Security Consideration For Accessing APPC/IMS and IMS/OTMA

A50

Alonia (Lonnie) Coleman
acoleman@us.ibm.com

Miami Beach, FL October 22-25, 2001

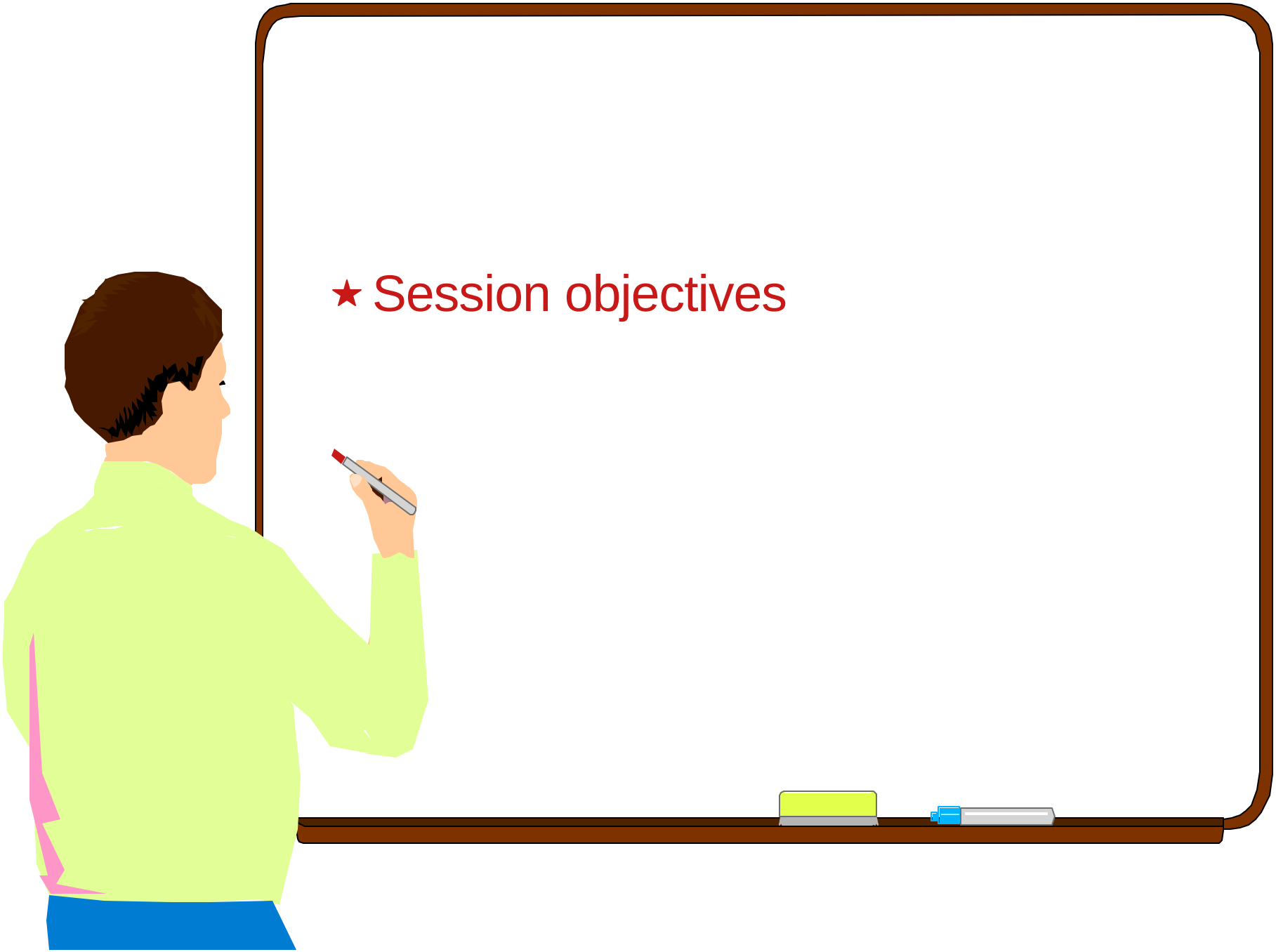
RETURN TO INDEX

Agenda

- **Session objectives**
- **Advanced Program-To-Program Communications (APPC)**
  - APPC overview
  - APPC security options
  - APPC/IMS security levels
    - NONE | PROFILE | CHECK | FULL
  - Allocate Program Specification Block/System Authorization Facility (APSB/SAF) security
- **IMS Connect**
  - IMS Connect overview
  - IMS Connect security

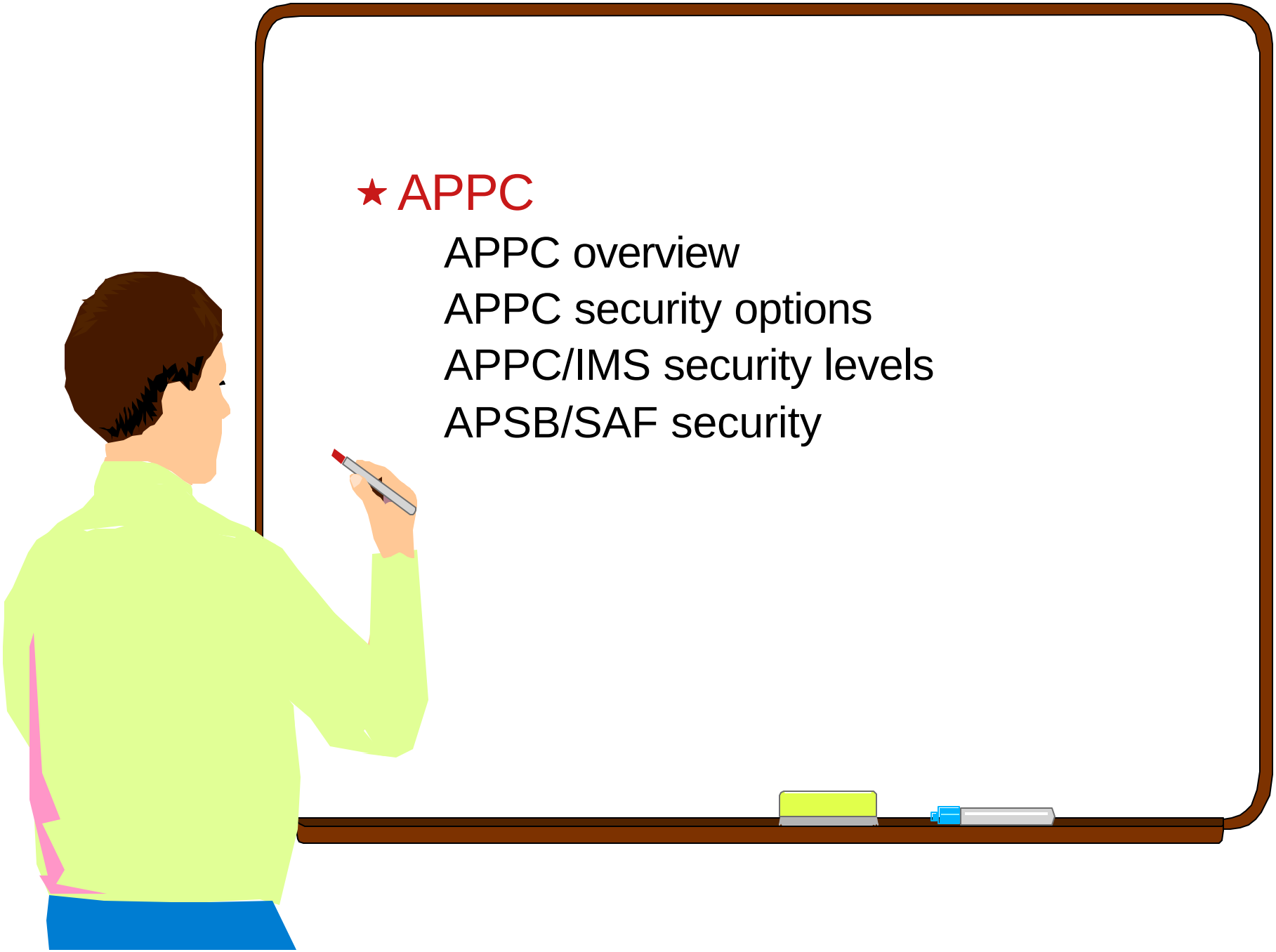
Agenda ...

- **MQSeries for OS/390**
  - MQSeries for OS/390 overview
  - MQSeries-IMS Bridge application security
- **Open Transaction Manager Access (OTMA)**
  - OTMA Security Levels
    - NONE | PROFILE | CHECK | FULL
- **Summary**

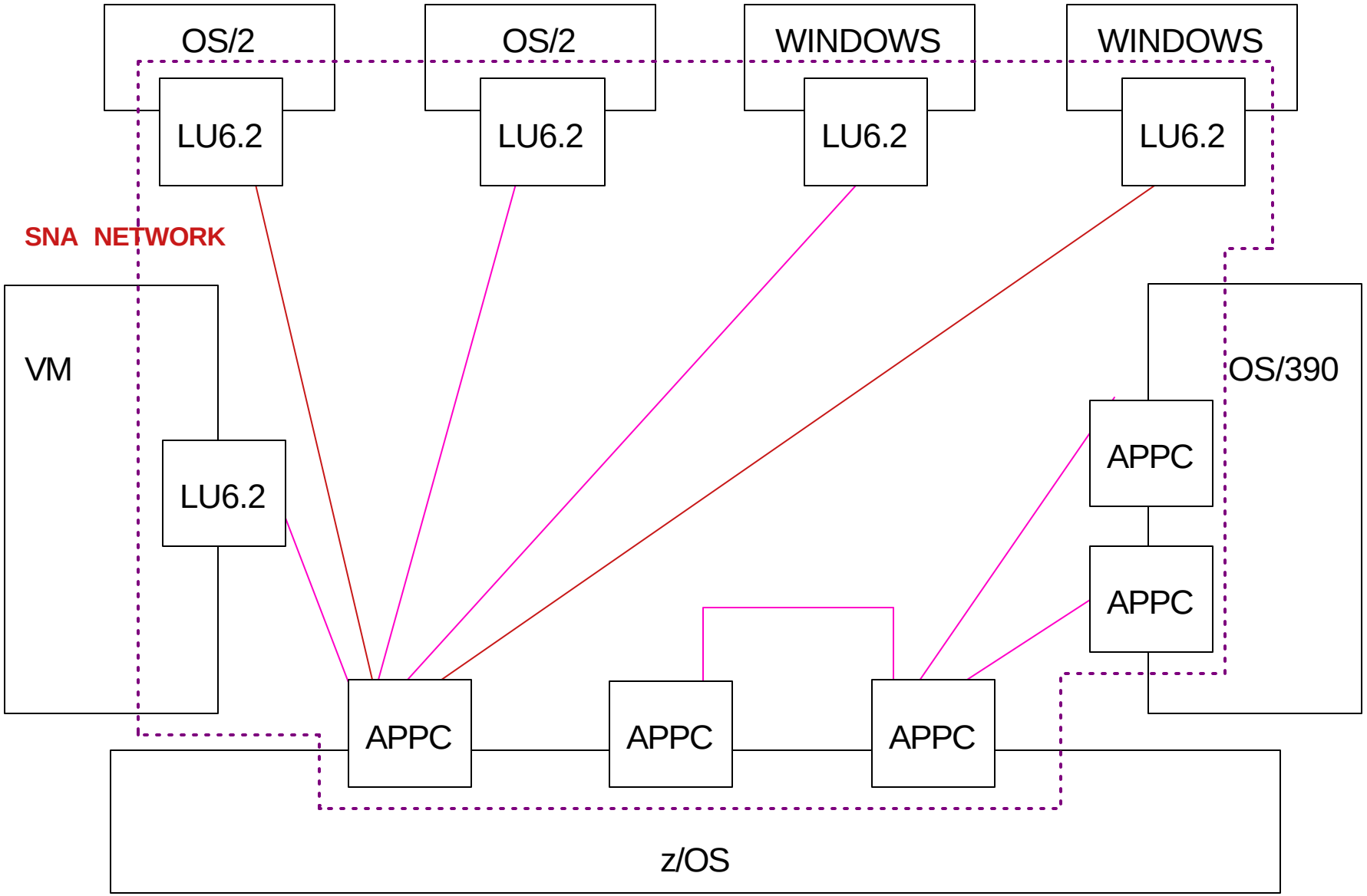

★ Session objectives

Session Objectives

- **Provide a technical overview of security for IMS resources accessed via**
  - APPC/IMS
  - IMS/OTMA clients
    - IMS Connect
    - MQSeries-IMS Bridge application
- **Provide examples of RACF commands used to secure access to IMS resources accessed from**
  - APPC environments
  - OTMA clients


★ APPC
APPC overview
APPC security options
APPC/IMS security levels
APSB/SAF security

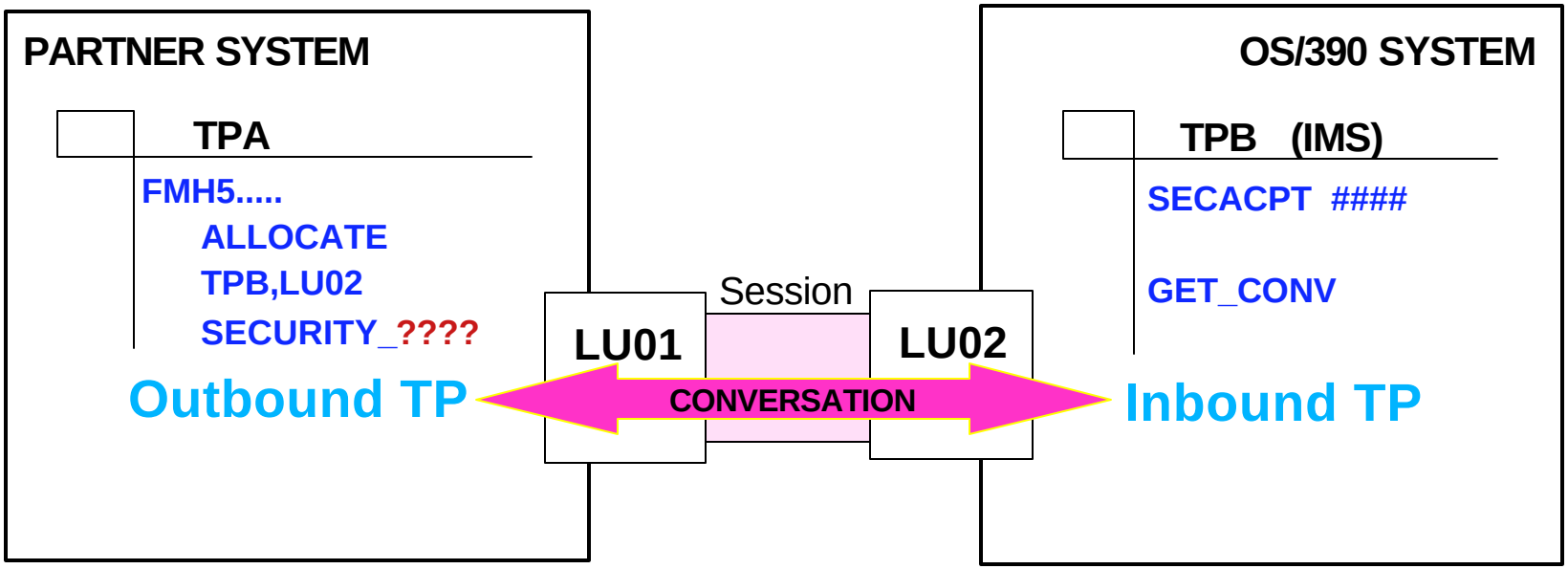
APPC Overview



APPC/MVS Logical Unit (LU)

- **APPC LU is defined to VTAM**
  - VTAM APPL definition statement in SYS1.VTAMLST
- **VTAM APPL statement**
  - Names MVS LU
  - Identifies LU as type LU 6.2
  - ***Defines security for the LU***
- **One APPC LU attempts to allocate conversation with another APPC LU**
  - APPC security may be controlled by
    - **APPC/VTAM**
    - **APPC/MVS**
    - **APPC/IMS**

APPC Conversations



Where **????** (security_type) is either:

NONE	No userid / no password
SAME	Userid only for already_verified Userid/password for 1st AVPV
PGM	Userid and password

Where #### is either:

NONE	Userid/password not allowed
CONV	Userid/password required
ALREADYV	Userid and (password -or- AV indicator)
PERSISTV	Userid, PV indicator, and ((password with sign-on-bit) or (signed-on-from bit))
AVPV	AV indicator and ((password with sign-on bit) or (signed-on from bit))

APPC Security Options

- **Accessing IMS From APPC Environments**
  - APPC/IMS interface may be ***secured at several levels***
    - APPC/VTAM
      - Session level security for ability of LUs to BIND in a session
    - APPC/MVS
      - Conversation level security for ability of LUs to establish a conversation on the session
    - APPC/IMS
      - Command and transaction security for ability of user to execute IMS command or transaction
- **Additional documentation for MVS and VTAM**
  - OS/390 MVS Planning: APPC/MVS Management
  - MVS/ESA Initialization and Tuning Reference
  - RACF Security Administrator's Guide & RACF System Programmer's Guide
  - VTAM Guide to Programming for LU 6.2

VTAM Security Options

- **Session-level LU-to-LU verification**
  - Protects logical units (LUs)
    - VTAM APPL statement security keywords
      - **VERIFY**

        NONE | OPTIONAL | REQUIRED
      - **SECLVL**

        ADAPT | LEVEL1 | LEVEL2
    - RACF **APPCLU** resource class
- **Control use of VTAM ACB for IMS**
  - RACF **VTAMAPPL** resource class
- **Encryption of data**

MVS Security Options

- **To protect conversations**
  - Can define conversation security levels that sessions allow
    - VTAM APPL statement **SECACPT** keyword specification
    - APPCLU SESSION**(CONVSEC(xxxxxxxx))**
      - Where xxxxxxxx is NONE | CONV | ALREADYV | PERSISTV | AVPV
  - Ability to control user access
    - To LUs using the RACF **APPL** resource class
    - From LUs using the RACF **APPCPORT** resource class
    - To TP profiles using the RACF **APPCTP**
    - To side information file using the **APPCSI** resource class
- **Can limit administrators who can define TPs to MVS**
- **Can control ability to collect API trace data**
  - RACF **FACILITY** resource class
- **Can minimize flow of passwords across network**
  - **Persistent verification (PV)**

APPC/IMS Overview

- **Function**
  - Part of IMS Transaction Manager (TM)
    - Allows IMS applications to communicate with other APPC applications / LU 6.2 devices
- **Two flavors of APPC/IMS application programs**
  - Implicit
    - Application makes normal DL/I calls
    - APPC/IMS manages the conversation
    - Uses IMS-wide security level to control APPC entered commands and transactions
  - Explicit
    - Application running in dependent region issues APPC/MVS verbs directly
    - Uses APSB/SAF security to control allocating **CPI-C*** driven application programs

*CPIC - Common Programming Interface for Communications

Implicit APPC Model

RACF TIMS/GIMS used for transaction authorization

RACF CIMS|DIMS used for command authorization

APPC/IMS manages conversation

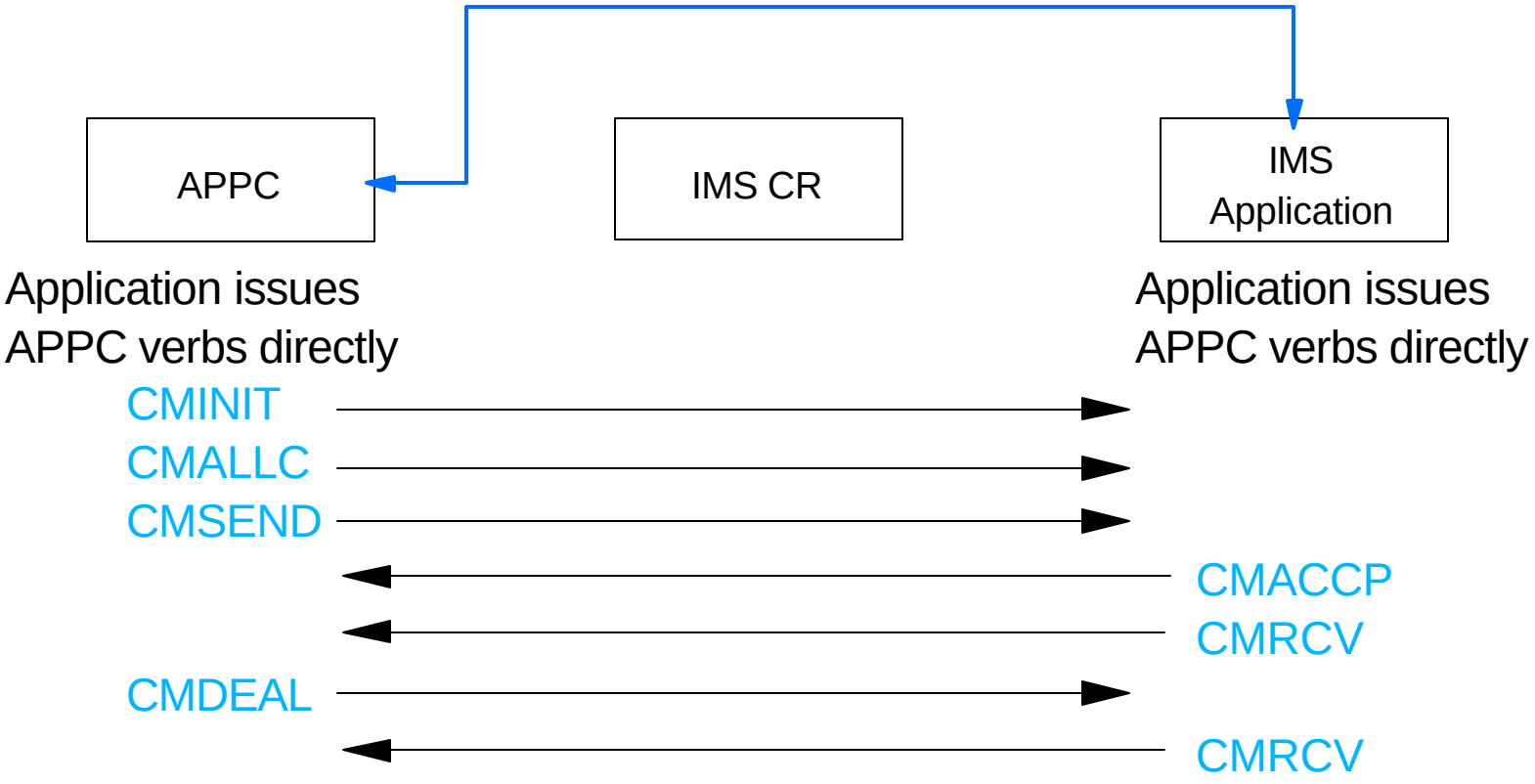
Application makes normal DL/I calls

APPCSE=**F** | C | P | N

/SEC APPC **FULL** | CHECK | PROFILE | NONE

Explicit APPC Model

RACF AIMS resource class used for
Allocate PSB / SAF (APSB/SAF) security



IMS Security Options

- **Ability to secure commands and transactions**
  - Commands
    - Default 'command' security
    - RACF CIMS | DIMS resource classes
    - Command Authorization Exit Routine (DFSCCMD0)
    - RACF and DFSCCMD0
  - Transactions
    - RACF TIMS | GIMS resource classes
    - Transaction Authorization Exit Routine (DFSCTRN0)
    - Security Reverification Exit Routine (DFSCTSE0)
    - RACF and DFSCTRN0
    - RACF, DFSCTRN0, and DFSCTSE0
- **CPIC driven applications**
  - Ability to allocate PSB secured using APSB/SAF security

APPC/IMS Security Levels

- **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
  - Command Authorization Exit (DFSCCMD0) called
- **IMS transactions**
  - Processed against TIMS | GIMS
  - Transaction Authorization Exit (DFSCTRN0) called
  - Security Reverification Exit (DFSCTSE0) called

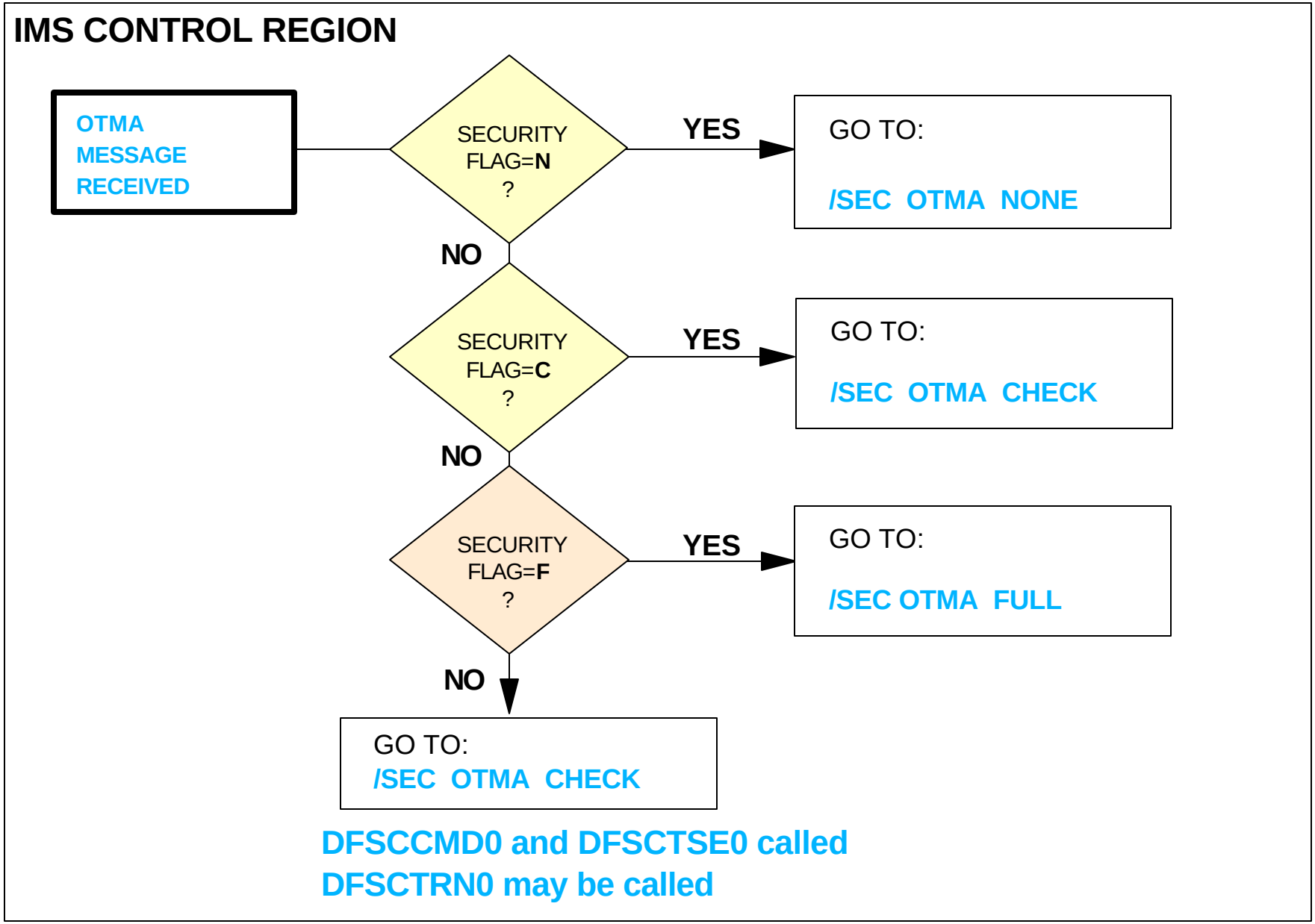
APPC/IMS NONE

- **No RACF call made for APPC input**
  - Set by
    - /SECURE APPC NONE or APPCSE=N
- **Commands**
  - Essentially restores APPC security to command defaults
  - /BRO, /LOG, /RDISPLAY, /RMLIST only commands allowed
  - Command Authorization Exit (DFSCCMD0) is called
- **Transactions**
  - All transactions allowed by RACF, which is not called
  - Transaction Authorization Exit (DFSCTRN0) is called
  - Security Reverification Exit (DFSCTSE0) is 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 or APPCSE=P
- **Commands**
  - Uses CIMS if command profiles exist
  - Uses default command security if command profile does not exist
  - Command Authorization Exit (DFSCCMD0) is called
- **Transactions**
  - Sets security level based on TP profile
    - If one exists and if it contains valid RACF information
      - Otherwise, defaults to CHECK
  - Transaction Authorization Exit (DFSCTRN0) may be called
  - Security Reverification Exit (DFSCTSE0) is called

/SECURE OTMA PROFILE Flow



APPC/IMS CHECK

- **Calls RACF using TIMS or CIMS**
  - Set by
    - /SECURE APPC CHECK or APPCSE=C
- **Commands**
  - Use profiles in CIMS
  - Assumes command authorized if no command profile exists
  - Command Authorization Exit (DFSCCMD0) is called
- **Transactions**
  - Uses profiles in TIMS
  - Assumes transaction authorized if no transaction profile exists
  - Transaction Authorization Exit (DFSCTRN0) may be called
  - Security Reverification Exit (DFSCTSE0) is called

APPC/IMS CHECK Considerations

- **ACEE is deleted after FASTAUTH processing has been completed**

- **When CHNG and/or AUTH calls issued with transaction code as destination**
  - RACF must be called again
    - Dynamically build ACEE
    - Perform FASTAUTH processing
    - Delete ACEE

- **Can cause large number of I/Os to RACF database**
  - Consider using: /SECURE APPC PROFILE
    or
    /SECURE APPC FULL

APPC/IMS FULL

- **Same as CHECK plus creates user ACEE in dependent region**
  - Set by
    - /SECURE APPC FULL APPCSE=F
      - **Default**
- **Commands**
  - Uses CIMS class
  - Assumes command authorized if no profile exists
  - Command Authorization Exit (DFSCCMD0) is called
- **Transactions**
  - Uses TIMS class
  - User authority copied to dependent region
  - Assumes transaction authorized if no profile exists
  - Transaction Authorization Exit (DFSCTRN0) may be called
  - Security Reverification Exit (DFSCTSE0) is called

APPC/IMS FULL Considerations

- **APPC/MVS associates dependent region ACEE with transaction authorization checking as a result of**
  - DL/I CHNG call
  - DL/I AUTH call
- **ACEE is built in dependent region**
  - Prior to message being passed to application
    - If application does not issue CHNG|AUTH call, building of ACEE resulted in unnecessary processing
      - Could impact performance to due to increased RACF I/O
- **With FULL**
  - Users ACEE exists in dependent region when CHNG | AUTH issued
    - Does not have to be dynamically built
    - Dynamic build of ACEE may have performance impact

APAR PQ47628

- ***Significantly*** **improves APPC/IMS - RACF performance**

- **Enhancement provides**
  - Transportable security environment
    - Allows a user's security environment (ACEE) to be
      - Easily retrieved
      - Transported to another address space
      - Transported to another system in a sysplex
  - RACROUTE REQUEST=VERIFY
    - Enhanced to use ***ENVR objects***
      - ENVRIN=
      - ENVROUT=
  - RACROUTE REQUEST=FASTAUTH
    - Enhanced to use ***ENVR objects***

APAR Impact on APPC/IMS Performance

- **IMS V6 (or higher) used with RACF V8 (or higher)**
  - Eliminates calls to RACF in APPC/IMS environments for
    - RACINIT
    - RACDELETE
  - FRACHECK done using object
- **Some customer results / experiences**
  - Takes significantly less time to perform APPC/IMS related security checking using RACF
    - Results may vary depending on customer environment

/SECURE Command

- **/SECURE APPC command**
  - Overrides
    - APPCSE= startup specification
    - RACF value in TP profile
      - When /SECURE APPC PROFILE is ***not*** the IMS APPC security level
  - Valid in DB/DC and DCCTL environments
  - Not recoverable over restart
  - Single segment command
  - Logged to secondary master

- **Security level in effect may be shown**
  - /DIS APPC command

Allocate PSB Call

- **Used to allocate PSB for CPI-C driven program**
  - PSB controls access to IMS databases and alternate PCBs
- **When APSB call issued from CPI-C driven program**
  - Can be rejected when AGN security is active
    - MPP region
      - APPC trancode not defined to IMS, thus trancode is not in AGN Table
- **APSB SAF security overrides AGN security**
  - Regardless of AGN= specification for region

APSB SAF Security

- **Activated by**
  - SECURITY TYPE=(RACFAGN,RACFTERM) or

    RCF≠N and ISIS=1
  - On a transaction by transaction basis
    - **RACF=FULL** (TP scheduler section of TP_Profile) ***and*** **/SECURE APPC PROFILE**
  - For all CPI-C driven transaction programs
    - **/SECURE APPC FULL**
  - Use of RACF AIMS Class
- **Deactivated by**
  - /SECURE APPC CHECK
  - /SECURE APPC NONE

APSB SAF Security ..

- **Secures PSB in RACF AIMS | Axxxxxxx Class**
  - Security check based on ***userid of end user*** who submitted CPI-C transaction
  - Unlike AGN security where security check based on PSB (dependent region) userid
  - Ensure AGN and PSB profile ***names do not conflict***
- **AGN Table security used when**
  - No profile defined for PSB in AIMS Class
  - AIMS class not activated
- **Requirements**
  - RACF 1.9.2 or higher
  - DB/DC or DCCTL environment

APSB SAF Security Example

Active APSB SAF security by starting IMS using either:

APPCSE=P (and specify RACF=FULL in TP_Profile) or **APPCSE=F**

Or issue the equivalent IMS command:

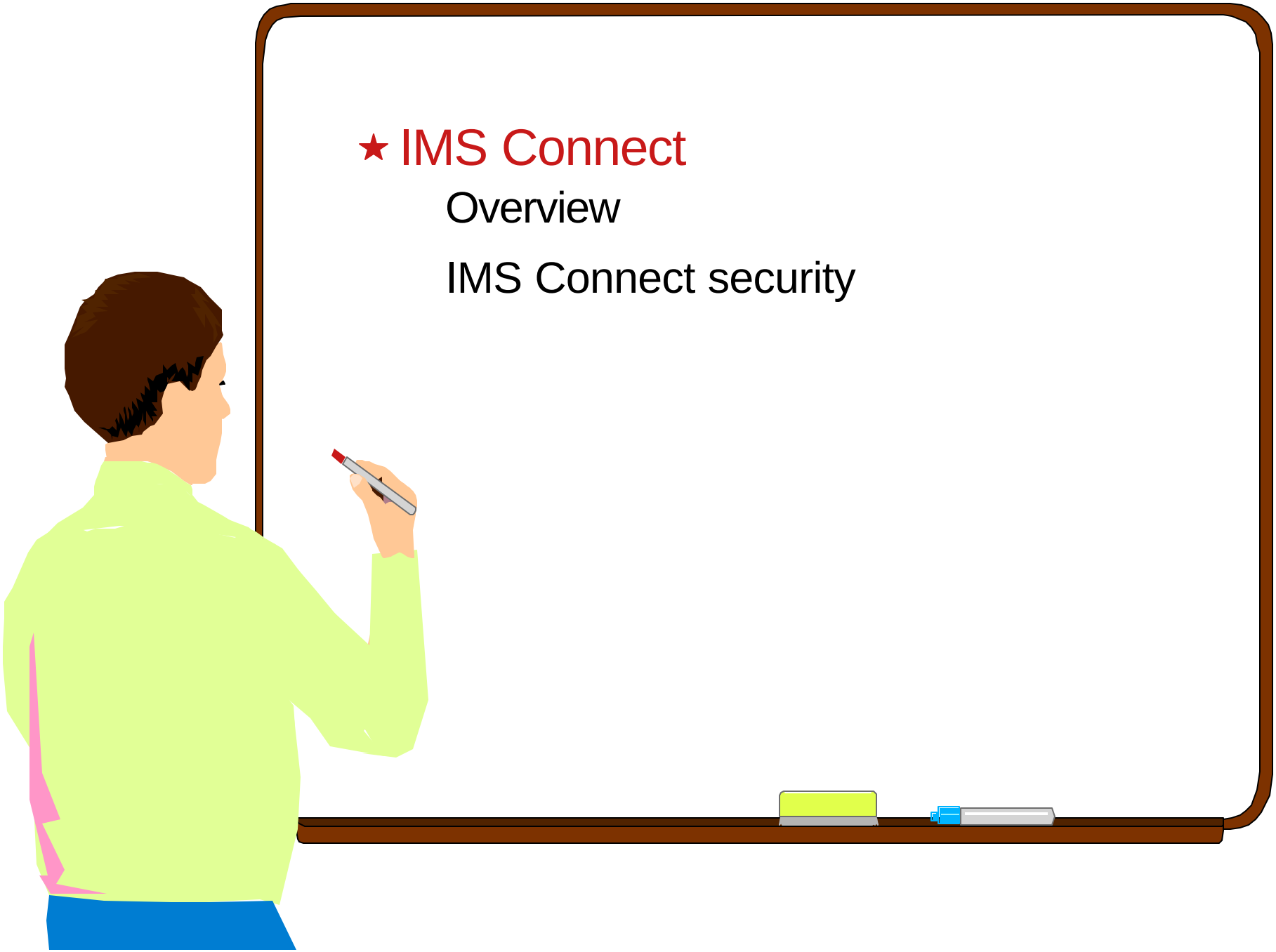
/SECURE APPC PROFILE or /SECURE APPC FULL

Use additional IMS startup options: **RCF≠N and ISIS=1**

RDEFINE AIMS CPICPSB1 OWNER(IMSADMIN) UACC(NONE)

PERMIT CPICPSB1 CLASS(AIMS) ID(GROUPX GROUPY USER1 APPCUSRS) ACCESS(READ) WHEN(APPCPORT(LUP1 LUP2 LUP3 LUP4)

SETR CLASSACT(AIMS)
SETR GLOBAL(AIMS) REFRESH
SETR GENERIC(AIMS) REFRESH
SETR RACLIST(AIMS) REFRESH


★ IMS Connect
Overview
IMS Connect security

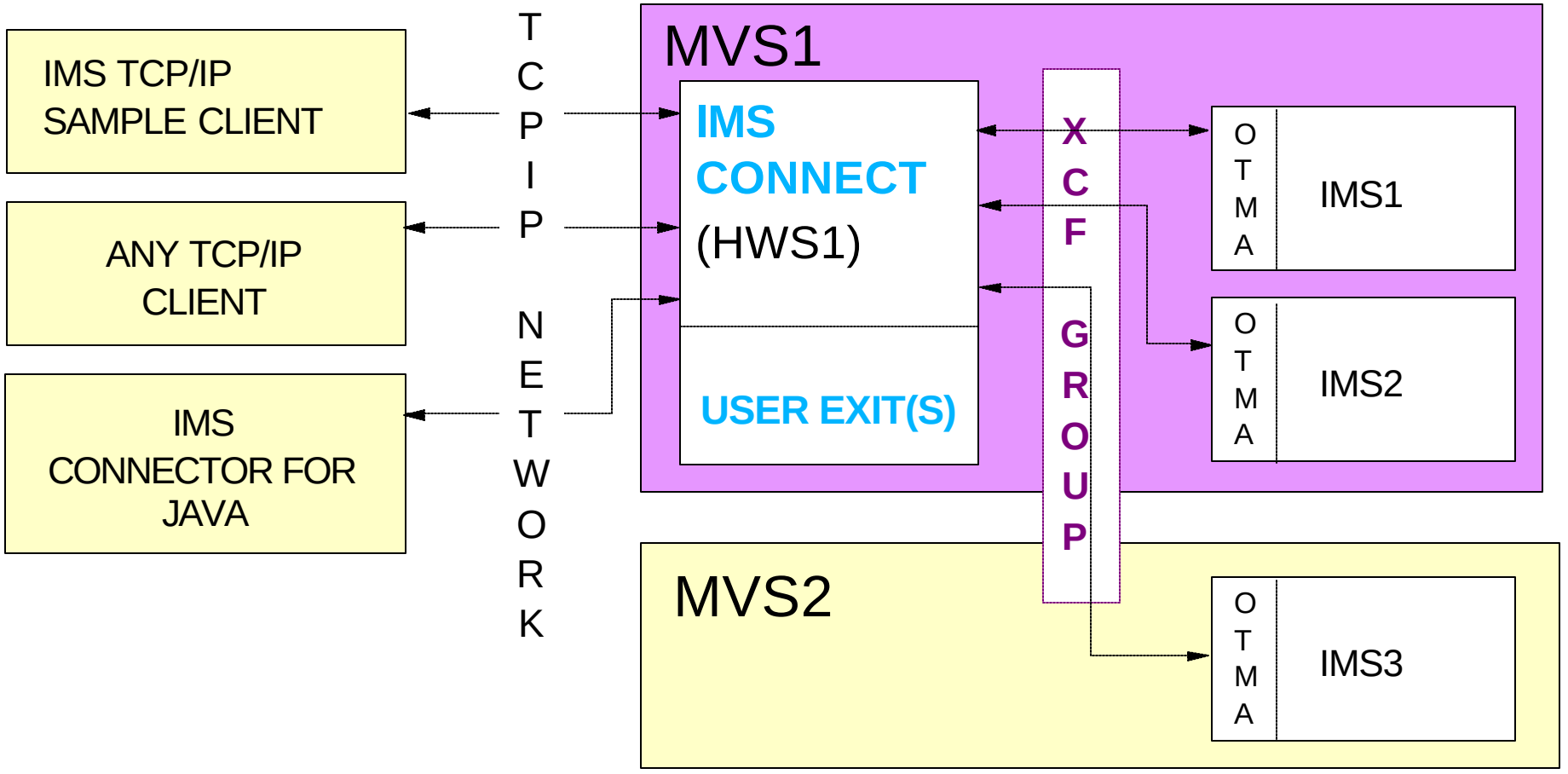
IMS Connect

- **Provides method for TCP/IP client applications to send messages (commands/transactions) to IMS/TM**
- **Supports multiple client applications**
  - IMS Connector for JAVA
  - IMS TCP/IP sample client application
  - Any TCP/IP client application
- **Is an IBM program product**
  - Separately priced product (5655-E51)
    - Replacement for IMS TCP/IP OTMA Connection (ITOC) product
  - Runs on MVS | OS/390 | z/OS platforms

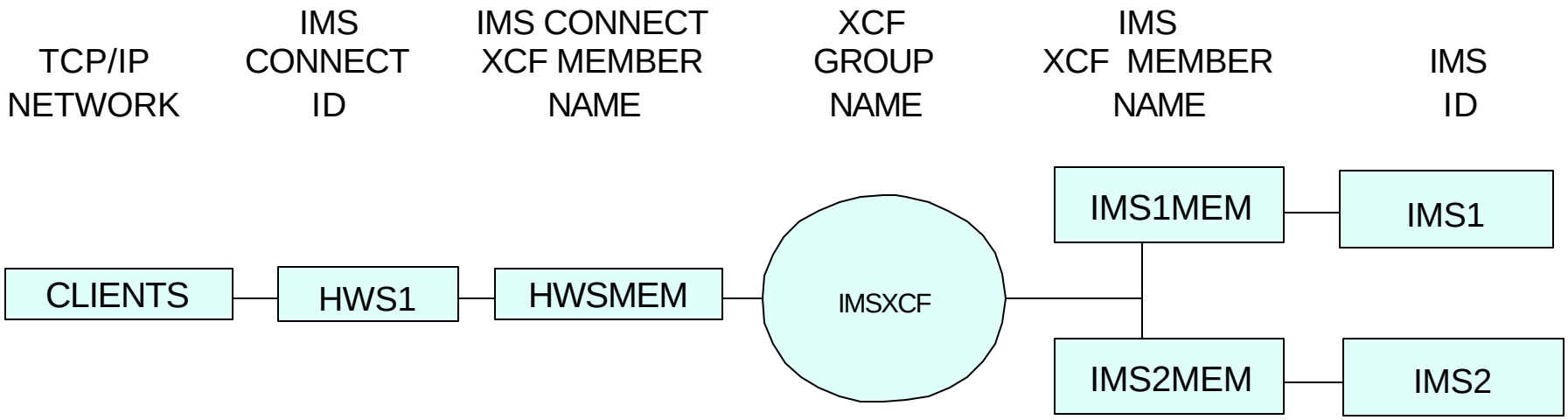
Primary Functions

- **Send/receive messages to/from OTMA**
  - Message input
    - Translate ASCII to EBCDIC
    - Build OTMA headers
  - Message output
    - Translate EBCDIC to ASCII
    - Remove OTMA headers
- **Userid validation and password verification**

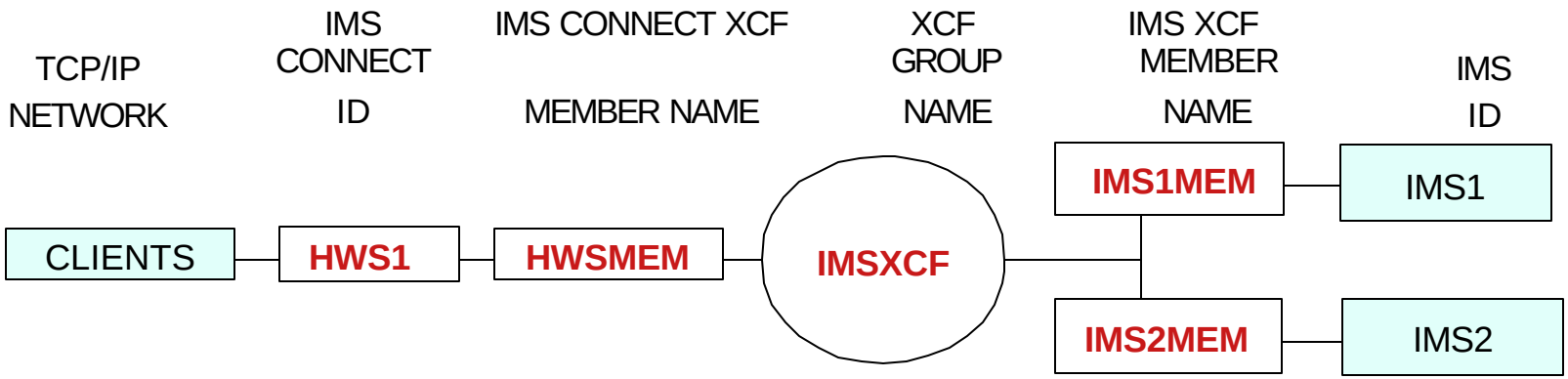
Communications

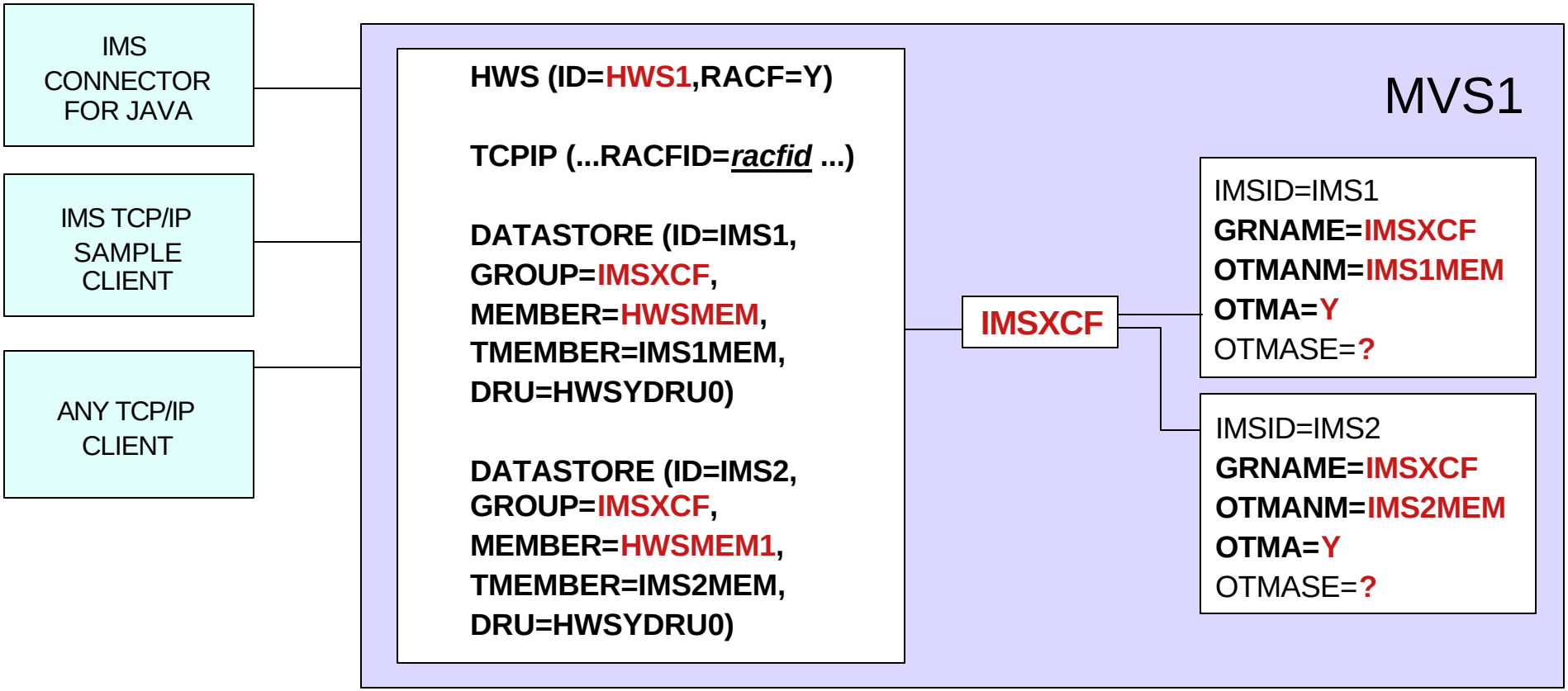


Simple Example of Using XCF



Startup Parameters

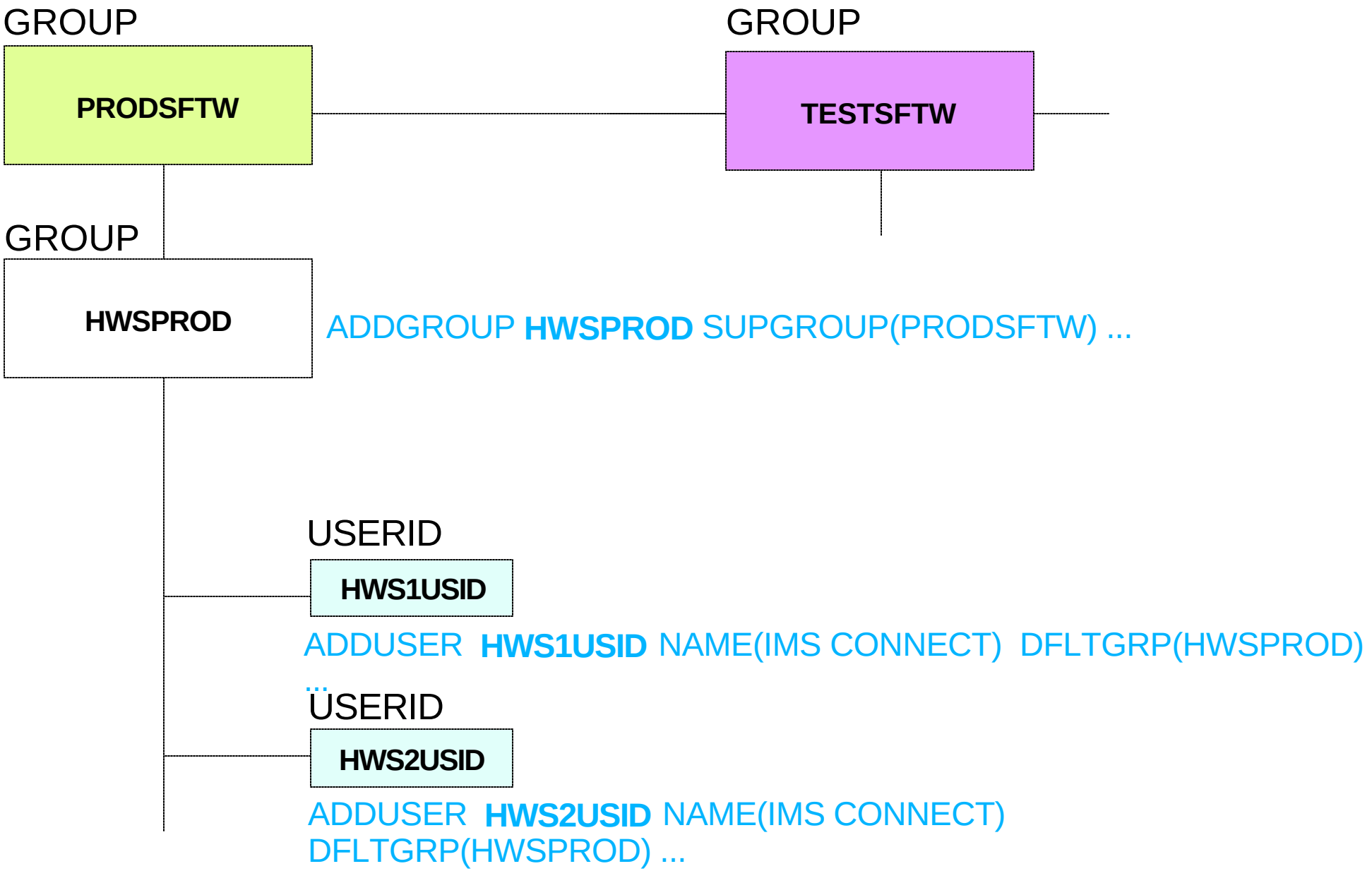




IMS Connect Security

- **Runtime libraries must be APF authorized**
- **MVS PPT must allow IMS Connect to use**
  - Supervisor state
  - Key 7 storage
- **IMS Connect**
  - Connects to IMS as OTMA client
  - HWSCFGxx file contains execution/start up parms
  - Can perform userid/password security checking
    - IMS Connect can call RACF to
      - VERIFY userid and password
      - Create UTOKEN for valid user
  - Passes verified userid's UTOKEN to IMS
  - Subsystem should have valid RACF userid and group

Defining IMS Connect's Userid and Group



Supplying IMS Connect's Userid

```
//HWS01    JOB   MSGLEVEL=1,TIME=1440,CLASS=Y,USERID=&USERID
//*****************************************************************
//*  BRINGING UP IMS CONNECT USING A JOB
//*****************************************************************
//HWS01    EXEC HWS,SOUT=A
//HWS      PROC RGN=4096K,SOUT=A,
//              BPECFG=BPECFGHT,
//              HWSCFG=HWSCFG00
//*
//*****************************************************************
//*  BRING UP AN IMS CONNECT                                      *
//*****************************************************************
//STEP1    EXEC PGM=HWSHWS00,REGION=&RGN,TIME=1440,
//              PARM='BPECFG=&BPECFG,HWSCFG=&HWSCFG'
//STEPLIB  DD   DSN=SHWSRESL,DISP=SHR
//         DD   DSN=SDFSRESL,DISP=SHR
//PROCLIB  DD   DSN=USER.PROCLIB,DISP=SHR
//SYSPRINT DD   SYSOUT=&SOUT
//SYSUDUMP DD   SYSOUT=&SOUT
//HWSRCORD DD   DSN=HWSRCDR,DISP=SHR
```

Ways To Supply IMS Connect's Userid

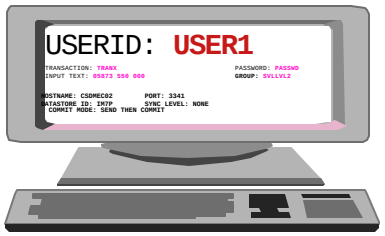
- **Started procedure**
  - RACF STARTED Class
    - Associate IMS Connect userid with started procedure
    - Generic profile default userid
- **Started Procedure Table (SPT)**
  - Code entry in table to associate IMS Connect userid with started procedure
  - Generic table entry default userid
- **JOB card USERID= parameter**
- **Use both STARTED Class and SPT**
  - STARTED Class to avoid unscheduled IPL
  - Update Started Procedure Table during scheduled IPL

End User Userid/Password Verification

- **Verification may be performed by**
  - User security exit | IMS Connect | IMS/OTMA | combination
    - **IMS/OTMA** verifies userid and group
      - User password is ***not*** verified
- **Activating IMS Connect userid/password verification**
  - RACF=Y in HWSCFGxx file or SETRACF ON command
    - Causes IMS Connect to call RACF
      - RACROUTE REQUEST=VERIFY,PASSCHK=YES
- **When RACF=N *and* security exit not used**
  - Password not sent to IMS
  - IMS calls to RACF
    - RACROUTE REQUEST=VERIFY,PASSCHK=NO
      - Potential security exposure in IMS because user authentication not performed

End User's Userid Passed To IMS

- **Userid used for authorizations originates from**
  - Client
    - Passed in message prefix data
    - Security data section (SE)



  - User message exit
    - Can create userid after IMS Connect receives input message
    - May generate userid when no client userid passed to exit

IMS Connect HWSCFGxx FILE

TCPIP (...RACFID=default_userid,**EXIT=**(EZAIMSO0,HWSJAVA0,...)

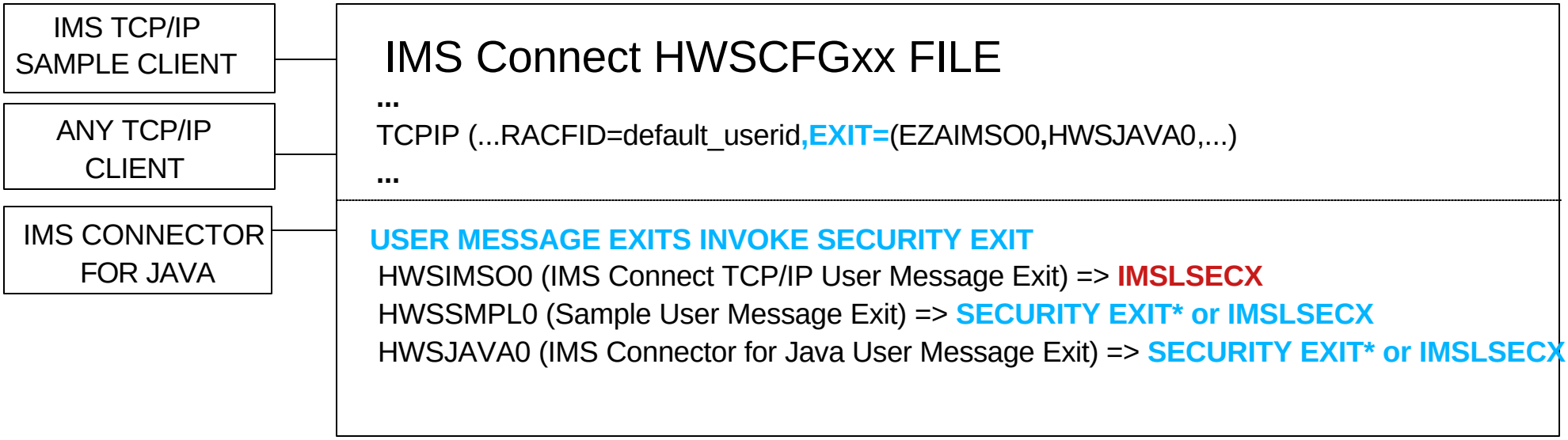
  - Default RACFID

IMS Connect HWSCFGxx FILE

TCPIP (...**RACFID=*default_racf_userid***,EXIT=(EZAIMSO0,HWSJAVA0,...)

User Message Exit Supplied Userid

- Security exit called by message exit
- Message exit HWSSMPL0
  - Security exit name supplied by user in HWSSMPL0
- Message exit HWSJAVA0
  - Security exit name supplied by user in HWSJAVA0
- Message exit HWSIMSO0
  - Security exit must be named **IMSLSECX**
    - IMSLSECX0 may be used with any user message exit
    - IMSLSECX sample provided by TCP/IP



*NAME OF THE SECURITY EXIT ROUTINE IS PROVIDED BY INSTALLATION

IMSLSECX Security Exit

- **May be called from any of the message exits**

- **Parameter list passed to exit include addresses of**
  - Client's IP address and port number
  - IMS transaction code
  - Data type setting
    - 0=ASCII | 1=EBCDIC)
  - Length of user data
  - User-supplied data
  - RACF USERID and password
    - USERID passed to IMS depends on value specified in IRM
  - RACF GROUPID
    - GROUPID passed to IMS depends on value specified in IRM

Security Exit *Not Invoked* By User Exit

USERID PASSED

USERID FIELD IN IRM?	IRM USERID FIELD BLANK/NULL?	RESULTS PASSED TO IMS IN OTMA SECURITY HEADER
YES	YES	**DEFAULT RACFID**
YES	NO	**IRM USERID**
NO	N/A	**DEFAULT RACFID**

GROUP NAME PASSED

GROUPID FIELD IN IRM?	IRM GROUPD FIELD BLANK/NULL?	RESULTS PASSED TO IMS IN OTMA SECURITY HEADER
YES	YES	**BLANKS/NULLS**
YES	NO	**IRM GROUPID**
NO	N/A	**BLANKS/NULLS**

IRM - IMS Request Message (Header)

Security Exit *Is Invoked* By User Exit

USERID PASSED

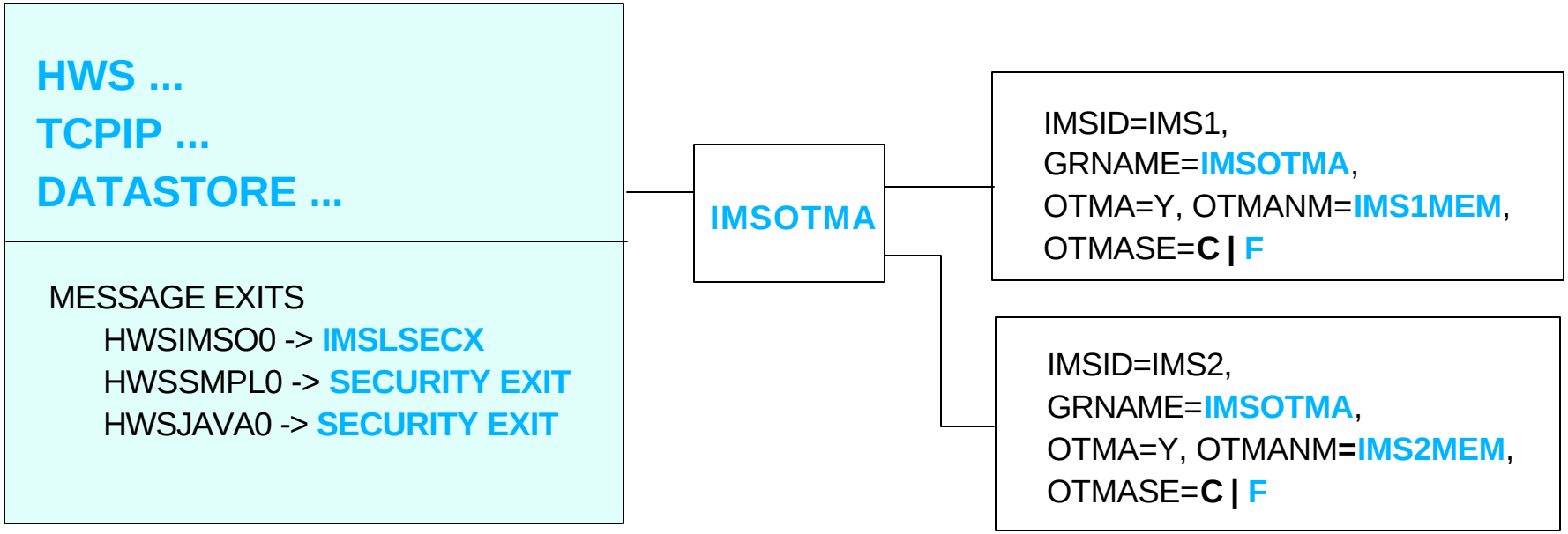
USERID FIELD IN IRM?	IRM USERID FIELD BLANK/NULL?	USERID RETURNED BY SECURITY EXIT?	RESULTS PASSED TO IMS IN OTMA SECURITY HEADER
YES	YES	NO	DEFAULT RACFID USERID
YES	YES	YES	SECURITY EXIT RETURNED USERID
YES	NO	NO	USERID PASSED IN IRM
YES	NO	YES	SECURITY EXIT RETURNED USERID
NO	N/A	NO	DEFAULT RACFID USERID
NO	N/A	YES	SECURITY EXIT RETURNED USERID

GROUP NAME PASSED

GROUPID FIELD IN IRM?	IRM GROUPID FIELD BLANK/NULL?	GROUPID RETURNED BY SECURITY EXIT?	RESULTS PASSED TO IMS IN OTMA SECURITY HEADER
YES	YES	NO	BLANK GROUPID
YES	YES	YES	SECURITY EXIT RETURNED GROUP NAME
YES	NO	NO	BLANK GROUPID
YES	NO	YES	SECURITY EXIT RETURNED GROUP NAME
NO	N/A	NO	BLANK GROUPID
NO	N/A	YES	SECURITY EXIT RETURNED GROUP NAME
YES	YES	NO	BLANK GROUPID
YES	YES	YES (RETURNED BLANKS)	BLANK GROUPID
YES	NO	NO	IRM GROUPID
YES	NO	YES (RETURNED BLANKS)	IRM GROUPID
NO	N/A	NO	BLANKS
NO	N/A	YES (RETURNED BLANKS)	BLANKS

Important: If security exit returns blank USERID, then GROUP returned by the exit is not used.

HWSCFGxx File



HWSCFGxx

```
HWS (ID=HWS1,RACF=Y)
TCPIP (...RACFID=default_userid,EXIT=(EZAIMSO0,HWSJAVA0,...)
DATASTORE (ID=IMS1,GROUP=IMSOTMA,MEMBER=HWSMEM,TMEMBER=IMS1MEM,DRU=HWSYDRU0)
DATASTORE (ID=IMS2,GROUP=IMSOTMA,MEMBER=HWSMEM1,TMEMBER=IMS2MEM,DRU=HWSYDRU0)
...
```

MVS PPT

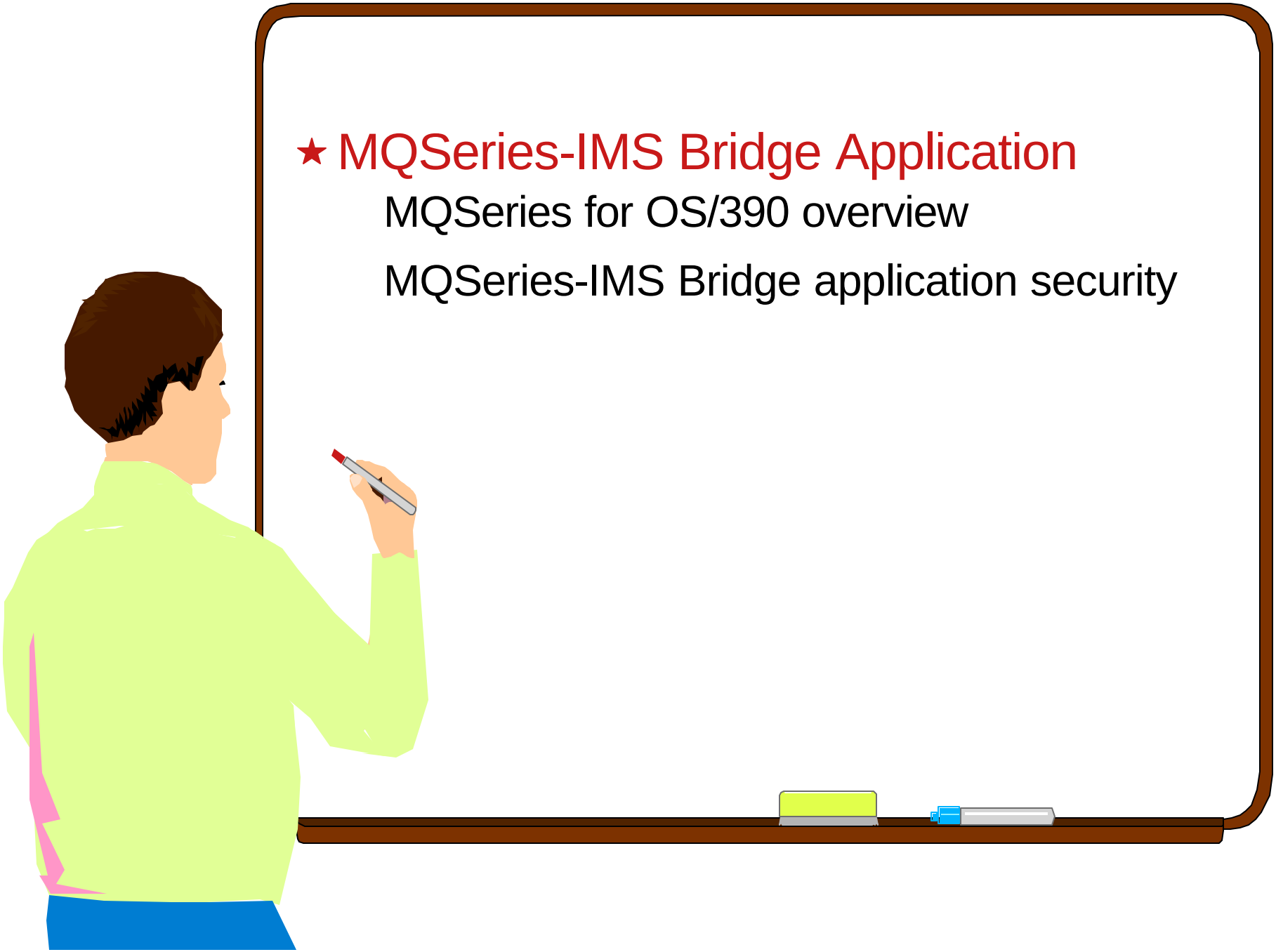
```
PPT PGMNAME(HWSHWS00)  /* PROGRAM NAME = HWSHWS00                          */
KEY(7)                 /* PROTECT KEY ASSIGNED IS 7                        */
PASS                   /* CANNOT BYPASS DATASET PASSWORD PROTECTION        */
SYST                   /* PROGRAM IS A SYSTEM TASK            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

IMS Connect & IMS Connection

- **After IMS Connect startup**
  - IMS Connect joins the XCF group as IMS
  - After successful client-bid connection request, IMS Connect
    1. Sends messages to IMS
    2. Processes any replies

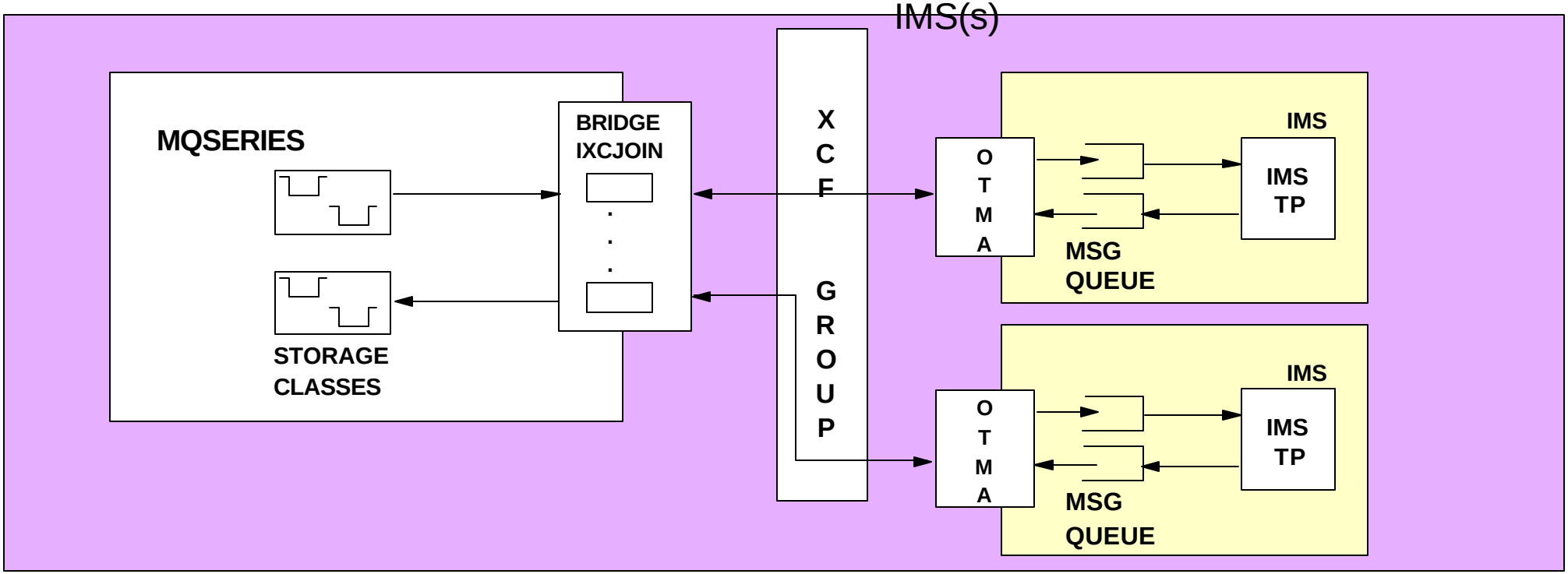
- **IMS Connect client-bid connection request**
  - IMS checks RACF **FACILITY class** profile
    - IMSXCF.XCFGROUP.HWS_XCF_MEMBER_NAME
      - **Example: IMSXCF.IMSOTMA.HWS1MEM**
    - IMS Connect subsystem userid must have at least ACCESS(READ)

- **RACF 1.9.2 or higher (or equivalent product)**


★ MQSeries-IMS Bridge Application
MQSeries for OS/390 overview
MQSeries-IMS Bridge application security

MQSeries for OS/390 Overview

- 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 to IMS
    - Is an OTMA client
    - May connect to 1 or more IMSs
    - Multiple MQs may connect to 1 IMS
      - Bridge must join same XCF group as IMS(s)



MQSeries - IMS Bridge Set Up

- **Define MQSeries to XCF group**
- **Define IMS to XCF group**
- **Define MQ objects**
  - Define MQSeries 'bridge' queues
  - Storage classes
  - Queue definitions
- **Operating the Bridge**
- **Set up the security that you require**
  - Implement MQ-IMS Bridge security options

Define MQSeries to XCF Group

- ***CSQZPARM*** **contains MQ system parameters**
  - OTMACON keyword on CSQ6SYSP macro
    OTMACON(group,member,druexit,age,tpipepref)

group	**XCF group name.** Required parameter when Bridge is to be used. Default is blanks for group name. Bridge not started when group name blanks.
member	**MQSeries XCF member name.** Default is queue manager name (i.e. CSQ1).
druexit	**Destination Resolution User Exit name.** Default name in IMS is DFSYDRU0. Suggested exit naming convention: DRU0CSQ1, DRU0CSQ2, DRU0CSQ3, ...
age	**ACEE aging value.** Number of seconds ACEE is valid in IMS.
tpipepref	**First 3 characters of transaction pipe (TPIPE) prefix name.** Default is CSQ. Do not change default TPIPE prefix name without good reason.

Define IMS to XCF Group

- **IMS procedure or IMS.PROCLIB(DFSPBxxx)**
  - OTMA=Y
  - GRNAME=*zzzzzzzz*
    - XCF group name
  - OYMANM=*xxxxxxxx*
    - XCF member name for IMS
- **XCF member name for IMS**
  - OTMANM | USERVAR | APPLID
    - OTMANM=xxxxxxxx used if specified
    - USERVAR=yyyyyyyy for XRF | RSR
      - OTMANM= not used with XRF | RSR
      - Specified in DFSPBxxx or DFSHSBxx
    - APPLID1=zzzzzzzz
      - Default XCF member name is VTAM APPLID

        COMM macro APPLID= (Used when OTMANM and USERVAR not specified)

        Overridden by APPLID**1**=

Define MQ Objects

- **Storage class definition**

```
DEFINE STGCLASS( 'BRIDGE' )-
XCFGNAME( 'IMSOTMA' ) -
XCFMNAME ( 'IMS1MEM' ) -
PSID( 02 )
```

- **'Bridge' queue definition**

```
DEFINE QLOCAL(BRIDGE.TEST.IMS.QUEUE) REPLACE -
DESCR  ( 'MQ-IMS bridge queue' ) -
STGCLASS(BRIDGE)
```

- **Reply queue definition**

```
DEFINE QLOCAL(BRIDGE.TEST.IMS.REPLYTO.QUEUE) REPLACE -
DESCR ( 'Queue used for reply messages' ) -
STGCLASS(REPLY)
```

Operating the Bridge

- **After MQSeries startup**
  - MQSeries joins the XCF group
  - Bridge is told about queues with XCF data
    - When a queue points to an IMS in the XCF group
      - MQSeries initiates client-bid resync
      - When client-bid is successful
        1. Bridge opens MQSeries queues
        2. Sends messages to IMS
        3. Processes any replies
- **No MQSeries commands to start/stop the Bridge**
  - IMS commands to start/stop OTMA
    - **/STA OTMA**
    - **/STO OTMA**

Set Up the Security You Require

- **Determine how much userid | password security checking is required for messages destined for IMS/OTMA**
  - MQ message-based security
- **Determine whether security checking will be performed for reply and/or exception messages**
  - Security checking done by MQ-IMS Bridge

MQ-IMS Bridge Security Options

- **Message-based security**
  - Unique to MQ-IMS Bridge application
  - Determined after successful client-bid connection request
  - Message-based security levels
    - **NONE | READ | UPDATE | CONTROL or ALTER**
- **Security checking done by bridge when**
  - Putting
    - A reply message
    - An exception message or confirm-of-arrival (COA) report message
  - No security checking when
    - Getting a message from bridge queue
    - Putting a message to the dead-letter queue

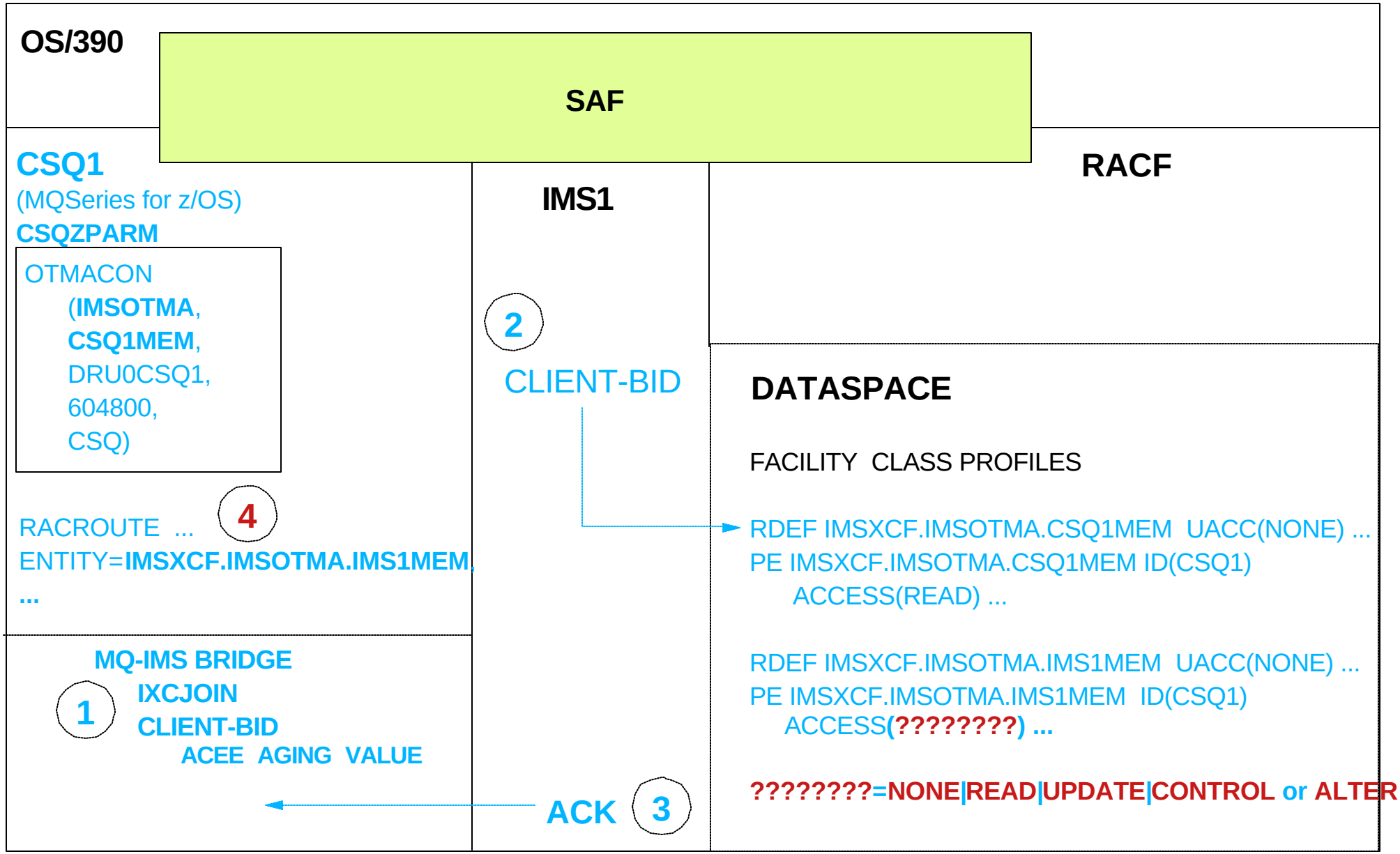
MQ-IMS Bridge and IMS Connection

- Bridge application joins same XCF group as IMS(s)
- Bridge issues client-bid connection request
  - IMS checks RACF FACILITY class profile
    - IMSXCF.XCF_GROUP_NAME.MQ_XCF_MEMBER_NAME
      - **Example: IMSXCF.IMSOTMA.CSQ1MEM**
    - MQ queue manager userid must have at least ACCESS(READ)
    - Profile ***ssid*.NO.SUBSYS.SECURITY** in **MQADMIN** class
      - Example: **CSQ1.NO.SUBSYS.SECURITY**
      - **Client-bid fails unless IMS OTMA security level is NONE**
- MQSeries checks RACF FACILITY class profile
  - IMSXCF.XCFGROUP.IMS_XCF_MEMBER_NAME
    - **Example: IMSXCF.IMSOTMA.IMS1MEM**
  - MQ qmgr userid access level used in message-based security
- RACF 1.9.2 or higher (or equivalent product)

Message-Based Security

- **MQ-IMS Bridge provides message-based security**
  - Authorization done using userid in the MQMD.UserIdentifier field
- **Validation of messages**
  - Level determined at client-bid time
  - Based on MQSeries queue manager access to profile
    - IMSXCF**.**XCF_group_name**.**IMS_XCF_member_name
- **Once validated the userid is passed to IMS**
  - Used for normal IMS security
- **IMS puts userid in IOPCB**
  - Userid in IOPCB used by IMS when necessary

Message-Based Security Illustration

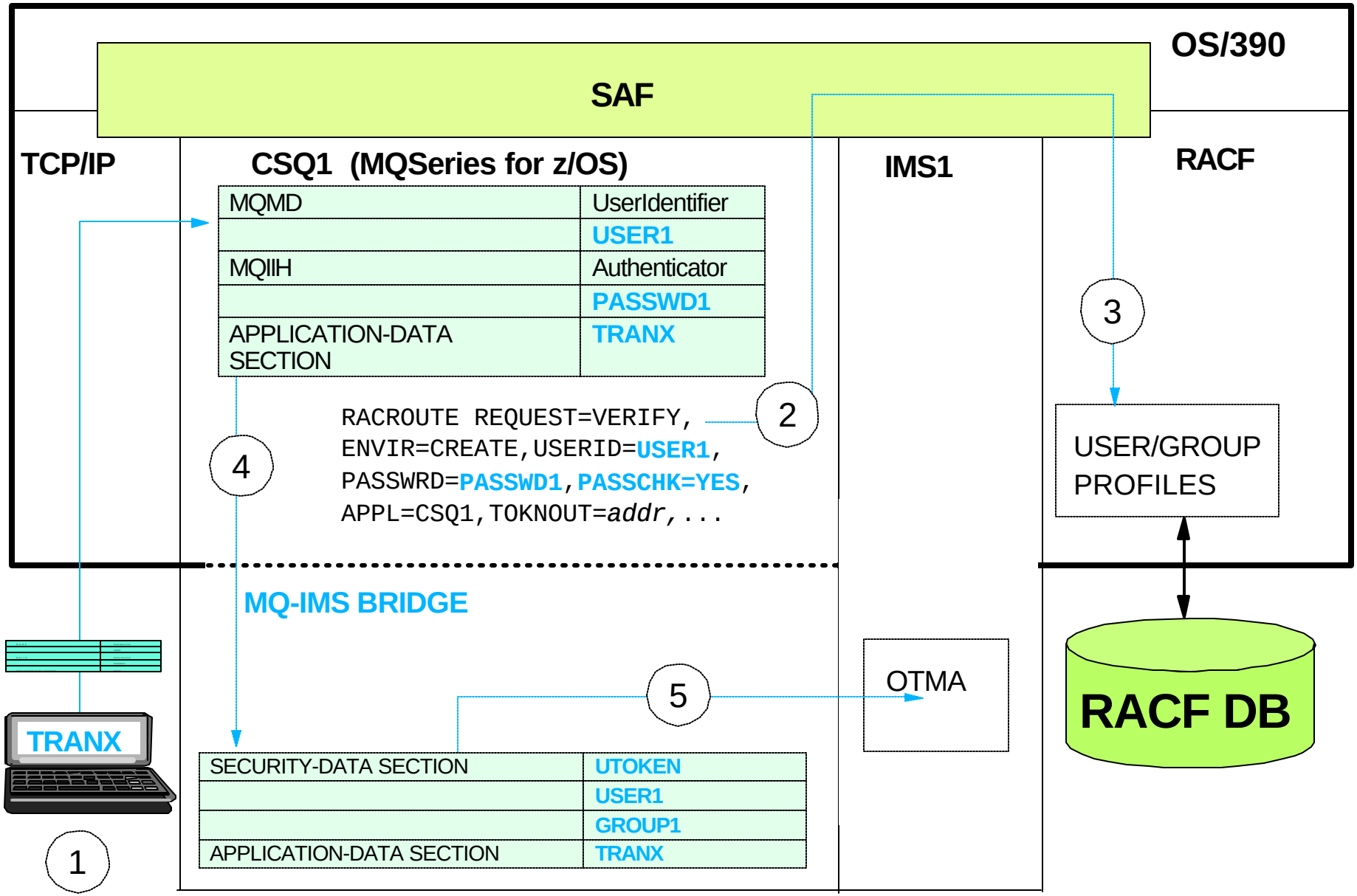


ACCESS(NONE)

- **Maximum security required when**
  - NONE, or when no profile found
  - Userid ***and*** password authentication required for every message
    - Must be valid RACF userid ***and*** password (or PassTicket)
  - UTOKEN created by MQSeries and passed to IMS
    - UTOKEN is ***not cached*** by MQSeries

- **MQADMIN *qmgr.NO.SUBSYS.SECURITY* profile**
  - Overrides both
    - IMSXCF.xcf_group_name.ims_xcf_memeber_name profile access level
    - No profile found condition
  - Considerations
    - Userid may not be passed to IMS
    - May lead to resource authorization failures in IMS

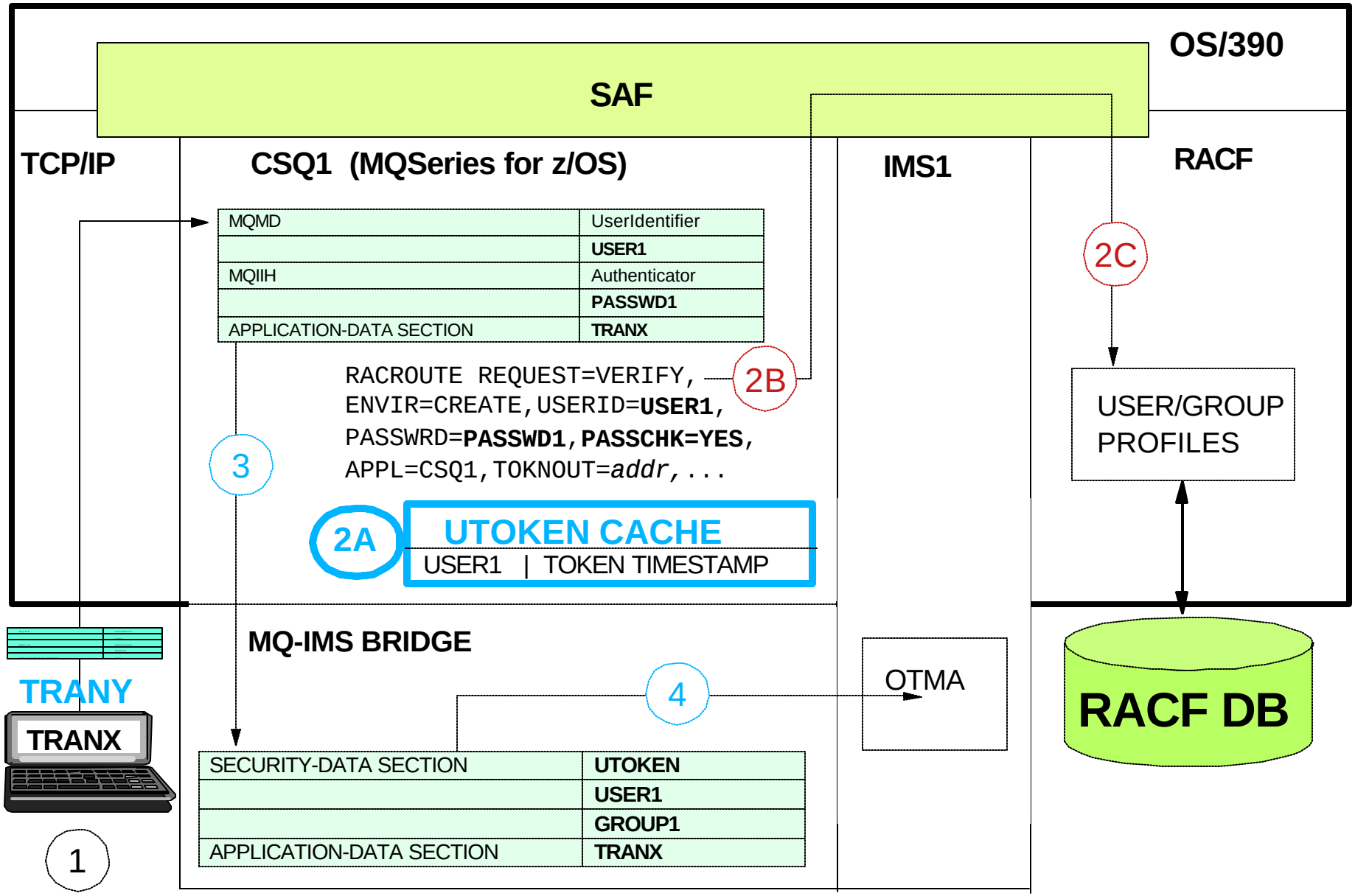
ACCESS(NONE) User Verification



ACCESS(READ)

- **The first time a userid is encountered, MQSeries**
  - Calls RACF to verify userid *and* password (or PassTicket)
    - MQMD field contains userid
    - MQIIH.Authenticator field contains the password/PassTicket
  - Result of check
    - Cached in MQSeries
    - Used on subsequent calls
- **UTOKEN built and passed to IMS**
- **If MQSeries has encountered the userid before**
  - Valid, cached UTOKEN passed to IMS
    - MQSeries calls RACF to create new UTOKEN only if required
      - For example, expired UTOKEN
  - Result of check cached in MQ and used on subsequent calls

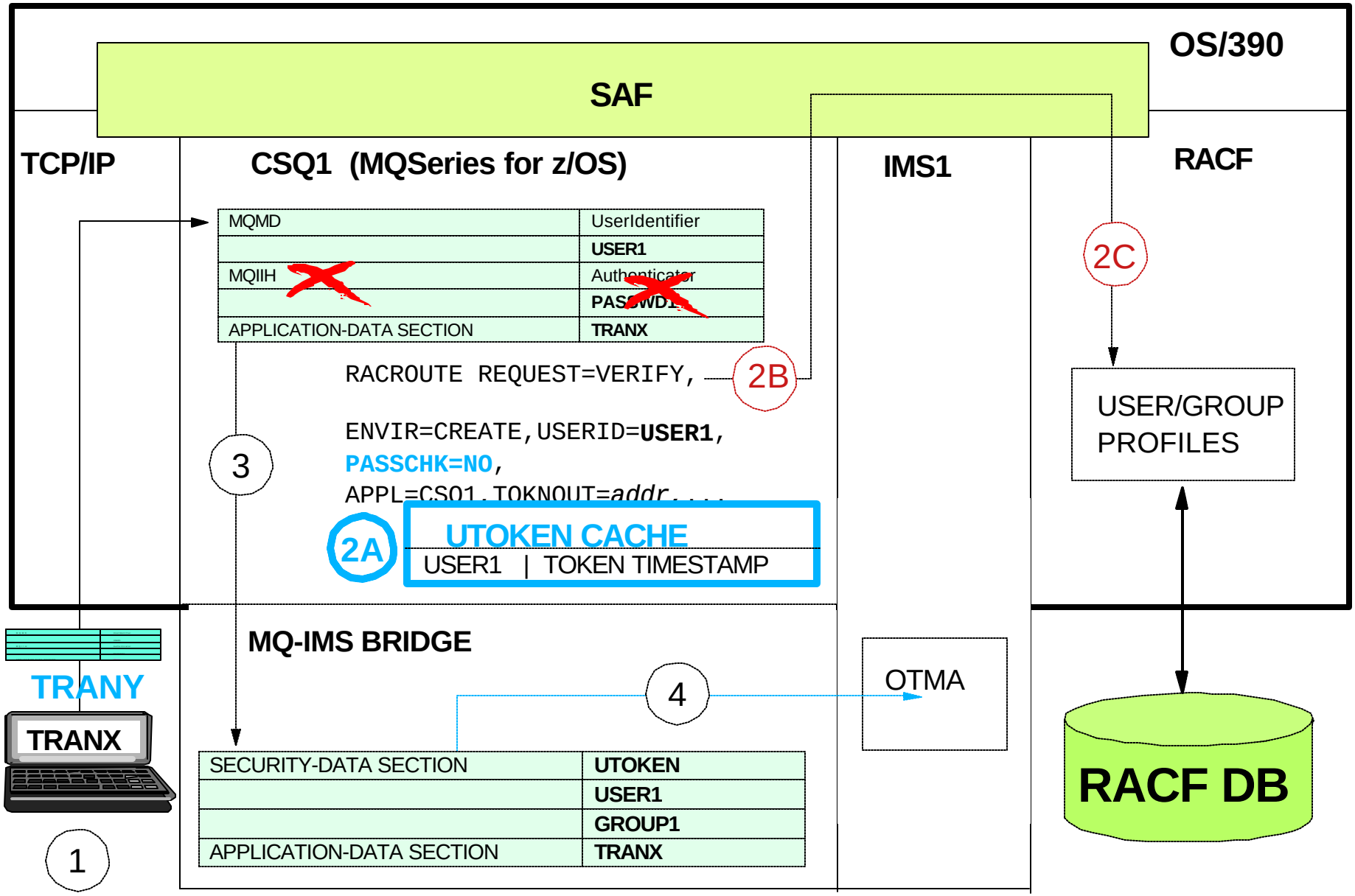
ACCESS(READ) User Verification



ACCESS(UPDATE)

- **MQSeries calls RACF to verify the userid**
  - Userid validated by RACF prior to passing message to IMS
  - Password/PassTicket is ***not*** verified
  - UTOKEN is
    - Built and passed to IMS
    - Cached in MQSeries

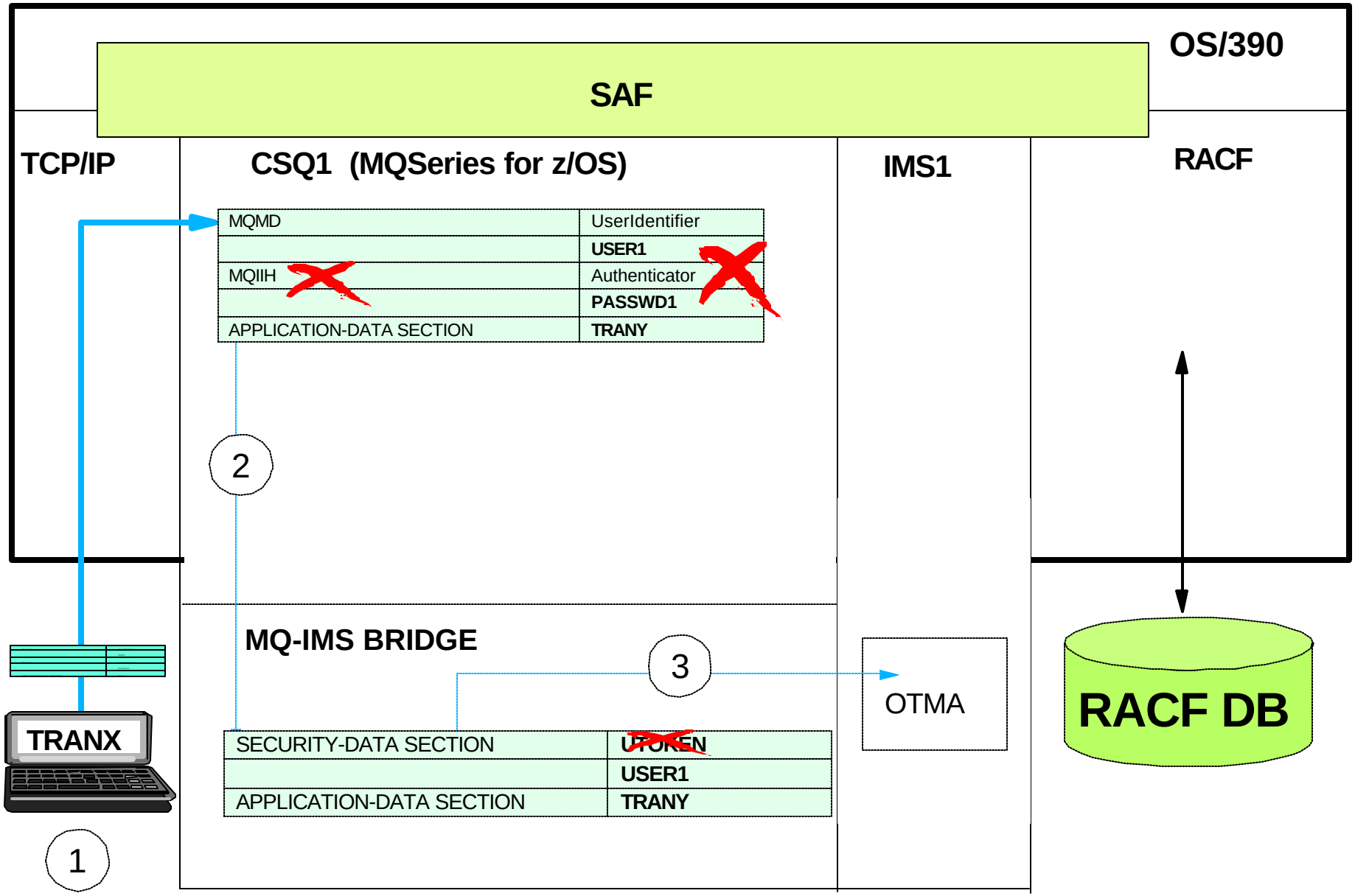
ACCESS(UPDATE) User Verification



ACCESS(CONTROL or ALTER)

- **Userids are *trusted***
  - No RACF checks
    - No UTOKENs built for any userids
- **Should only use for**
  - Development systems
  - Test systems

ACCESS (CONTROL or ALTER) User Verification



Considerations for MQ Userid Access Level

- **Access level lasts for duration of the connection**
- **To change access level**
  - Profile must be changed
    - Requires a refresh to activate changes
      - SETROPTS RACLIST(FACILITY) REFRESH
    - Access level in profile may be affected by
      - OTMASE= parameter
      - /SECURE OTMA command specification
  - Bridge must be stopped
    - Bridge stopped and restarted by stopping and restarting OTMA
- **Password or PassTicket may be used, but**
  - MQSeries-IMS bridge does not encrypt data
- **Cached UTOKEN info is held for duration defined by MQSeries ALTER SECURITY command**

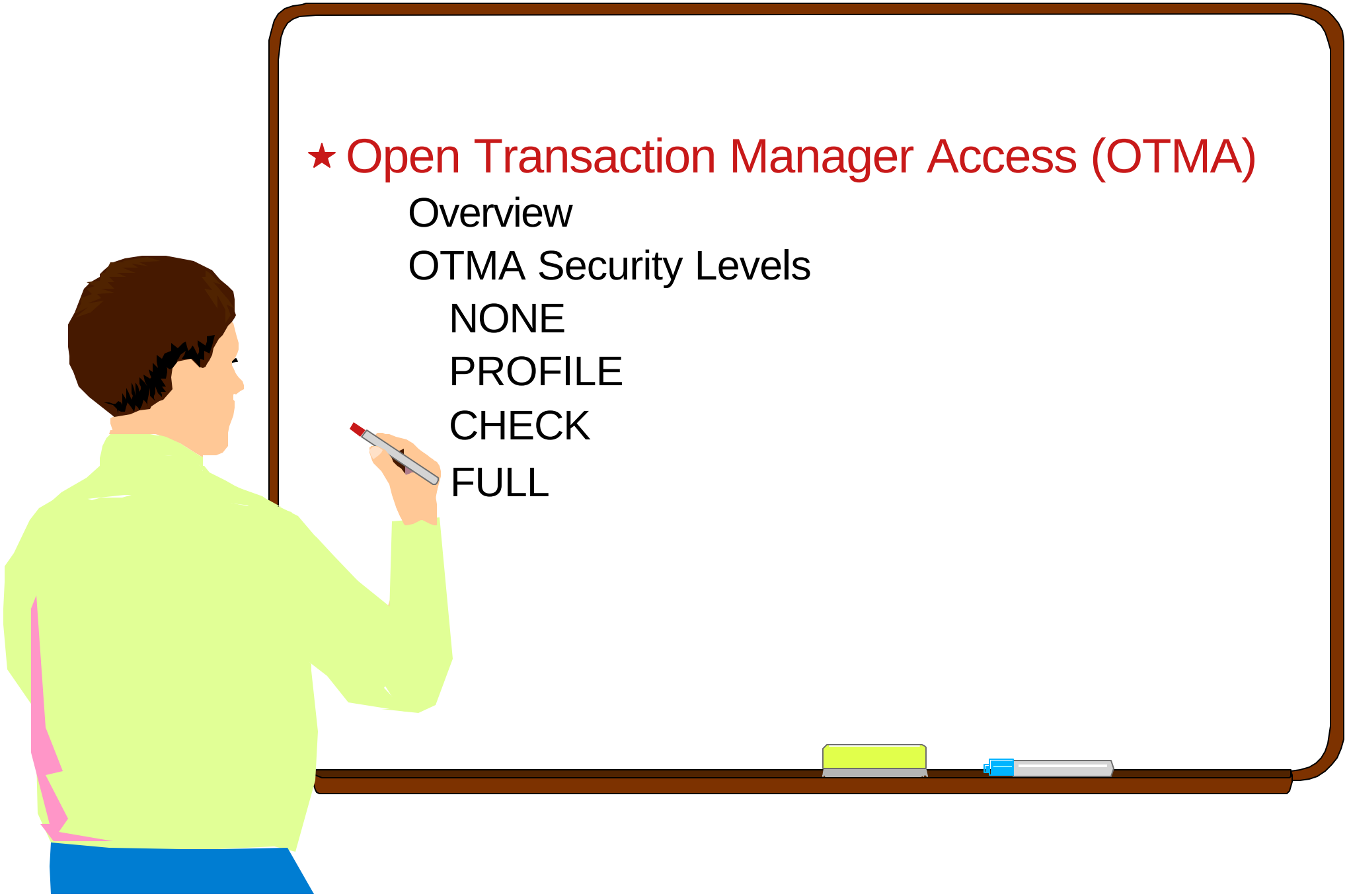
  ALTER SECURITY INTERVAL(integer) TIMEOUT(integer)

Messages Passed By The Bridge

- **Each message passed to IMS over the Bridge has**
  - A ***userid***
  - The ***security scope*** (NONE, CHECK, or FULL)
    - Scope present when ***MQIIH*** message header structure is present
      - Default is ***CHECK*** if MQIIH not present
  - A ***UTOKEN***
    - Exceptions
      - MQSeries userid has ACCESS(CONTROL) or ACCESS(ALTER) in IMSXCF**.**xcf_group_name**.**mq**.**xcf_member_name
        RDEF FACILITY IMSXCF.IMS1.IMSA1 UACC(NONE
        PE IMSXCF.IMS1.IMSA1 CLASS(FACILITY) ID(MQUSID)
        ACCESS(CONTROL) or ***ACCESS(ALTER)***
      - ***qmgr*.NO.SUBSYS.SECURITY** in **MQADMIN** class
        No userid passed in client-bid message

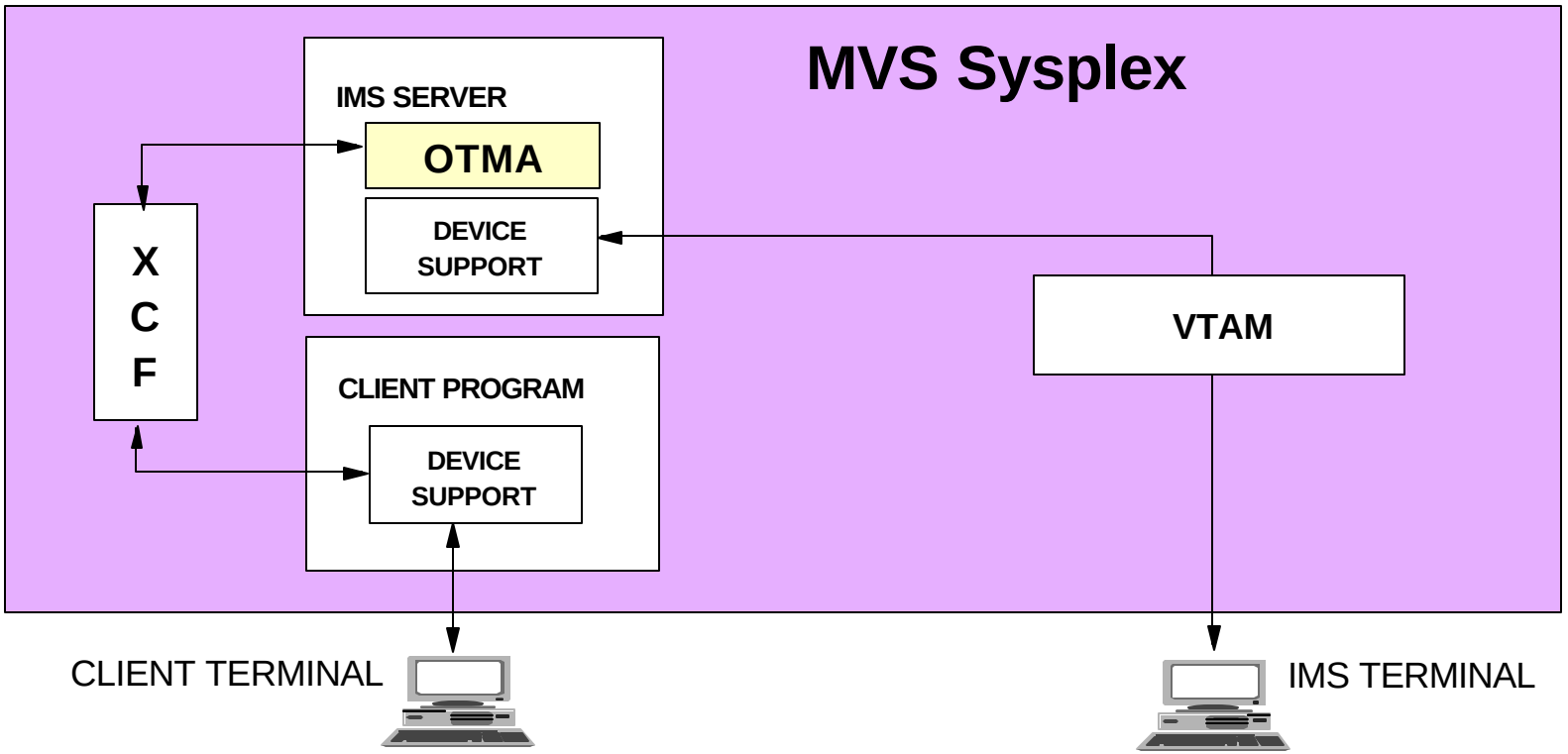
IMS Security Checking For Bridge Messages

- **IMS security checking for messages received from the bridge**
  - Governed by IMS security level for OTMA
    - /SECURE OTMA xxxx or OTMASE=x
      - Where xxxx is NONE, PROFILE, CHECK, or FULL
      - Where x is N, P, C, or F
- **UserIdentifier field of the MQMD structure must be passed to IMS when OTMA security level is**
  - /SEC OTMA CHECK or OTMASE=C
  - /SEC OTMA FULL or OTMASE=F
- **If OTMA security level PROFILE**
  - SecurityScope field in the MQIIH
    - Determines if RACF called or not
      - RACF called for 'C' and 'F'; RACF not called for 'N'
    - ***Ignored*** by IMS when OTMA security level is CHECK or FULL


★ Open Transaction Manager Access (OTMA)
Overview
OTMA Security Levels
NONE
PROFILE
CHECK
FULL

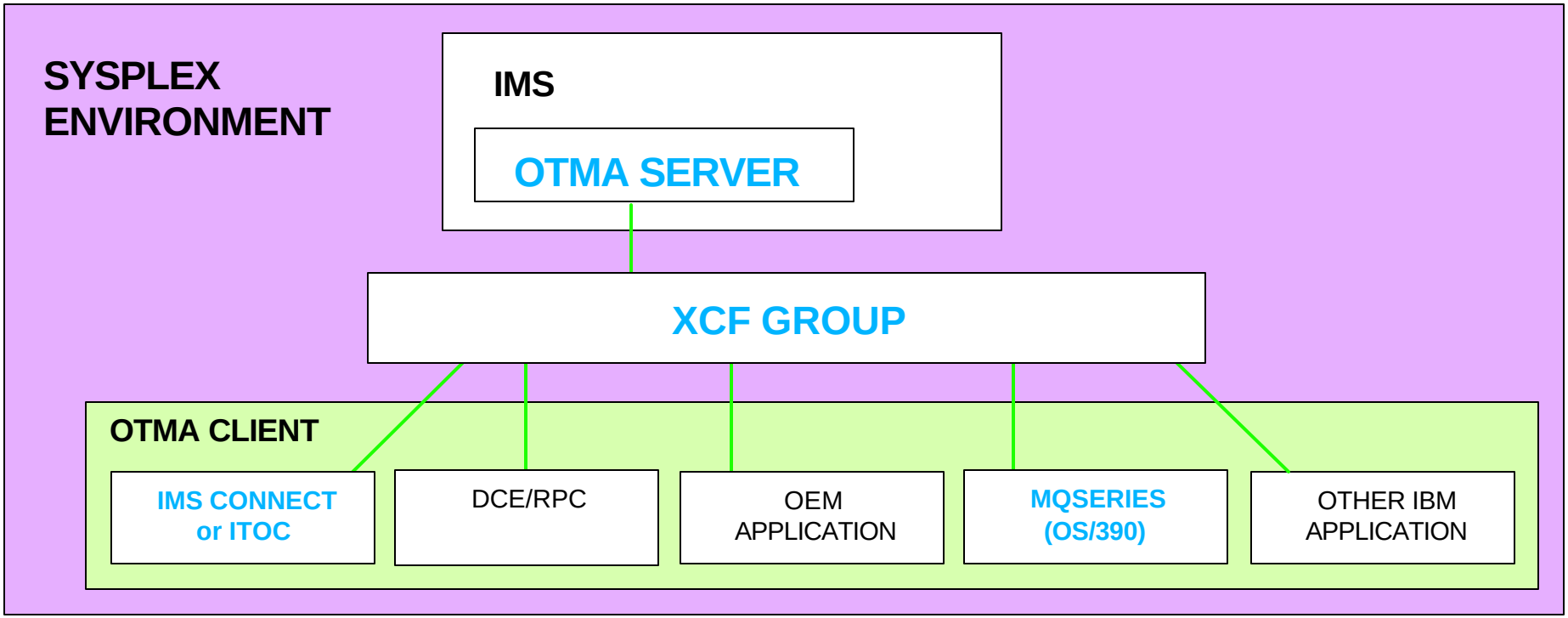
Open Transaction Manager Access

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



Accessing IMS From OTMA Clients

- An OTMA client
  - Gateway for transactions outside IMS to enter IMS
    - Sends IMS commands | IMS transactions to IMS/OTMA
    - Receives output
  - Must be a member of an ***XCF group*** and use the OTMA protocol
    - Joins same XCF group as IMS



IMS/OTMA Security

- **OTMA security is optional**
  - Security may be performed by ***client***
    - MQSeries
    - IMS Connect or ITOC
    - TCP/IP client server application (i.e. IMS Connector for JAVA)
  - Security checking may be done by ***IMS***
    - Determined by OTMA security level
      - NONE | PROFILE | CHECK | ***FULL***

IMS/OTMA Security Options

- **OTMA *client-bid* request**
  - OS/390 subsystem request to connect to IMS
    - In order to subsequently send/receive messages to/from IMS/OTMA
  - RACF FACILITY class

- **Using RACF (or equivalent), IMS can verify**
  - RACF userid and group
  - Userid authority to execute IMS command
    - RACF CIMS | DIMS classes
  - Userid authority to execute IMS transaction
    - RACF TIMS | GIMS classes

OTMA Client-Bid

- **OTMA client must perform 'client-bid' request**
  - Client-bid message must be ***1st*** message passed to IMS
    - Bid message sent after
      - OTMA client has joined same XCF group as IMS

        When IMS joined XCF group 1st
      - IMS '*server available*' message sent to OTMA client

        When OTMA client joined XCF group 1st

- **Client-bid may be rejected**
  - If OTMA client not authorized to FACILITY profile with UACC(READ) or higher
    - Exception
      - OTMA security level is NONE

        Set by: **/SECURE OTMA NONE** command or **OTMASE=N** startup parameter

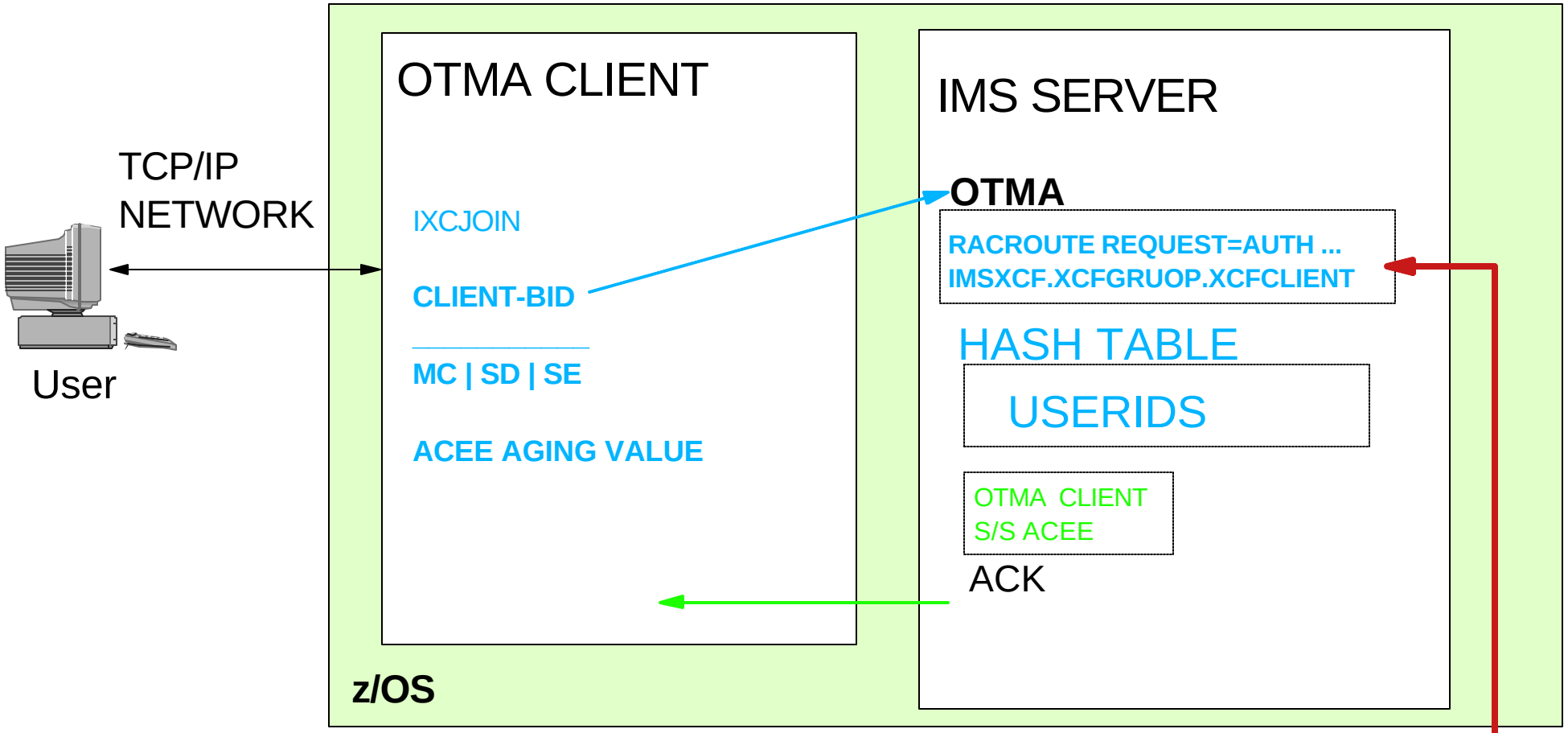
Client-Bid Message

- **Message Control Information (MCI) header**
  - MCI message prefix indicates message is a client-bid message
- **Security Data (SE) header**
  - SE message prefix contains security information associated with input message
    - ***Security flag*** in client-bid message
      - Used when OTMA security level is PROFILE

        OTMASE=P or /SECURE OTMA PROFILE
      - Valid values for security flag

        N | C | F
      - Security flag in bid message ***ignored*** if OTMA security level is **NONE**
  - ***UTOKEN*** if OTMA client verified userid (and optionally, password)
  - ***Userid***
  - ***SAF profile*** (RACF GROUP name)

OTMA Client- Bid Illustration

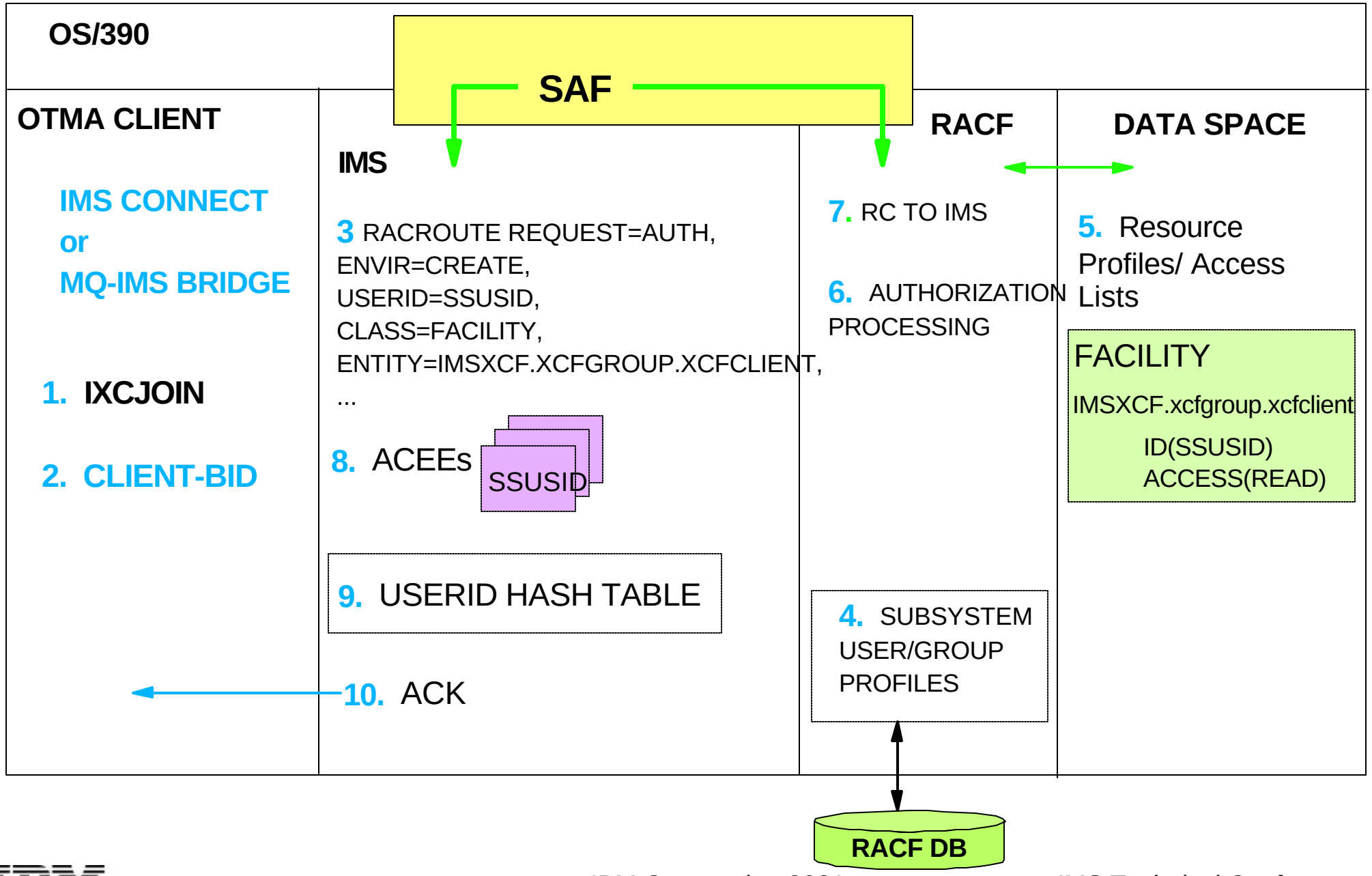


FLOW	SECTION	CONTENT OF PREFIX SECTION
CLIENT-BID	MC	MESSAGE TYPE=COMMAND, COMMAND TYPE=CLIENT-BID , ...
	SD	MEMBER NAME=HWSMEM, ACEE AGING VALUE, HASH TABLE SIZE, ...
	SE	**SECURITY FLAG (N | C | F)** **UTOKEN** **USERID** **SAF PROFILE**

BID IGNORED IF IMS SECURITY LEVEL IS NONE

BID REJECTED IF CLIENT NOT AUTHORIZED

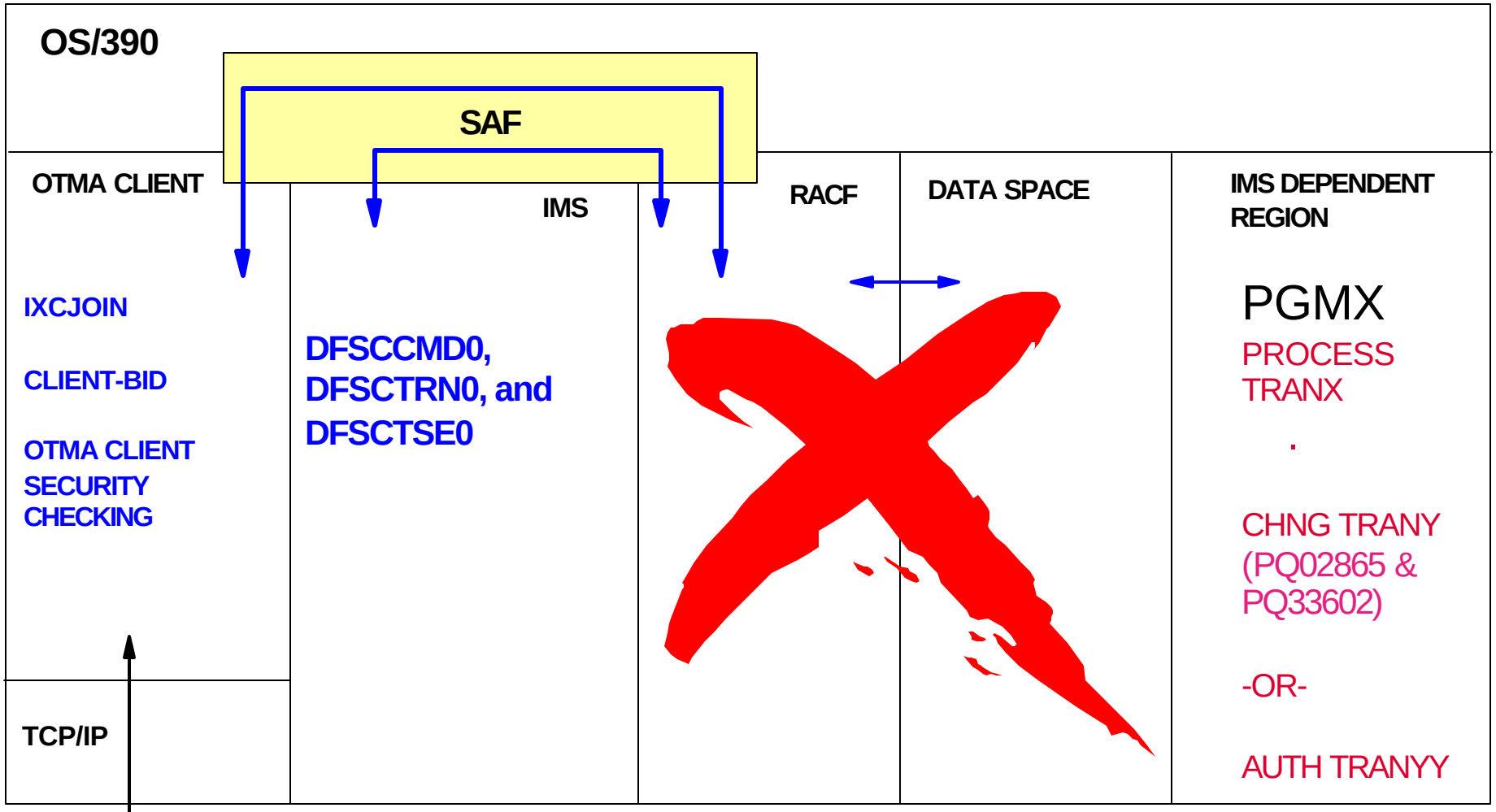
RACF Client-Bid Authorization



OTMA Security Levels

- **IMS OTMA security level set by**
  - OTMASE= startup parameter
    - N | P | C | ***F***
  - /SECURE OTMA command
    - NONE | PROFILE | CHECK | ***FULL*** (default)
    - Command overrides startup parameter
- **Commands**
  - Processed against RACF CIMS | DIMS classes
  - DFSCCMD0 called
    - Command verb passed
- **Transactions**
  - Processed against RACF TIMS | GIMS classes
  - DFSCTRN0 *may be* called
  - DFSCTSE0 called for CHNG and AUTH calls

/SECURE OTMA NONE or OTMASE=N



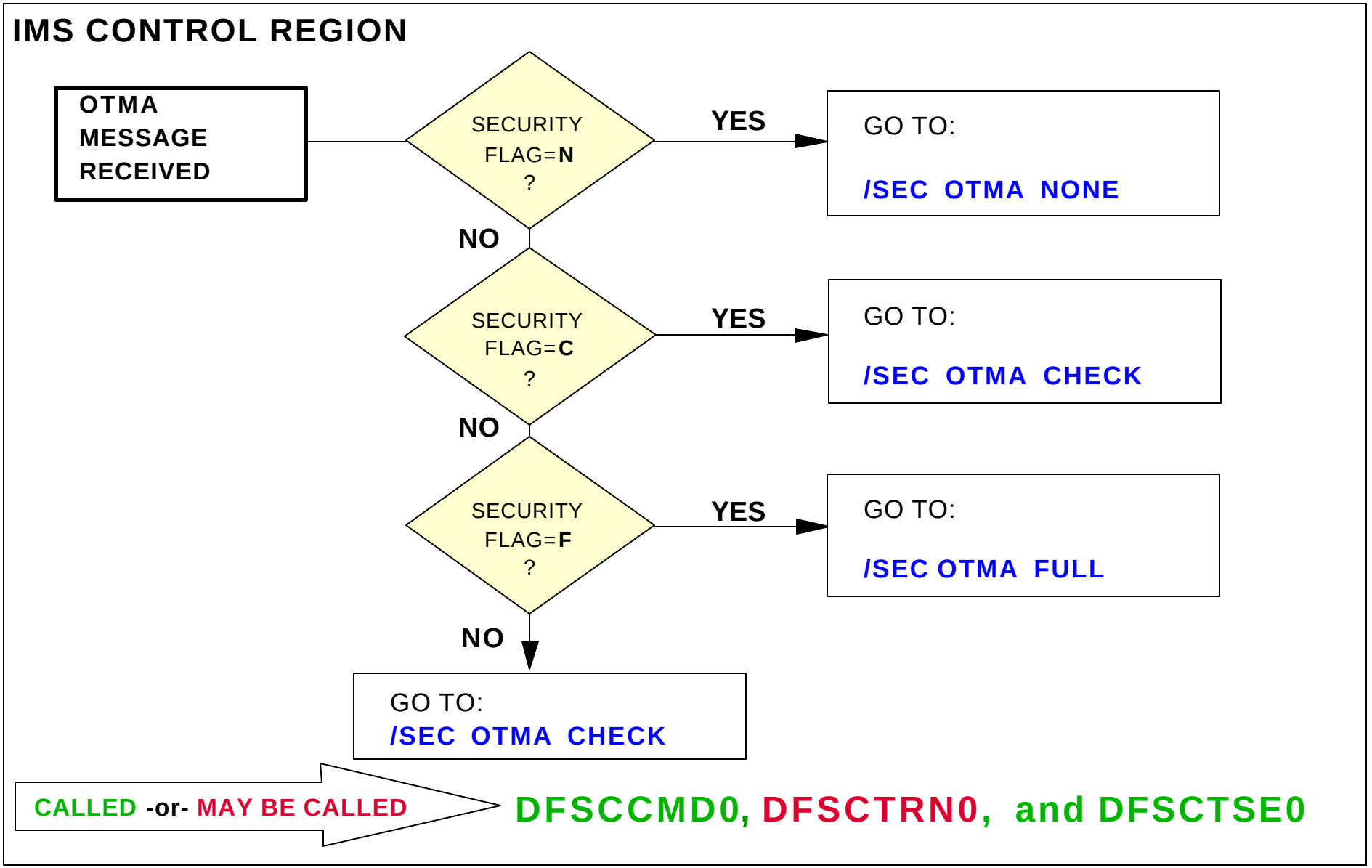
RACF IS NOT CALLED BY IMS FOR MESSAGES RECEIVED VIA OTMA
COMMANDS: /BRO, /LOCK, /LOG, /RDISPLAY, /UNLOCK; DFSCCMD0 EXIT CALLED
TRANSACTIONS: ALL TRANSACTIONS ALLOWED BY RACF; DFSCTRN0 AND DFSCTSE0 EXITS CALLED

/SECURE OTMA PROFILE or OTMASE=P

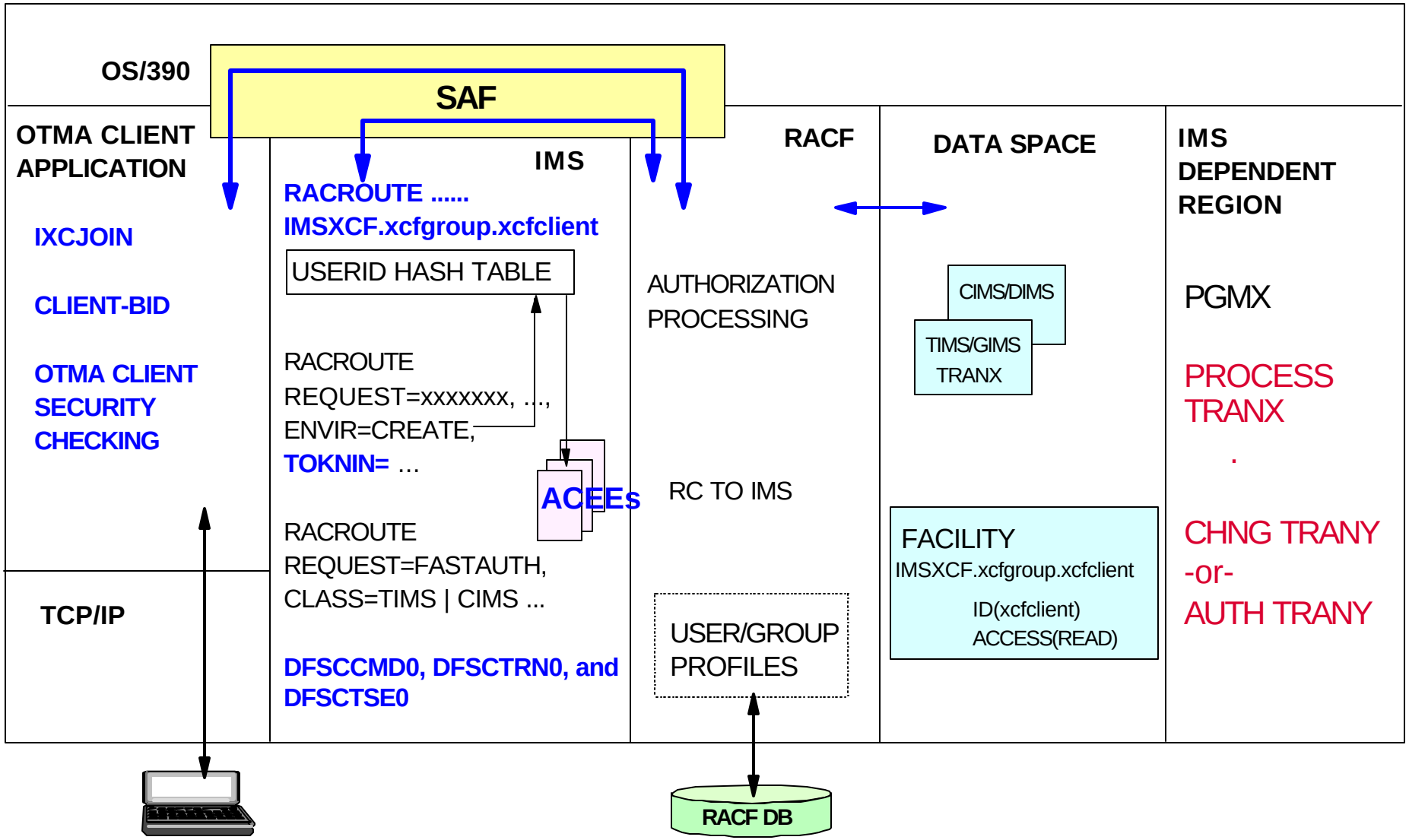
- **Application programmer sets security flag in each message**
  - 1 byte security flag field in SECURITY-DATA section of MCI prefix
  - Flag specification determines whether RACF is called
    - Indicates RACF security checking is
      - N for NONE
      - C for CHECK
      - F for FULL

BYTE	LENGTH	CONTENT	VALUE	MEANING
0	2	LENGTH		LENGTH OF SECURITY-DATA SECTION
2	1	SECURITY FLAG		
			N	NO RACF CHECKING
			C	RACF CHECK TRANSACTIONS AND COMMANDS
			F	RACF CHECKS TRANSACTIONS, COMMANDS, AND REGIONS
...				

PROFILE Illustration

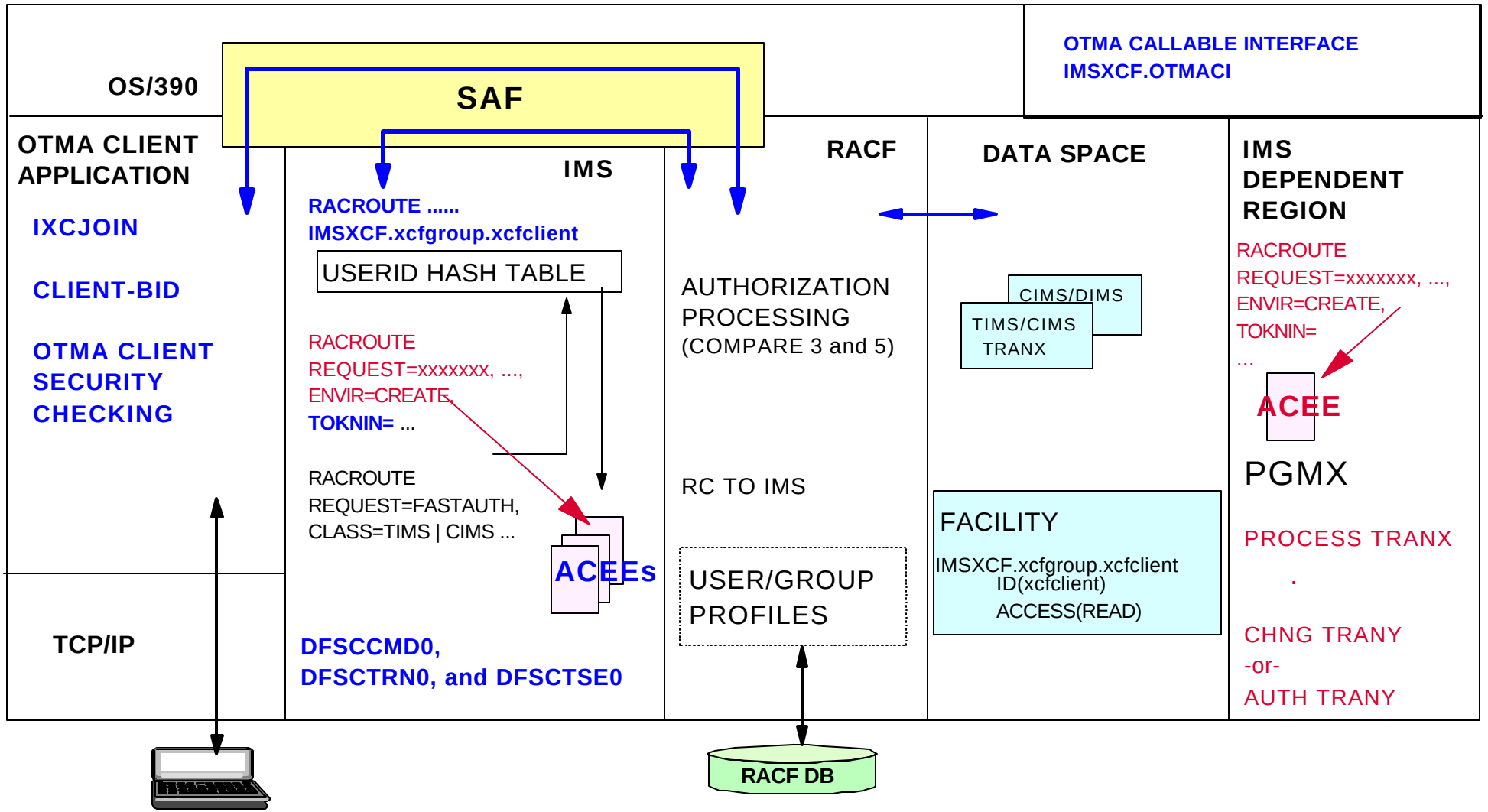


/SECURE OTMA CHECK or OTMASE=C

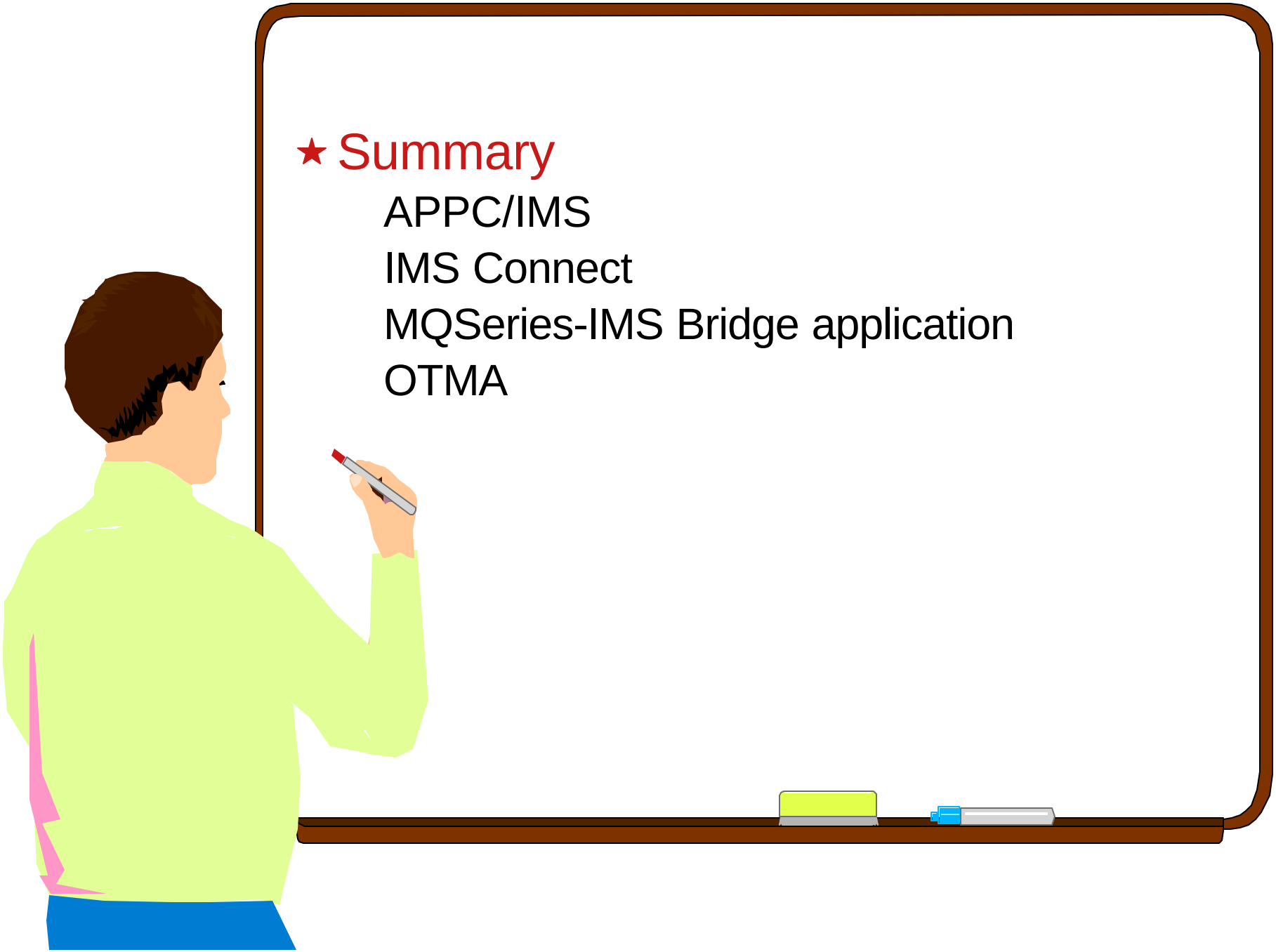


COMMAND | TRANSACTION AUTHORIZED BY RACF IF NO PROFILE
DFSCCMD0 and DFSCTSE0 called; DFSCTSE0 may be called

/SECURE OTMA FULL or OTMASE=F



COMMAND | TRANSACTION AUTHORIZED BY RACF IF NO PROFILE
DFSCCMD0 and DFSCTSE0 CALLED; DFSCTRN0 MAY BE CALLED
SECURITY CONTROL BLOCK (ACEE) COPIED TO IMS DEPENDEN REGION


★ Summary
APPC/IMS
IMS Connect
MQSeries-IMS Bridge application
OTMA

APPC/IMS Summary

- **APPC security options**
  - VTAM
  - MVS
  - IMS
    - Command authorization | transaction authorization
- **APPC/IMS security levels**
  - FULL (the default) | CHECK | PROFILE | NONE
  - Implicit APPC applications
- **APSB/SAF security**
  - Explicit APPC applications

IMS Connect Summary

- **Program Product used to**
  - Transmit messages between TCP/IP clients and IMS
  - Translate ASCII to EBCDIC for input messages
  - Translate EBCDIC to ASCII for output messages

- **Security options**
  - IMS Connect
    - Userid and password verification
    - Obtain UTOKEN for verified userids
  - IMSLSECX or user security exit routine
    - Invoked from user message exit routine
    - Can perform userid (and optionally, password) verification
    - Can verify TCP/IP address and/or port number

MQSeries-IMS Bridge Summary

- **MQSeries for OS/390 (or z/OS)**
  - Program product used to
    - Transmit messages ***asynchronously*** between TCP/IP clients and IMS/OTMA
    - Perform message translation
  - Provides the MQ-IMS Bridge application to send/receive messages to/from IMS/OTMA
- **Security options**
  - Message-based security
    - Userid (and optionally password) verification
    - May be configured to obtain and cache UTOKENs for verified userids
  - MQSeries for OS/390 security
    - Putting a message to the reply-to queue
    - Putting an exception message or confirm-of-arrival report message

IMS/OTMA Summary

- **OTMA provides**
  - Gateway for transaction outside IMS to enter IMS
    - Sends IMS commands | IMS transactions to IMS/OTMA
    - Receives output
- **IMS and OTMA clients**
  - Must be members of the same ***XCF group*** and
  - Use the OTMA protocol
- **OTMA security level determines if RACF called to**
  - Verify userid (and optionally, group) in incoming message
  - Userid authorization to execute IMS command
  - Userid authorization to execute IMS transaction
- **OTMA security levels**
  - NONE | PROFILE | CHECK | ***FULL***