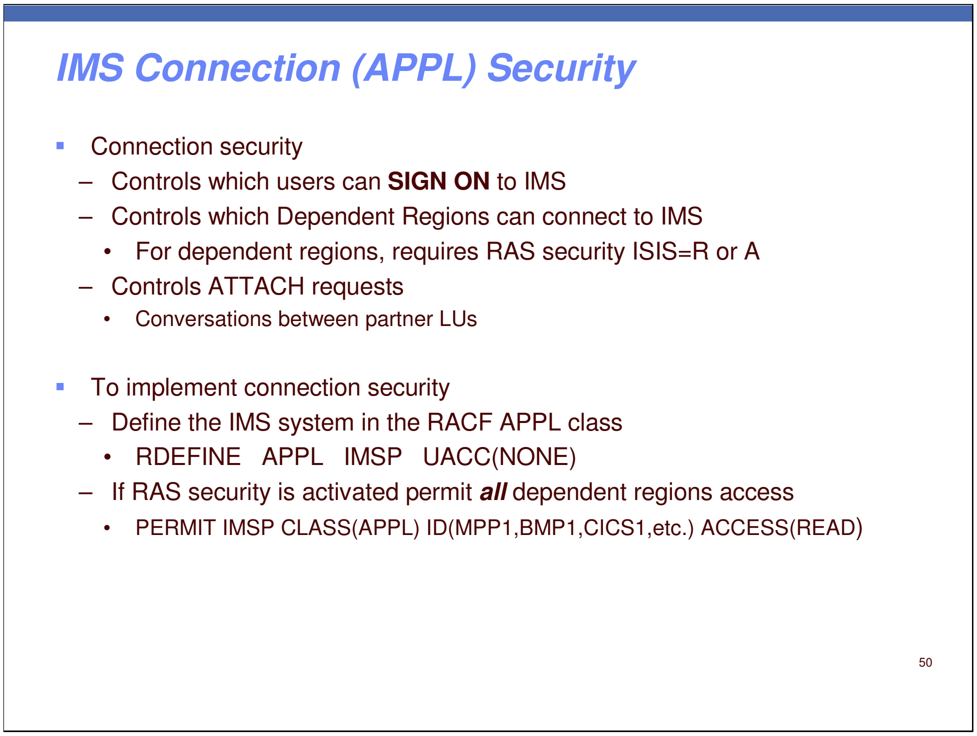


When the User Signs On

```
RACROUTE REQUEST=VERIFY,
                        ENVIR=CREATE
                        USERID=
                        GROUP=
                        PASSCHK=YES/NO
                        PASSWRD=
                        APPL=
                        TERMID=
                        ACEE=addr…..
```

- RACF verifies access to the **application** (imsid)

49



IMS Connection (APPL) Security

- Connection security
  - Controls which users can **SIGN ON** to IMS
  - Controls which Dependent Regions can connect to IMS
    - For dependent regions, requires RAS security ISIS=R or A
  - Controls ATTACH requests
    - Conversations between partner LUs
- To implement connection security
  - Define the IMS system in the RACF APPL class
    - RDEFINE APPL IMSP UACC(NONE)
  - If RAS security is activated permit ***all*** dependent regions access
    - PERMIT IMSP CLASS(APPL) ID(MPP1,BMP1,CICS1,etc.) ACCESS(READ)

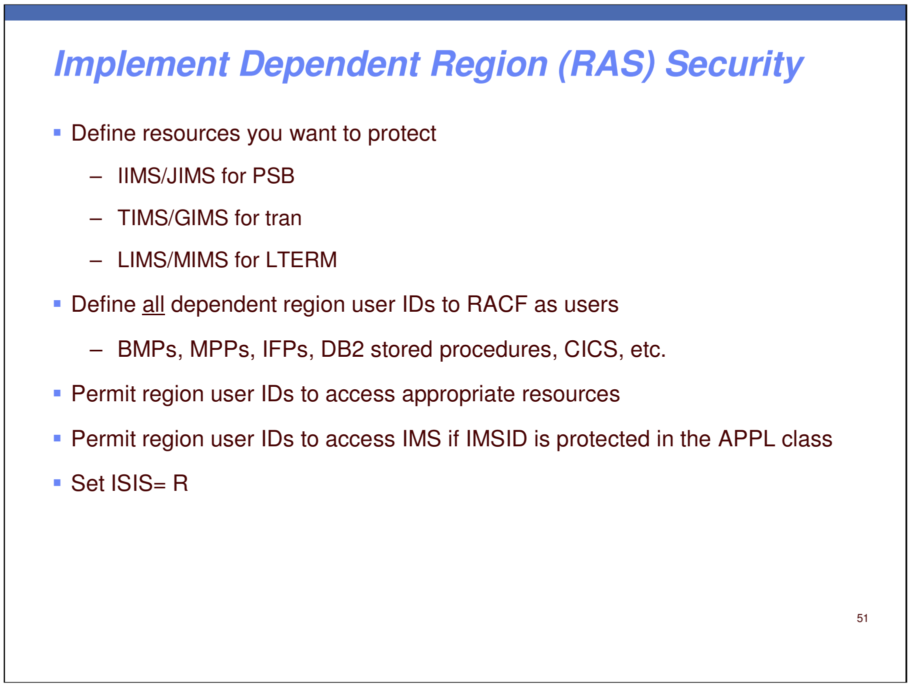
IMS Connection Security has two aspects.

Firstly, security when external clients attempt to connect to IMS.

The second aspect, is when dependent regions start up and try to connect to the Control Region. A prerequisite for this is that Resource Access Security (RAS) be enabled.

The IMSID must be RDEFINEd in the RACF APPL class. Then, the end-user userids who are to be allowed to sign on, must be PERMITted in RACF to access the relevant IMS systems in the APPL class.

Dependent region connection security is similar. The dependent region user IDs must be PERMITted to access the relevant IMS systems. In this case, the region user IDs will include all the BMP user IDs, as well as MPP and IFP region IDs, CICS region IDs, DB2 stored procedure user IDs, etc..

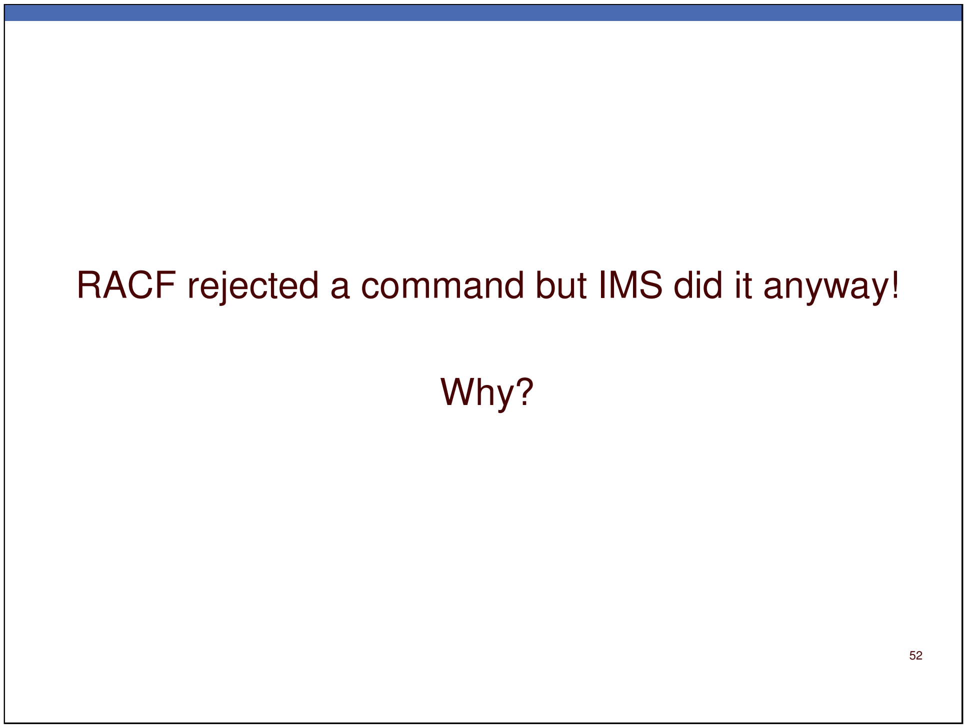


Implement Dependent Region (RAS) Security

- Define resources you want to protect
  - IIMS/JIMS for PSB
  - TIMS/GIMS for tran
  - LIMS/MIMS for LTERM
- Define all dependent region user IDs to RACF as users
  - BMPs, MPPs, IFPs, DB2 stored procedures, CICS, etc.
- Permit region user IDs to access appropriate resources
- Permit region user IDs to access IMS if IMSID is protected in the APPL class
- Set ISIS= R

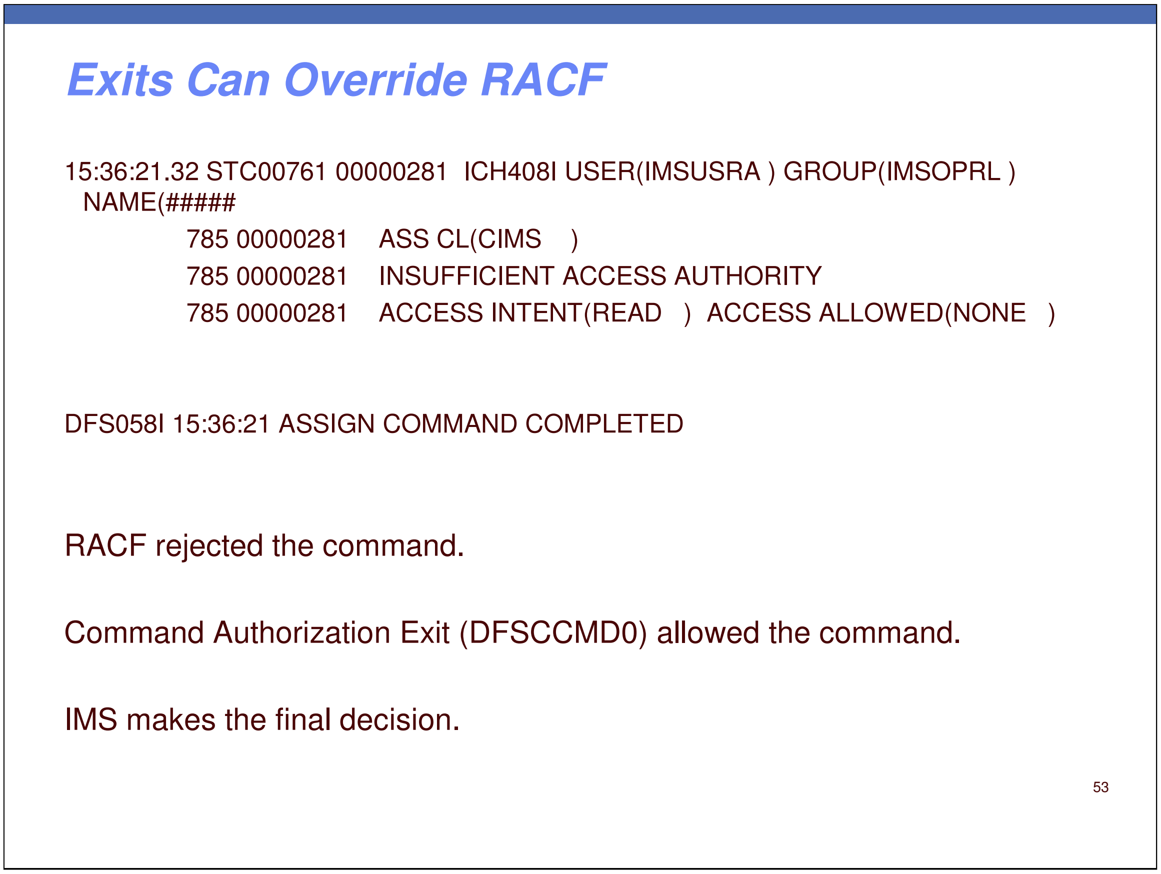
51

If IMS is protected in the RACF APPL class, when you activate RAS (ISIS=R or A) IMS will call RACF to check that the dependent region user ID is authorized to access IMS when the dependent region requests to connect to IMS. This “connection check” is not done unless RAS security is activated.



RACF rejected a command but IMS did it anyway!

Why?



Exits Can Override RACF

```
15:36:21.32 STC00761 00000281  ICH408I USER(IMSUSRA ) GROUP(IMSOPRL )
  NAME(#####
             785 00000281    ASS CL(CIMS    )
             785 00000281    INSUFFICIENT ACCESS AUTHORITY
             785 00000281    ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )
```

```
DFS058I 15:36:21 ASSIGN COMMAND COMPLETED
```

RACF rejected the command.

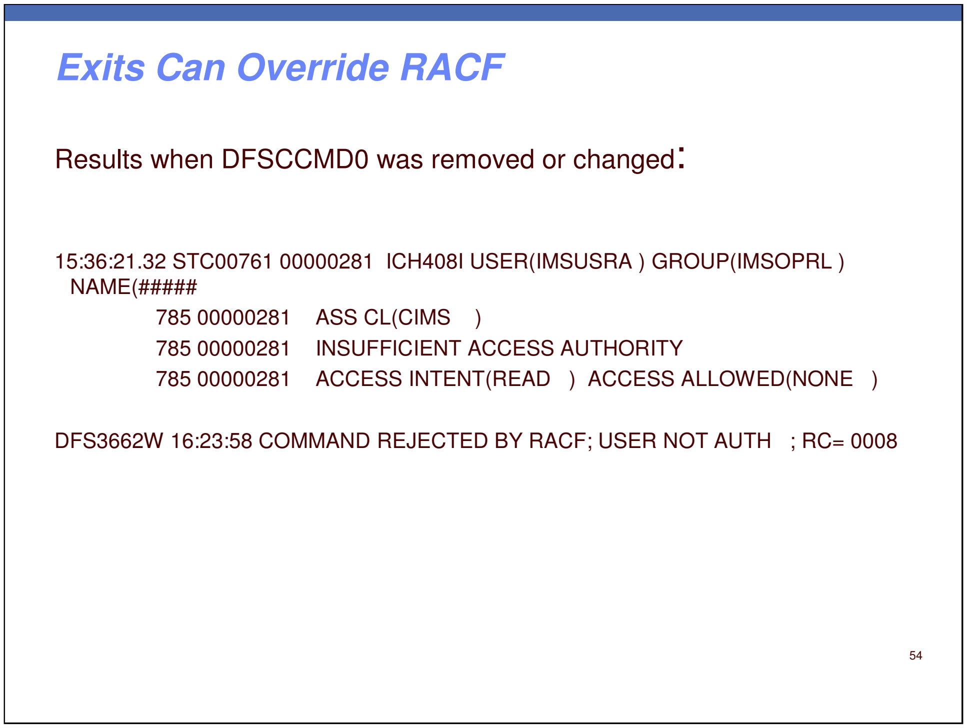
Command Authorization Exit (DFSCCMD0) allowed the command.

IMS makes the final decision.

53

There is no way to explicitly request the Command Authorization Exit for commands from static and dynamic terminals. Therefore the exit will be invoked if it exists in RESLIB.

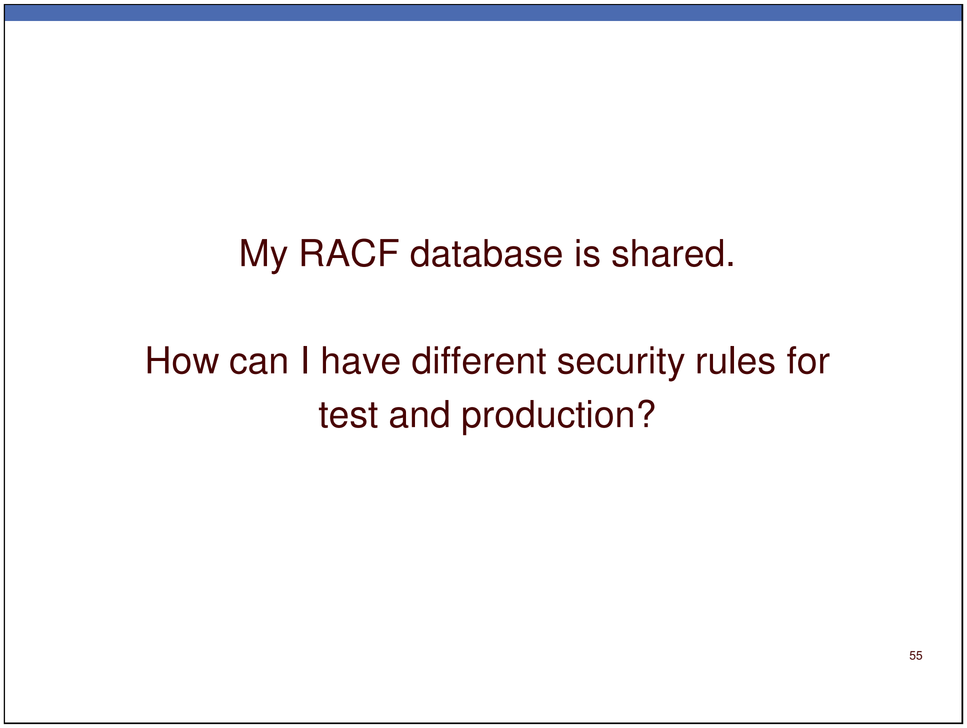
RACF issued the ICH408I message because IMS called RACF with LOG=ASIS.



Exits Can Override RACF

Results when DFSCCMD0 was removed or changed:

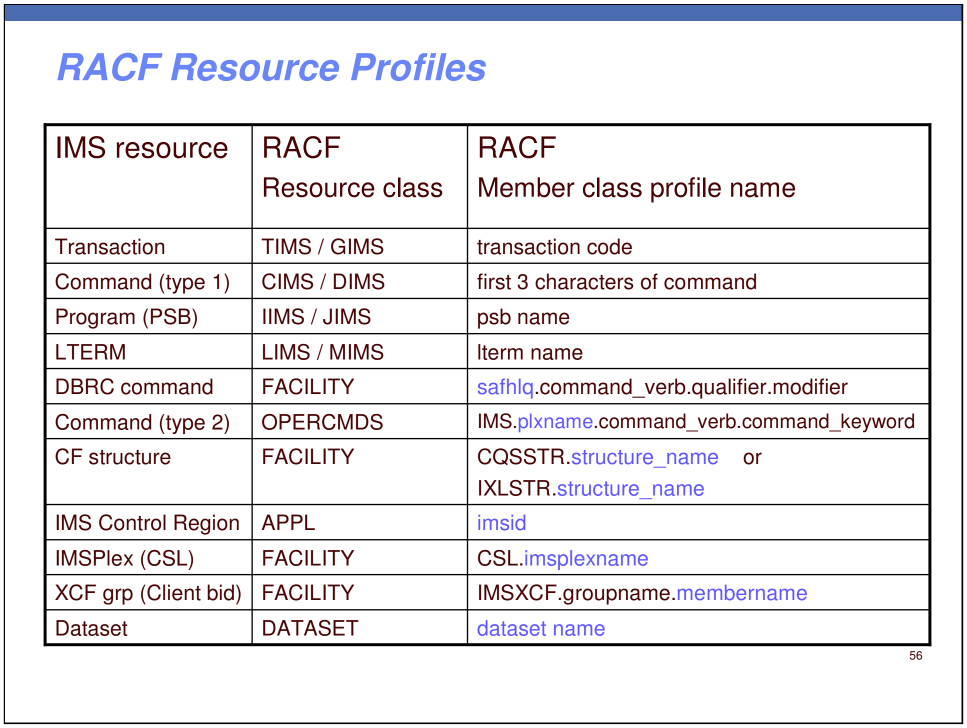
```
15:36:21.32 STC00761 00000281  ICH408I USER(IMSUSRA ) GROUP(IMSOPRL )
  NAME(#####
              785 00000281    ASS CL(CIMS    )
              785 00000281    INSUFFICIENT ACCESS AUTHORITY
              785 00000281    ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )

DFS3662W 16:23:58 COMMAND REJECTED BY RACF; USER NOT AUTH   ; RC= 0008
```



My RACF database is shared.

How can I have different security rules for test and production?

55

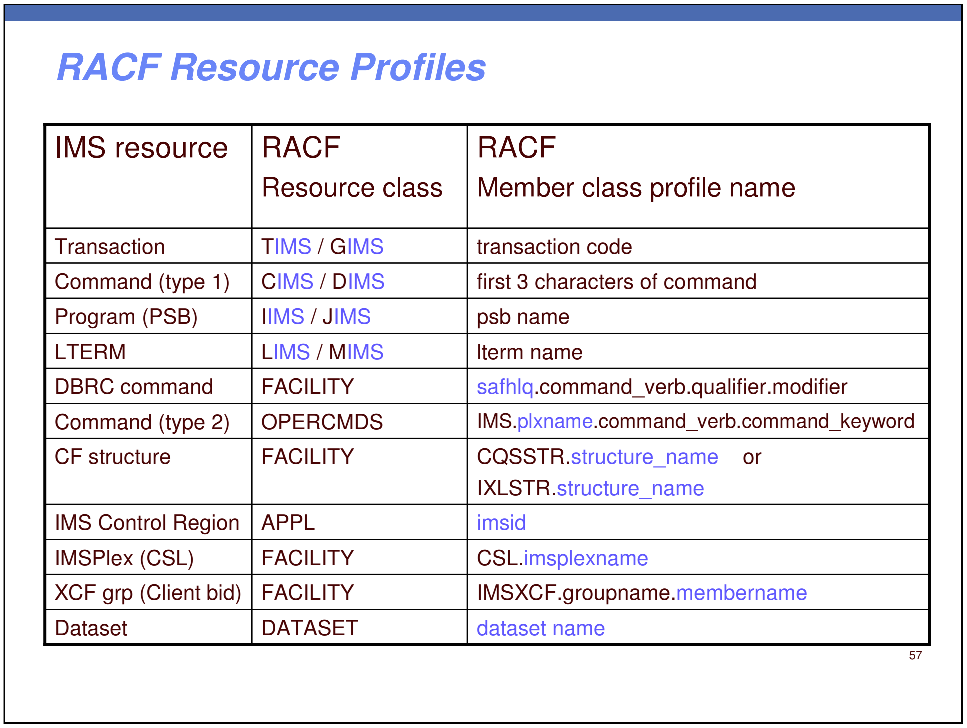


RACF Resource Profiles

IMS resource	RACF Resource class	RACF Member class profile name
Transaction	TIMS / GIMS	transaction code
Command (type 1)	CIMS / DIMS	first 3 characters of command
Program (PSB)	IIMS / JIMS	psb name
LTERM	LIMS / MIMS	lterm name
DBRC command	FACILITY	safhlq.command_verb.qualifier.modifier
Command (type 2)	OPERCMDS	IMS.plxname.command_verb.command_keyword
CF structure	FACILITY	CQSSTR.structure_name or IXLSTR.structure_name
IMS Control Region	APPL	imsid
IMSPlex (CSL)	FACILITY	CSL.imsplexname
XCF grp (Client bid)	FACILITY	IMSXCF.groupname.membername
Dataset	DATASET	dataset name

Member class profile names must conform to rules.

Grouping class profile names can be any 1-8 alphanumeric characters you choose.

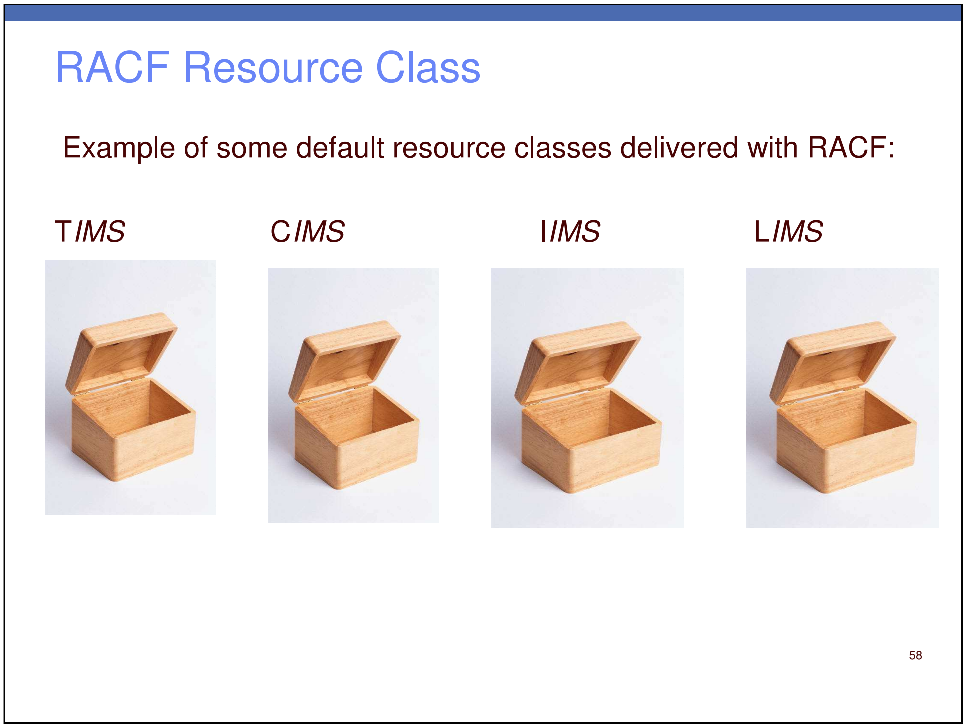


RACF Resource Profiles

IMS resource	RACF Resource class	RACF Member class profile name
Transaction	TIMS / GIMS	transaction code
Command (type 1)	CIMS / DIMS	first 3 characters of command
Program (PSB)	IIMS / JIMS	psb name
LTERM	LIMS / MIMS	lterm name
DBRC command	FACILITY	safhlq.command_verb.qualifier.modifier
Command (type 2)	OPERCMDS	IMS.plxname.command_verb.command_keyword
CF structure	FACILITY	CQSSTR.structure_name or IXLSTR.structure_name
IMS Control Region	APPL	imsid
IMSPlex (CSL)	FACILITY	CSL.imsplexname
XCF grp (Client bid)	FACILITY	IMSXCF.groupname.membername
Dataset	DATASET	dataset name

Member class profile names must conform to rules.

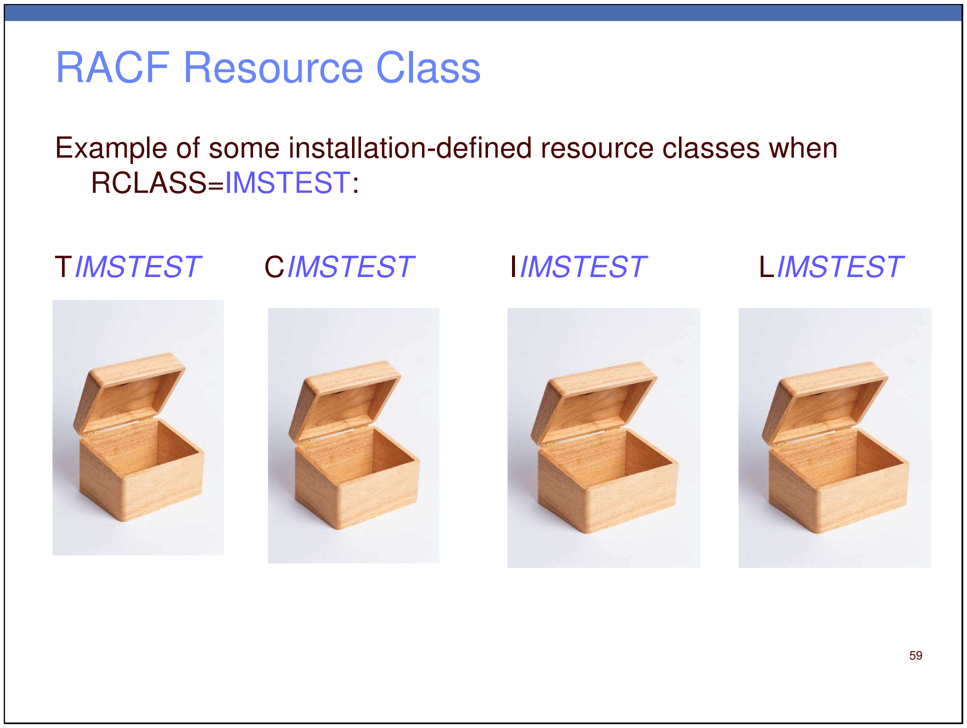
Grouping class profile names can be any 1-8 alphanumeric characters you choose.



RACF Resource Class

Example of some default resource classes delivered with RACF:

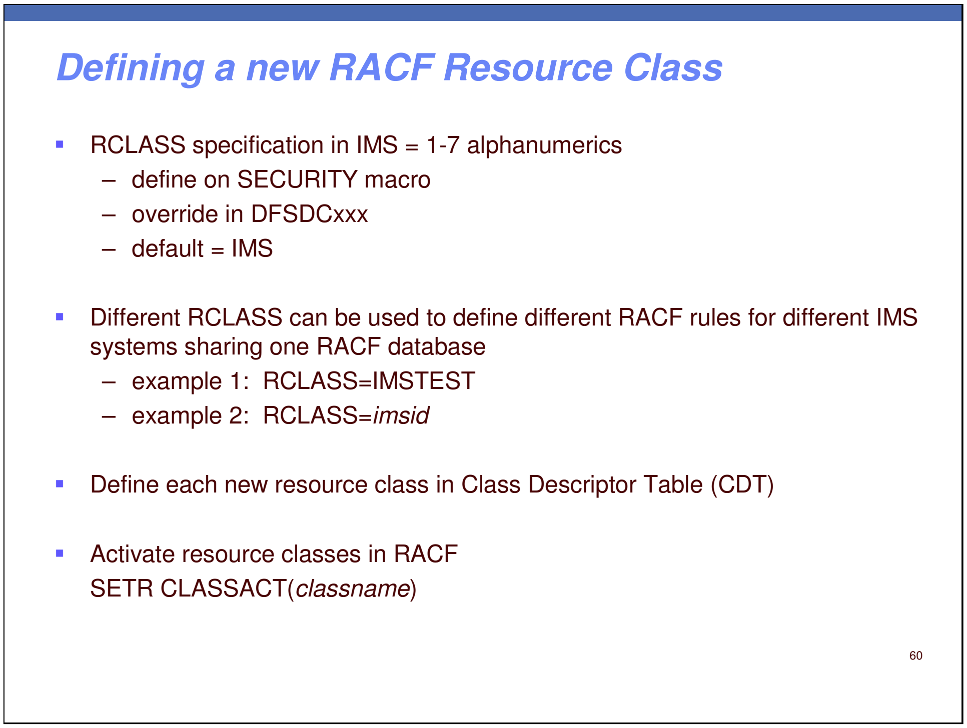
T*IMS* C*IMS* I*IMS* L*IMS*



RACF Resource Class

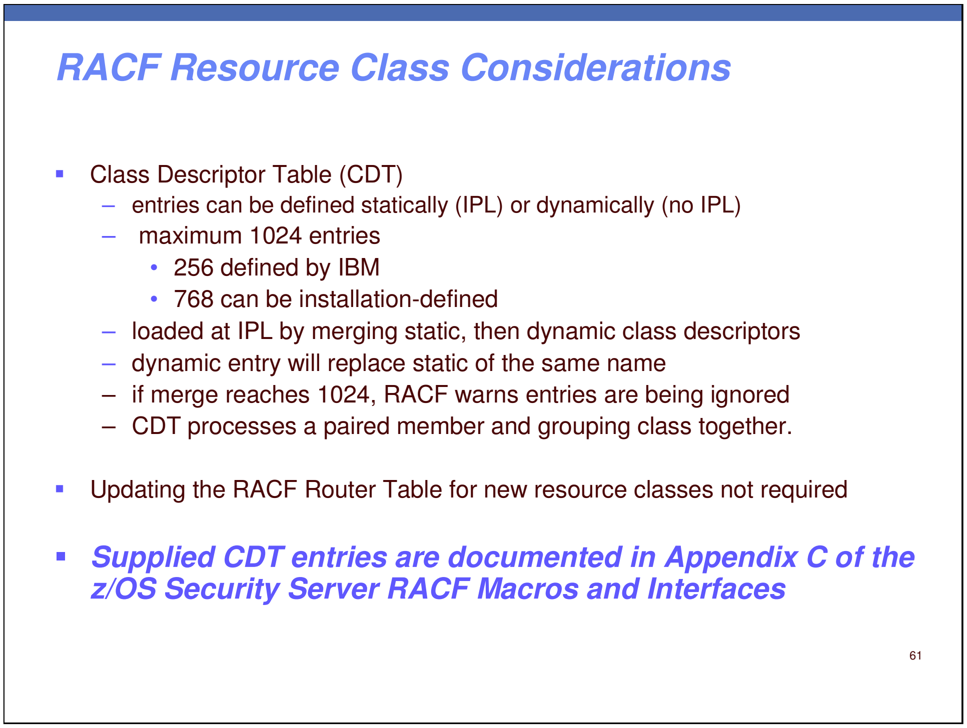
Example of some installation-defined resource classes when RCLASS=IMSTEST:

T*IMSTEST* C*IMSTEST* I*IMSTEST* L*IMSTEST*



Defining a new RACF Resource Class

- RCLASS specification in IMS = 1-7 alphanumerics
  - define on SECURITY macro
  - override in DFSDCxxx
  - default = IMS
- Different RCLASS can be used to define different RACF rules for different IMS systems sharing one RACF database
  - example 1: RCLASS=IMSTEST
  - example 2: RCLASS=*imsid*
- Define each new resource class in Class Descriptor Table (CDT)
- Activate resource classes in RACF
  SETR CLASSACT(*classname*)

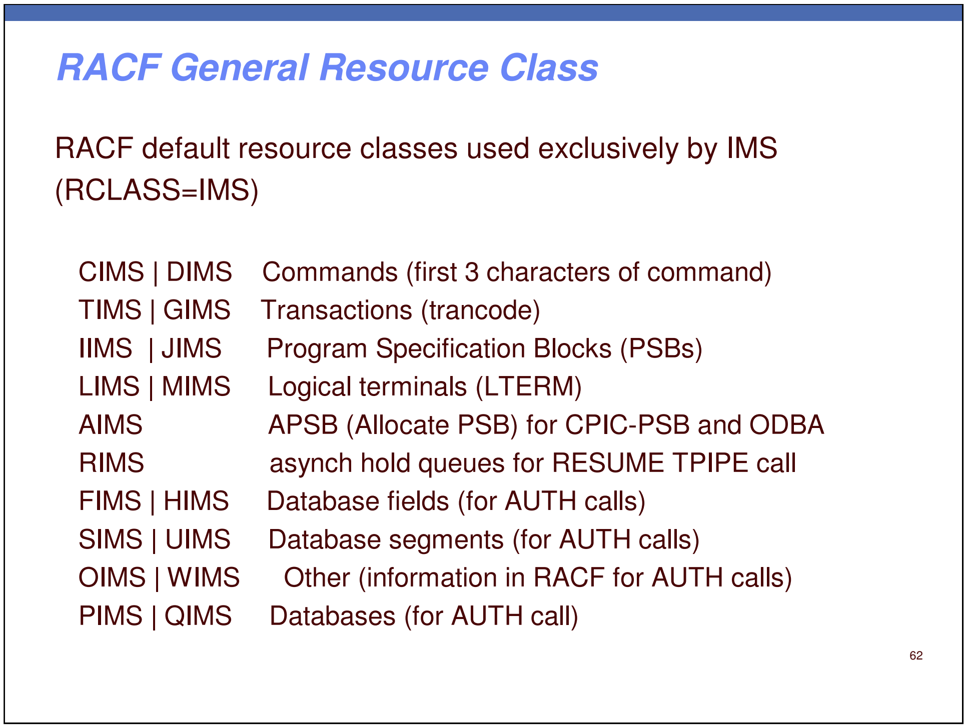


RACF Resource Class Considerations

- Class Descriptor Table (CDT)
  - entries can be defined statically (IPL) or dynamically (no IPL)
  - maximum 1024 entries
    - 256 defined by IBM
    - 768 can be installation-defined
  - loaded at IPL by merging static, then dynamic class descriptors
  - dynamic entry will replace static of the same name
  - if merge reaches 1024, RACF warns entries are being ignored
  - CDT processes a paired member and grouping class together.
- Updating the RACF Router Table for new resource classes not required
- ***Supplied CDT entries are documented in Appendix C of the z/OS Security Server RACF Macros and Interfaces***

61

An important attribute of every CDT entry is its POSIT value. There are 1024 possible numeric POSIT values. You can specify POSIT values 19–56 and 128–527. However, certain POSIT values are reserved for IBM use. Restriction: POSIT values 0–18, 57–127, and 528–1023 are reserved for IBM use and should not be used for your dynamic class entries **unless you intend to share SETROPTS options with an IBM supplied class.** (For example, you might choose to have an installation-defined CICS class share SETROPTS options with an IBM supplied CICS class.) If you use a reserved POSIT number that is not currently used for an IBM supplied class, be aware that in the future IBM might create a supplied class with this POSIT number. If this conflict occurs, processing results for your class will be unpredictable. Classes with the same POSIT value are administered as a single class when you specify a class option, such as CLASSACT or RACLIST, on the RACF SETROPTS command or grant CLAUTH authority to one of them. You would add a new class with a unique POSIT value when you want to administer it separately from any other class..."



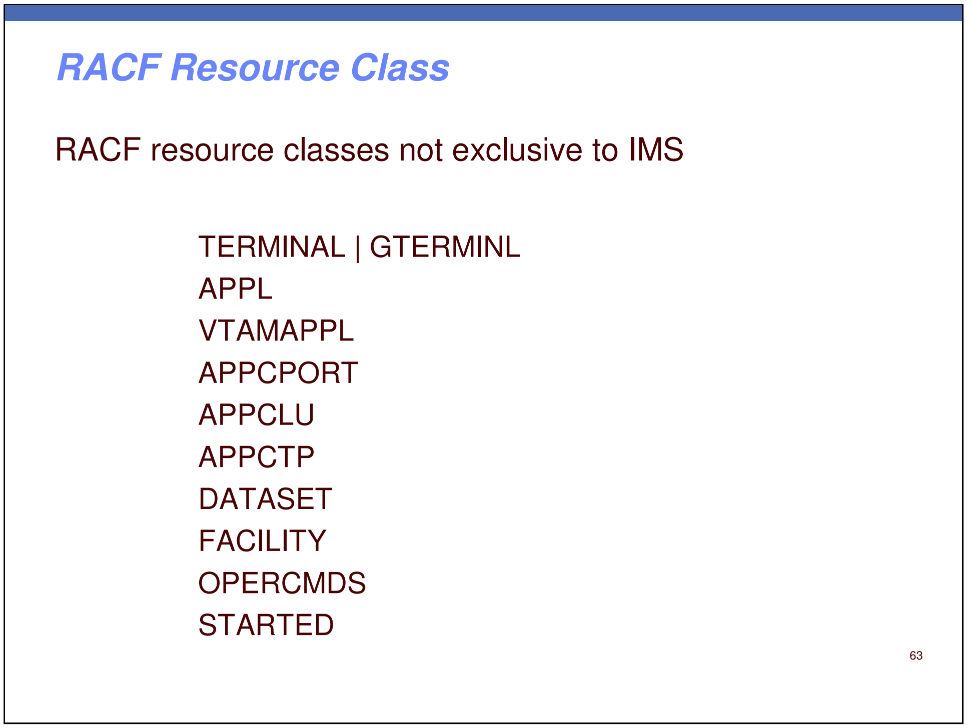
RACF General Resource Class

RACF default resource classes used exclusively by IMS (RCLASS=IMS)

CIMS | DIMS	Commands (first 3 characters of command)
TIMS | GIMS	Transactions (trancode)
IIMS | JIMS	Program Specification Blocks (PSBs)
LIMS | MIMS	Logical terminals (LTERM)
AIMS	APSB (Allocate PSB) for CPIC-PSB and ODBA
RIMS	asynch hold queues for RESUME TPIPE call
FIMS | HIMS	Database fields (for AUTH calls)
SIMS | UIMS	Database segments (for AUTH calls)
OIMS | WIMS	Other (information in RACF for AUTH calls)
PIMS | QIMS	Databases (for AUTH call)

These RACF resource classes are used exclusively by IMS. These classes are listed on the visual. The default classes are classes provided in the RACF Class Descriptor Table and are already activated.

Note that the AIMS and RIMS classes does not have a grouping class associated with them.

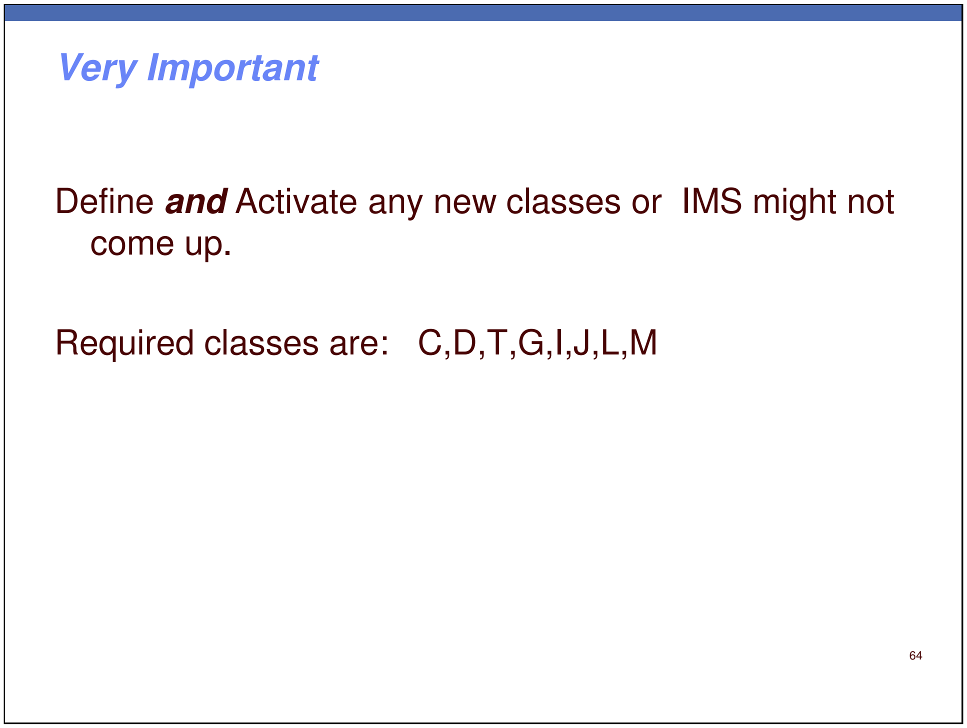


RACF Resource Class

RACF resource classes not exclusive to IMS

TERMINAL | GTERMINL
APPL
VTAMAPPL
APPCPORT
APPCLU
APPCTP
DATASET
FACILITY
OPERCMDS
STARTED

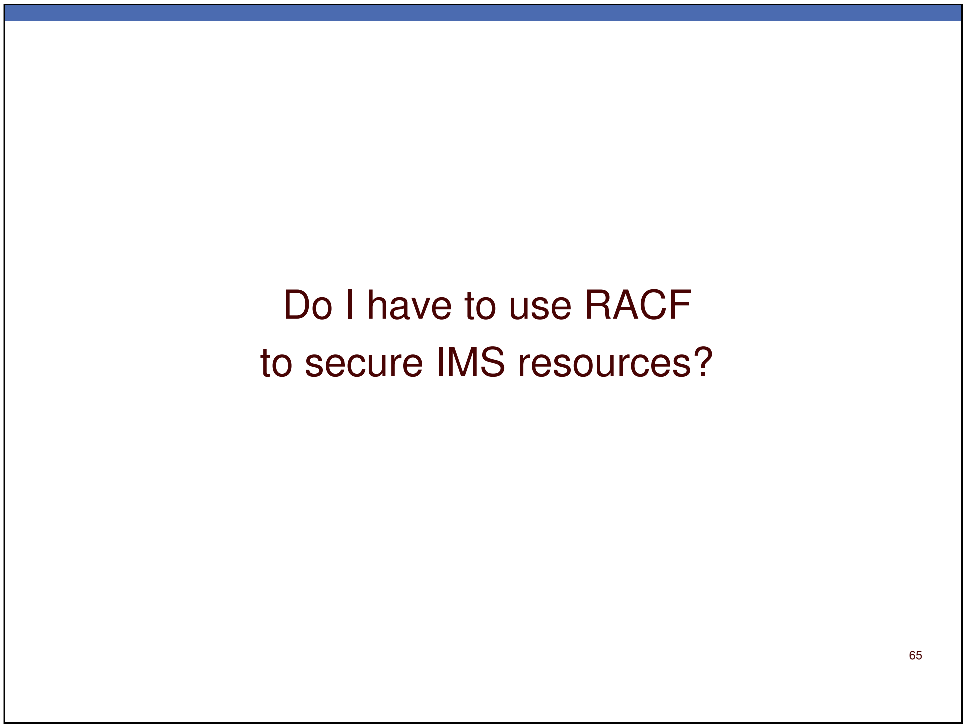
In addition to the RACF classes used exclusive for IMS resource security definitions, a number of other RACF classes may be used to secure access to IMS resources. The other classes may be used by other subsystems, such as CICS, TSO, and other MVS subsystems.



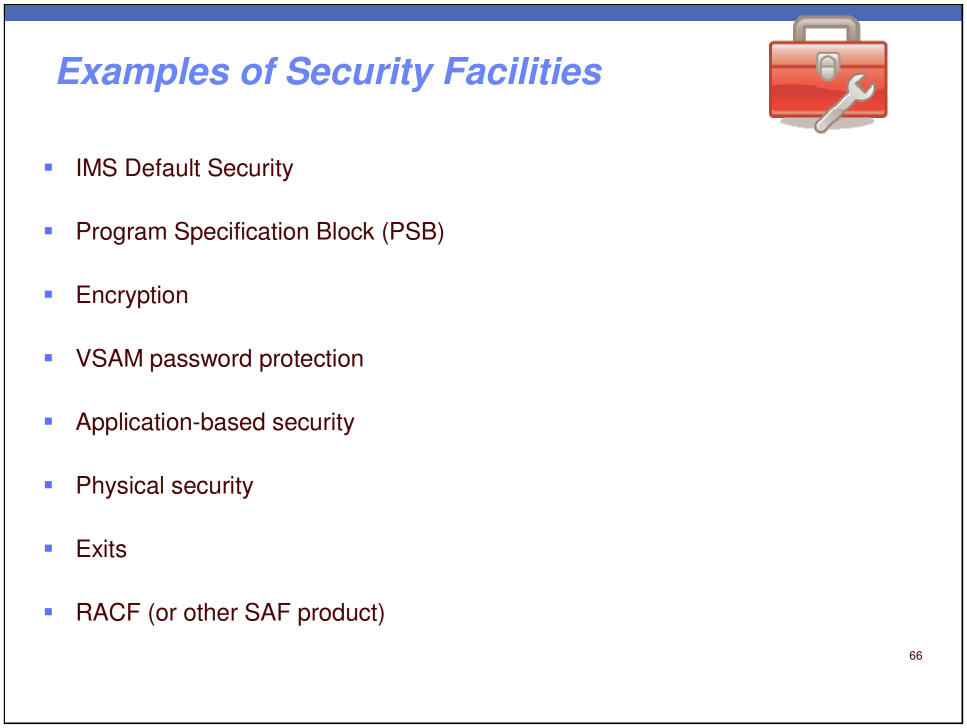
Very Important

Define ***and*** Activate any new classes or IMS might not come up.

Required classes are: C,D,T,G,I,J,L,M

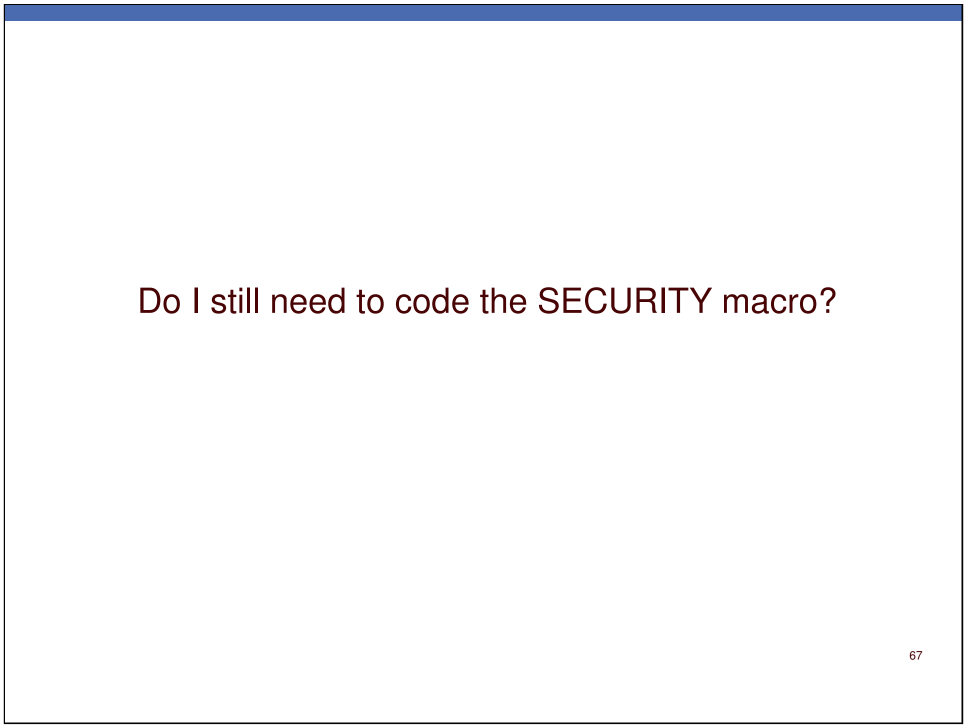


Do I have to use RACF
to secure IMS resources?



Examples of Security Facilities

- IMS Default Security
- Program Specification Block (PSB)
- Encryption
- VSAM password protection
- Application-based security
- Physical security
- Exits
- RACF (or other SAF product)

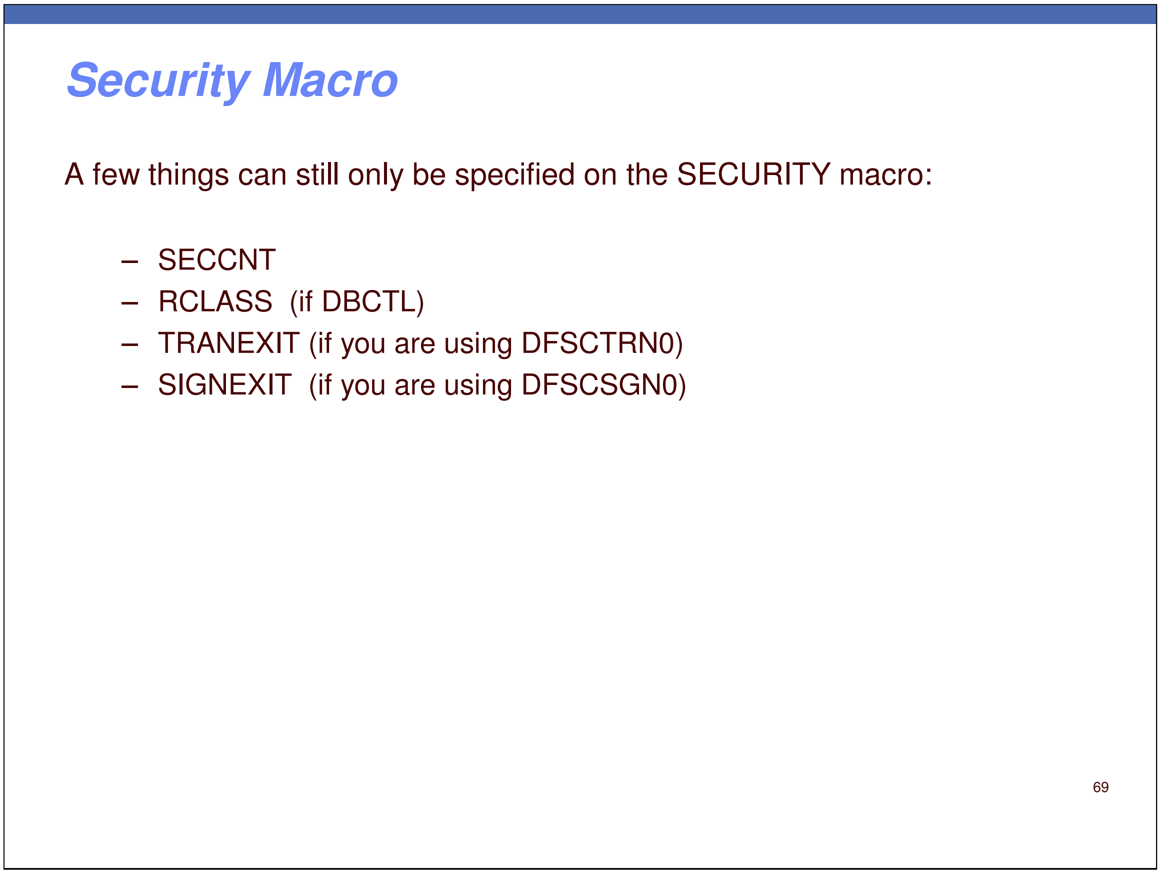


Do I still need to code the SECURITY macro?

Security Macro

IMS V11 SECURITY macro specifies RACF and/or EXIT security options

SECURITY					
	SECCNT=	0	1	2	3
	RCLASS=				
	SECLVL=				
	TYPE=				



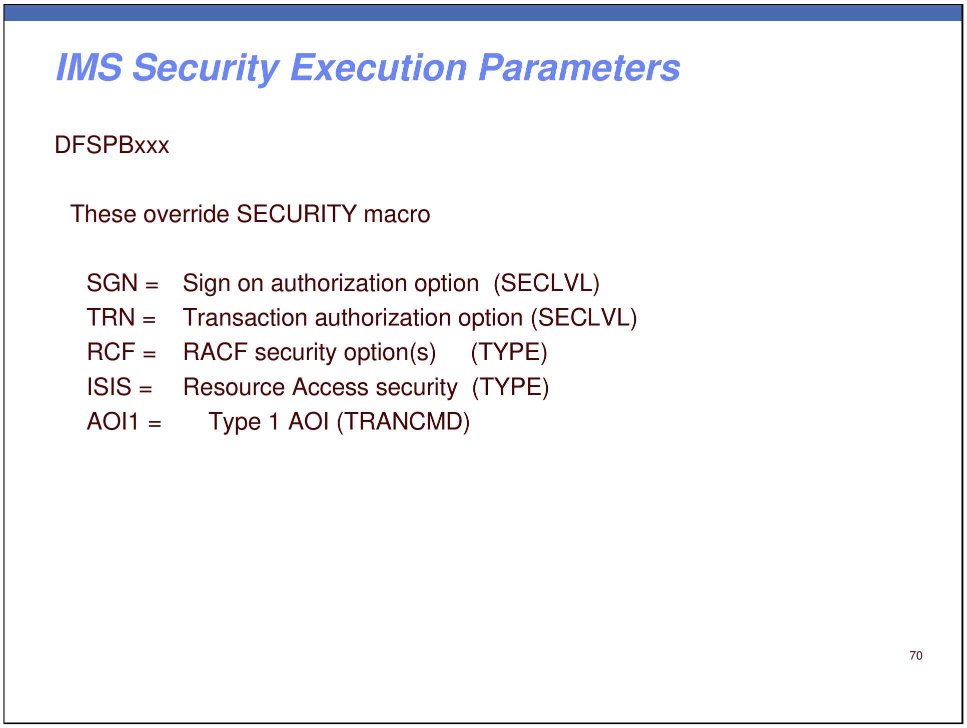
Security Macro

A few things can still only be specified on the SECURITY macro:

- SECCNT
- RCLASS (if DBCTL)
- TRANEXIT (if you are using DFSCTRN0)
- SIGNEXIT (if you are using DFSCSGN0)

SIGNEXIT specifies the use of the older signon exit, DFSCSGN0.

The newer signon exit, DFSSGNX0, is included in the system when you specify ETO=Y.

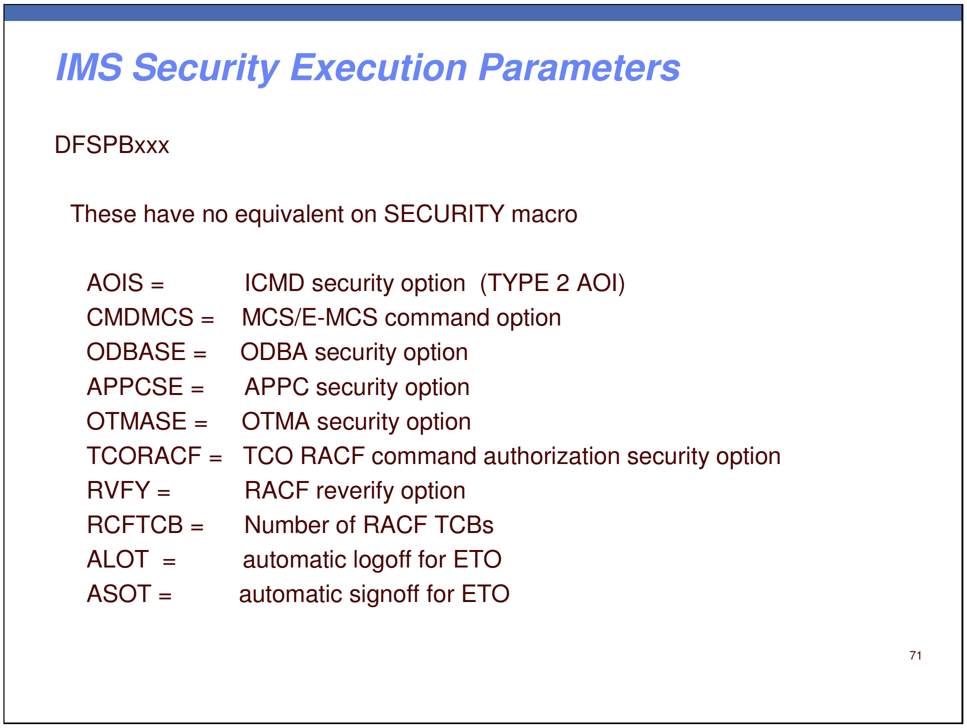


IMS Security Execution Parameters

DFSPBxxx

These override SECURITY macro

SGN =	Sign on authorization option (SECLVL)
TRN =	Transaction authorization option (SECLVL)
RCF =	RACF security option(s) (TYPE)
ISIS =	Resource Access security (TYPE)
AOI1 =	Type 1 AOI (TRANCMD)

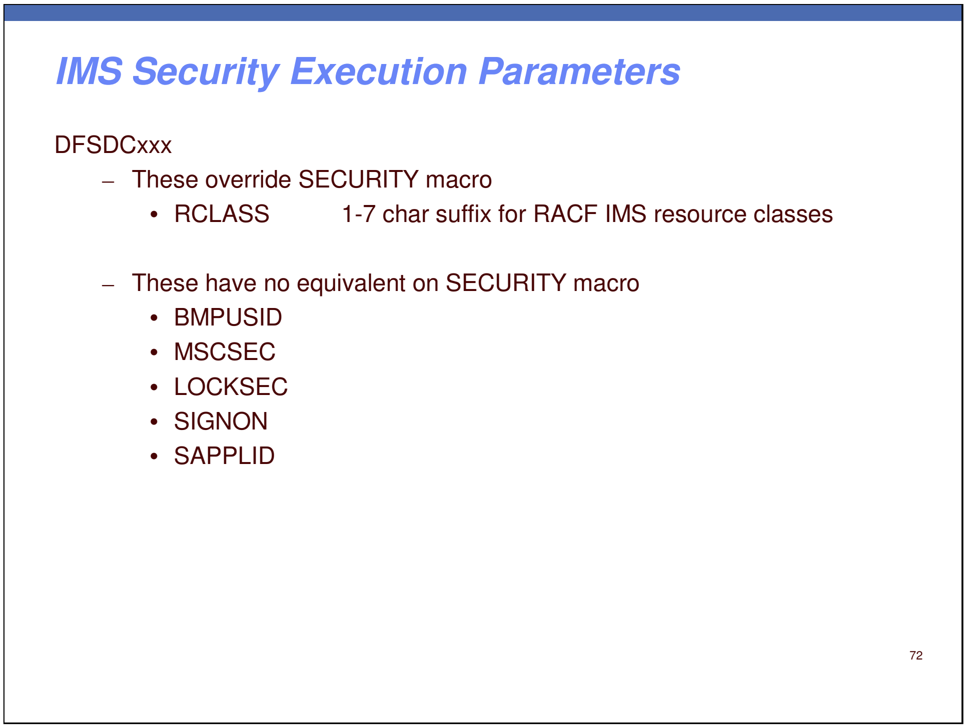


IMS Security Execution Parameters

DFSPBxxx

These have no equivalent on SECURITY macro

AOIS =	ICMD security option (TYPE 2 AOI)
CMDMCS =	MCS/E-MCS command option
ODBASE =	ODBA security option
APPCSE =	APPC security option
OTMASE =	OTMA security option
TCORACF =	TCO RACF command authorization security option
RVFY =	RACF reverify option
RCFTCB =	Number of RACF TCBs
ALOT =	automatic logoff for ETO
ASOT =	automatic signoff for ETO

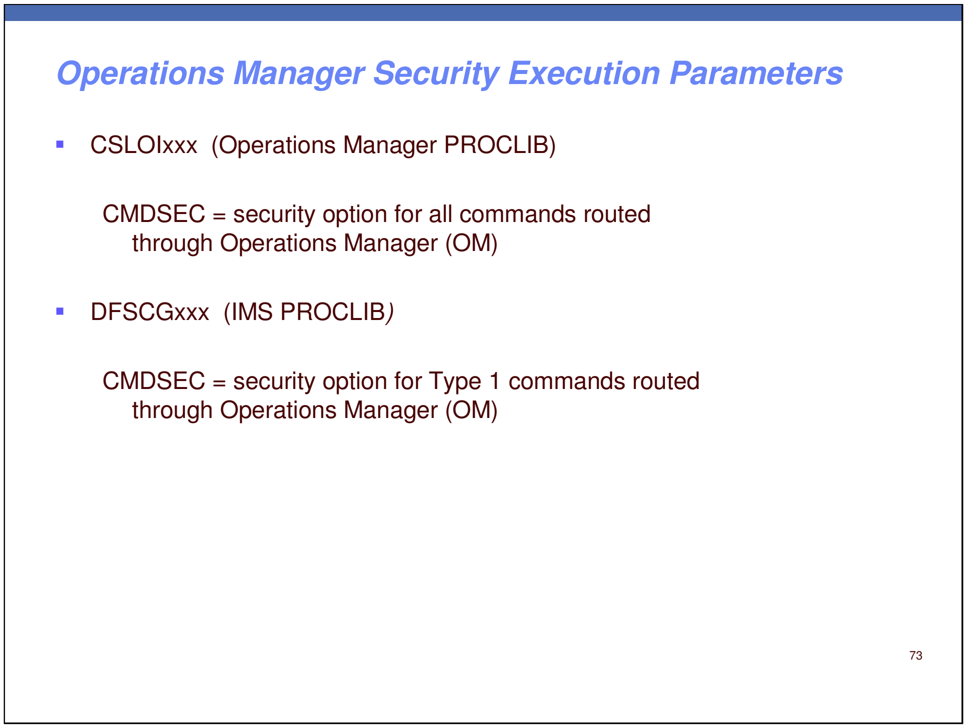


IMS Security Execution Parameters

DFSDCxxx

- These override SECURITY macro
  - RCLASS 1-7 char suffix for RACF IMS resource classes

- These have no equivalent on SECURITY macro
  - BMPUSID
  - MSCSEC
  - LOCKSEC
  - SIGNON
  - SAPPLID



Operations Manager Security Execution Parameters

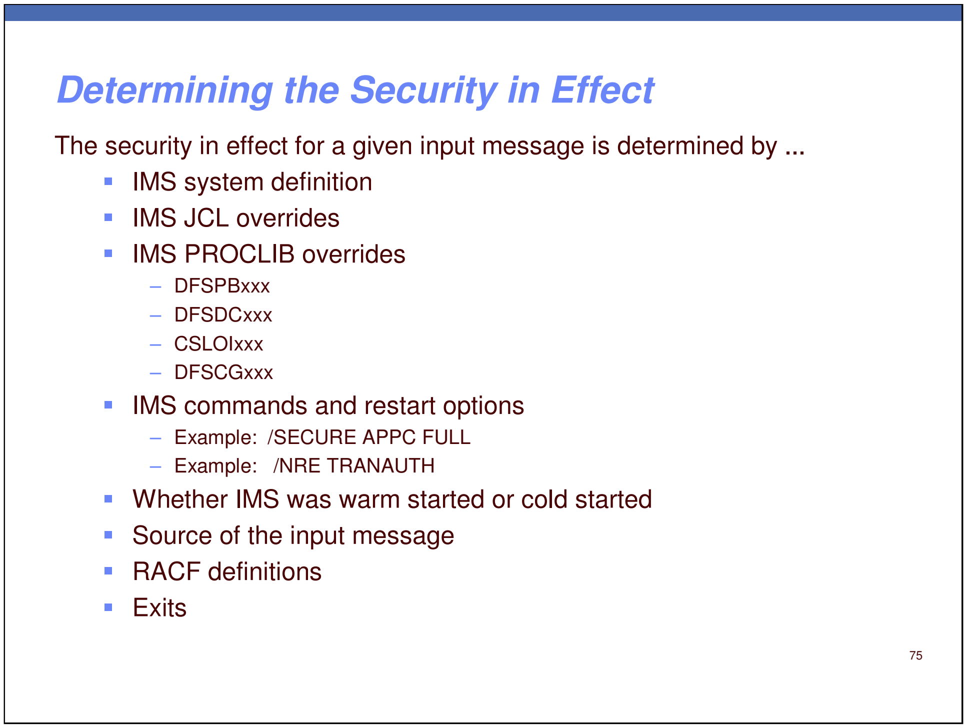
- CSLOIxxx (Operations Manager PROCLIB)

  CMDSEC = security option for all commands routed
  through Operations Manager (OM)

- DFSCGxxx (IMS PROCLIB*)*

  CMDSEC = security option for Type 1 commands routed
  through Operations Manager (OM)

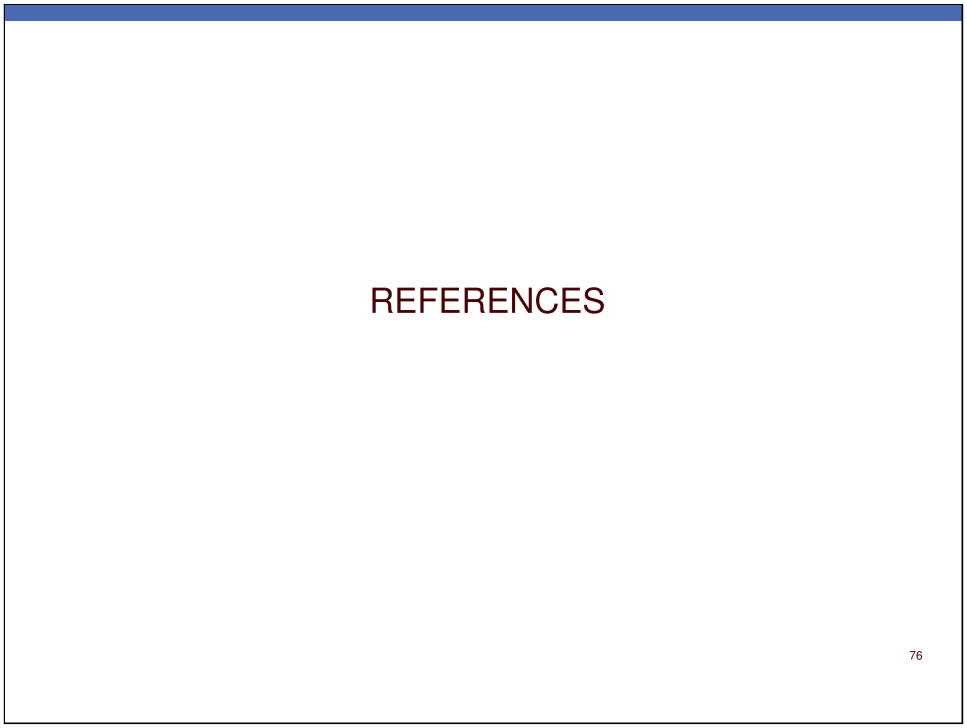
How do I know what security I have?



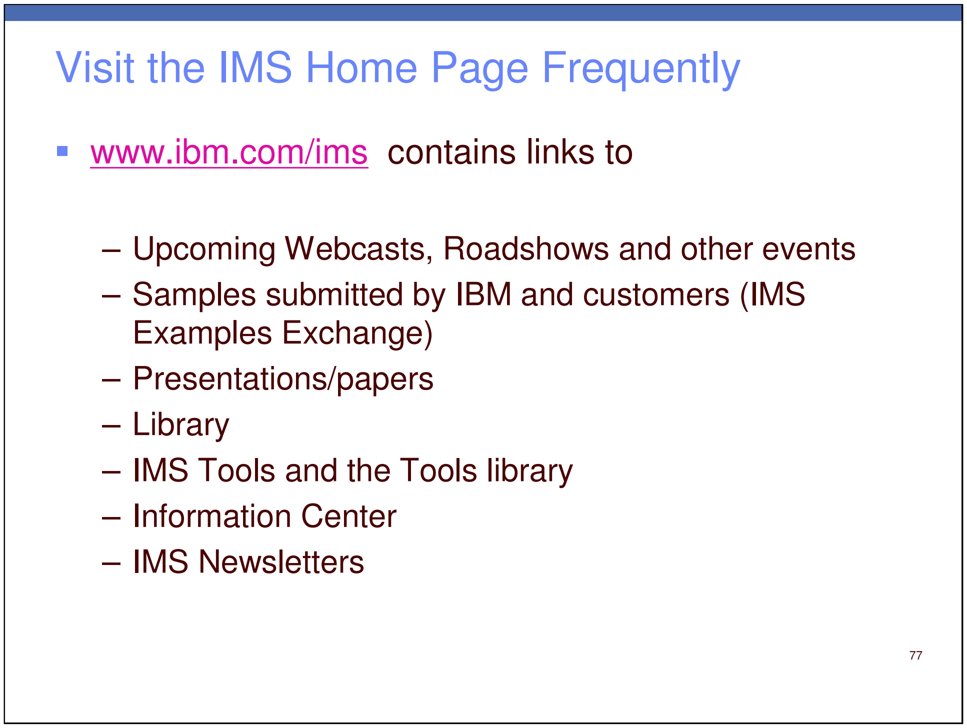
Determining the Security in Effect

The security in effect for a given input message is determined by ...

- IMS system definition
- IMS JCL overrides
- IMS PROCLIB overrides
  - DFSPBxxx
  - DFSDCxxx
  - CSLOIxxx
  - DFSCGxxx
- IMS commands and restart options
  - Example: /SECURE APPC FULL
  - Example: /NRE TRANAUTH
- Whether IMS was warm started or cold started
- Source of the input message
- RACF definitions
- Exits



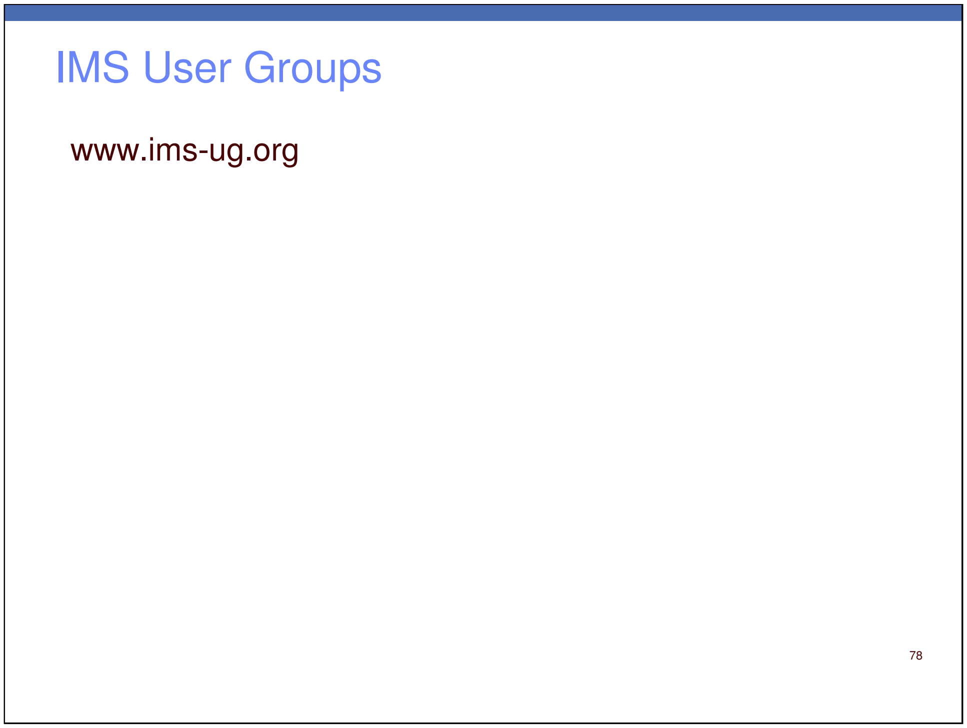
REFERENCES



Visit the IMS Home Page Frequently

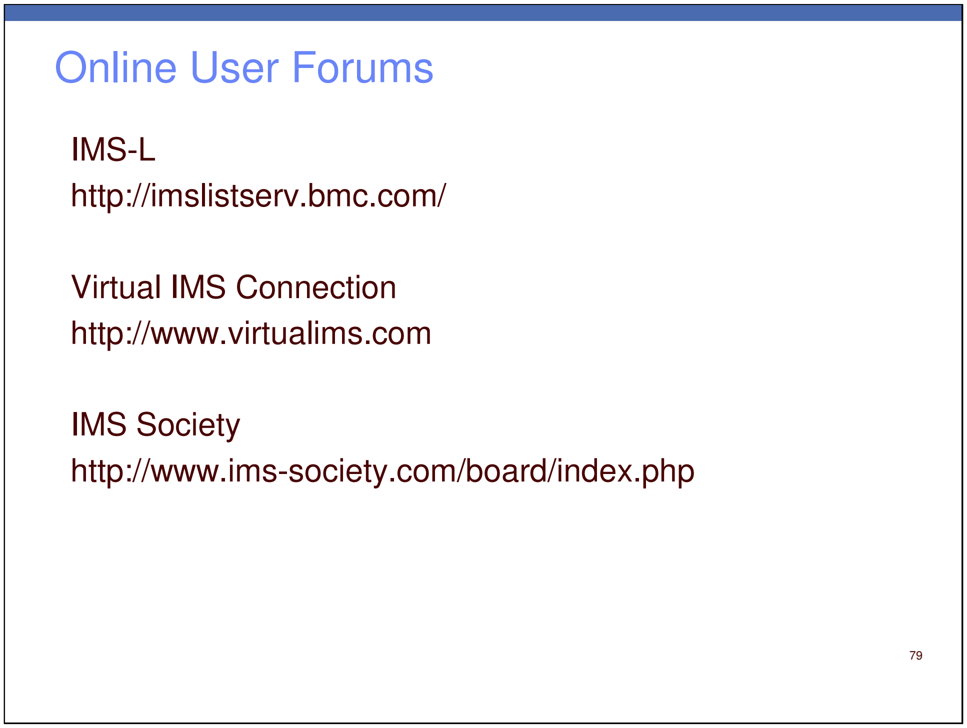
- www.ibm.com/ims contains links to
  - – Upcoming Webcasts, Roadshows and other events
  - – Samples submitted by IBM and customers (IMS Examples Exchange)
  - – Presentations/papers
  - – Library
  - – IMS Tools and the Tools library
  - – Information Center
  - – IMS Newsletters

77



IMS User Groups

www.ims-ug.org

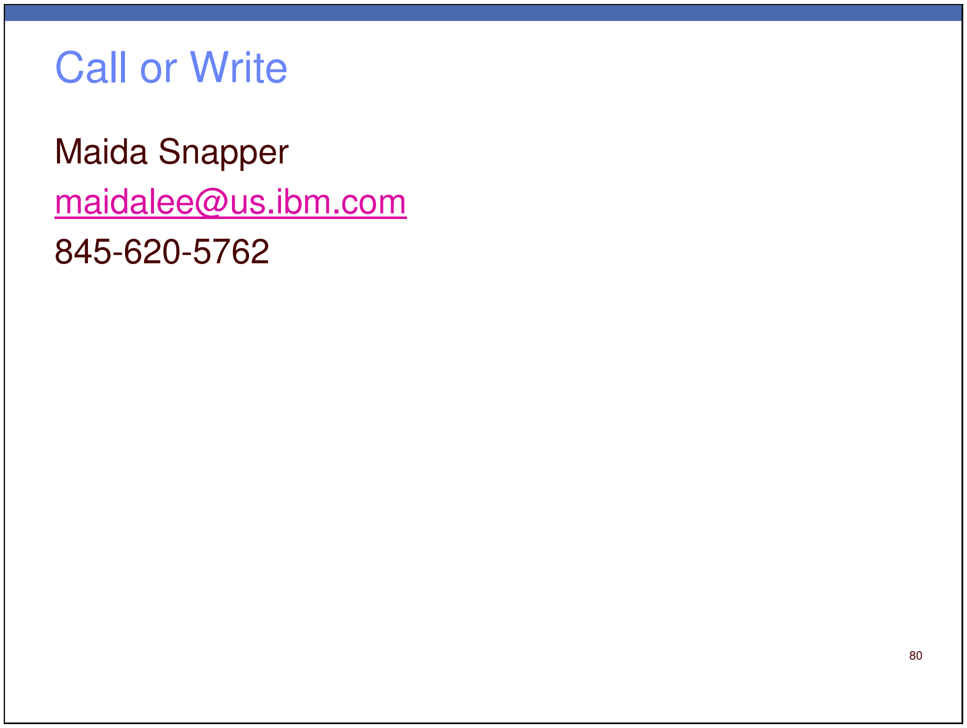


Online User Forums

IMS-L
http://imslistserv.bmc.com/

Virtual IMS Connection
http://www.virtualims.com

IMS Society
http://www.ims-society.com/board/index.php



Call or Write

Maida Snapper

maidalee@us.ibm.com

845-620-5762