IMS TECHNICAL CONFERENCE

October 23 — 26, 2000
Anaheim Marriott
Anaheim, California

Alonia (Lonnie) Coleman
acoleman@us.ibm.com
IBM Dallas Systems Center

IBM Dallas DSC SYSTEMS CENTER

THE WORLD DEPENDS ON IT

IMS

E45

SESSION 2

IMS Security

Security Considerations For Database/Data Communications (DB/DC) Environments

RETURN TO INDEX

Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

IMS Security: Considerations For DB/DC

Objective

This presentation is designed to provide the IMS Systems Programmer with the details required to work with the RACF Security Administrator in establishing effective RACF security for IMS resources. The presentation has a focus on IMS/TM systems that use RACF as the System Authorization Facility (SAF) provider. While the content is specific to RACF; the concepts apply equally to any security product that uses the SAF interface.

Agenda

- IMS security overview
- Securing access to IMS resources
  - The control region
  - Terminal access
  - Command security
  - Transaction security

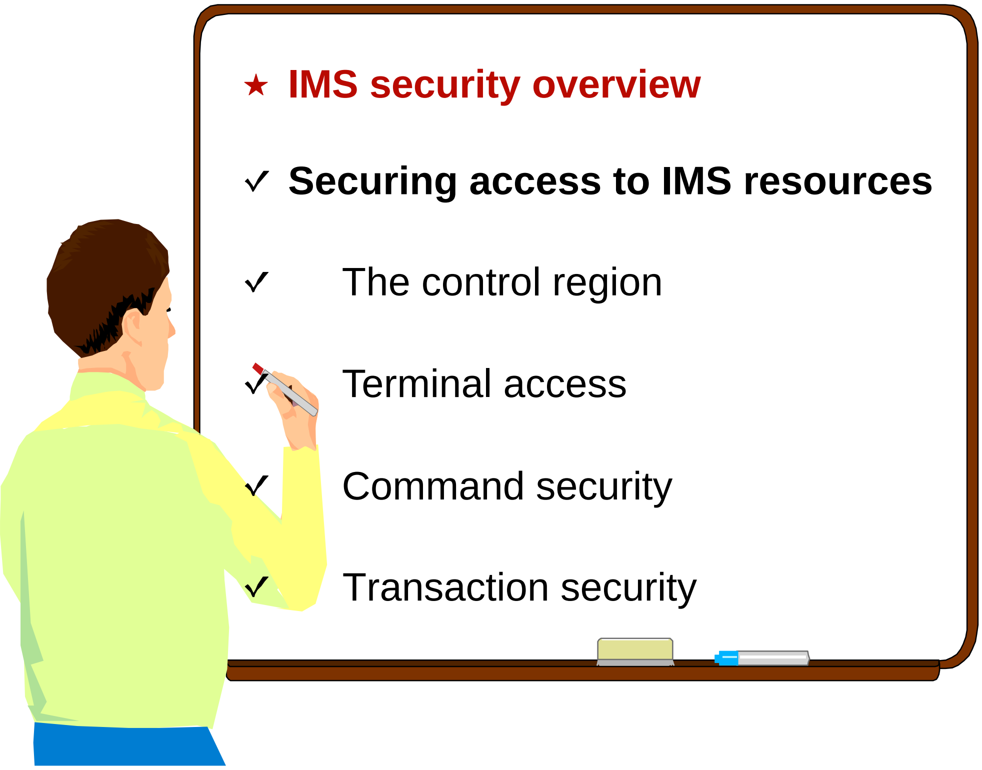
Available Education

Course title: **Implementing IMS Security**
Course number: **CM431**
Section: **AB8A**

Duration: **4.0 days**
Class status: **Open**
Start date: **10/16/00**
End date: **10/19/00**
Start time: **09:00 AM**

Street address: **330 N Wabash Ave.**
City, state: **Chicago, IL**

Enrollments: **1-800-IBM-TEACH**
http://www.ibm.com/services/learning/us



★ **IMS security overview**

✓ **Securing access to IMS resources**

✓ The control region

✓ Terminal access

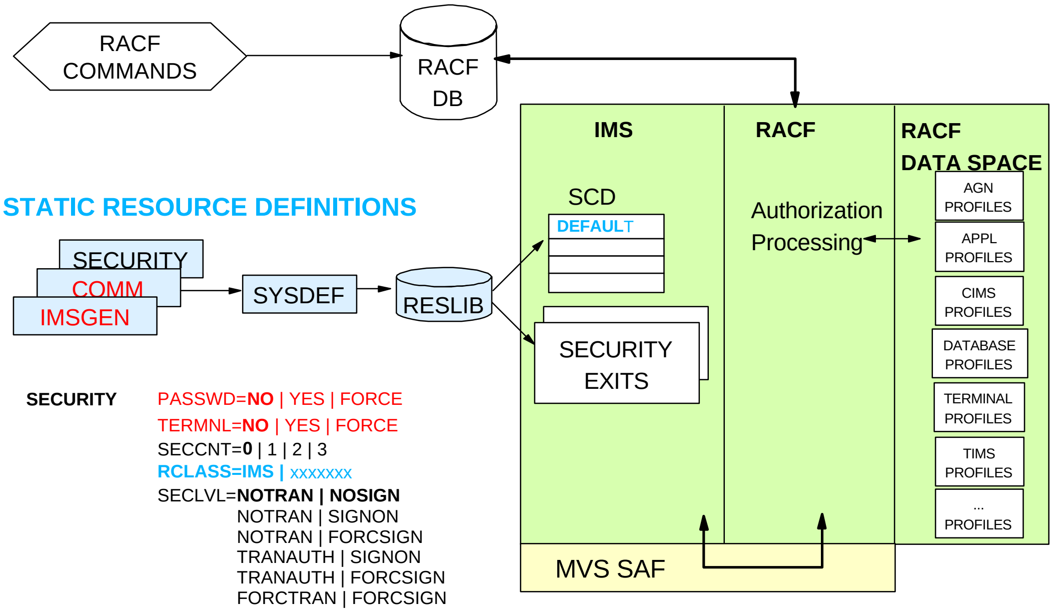
✓ Command security

✓ Transaction security

IMS Security Overview

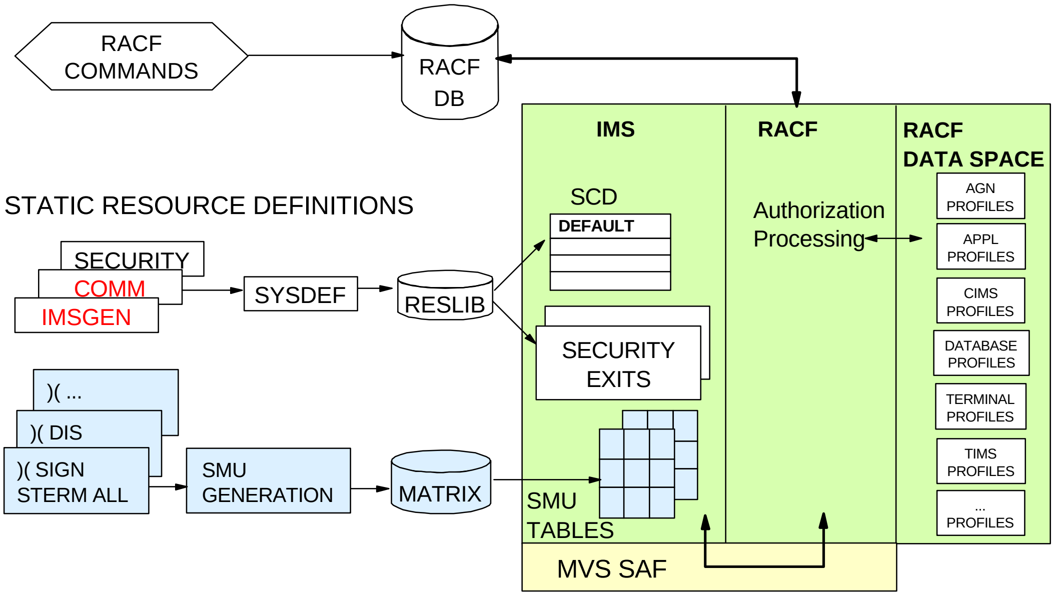
- **The following facilities are available to the IMS installation to protect IMS resources**
  - Default security (IMS provided)
    - **IMS commands only**
  - Security Maintenance Utility (SMU)
    - Terminal and password based security checking
    - **No userid authorization facilities/logic**
  - External Security Product (RACF, et al)
    - **Userid based authorization processing**
  - Security Exits
  - In many cases, multiple facilities may be used to protect a single resource
    - Example: You can use RACF, a user exit routine, ***and*** SMU to protect a transaction

IMS Security Overview



```
SECURITY      PASSWD=NO | YES | FORCE
              TERMNL=NO | YES | FORCE
              SECCNT=0 | 1 | 2 | 3
              RCLASS=IMS | xxxxxxx
              SECLVL=NOTRAN | NOSIGN
                     NOTRAN | SIGNON
                     NOTRAN | FORCSIGN
                     TRANAUTH | SIGNON
                     TRANAUTH | FORCSIGN
                     FORCTRAN | FORCSIGN
              TRANCMD=NO | YES | FORCE
              TYPE=NOAGN | RACFAGN | AGN,
                   NORACTRM |   RACFTERM,
                   NOTRANEX | TRANEXIT,
                   NOSIGNEX | SIGNEXIT,
                   NORACFCM | RACFCOM
```

IMS Security Overview ...



RACF COMMANDS

RACF DB

STATIC RESOURCE DEFINITIONS

SECURITY

COMM

IMSGEN

SYSDEF

RESLIB

)(...

)(DIS

)(SIGN STERM ALL

SMU GENERATION

MATRIX

IMS

SCD

DEFAULT

SECURITY EXITS

SMU TABLES

RACF

Authorization Processing

RACF DATA SPACE

AGN PROFILES

APPL PROFILES

CIMS PROFILES

DATABASE PROFILES

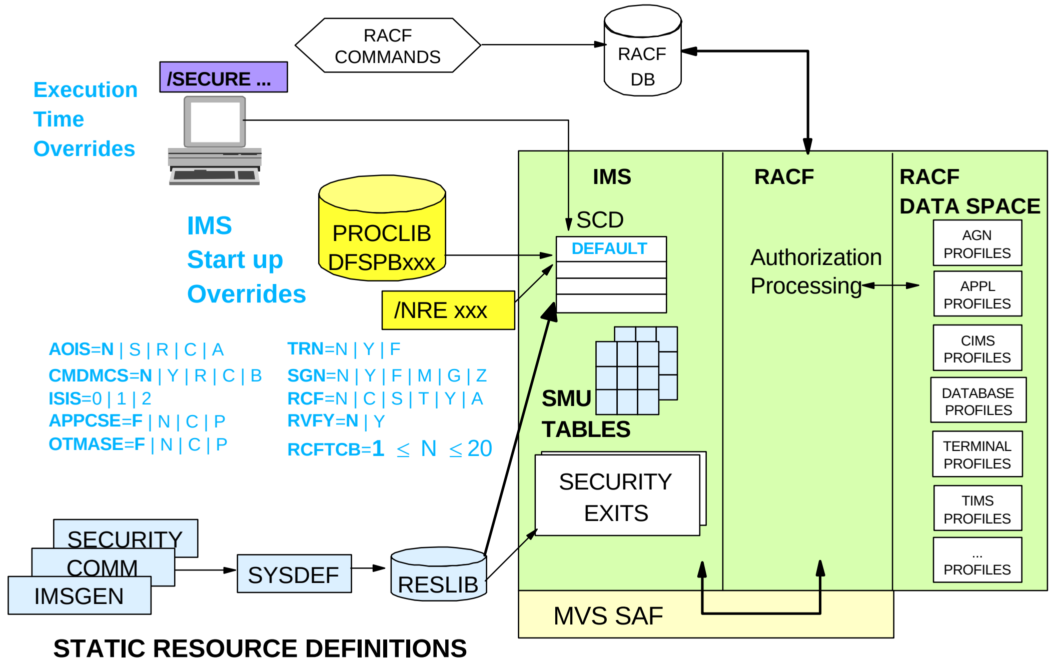
TERMINAL PROFILES

TIMS PROFILES

... PROFILES

MVS SAF

IMS Security Overview ...



RACF COMMANDS

RACF DB

Execution Time Overrides

/SECURE ...

IMS Start up Overrides

PROCLIB DFSPBxxx

/NRE xxx

AOIS=N | S | R | C | A

CMDMCS=N | Y | R | C | B

ISIS=0 | 1 | 2

APPCSE=F | N | C | P

OTMASE=F | N | C | P

TRN=N | Y | F

SGN=N | Y | F | M | G | Z

RCF=N | C | S | T | Y | A

RVFY=N | Y

RCFTCB=1 ≤ N ≤ 20

IMS

SCD

DEFAULT

SMU TABLES

SECURITY EXITS

RACF

Authorization Processing

RACF DATA SPACE

AGN PROFILES

APPL PROFILES

CIMS PROFILES

DATABASE PROFILES

TERMINAL PROFILES

TIMS PROFILES

... PROFILES

MVS SAF

SECURITY

COMM

IMSGEN

SYSDEF

RESLIB

STATIC RESOURCE DEFINITIONS

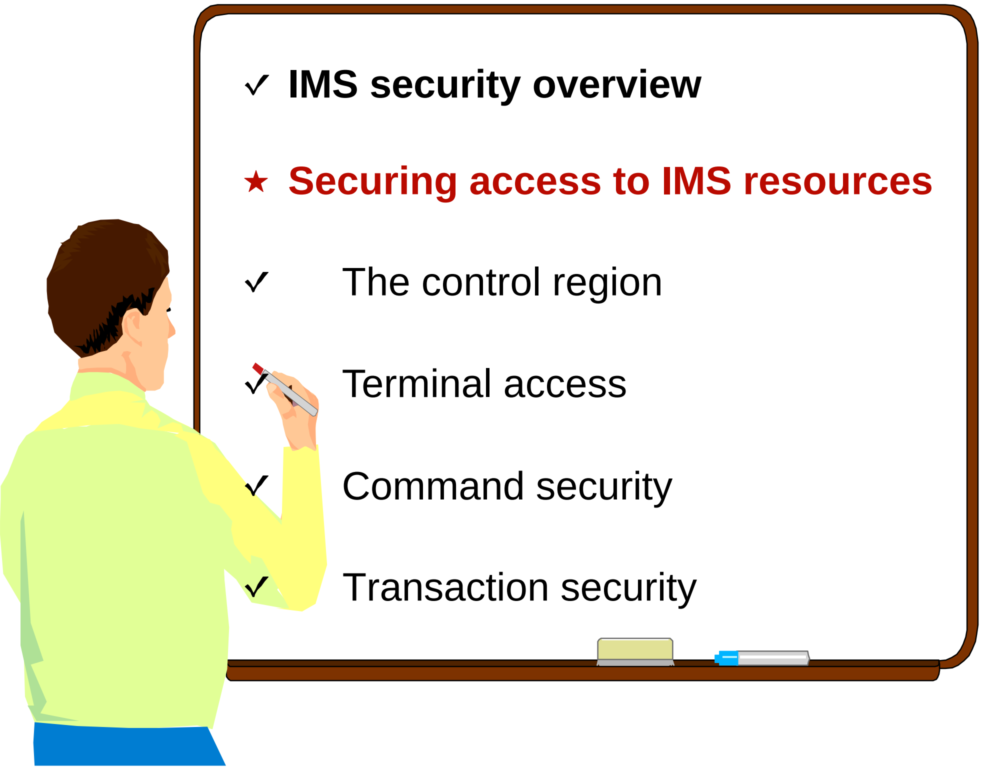
IMS Security Overview ...

- **At IMS start up**
  - Some security specifications may be overridden by
    - IMS start up parameters in JCL or PROCLIB

      AOIS=N | S | R | C | A
      CMDMCS=N | Y | R | C | B
      ISIS=0 | 1 | 2
      APPCSE=F | N | C | P
      OTMASE=F | N | C | P

      TRN=N | Y | F
      SGN=N | Y | F | M | G | Z
      RCF=N | C | S | T | Y | A
      RVFY=N | Y
      RCFTCB=1 ≤ N ≤ 20

    - /NRE and /ERE COLDSYS restart commands and keywords
      - **Example: /NRE NOTRANAUTH**
  - Start up parameters control security for commands and/or transactions received from
    - APPC | OTMA
    - Type 2 automated operator programs
    - MCS/EMCS consoles
- **During IMS execution**
  - /SECURE command and keywords
    - **Example: /SECURE APPC NONE**



✓ **IMS security overview**

★ **Securing access to IMS resources**

✓ The control region

✓ Terminal access

✓ Command security

✓ Transaction security

Securing Access To IMS Resources

- **IMS approach to security**
  - Require users to identify themselves
  - Secure IMS resources
    - The IMS control region
    - Terminal access
    - Transactions
    - Commands
    - Databases and/or data sets
    - Program specification blocks (PSBs)
- **May restrict dependent region to executing specific programs**
- **Can determine what a program can do while executing**
  - Can the program issue:
    - ALLOCATE PSB (APSB) call
    - ISSUE COMMAND (ICMD) call
- **IMS resources may be accessed from other sources**
  - World wide web
  - Advanced-Program-to-Program Communications (APPC) devices
  - Open Transaction Manager Access (OTMA) clients
    - MQSeries
    - IMS Connect
    - IMS TCP/IP OTMA Connection (ITOC)
  - Customer Information Control System (CICS)
  - OS/390 address space
    - Open Database Access (ODBA)
  - Other IMS systems
    - Multiple Systems Coupling (MSC)
    - Intersystem Communications (ISC)
    - Shared queues systems
- **Security should by performed on *source system***

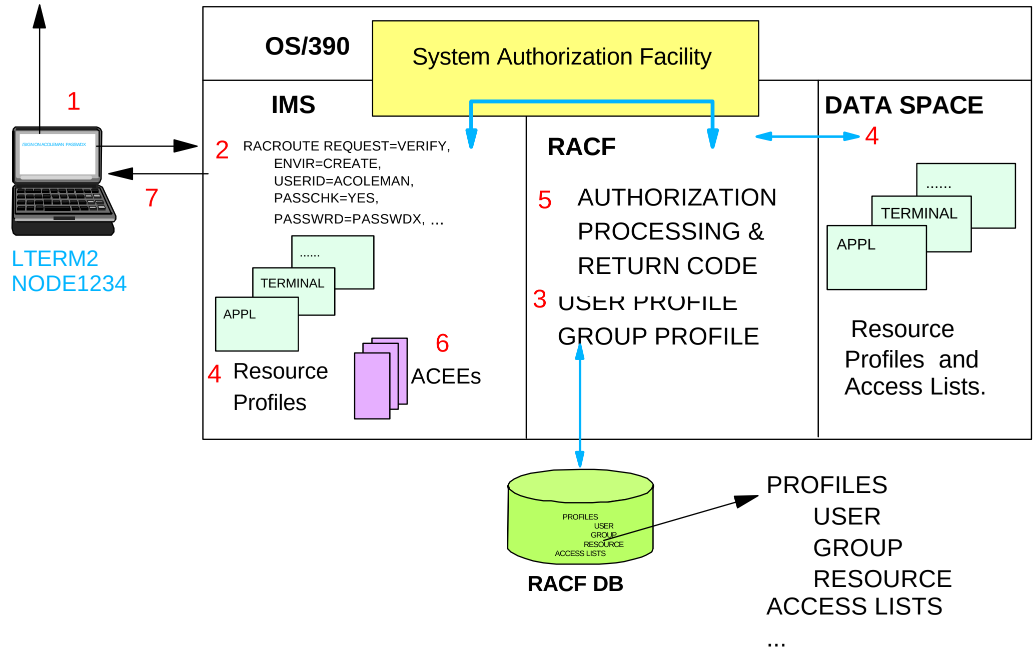
Key Concepts

- **IMS uses *sign on* process to identify and authenticate *end users***
  - Users enter /**SIGN ON** command with RACF
    - Userid
    - Password
    - Group name (optional)

      /SIGN ON STILWELL MAKENA GROUP DSCGRP
  - Userid may be created for *non*-end users
    - Programs, Time controlled operations (TCO), PSB, etc.
- **IMS uses RACF to *validate* userid and *verify* user using profiles predefined to RACF**
  - Has user been defined to RACF?
  - Is the password valid for this userid?
  - Has userid been revoked?
  - ....
- **This userid is the *basis for all subsequent RACF authorizations***

User Verification Is Done At Sign On

/SIGN ON ACOLEMAN PASSWDX GROUP DSC (or **TOKEN** for APPC & OTMA)



1

7

LTERM2
NODE1234

OS/390

System Authorization Facility

IMS

2 RACROUTE REQUEST=VERIFY,
ENVIR=CREATE,
USERID=ACOLEMAN,
PASSCHK=YES,
PASSWRD=PASSWDX, ...

......
TERMINAL
APPL

4 Resource
Profiles

6
ACEEs

RACF

5 AUTHORIZATION
PROCESSING &
RETURN CODE

3 USER PROFILE
GROUP PROFILE

DATA SPACE

4

......
TERMINAL
APPL

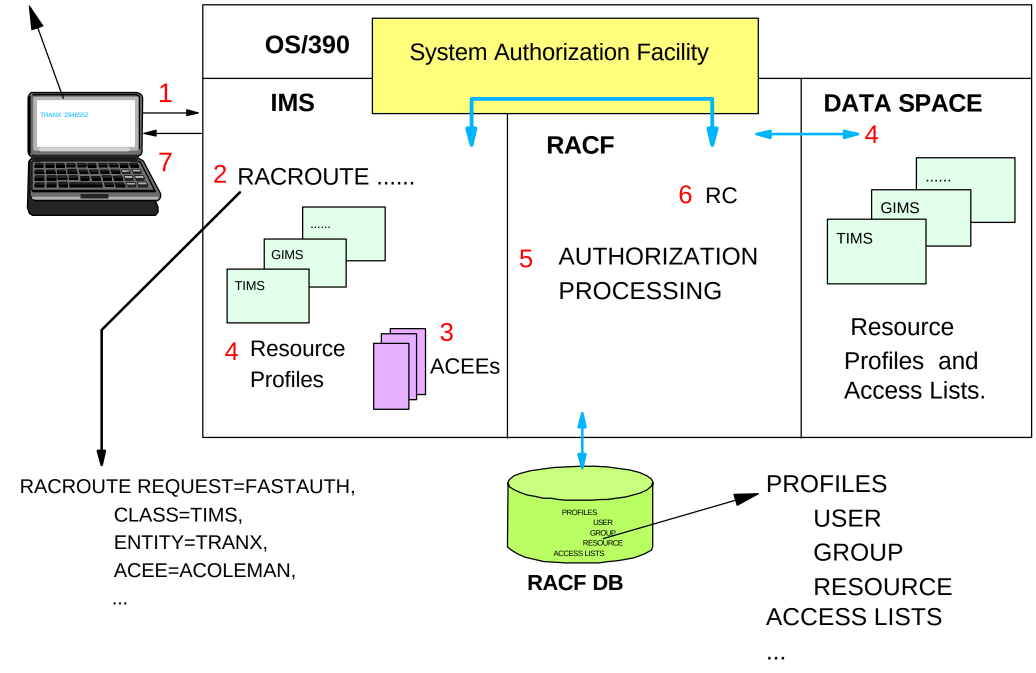
Resource
Profiles and
Access Lists.

RACF DB

PROFILES
USER
GROUP
RESOURCE
ACCESS LISTS
...

Resource Authorization Done After Sign On

TRANX 2946552



1

7

OS/390

System Authorization Facility

IMS

2 RACROUTE ......

......
GIMS
TIMS

4 Resource
Profiles

3
ACEEs

RACF

6 RC

5 AUTHORIZATION
PROCESSING

DATA SPACE

4

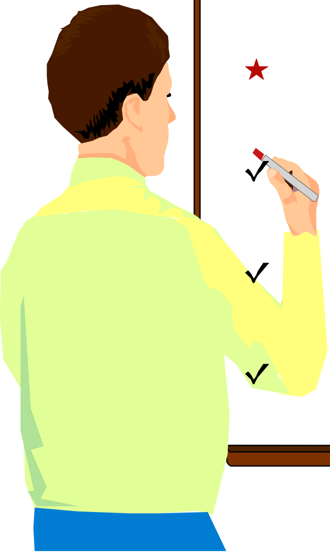
......
GIMS
TIMS

Resource
Profiles and
Access Lists.

RACROUTE REQUEST=FASTAUTH,
CLASS=TIMS,
ENTITY=TRANX,
ACEE=ACOLEMAN,
...

RACF DB

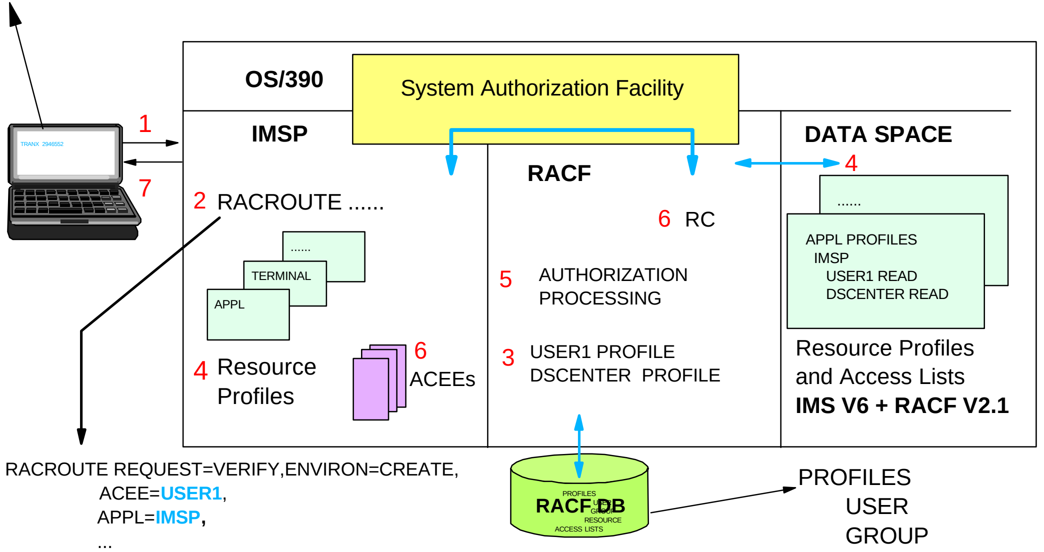
PROFILES
USER
GROUP
RESOURCE
ACCESS LISTS
...



- ✓ **IMS security overview**
- ✓ **Securing access to IMS resources**
- ★ **The control region**
- ✓ Terminal access
- ✓ Command security
- ✓ Transaction security

The IMS Control Region

SIGN ON USER1 PASSWD1 GROUP DSCENTER



```
RACROUTE REQUEST=VERIFY,ENVIRON=CREATE,
              ACEE=USER1,
              APPL=IMSP,
              ...
```

PROFILES
USER
GROUP
RESOURCE
ACCESS LISTS
...

ACTIVATED BY:

```
SECURITY ...SECLVL=(...,SIGNON | FORCSIGN)
            RCLASS=IMS | xxxxxxx
            TYPE=(...RACFTERM...)
```

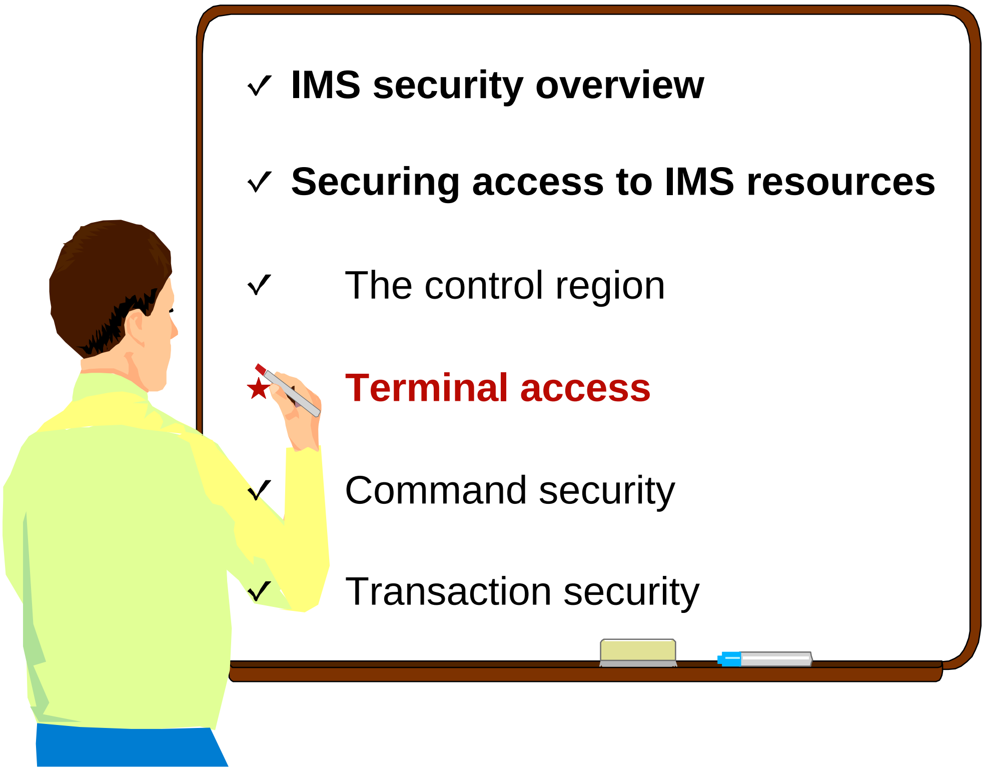
SGN=Y | F, RCF≠N, and)(SIGN STERM ALL or RACF TERMINAL class

RACF APPL class

Sample RACF Commands

EXAMPLE: AUTHORIZE USER1, MEMBERS OF GROUP1, AND MEMBERS OF GROUP2 TO ACCESS IMSP.

```
SETROPTS CLASSACT(APPL)
SETR GLOBAL(APPL)
SETR GENERIC(APPL)
SETR RACLIST(APPL)


RDEFINE APPL IMSP OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSP CLASS(APPL) ID(GROUP1 GROUP2 USER1)
  ACCESS(READ)


SETR GLOBAL(APPL) REFRESH
SETR GENERIC(APPL) REFRESH
SETR RACLIST(APPL) REFRESH
SETR REFRESH
```



✓ **IMS security overview**

✓ **Securing access to IMS resources**

✓ The control region

★ **Terminal access**

✓ Command security

✓ Transaction security

Terminal Access

- **RACF security may be used to secure access to terminals**
  - Restrict specific groups to specific terminals
    - Control use of undefined terminals
    - Restricting times terminal can be used
    - Security labels
  - Classes shared by multiple address spaces (i.e. IMS, TSO, CICS, etc.)
- **Authorization check performed during**
  - Log on to TSO
  - Sign on to IMS
    - VTAM nodes and BTAM terminals
      - Supports both static and ETO terminals
      - Profile names match VTAM node name | BTAM line and terminal combination
    - User can only sign on from authorized terminals

- **Terminal access for 'undefined' terminal**
  - Terminal ***not*** protected by a RACF profile
- **RACF commands to allow**
  - Undefined terminals to be used for logging on

SETROPTS TERMINAL(READ)

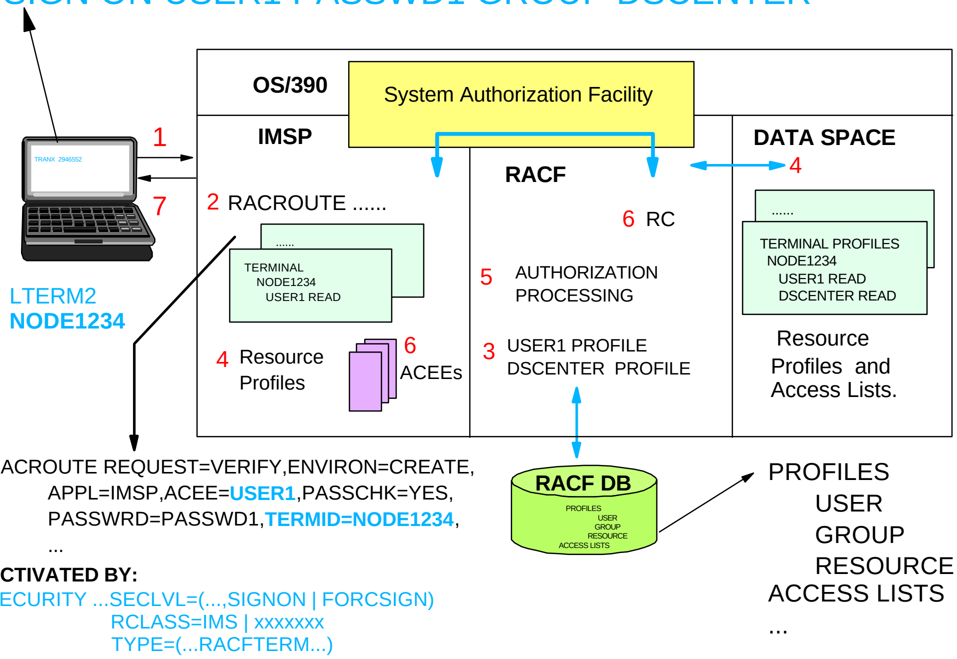
- Prevent undefined terminals from being used

SETROPTS TERMINAL(NONE)

Warning : Before you specify NONE, be sure that you define some terminals to RACF and give the appropriate users and groups proper authorization to use them. Otherwise, no one can log on to your system

Terminal Access Authorization Flow

SIGN ON USER1 PASSWD1 GROUP DSCENTER



```
RACROUTE REQUEST=VERIFY,ENVIRON=CREATE,
      APPL=IMSP,ACEE=USER1,PASSCHK=YES,
      PASSWRD=PASSWD1,TERMID=NODE1234,
      ...
```

ACTIVATED BY:

SECURITY ...SECLVL=(...,SIGNON | FORCSIGN)
RCLASS=IMS | xxxxxxx
TYPE=(...RACFTERM...)

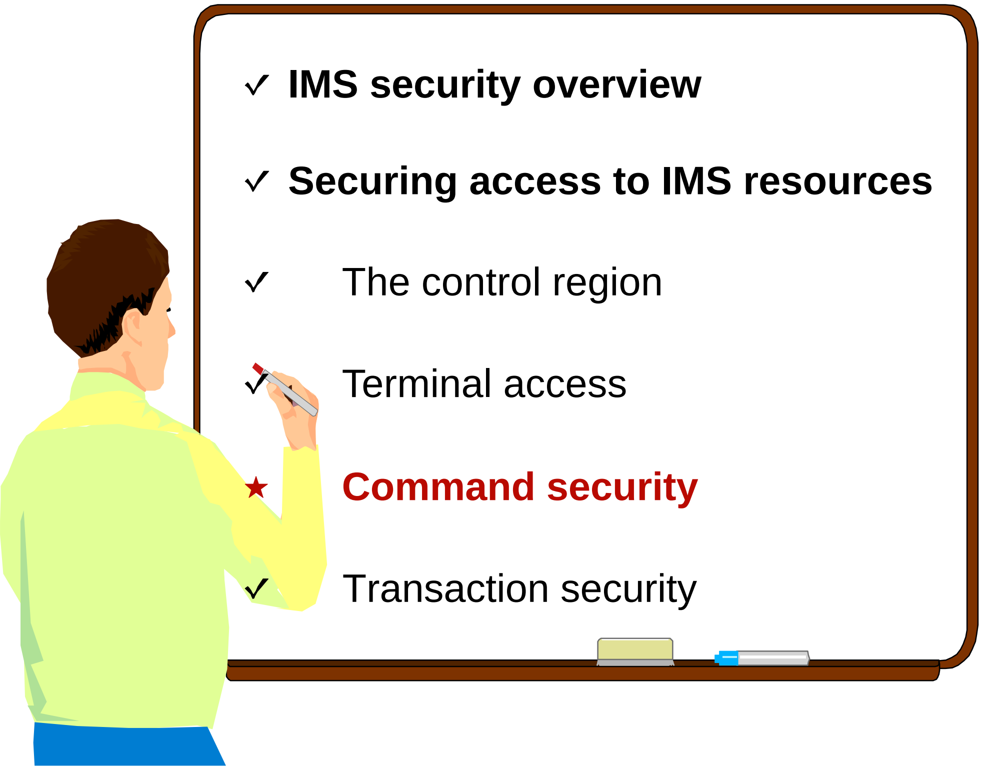
SGN=Y | F, RCF≠N, and)(SIGN STERM ALL or RACF TERMINAL class

RACF TERMINAL | GTERMINL classes

Terminal Class Example

EXAMPLE: AUTHORIZE USER1, MEMBERS OF GROUP1, AND MEMBERS OF GROUP2 TO ACCESS NODE1234 ON WEEKDAYS.

```
SETR CLASSACT(TERMINAL)
SETR GENERIC(TERMINAL)
SETR RACLIST(TERMINAL)

RDEF TERMINAL NODE1234 OWNER(IMSADMIN) UACC(NONE)
PE NODE1234 CLASS(TERMINAL) ID(USER1 GROUP1 GROUP2)
          ACCESS(READ) WHEN(DAYS(WEEKDAYS))

SETR GENERIC(TERMINAL) REFRESH
SETR RACLIST(TERMINAL) REFRESH
SETR REFRESH
```



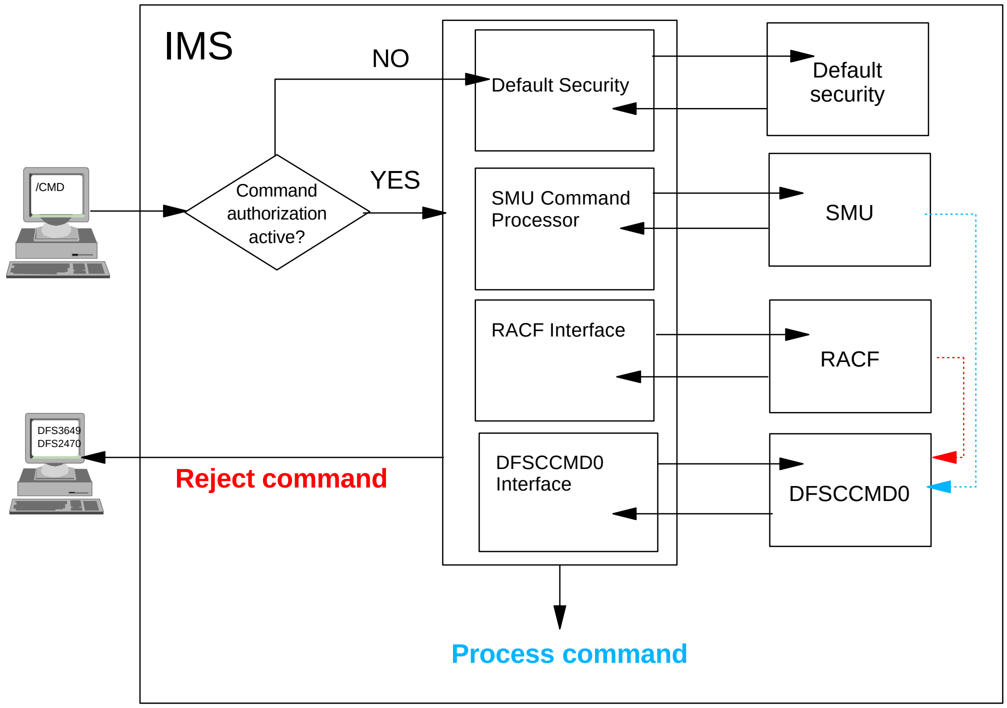
- ✓ **IMS security overview**
- ✓ **Securing access to IMS resources**
  - ✓ The control region
  - ✓ Terminal access
  - ★ **Command security**
  - ✓ Transaction security

Command Security

- **Determines if userid is authorized to enter command**
- **Sign on and userid validation and verification are recommended**
- **May be performed by multiple facilities**
  - Default security (the default)
  - SMU or RACF
    - Note: SMU supports commands issued from static terminals and Type1 automated operator programs
  - Command Authorization Exit Routine (DFSCCMD0)
  - Combination of the above facilities
- **Source terminal used to enter command affects authorization processing**
- **Commands processed in control region**

- **SECURITY macro specifications**
  - Commands entered from static terminals
    - PASSWD=, TERMNL=, TRANCMD=
    - TYPE=RACFCOM + ETO
- **IMS start up parameters**
  - Parameters request RACF
    - RCF=**S** | A (static and ETO)
    - RCF=**C** | Y (ETO only)
    - APPCSE=C | F (APPC devices)
    - OTMASE=C | F (OTMA clients)
    - AOIS=R | C | A (automated operator Type 2 applications)
    - CMDMCS=R | C | B (MCS/E-MCS consoles)
- **/NRE or /ERE COLDSYS restart command keywords**
    - CMDAUTH | CMDAUTHE (static and ETO | ETO only)
    - TRANCMDS (AO Type1)
    - PASSWORD (SMU password security)
    - TERMINAL (SMU LTERM security)

IMS Terminal Entered Commands



IMS

/CMD

Command authorization active?

NO

YES

Default Security

SMU Command Processor

RACF Interface

DFSCCMD0 Interface

Default security

SMU

RACF

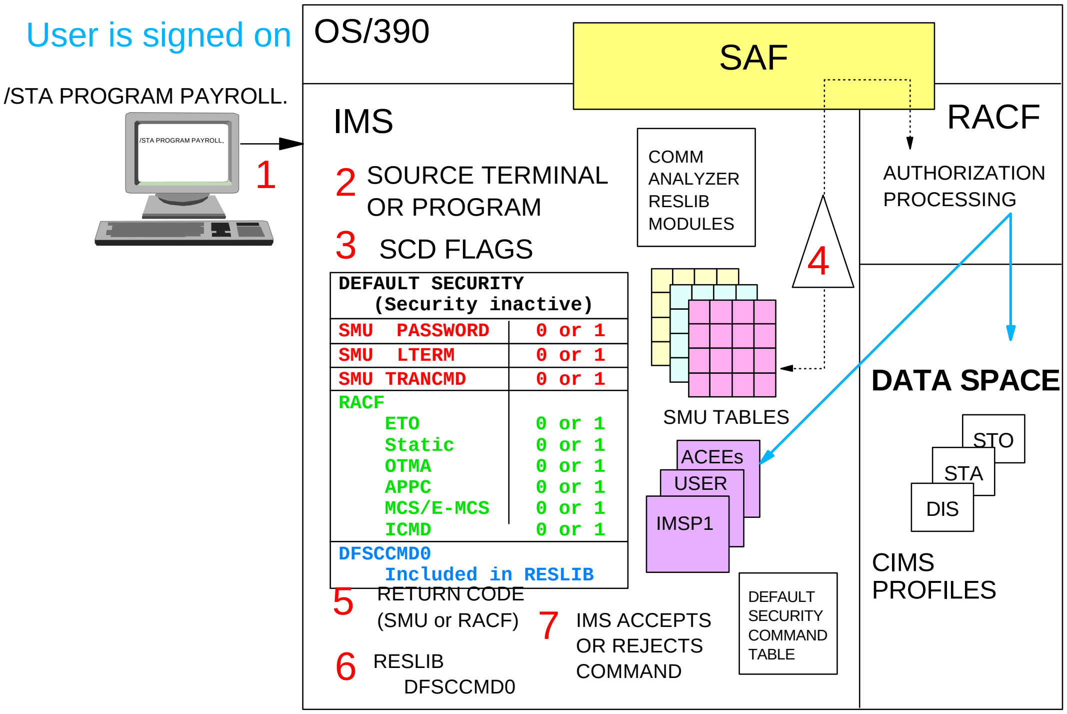
DFSCCMD0

DFS3649
DFS2470

Reject command

Process command

Command Security Overview



DEFAULT SECURITY (Security inactive)	
SMU PASSWORD	0 or 1
SMU LTERM	0 or 1
SMU TRANCMD	0 or 1
RACF	
ETO	0 or 1
Static	0 or 1
OTMA	0 or 1
APPC	0 or 1
MCS/E-MCS	0 or 1
ICMD	0 or 1
DFSCCMD0 Included in RESLIB	

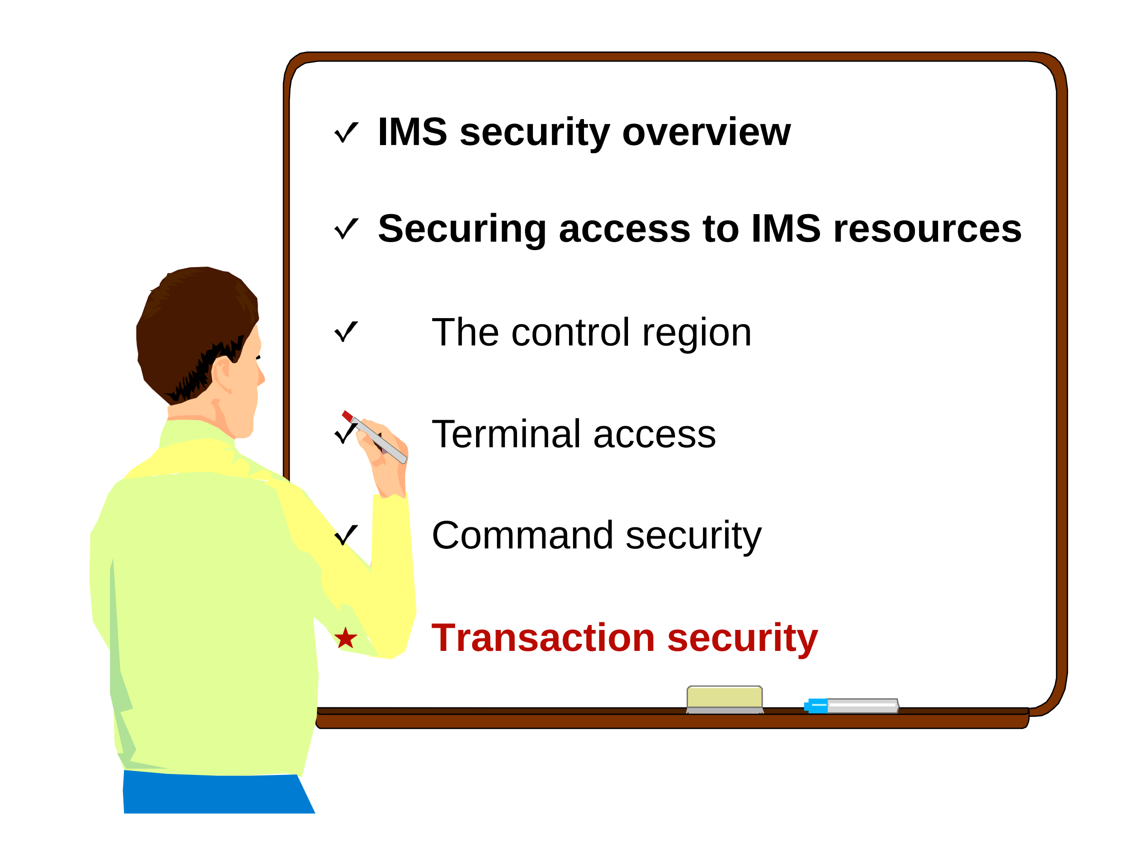
RACF Command Profile Examples

Sample RACF commands to secure the /OPN command; the group of commands /DIS, /STA, and /STO; the group of commands /ASS and /CHA; and all (*) commands.

```
RDEFINE CIMS OPN OWNER(IMSADMIN) UACC(NONE)
PERMIT OPN CLASS(CIMS) ID(GROUPX) ACCESS(READ)

RDEF DIMS IMSUSER ADDMEM(DIS STA STO) OWNER(IMSADMIN)  UACC(NONE)
PERMIT IMSUSER CLASS(DIMS) ID(GROUPY) ACCESS(READ)

RDEFINE DIMS AOCMDS ADDMEM(ASS CHA) OWNER(IMSADMIN) UACC(NONE)
PERMIT AOCMDS CLASS(DIMS) ID(T2AOPGM1 CICSAOR1 GROUPZ) ACCESS(READ)

RDEFINE CIMS * OWNER(IMSADMIN) UACC(NONE)
PERMIT * CLASS(CIMS) ID(TCOUSID GROUPX GROUPY GROUPZ)

RDEFINE CIMS STO OWNER(IMSADMIN) UACC(NONE)
PERMIT STO CLASS(CIMS) ID(DBAGROUP) ACCESS(READ)
RALTER CIMS STO APPLDATA('REVERIFY') UACC(NONE)
```

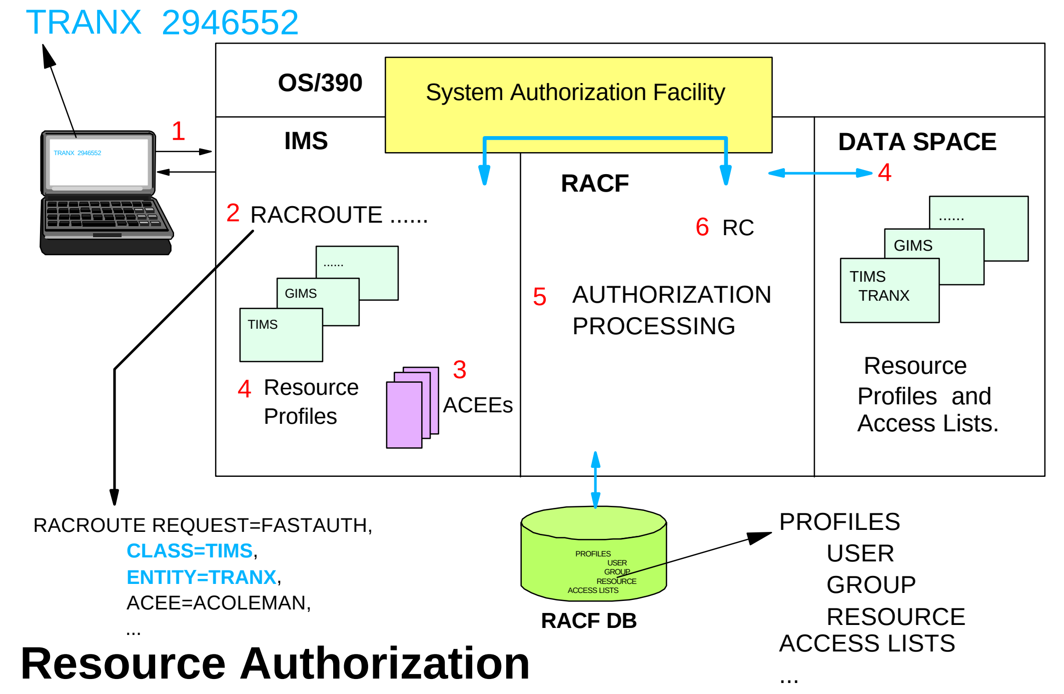
At terminal (cleared screen):
/STO(userpw) TRANSACTION PAYTRAN.

Otherwise DFS3662W RC=36 (no password)



- ✓ **IMS security overview**
- ✓ **Securing access to IMS resources**
- ✓ The control region
- ✓ Terminal access
- ✓ Command security
- ★ **Transaction security**

RACF Transaction Security Flow



TRANX 2946552

1

OS/390

System Authorization Facility

IMS

2 RACROUTE ......

......

GIMS

TIMS

4 Resource Profiles

3 ACEEs

RACF

6 RC

5 AUTHORIZATION PROCESSING

DATA SPACE

4

......

GIMS

TIMS TRANX

Resource Profiles and Access Lists.

```
RACROUTE REQUEST=FASTAUTH,
         CLASS=TIMS,
         ENTITY=TRANX,
         ACEE=ACOLEMAN,
         ...
```

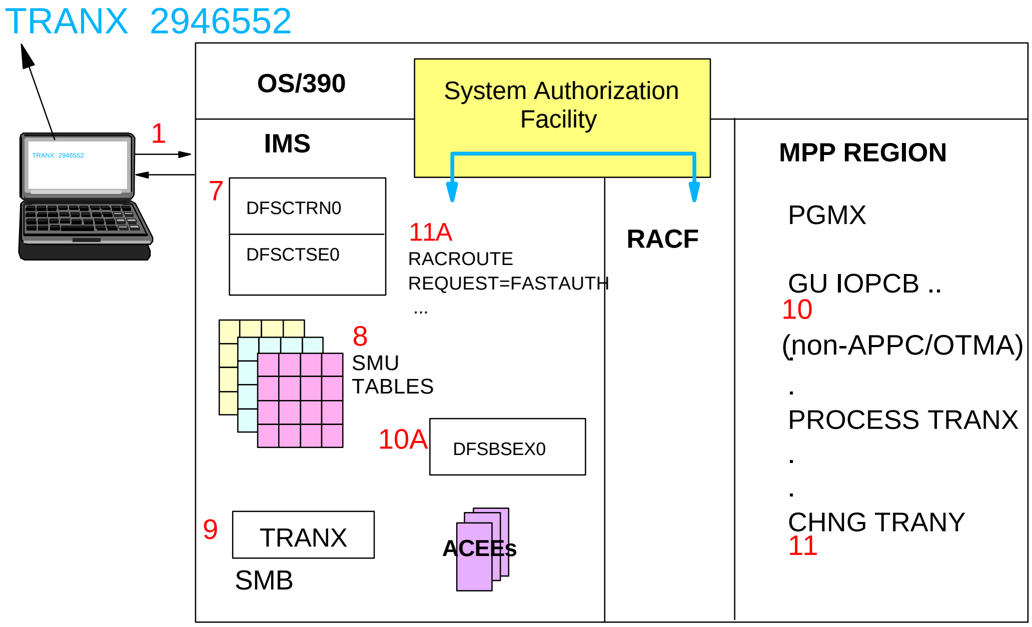
PROFILES USER GROUP RESOURCE ACCESS LISTS

RACF DB

PROFILES
USER
GROUP
RESOURCE
ACCESS LISTS
...

Resource Authorization Done After Sign On

RACF Transaction Security Flow ...



TRANX 2946552

1

OS/390

System Authorization Facility

IMS

7

DFSCTRN0

DFSCTSE0

11A

RACROUTE

REQUEST=FASTAUTH

...

RACF

MPP REGION

PGMX

GU IOPCB ..

10

(non-APPC/OTMA)

.

PROCESS TRANX

.

.

CHNG TRANY

11

8

SMU

TABLES

10A

DFSBSEX0

9

TRANX

SMB

ACEEs

Transaction Security

- **Determines if userid | group is authorized to enter transaction**
- **To be effective, sign on and userid validation/verification are recommended**
- **May be performed by multiple facilities**
  - SMU and RACF
  - RACF
  - Several exit routines may provide or affect transaction authorization
    - Transaction Authorization Exit (DFSCTRN0)
    - Security Reverification Exit (DFSCTSE0)
    - Build Security Environment (DFSBSEX0)
  - Combination of above facilities
- **Source terminal used for inputting transaction affects authorization processing**
- **Default - no transaction authorization checking**
- **If transaction authorization security is active**
  - IMS requires transaction authorization check at these times
    - Before placing transaction on scheduler message block (SMB)
    - /CHNG call
    - /AUTH call
    - ISRT SPA for conversational transaction (deferred conversational program-to-program switch)
    - When these commands contain a transaction name
    - /SET, /LOCK, and /UNLOCK

RACF Transaction Authorization

- **Can secure all transactions, regardless of source**
  - Static and ETO terminals, APPC, OTMA, ...
  - Password reverification (optional)
- **Uses TIMS | GIMS resource classes**
  - Existence of transaction profile forces user sign on
    - Transaction authorization active in IMS
- **Program-to-program switches secured by *userid***
- **Security level set for each transaction**
  - UACC(NONE) or UACC(READ)
- **Each user | group may be assigned different access level**
  - ID(GROUPX) ACCESS(NONE)
  - ID(GROUPY) ACCESS(READ)
    - Highest level required for transaction authorization

Activating Transaction Authorization

SECURITY MACRO	PASSWD=YES | FORCE
	TERMNL=YES | FORCE
	TRANCMD=YES | FORCE

	RCLASS=IMS
	SECLVL=(TRANAUTH,SIGNON)
	SECLVL=(TRANAUTH,FORCSIGN)
	SECLVL=(FORCTRAN,FORCSIGN)
	TYPE=(RACFAGN | AGNEXIT,RACFTERM,TRANEXIT,)

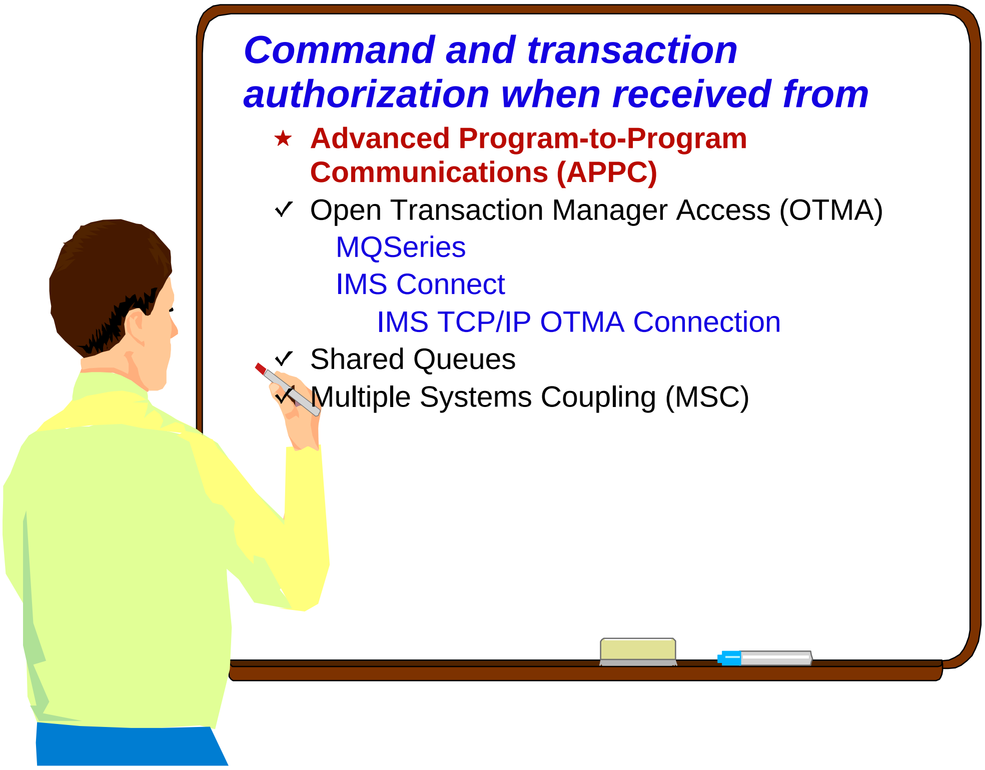
STARTUP PARAMETERS	RCF=T | Y | A
	RVFY=Y
	TRN=Y | F
	ISIS=1 | 2
	APPCSE=F | C | P
	OTMASE=F | C | P

/NRE or /ERE COLDSYS	TRANAUTH
IMS SYSTEM	CHNG CALL (TO A MODIFIABLE PCB) AUTH CALL ISRT (DEFERRED CONVERSATION PGM-TO-PGM SWITCH) /SET, /LOCK, and /UNLOCK (TRANSACTION NAME)

RACF Transaction Authorization Examples

Sample RACF commands to secure IMS transactions and authorize groups of users. 'REVERIFY' requires user to reenter user password with transaction input.

```
RDEFINE TIMS DEBSTRNX OWNER(IMSADMIN) UACC(NONE)
PERMIT DEBSTRNX CLASS(TIMS) ID(GROUPX) ACCESS(READ)

RDEFINE GIMS IMSTRANS OWNER(IMSADMIN) UACC(NONE)
RALTER GIMS IMSTRANS ADDMEM(DEBSTRN1,PART,ADDTRAN)
PERMIT IMSTRANS CLASS(GIMS)  ID(GROUPY) ACCESS(READ)

RDEFINE TIMS DEBSTRN2 OWNER (IMSADMIN) UACC(NONE)
    APPLDATA('REVERIFY') ⬅
PERMIT DEBSTRN2 CLASS(TIMS) ID(GROUPZ) ACCESS(READ)

RDEFINE TIMS CDEBSTRN OWNER(IMSADMIN) UACC(NONE)
RALTER TIMS CDEBSTRN APPLDATA('REVERIFY')
PERMIT CDEBSTRN CLASS(TIMS) ID(GROUP1) ACCESS(READ)
```

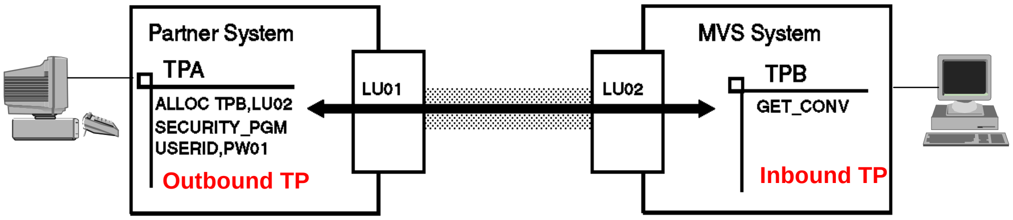


Command and transaction authorization when received from

- ★ **Advanced Program-to-Program Communications (APPC)**
- ✓ Open Transaction Manager Access (OTMA)
  - MQSeries
  - IMS Connect
    - IMS TCP/IP OTMA Connection
- ✓ Shared Queues
- ✓ Multiple Systems Coupling (MSC)

APPC Transaction Authorization

- **APPC/IMS interface may be *secured at several levels***
  - APPC/VTAM
    - Session level security
    - LU to LU security
  - APPC/MVS
    - Conversation level security
  - APPC/IMS
    - Command and transaction security



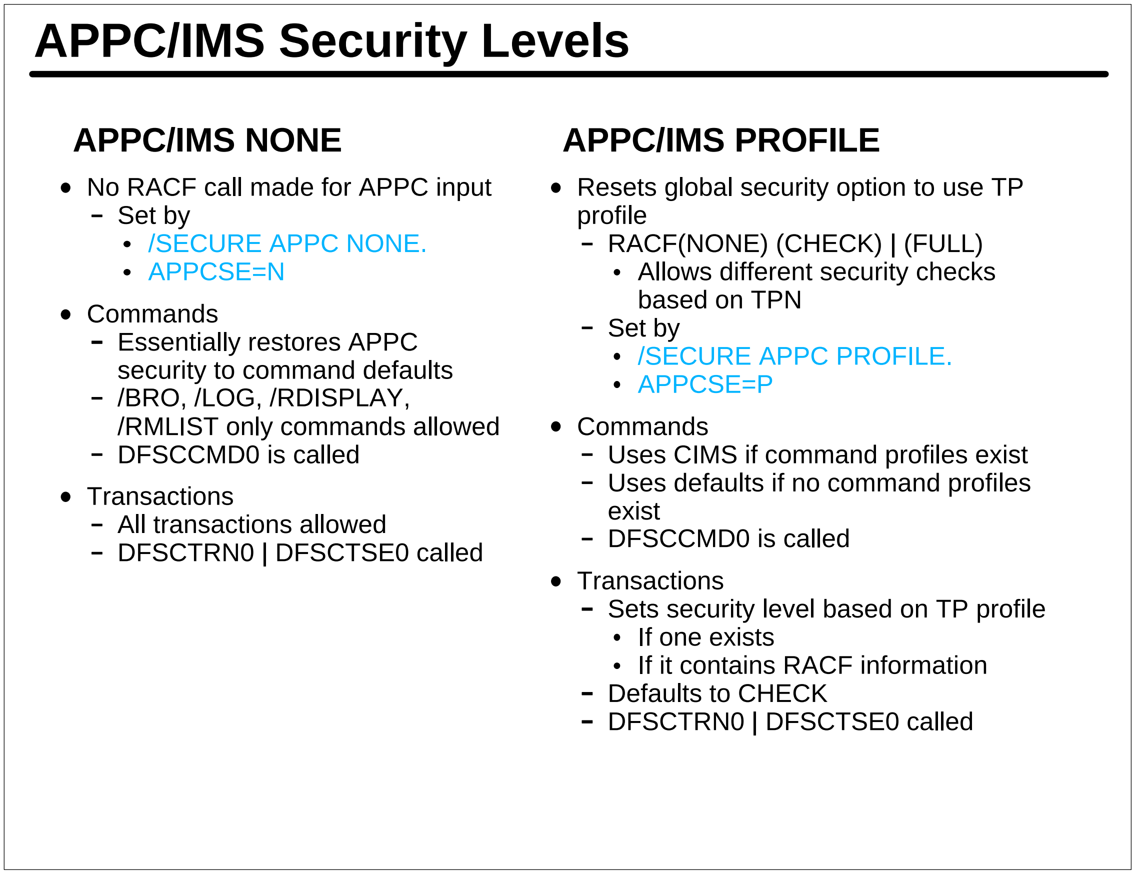
FMH-5

...	INDICATORS AV | PV | SOR | SOF	...	TPNAME	ACCESS SECURITY LENGTH (Binary) OR X'00' IF NO FIELDS	SECURITY ACCESS SUBFIELDS (OPTIONAL) GROUP | PASSWORD | USERID	**SECURITY DATA**

APPC/IMS Transaction Authorization

- **IMS-wide security level set by**
  - APPCSE= startup parameter specification
    - APPCSE=N | P | C | *F*
  - /SECURE APPC command
    - /SECURE APPC NONE | PROFILE | CHECK | *FULL*
    - Overrides APPCSE= specification
- **IMS commands**
  - Processed against CIMS | DIMS
  - DFSCCMD0 called
- **IMS transactions**
  - Processed against TIMS | GIMS
  - DFSCTRN0 called and Security Reverification Exit Routine (DFSCTSE0) called for CHNG and AUTH calls

- ***/SECURE APPC command***
  - Overrides
    - APPCSE= startup specification
    - RACF value in TP profile when /SECURE APPC PROFILE is ***not*** the IMS-wide APPC security level
  - Valid in DB/DC and DCCTL environments
  - Logged to secondary master
  - Security level shown on /DIS APPC command



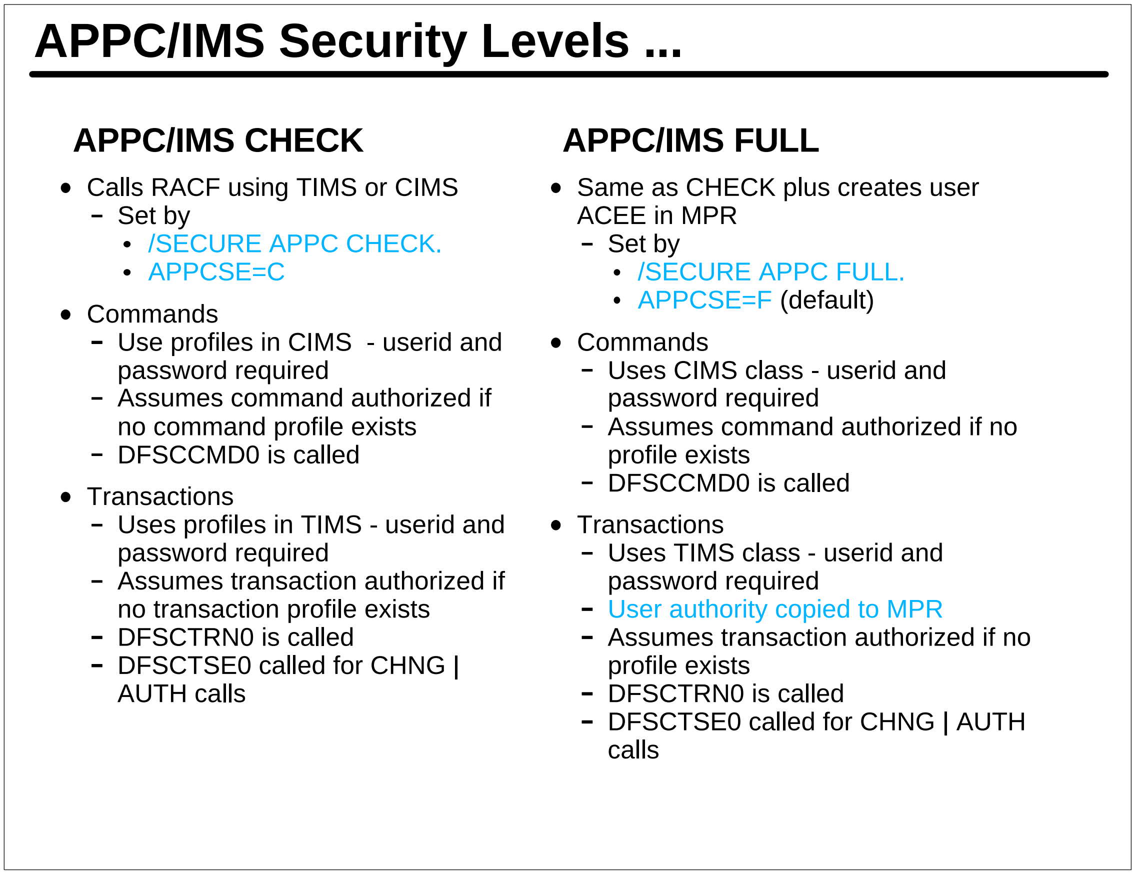
APPC/IMS Security Levels

APPC/IMS NONE

- No RACF call made for APPC input
  - Set by
    - /SECURE APPC NONE.
    - APPCSE=N
- Commands
  - Essentially restores APPC security to command defaults
  - /BRO, /LOG, /RDISPLAY, /RMLIST only commands allowed
  - DFSCCMD0 is called
- Transactions
  - All transactions allowed
  - DFSCTRN0 | DFSCTSE0 called

APPC/IMS PROFILE

- Resets global security option to use TP profile
  - RACF(NONE) (CHECK) | (FULL)
    - Allows different security checks based on TPN
  - Set by
    - /SECURE APPC PROFILE.
    - APPCSE=P
- Commands
  - Uses CIMS if command profiles exist
  - Uses defaults if no command profiles exist
  - DFSCCMD0 is called
- Transactions
  - Sets security level based on TP profile
    - If one exists
    - If it contains RACF information
  - Defaults to CHECK
  - DFSCTRN0 | DFSCTSE0 called



APPC/IMS Security Levels ...

APPC/IMS CHECK

- Calls RACF using TIMS or CIMS
  - Set by
    - /SECURE APPC CHECK.
    - APPCSE=C
- Commands
  - Use profiles in CIMS - userid and password required
  - Assumes command authorized if no command profile exists
  - DFSCCMD0 is called
- Transactions
  - Uses profiles in TIMS - userid and password required
  - Assumes transaction authorized if no transaction profile exists
  - DFSCTRN0 is called
  - DFSCTSE0 called for CHNG | AUTH calls

APPC/IMS FULL

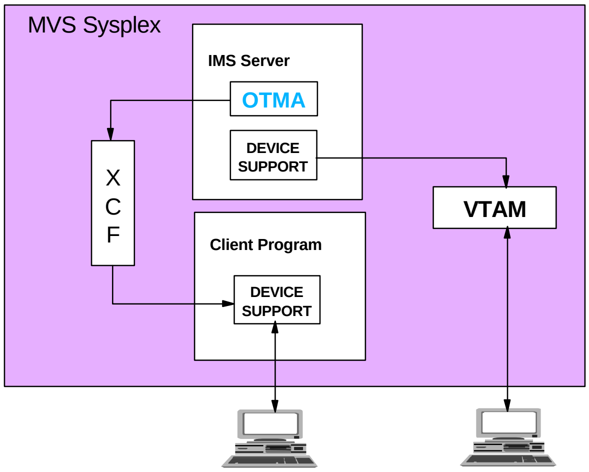
- Same as CHECK plus creates user ACEE in MPR
  - Set by
    - /SECURE APPC FULL.
    - APPCSE=F (default)
- Commands
  - Uses CIMS class - userid and password required
  - Assumes command authorized if no profile exists
  - DFSCCMD0 is called
- Transactions
  - Uses TIMS class - userid and password required
  - User authority copied to MPR
  - Assumes transaction authorized if no profile exists
  - DFSCTRN0 is called
  - DFSCTSE0 called for CHNG | AUTH calls

Command and transaction authorization when received from

- ✓ Advanced Program-to-Program Communications (APPC)
- ★ **Open Transaction Manager Access (OTMA)**
  - MQSeries
  - IMS Connect
    - IMS TCP/IP OTMA Connection
- ✓ Shared Queues
- ✓ Multiple Systems Coupling (MSC)

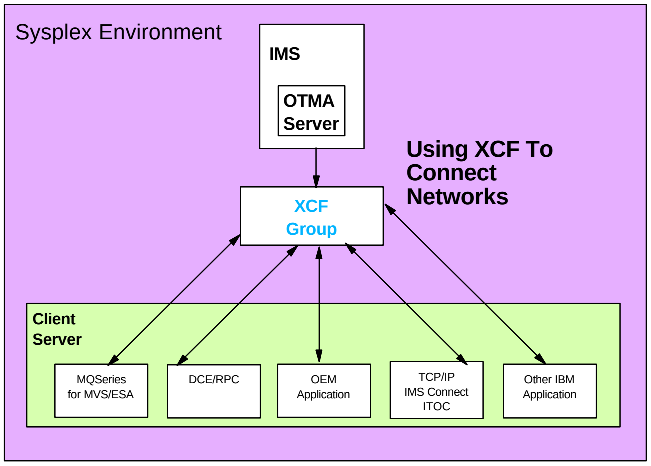
Open Transaction Manager Access (OTMA)

- **What is OTMA?**
  - High performance client-server protocol
    - Uses MVS Cross-System Coupling Facility (XCF) services
  - Allows MVS programs (clients) to access IMS applications



Accessing IMS From OTMA Clients

- **An OTMA client**
  - Is an MVS application program that
    - Sends IMS commands | transactions to IMS
    - Receives output
    - Must be a member of an ***XCF group*** and use the OTMA protocol
  - Gateway for transaction outside IMS to enter IMS

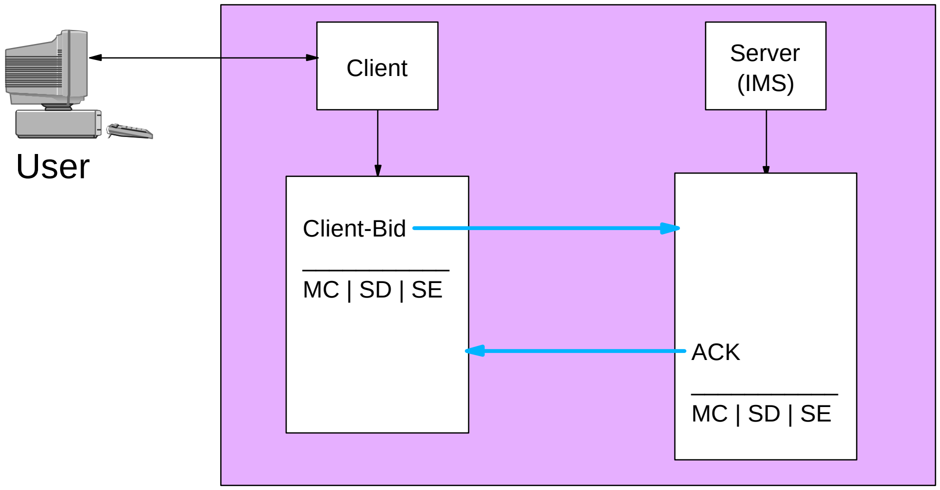


OTMA Security

- **OTMA security is optional**
  - May be performed by client (i.e. MQSeries, ITOC, etc.)
- **Uses RACF for IMS commands**
  - CIMS | DIMS classes
- **Uses RACF for IMS transactions**
  - TIMS | GIMS classes
- **Uses RACF to secure XCF groups**
  - FACILITY class
- **No SMU support**

- **OTMA Client Bid**
  - Request to connect to IMS
  - Bid request set in MCI of message prefix
- **Bid Includes**
  - Security level (flag) for message
    - N (for NONE)
      No RACF checking, assume userid/password already verified
    - C (for CHECK)
      RACF checks authorization
    - F (for FULL)
      RACF checks authorization and user's ACEE copied to MPR
  - UTOKEN (may have been authorized prior to IMS receipt)
  - Userid
  - SAF profile (RACF group name)
- **Security level in bid *ignored* if security level is**
  - /SECURE OTMA NONE or OTMASE=N

OTMA Client Bid ...



FLOW	SECTION	CONTENT OF PREFIX SECTION
Client-Bid	MC	...
	SD	...
	SE	SECURITY FLAG (N | C | F) UTOKEN USERID SAF PROFILE

Ignored if IMS security level is **NONE**

OTMA Security Levels

- **IMS-wide security level set by**
  - /SECURE OTMA command
    - NONE
    - PROFILE
    - CHECK
    - ***FULL*** (default)
  - APPCSE= startup parameter
    - N | P | C | ***F***
- **Commands**
  - Processed against CIMS | DIMS
  - DFSCCMD0 called
- **Transactions**
  - Processed against TIMS | GIMS
  - DFSCTRN0 called
  - DFSCTSE0 called for CHNG and AUTH calls

OTMA Security Levels ...

OTMA - NONE

- Set by
  - /SECURE OTMA NONE.
  - OTMASE=N
- Commands
  - Essentially restores OTMA security to defaults
  - /BRO, /LOCK, /LOG, /RDISPLAY, /UNLOCK commands only
  - DFSCCMD0 is called
- Transactions
  - All transactions allowed
  - DFSCTRN0 | DFSCTSE0 called

OTMA - PROFILE

- Set by
  - /SECURE OTMA PROFILE.
  - OTMASE=P
- Commands
  - Uses CIMS | DIMS if command profiles exist
  - Uses default security if no command profiles exist
  - DFSCCMD0 is called
- Transactions
  - Set by SECURITY DATA section of Client-Bid
  - NONE, CHECK, FULL
  - If not specified, defaults to CHECK
  - Uses TIMS | GIMS for CHECK and FULL
  - DFSCTRN0 | DFSCTSE0 called

OTMA Security Levels ...

OTMA - CHECK

- Set by
  - /SECURE OTMA CHECK.
  - OTMASE=C
- Commands
  - Use profiles in CIMS | DIMS
    - Userid and password required
  - Assumes command authorized if no command profile exists
  - DFSCCMD0 is called
- Transactions
  - Uses profiles in TIMS | GIMS
    - Userid and password required
  - Assumes transaction authorized if no transaction profile exists
  - DFSCTRN0 | DFSCTSE0 called

OTMA - FULL

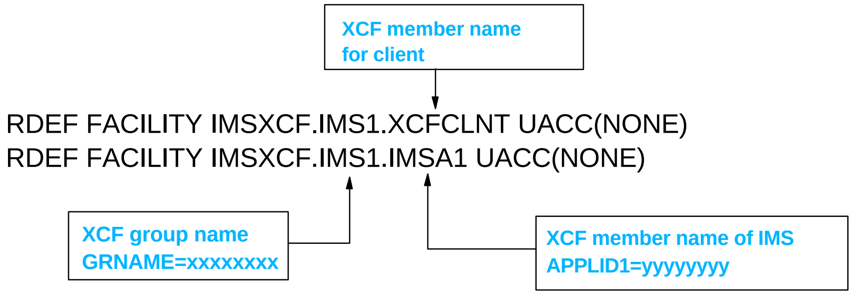
- Set by
  - /SECURE OTMA FULL.
  - OTMASE=F
  - Default level at startup

- Commands
  - Uses CIMS | DIMS classes
    - Userid and password required
  - Assumes command authorized if no profile exists
  - DFSCCMD0 is called

- Transactions
  - Uses TIMS | GIMS classes
    - Userid and password required
  - User authority copied to MPR
  - Assumes transaction authorized if no profile exists
  - DFSCTRN0 | DFSCTSE0 called

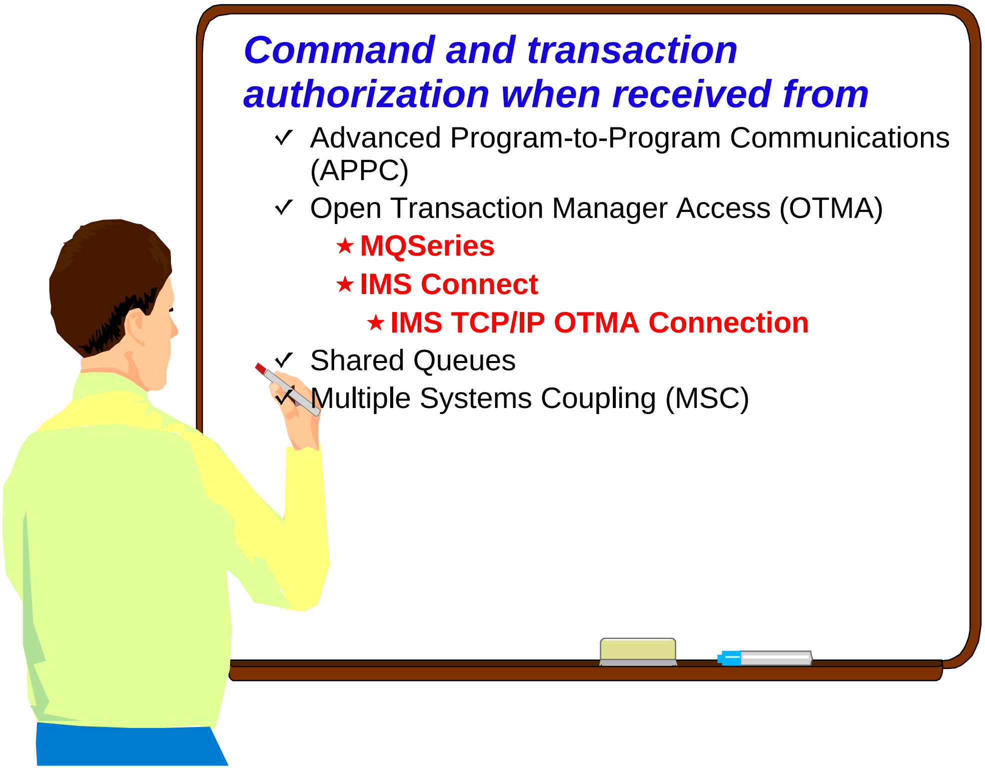
OTMA - XCF Profiles

- **OTMA XCF groups**
  - Protected in FACILITY class of RACF
- **Profile format:**
  - IMSXCF.groupname.membername
  - Client should have at least READ access
  - Client bid not allowed if profile does not exist


XCF member name for client
XCF group name GRNAME=xxxxxxxx
XCF member name of IMS APPLID1=yyyyyyyy

```
RDEF FACILITY IMSXCF.IMS1.XCFCLNT UACC(NONE)
RDEF FACILITY IMSXCF.IMS1.IMSA1 UACC(NONE)
```

```
PE IMSXCF.IMS1.XCFCLNT CLASS(FACILITY) ID(CLIENTID) ACCESS(READ)
PE IMSXCF.IMS1.IMSA1 CLASS(FACILITY) ID(CLIENTID) ACCESS(READ)
```



Command and transaction authorization when received from

- ✓ Advanced Program-to-Program Communications (APPC)
- ✓ Open Transaction Manager Access (OTMA)
  - ★ **MQSeries**
  - ★ **IMS Connect**
    - ★ **IMS TCP/IP OTMA Connection**
- ✓ Shared Queues
- ✓ Multiple Systems Coupling (MSC)

OTMA Clients

- **Join the same XCF group as IMS**
- **Client message contains security information**
  - Userid
  - Password or PassTicket
  - Group (optional)
  - ...

FLOW	SECTION	CONTENT OF PREFIX SECTION
Client-Bid	MC	...
	SD	...
	SE	SECURITY FLAG (N | C | F) UTOKEN USERID SAF PROFILE

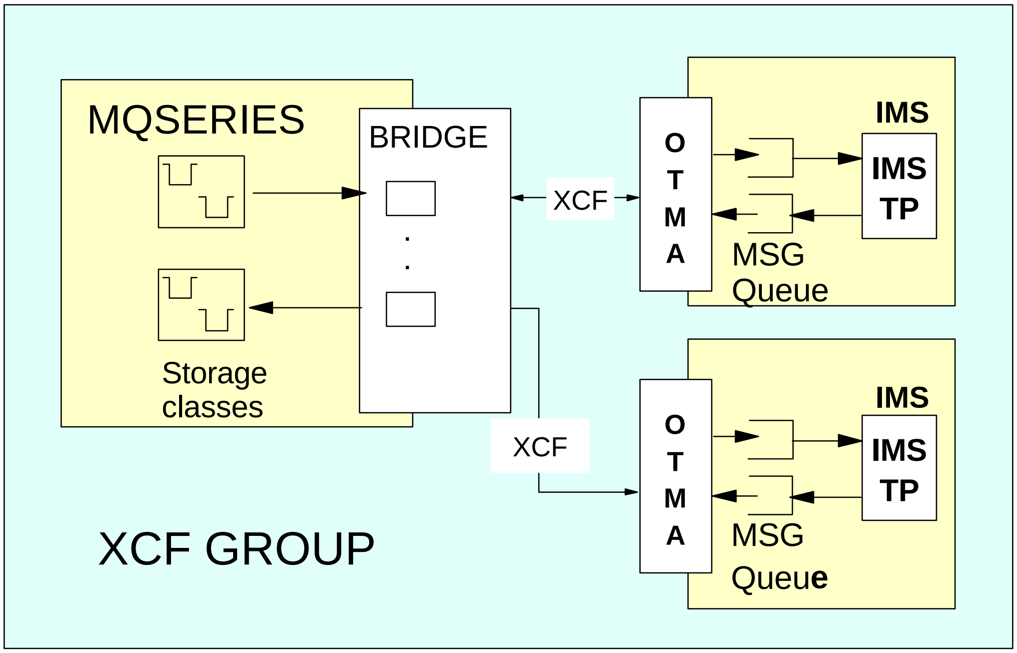
Ignored if IMS security level is **NONE**

- **IMS calls RACF to verify security information**
  - Security environment (ACEE) created for RACF defined/verified users
- **Resource authorization processing same as usual**

OTMA Clients ...

- **MQSeries**
  - Allows OS/390 applications to use message queuing to participate in message driven processing
  - Implement common API
  - Message Queue Interface (MQI)
  - MQSeries-IMS Bridge
    - Component of MQSeries for OS/390
    - Allows access from MQSeries applications to IMS
- **IMS Connect**
  - Replacement for IMS TCP/IP OTMA Connection (ITOC)
- **IMS TCP/IP OTMA Connection (ITOC)**
  - TCP/IP server
    - Provides communications linkages between TCP/IP clients and IMS datastore
  - Enables TCP/IP clients to exchange messages with IMS OTMA

MQSeries



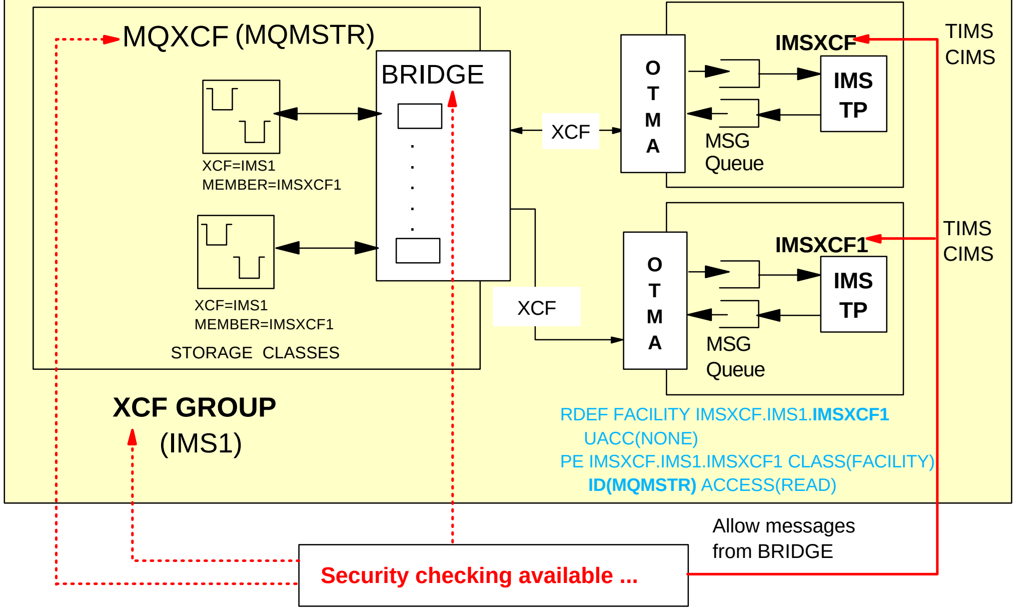
MQSeries ...

Connect to
XCF group

Allow messages
from BRIDGE

```
RDEFINE FACILITY IMSXCF.IMS1.MQXCF
   UACC(NONE)
PE IMSXCF.IMS1.MQXCF CLASS(FACILITY)
  ID(MQMSTR) ACCESS(READ)
```

```
RDEF FACILITY IMSXCF.IMS1.IMSXCF
   UACC(NONE)
PE IMSXCF.IMS1.IMSXCF CLASS(FACILITY)
   ID(MQMSTR) ACCESS(READ)
```

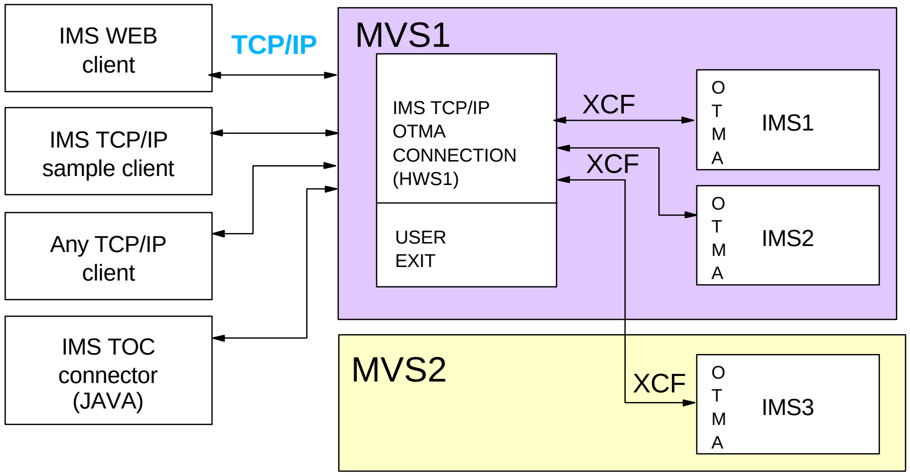


```
RDEF FACILITY IMSXCF.IMS1.IMSXCF1
   UACC(NONE)
PE IMSXCF.IMS1.IMSXCF1 CLASS(FACILITY)
   ID(MQMSTR) ACCESS(READ)
```

Allow messages
from BRIDGE

IMS Connect / IMS TOC (ITOC)

- **IMS Connect**
  - Replacement for IMS TCP/IP OTMA Connection



IMS Connect / IMS TOC (ITOC) ...

- **Runtime libraries must be APF authorized**

- **MVS PPT must allow ITOC to use**
  - Supervisor state
  - Key 7 storage

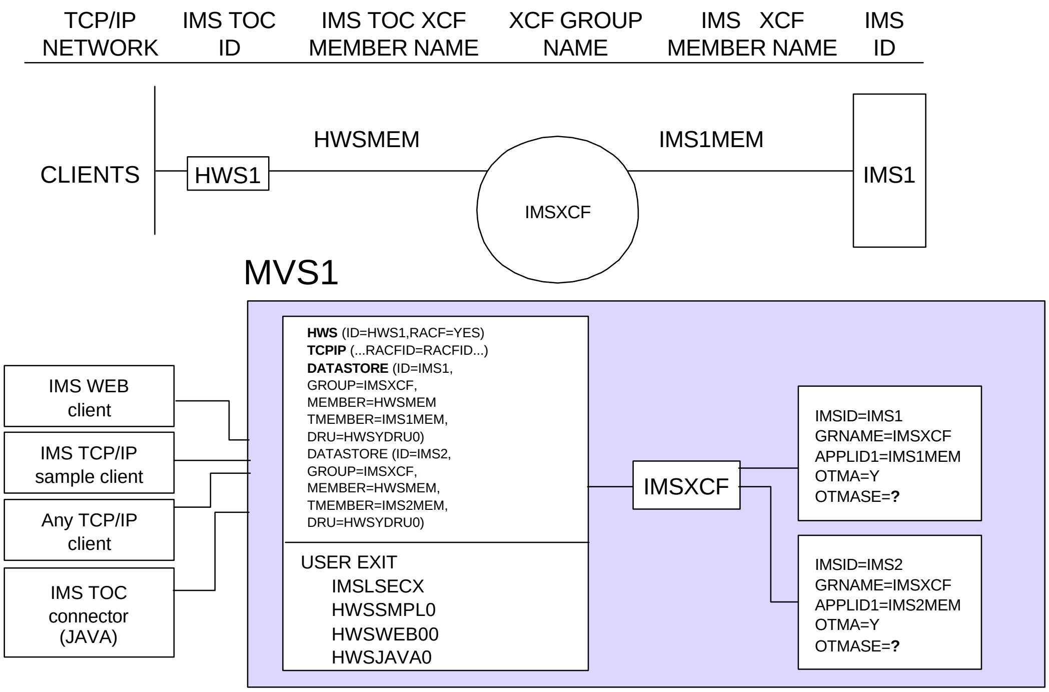
- **Connects to IMS as OTMA client**

- **ITOC can perform RACF user/password verification**
  - RACF=Y/N in HWSCFG configuration file

- **Userid originates from:**
  - Client - passed in message prefix data
  - User exit AFTER the ITOC receives the input message

IMS Connect / IMS TOC (ITOC) ...

Simple Example



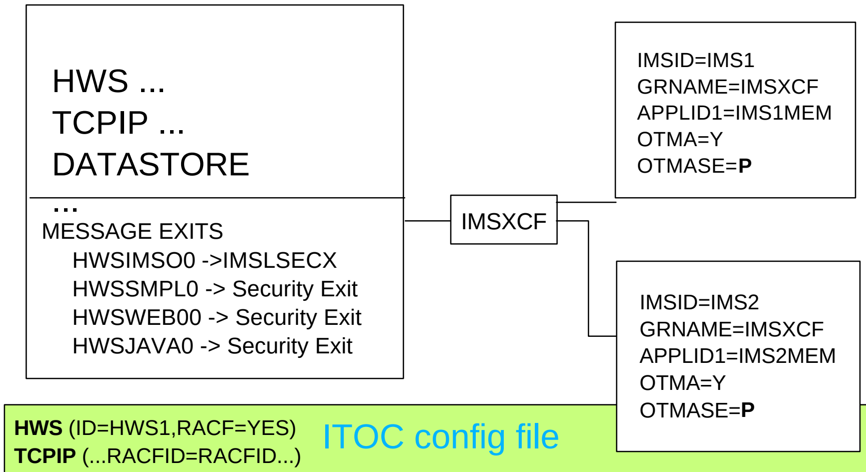
```
HWS (ID=HWS1,RACF=YES)
TCPIP (...RACFID=RACFID...)
DATASTORE (ID=IMS1,
GROUP=IMSXCF,
MEMBER=HWSMEM
TMEMBER=IMS1MEM,
DRU=HWSYDRU0)
DATASTORE (ID=IMS2,
GROUP=IMSXCF,
MEMBER=HWSMEM,
TMEMBER=IMS2MEM,
DRU=HWSYDRU0)
```

```
USER EXIT
    IMSLSECX
    HWSSMPL0
    HWSWEB00
    HWSJAVA0
```

```
IMSID=IMS1
GRNAME=IMSXCF
APPLID1=IMS1MEM
OTMA=Y
OTMASE=?
```

```
IMSID=IMS2
GRNAME=IMSXCF
APPLID1=IMS2MEM
OTMA=Y
OTMASE=?
```

IMS Connect / IMS TOC (ITOC) ...



```
HWS ...
TCPIP ...
DATASTORE
...
MESSAGE EXITS
    HWSIMSO0 ->IMSLSECX
    HWSSMPL0 -> Security Exit
    HWSWEB00 -> Security Exit
    HWSJAVA0 -> Security Exit
```

```
IMSID=IMS1
GRNAME=IMSXCF
APPLID1=IMS1MEM
OTMA=Y
OTMASE=P
```

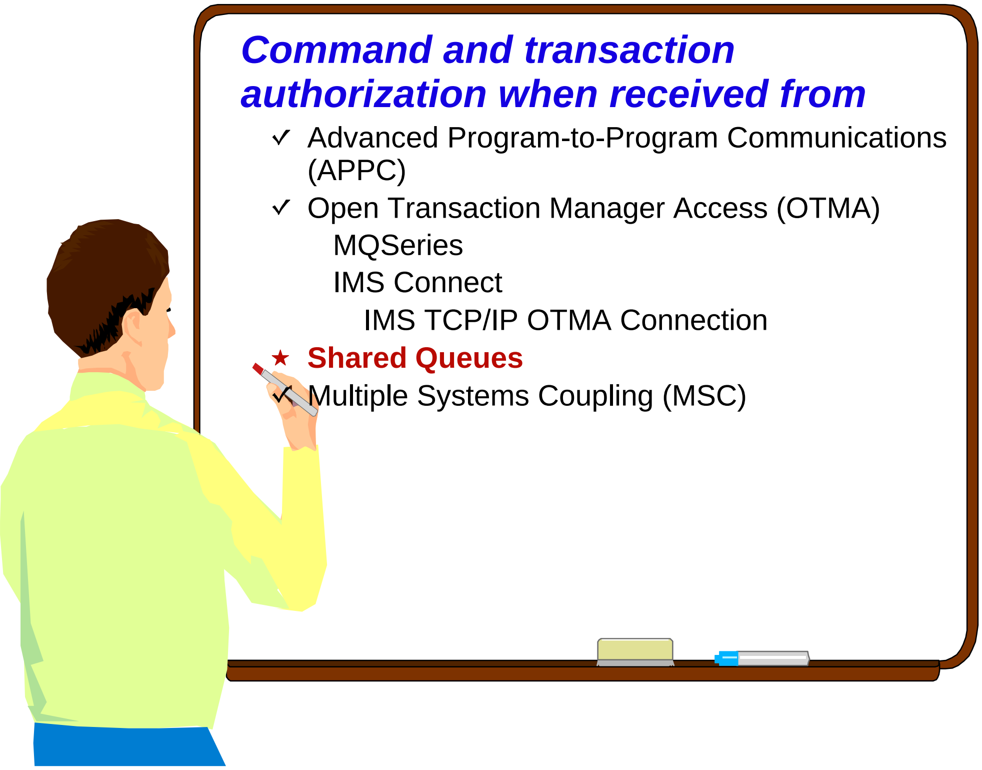
```
IMSID=IMS2
GRNAME=IMSXCF
APPLID1=IMS2MEM
OTMA=Y
OTMASE=P
```

ITOC config file

```
HWS (ID=HWS1,RACF=YES)
TCPIP (...RACFID=RACFID...)
DATASTORE (ID=IMS1,GROUP=IMSXCF,MEMBER=HWSMEM,TMEMBER=IMS1MEM,DRU=HWSYDRU0)
DATASTORE (ID=IMS2,GROUP=IMSXCF,MEMBER=HWSMEM,TMEMBER=IMS2MEM,DRU=HWSYDRU0)
...
```

MVS PPT

```
PPT PGMNAME(HWSHWS00)     /* PROGRAM NAME = HWSHWS00          *
           KEY(7)              /* PROTECT KEY ASSIGNED IS 7        */
           PASS                /* CANNOT BYPASS PASSWORD PROTECTION */
           SYST                /* PROGRAM IS A SYSTEM TASK         */
           .
           .
```

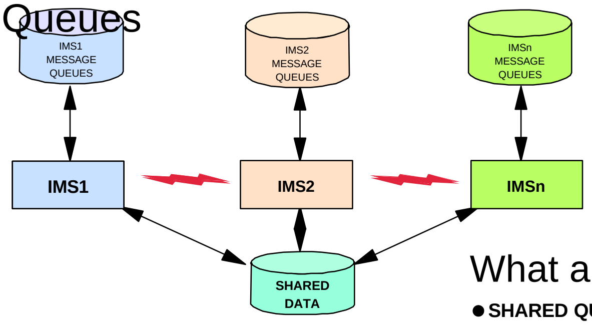


Command and transaction authorization when received from

- ✓ Advanced Program-to-Program Communications (APPC)
- ✓ Open Transaction Manager Access (OTMA)
  - MQSeries
  - IMS Connect
    - IMS TCP/IP OTMA Connection
- ★ **Shared Queues**
- ✓ Multiple Systems Coupling (MSC)

Shared Queues

IMS - Without Shared Queues



IMS1 MESSAGE QUEUES

IMS2 MESSAGE QUEUES

IMSn MESSAGE QUEUES

IMS1

IMS2

IMSn

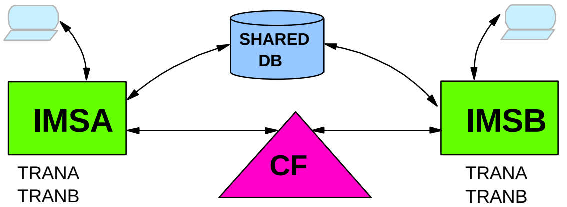
SHARED DATA

IMSs could share the data, but each IMS had ***exclusive*** use of its own message queues

What are Shared Queues?

- **SHARED QUEUES**
  - SHARED MESSAGE QUEUES
  - SHARED EMH QUEUES

PROVIDES APPLICATION WORKLOAD BALANCING



SHARED DB

IMSA

CF

IMSB

TRANA
TRANB

LTERM1
LTERM2

SHARED MESSAGE QUEUES
SHARED EMH QUEUES

TRANA
TRANB

LTERM1
LTERM2

RACF Security Considerations

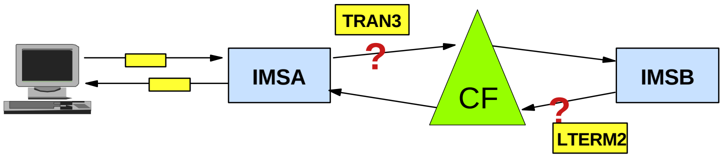
- **Support for RACF transaction authorization for *dynamic transactions***
  - Resources do not have to be statically defined
    - IMS systems in shared queues group can share RACF database
  - IMSA can call RACF to perform transaction for TRAN3 when entered from terminal attached to IMSA
    - Even when TRAN3 not defined to IMSA
- **If RACF database not shared by IMS systems in shared queues group**
  - **RACF definitions (profiles) should be synchronized to achieve same results on security checking on all IMS systems in the shared queues group**
    - Regardless of IMS system that makes security check

IMSA

TRANSACT	TRAN1
TRANSACT	TRAN2
NAME	LTRM1
NAME	LTRM2

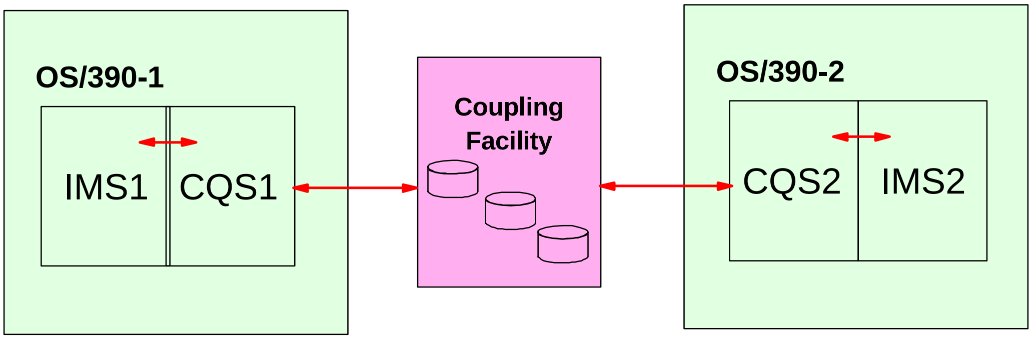
IMSB

TRANSACT	TRAN1
TRANSACT	TRAN3
NAME	LTRM1
NAME	LTRM3



Shared Queues Security

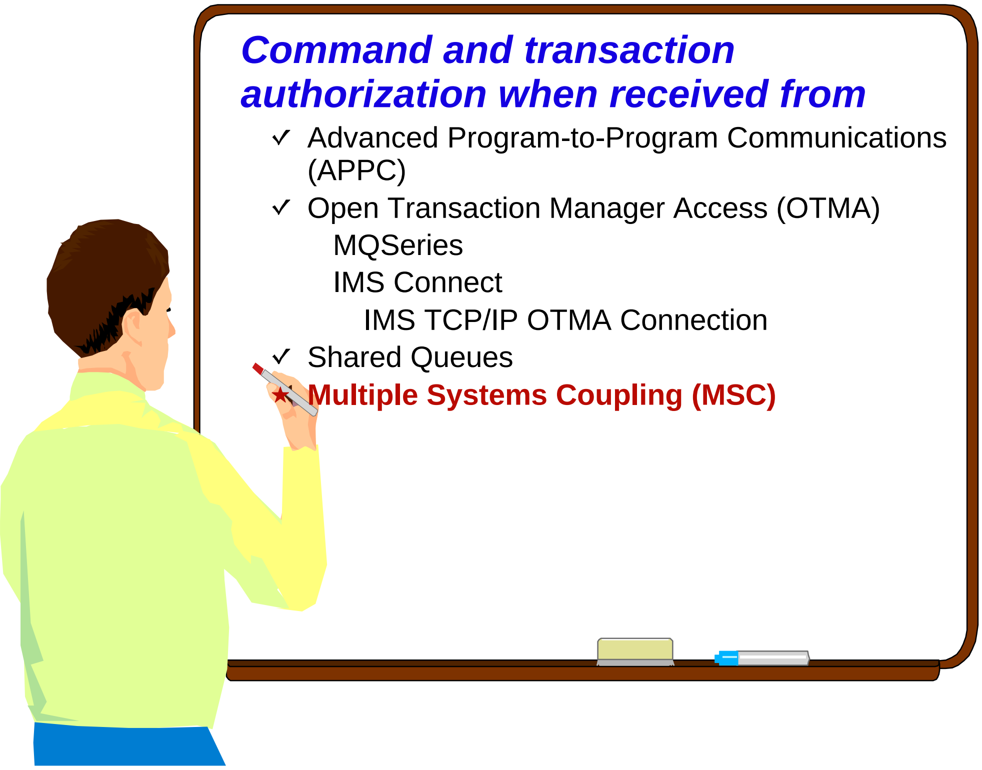
- **XCF profiles**
  - Secure connections to CQS
  - Uses FACILITY class



```
RDEF FACILITY CQSSTR.IMS_MSGQ1 UACC(NONE)
PE CQSSTR.IMS_MSGQ1 CLASS(FACILITY) ID(IMS1 IMS2) ACCESS(UPDATE)

RDEFINE FACILITY IXLSTR.IMS_MSGQ1 UACC(NONE)
PERMIT IXLSTR.IMS_MSGQ1 CLASS(FACILITY) ID(IMS1 IMS2) ACCESS(UPDATE)
```

Shared Queues Security Considerations

- **Some exits coded to use CTB address to find ACEE**
  - Command Authorization Exit Routine (DFSCCMD0)
  - Transaction Authorization Exit Routine (DFSCTRN0)
  - Security Reverification Exit Routine (DFSCTSE0)
- **In shared queues environments**
  - CTB address contains zeroes in back-end systems
- **Exits using CTB address may have to be changed**
  - To work in a manner that ***does not*** require CTB to get to ACEE
    - Such as, RACROUTE REQUEST=EXTRACT macro
  - To work regardless if shared queues are used or not
    - Some installations run shared queues and non-shared queues environments
- **IMS dynamically creates security environment in dependent region when CHNG or AUTH call issued from**
  - Back-end system
  - Front-end system where user has signed off
- **Dynamic creation of lots of ACEEs has performance implications**
- **Build Security Environment Exit Routine (DFSBSEX0)**
  - May be coded to allow
    - ***Bypass*** of dynamic creation of ACEE in dependent region for CHNG and AUTH calls
    - ***Bypass*** some part of the security checking process



Command and transaction authorization when received from

✓ Advanced Program-to-Program Communications (APPC)

✓ Open Transaction Manager Access (OTMA)

MQSeries

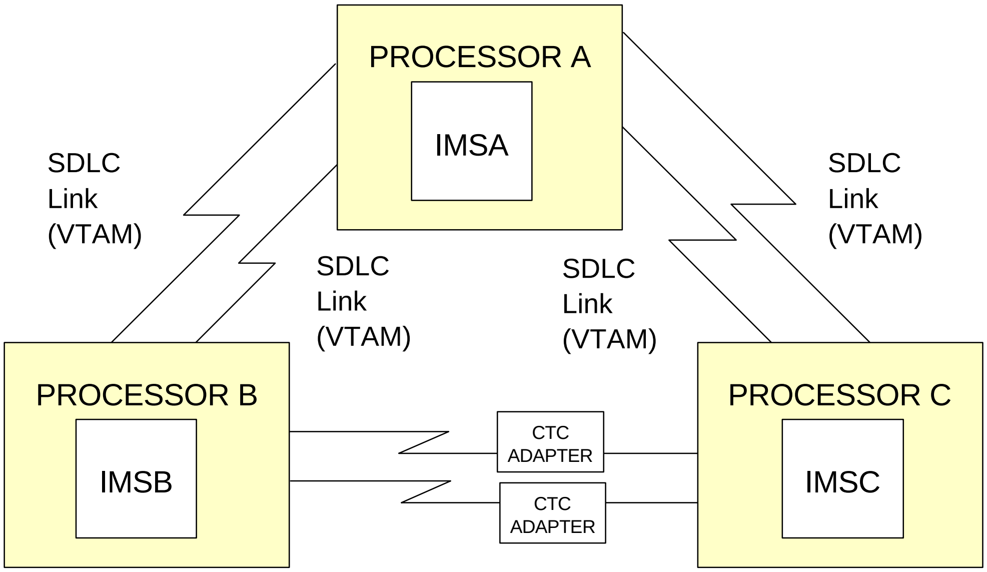
IMS Connect

IMS TCP/IP OTMA Connection

✓ Shared Queues

★ **Multiple Systems Coupling (MSC)**

Multiple Systems Coupling



MSC Security

- **Transaction authorization may be performed by**
  - RACF
    - Userid based transaction authorization
  - SMU
    - LTERM based (logical link path name) transaction authorization
  - User Exit Routines
    - Transaction Authorization Exit Routine (DFSCTRN0)
    - Security Reverification Exit Routine (DFSCTSE0)
    - Build Security Environment Exit Routine (DFSBSEX0)

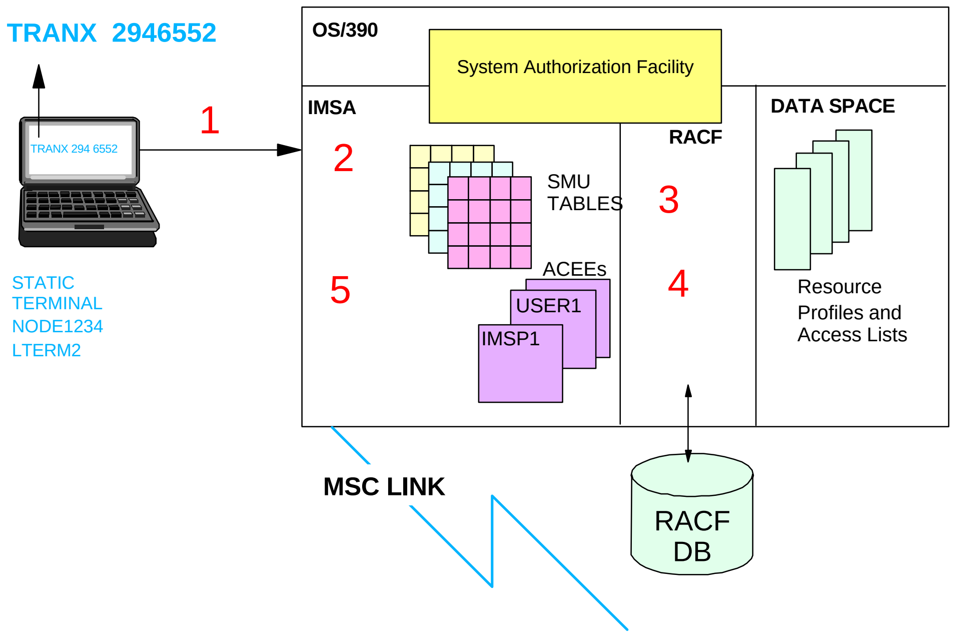
- **Inputting (source) system**
  - Perform transaction authorization on inputting system
    - Transaction is statically defined as 'remote' transaction
  - Security facilities to perform transaction authorization
    - RACF
    - TIMS and GIMS
    - SMU
    - TERMINAL security using LTERM-based transaction authorization
    - Transaction Authorization Exit Routine (DFSCTRN0)
    - Build Security Environment Exit Routine (DFSBSEX0)
    - Useful when sign on is not performed
    - Can build security environment (ACEE)

Implementing Security For MSC Systems

- **Destination system**
  - Security check performed for CHNG and AUTH calls issued in back-end system
    - RACF
    - SMU
    - Transaction Authorization Exit Routine (DFSCTRN0)
    - Security Reverification Exit Routine (DFSCTSE0)
- **Other security option is**
  - SMU LTERM based transaction authorization
    - Use logical link path (MSNAME) in lieu of LTERM name
- **Important note**
  - RACF profiles should be kept synchronized on inputting and destination systems to avoid RACF authorization processing issues

- **MSC security checking illustration**
- **ASSUMPTIONS:**
  - **(USER1 has previously performed sign on : /SIGN ON USER1 PW1**
    - SGN=Y | F (Sign on security is active)
    - TRN=Y | F (Transaction authorization is active)
  - RCF=T | Y | A (RACF is called to perform sign on security checking and transaction security checking
  - SMU PASSWORD and TERMINAL (STERM and LTERM) security checking are active
  - DFSCTRN0 and DFSCTSE0 have been included in the system
  - IMS V6.1 and RACF 2.1 (or higher)

MSC Security Checking Illustration ...



TRANX 2946552

TRANX 294 6552

STATIC TERMINAL
NODE1234
LTERM2

1

OS/390

System Authorization Facility

IMSA

2

SMU TABLES

5

ACEEs

USER1

IMSP1

RACF

3

4

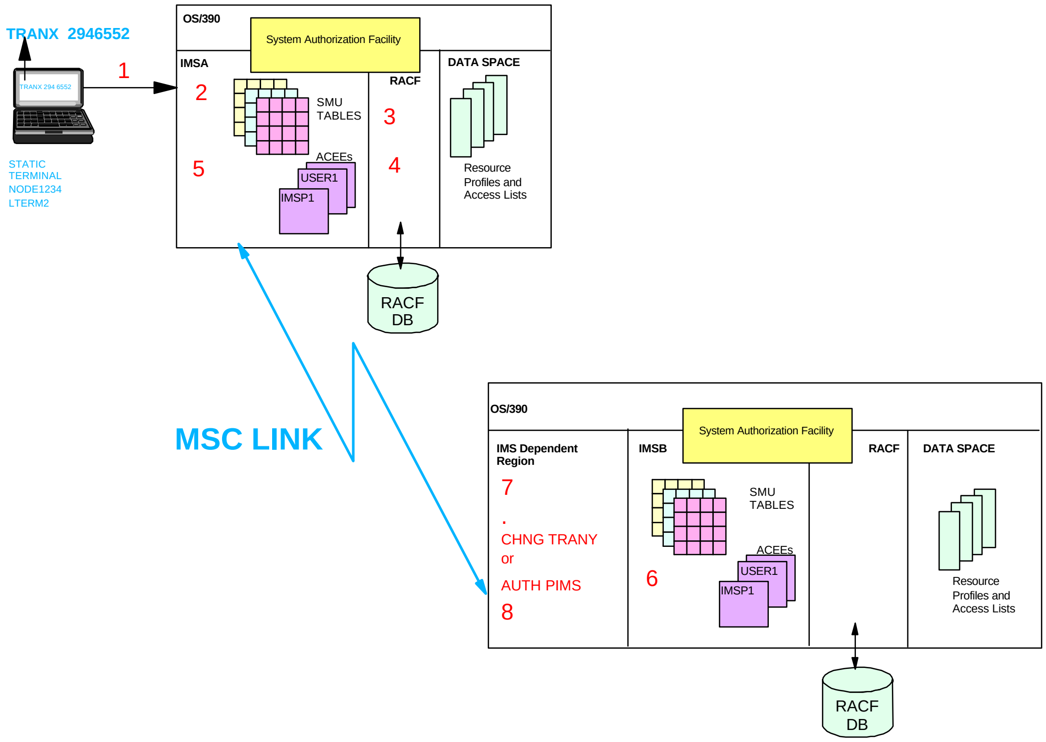
DATA SPACE

Resource Profiles and Access Lists

MSC LINK

RACF DB

MSC Security Checking Illustration ...



Summary

Summary

- **IMS Security: DB/DC Environments**
  - The control region
    - RACF APPL class
  - Terminal access
    - RACF TERMINAL | GTERMINL classes
    - Sign on security using SMU and RACF
  - Command security
    - Source of command
      - SMU

        Static and CMD call
      - RACF

        Static | ETO | APPC | OTMA | ICMD call | MCS/E-MCS
      - Command Authorization Exit Routine (DFSCCMD0)
    - Default security
      - IMS commands

Summary

- **IMS Security: DB/DC Environments**
  - Transaction security
    - Source of transaction
      - SMU

        Static
      - RACF

        Static | ETO | APPC | OTMA | dynamic transactions for shared queues
      - Transaction Authorization Exit Routine (DFSCTRN0)
      - Security Reverification Exit Routine (DFSCTSE0)

        CHNG call, AUTH call, and deferred pgm-to-pgm switch
      - Build Security Environment Exit Routine (DFSBSEX0)

        Control dynamic build of security environment (ACEE) for non-signed on user

RETURN TO INDEX