e-business powered by IMS

the world depends on it

IMS and RACF

Alonia (Lonnie) Coleman
IMS Technical Consulting
Dallas Systems Center

Agenda

- **Accessing IMS**
- **Key concepts**
  - IMS resources that may be secured
  - Source of input
  - Security facilities used to secure IMS resources
  - IMS resources that may be secured using RACF
- **IMS-RACF security**
  - Commands
  - Transactions
  - Terminals
  - Control region
  - Data sets
  - Databases
  - Connections to control region
  - Program specification blocks

Presentation objectives:

Provides a basic, high level overview of the security options available in IMS-RACF environments.

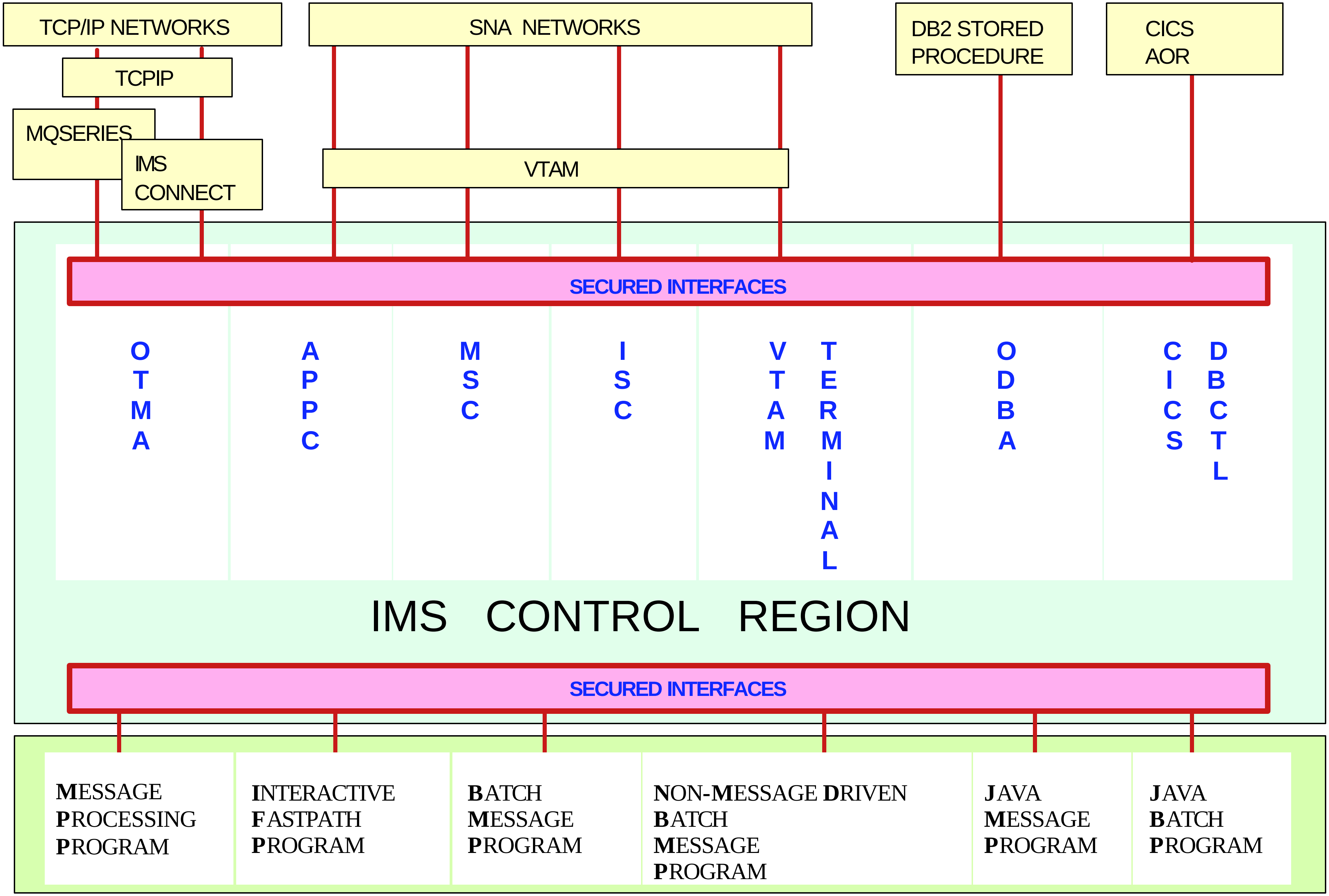
Identify the types of security that are available when access to IMS resources (such as transactions and commands) are entered from various environments (e.g. ETO terminal, APPC terminal, OTMA client, MSC systems, DBCTL environments, etc.).

Acronyms

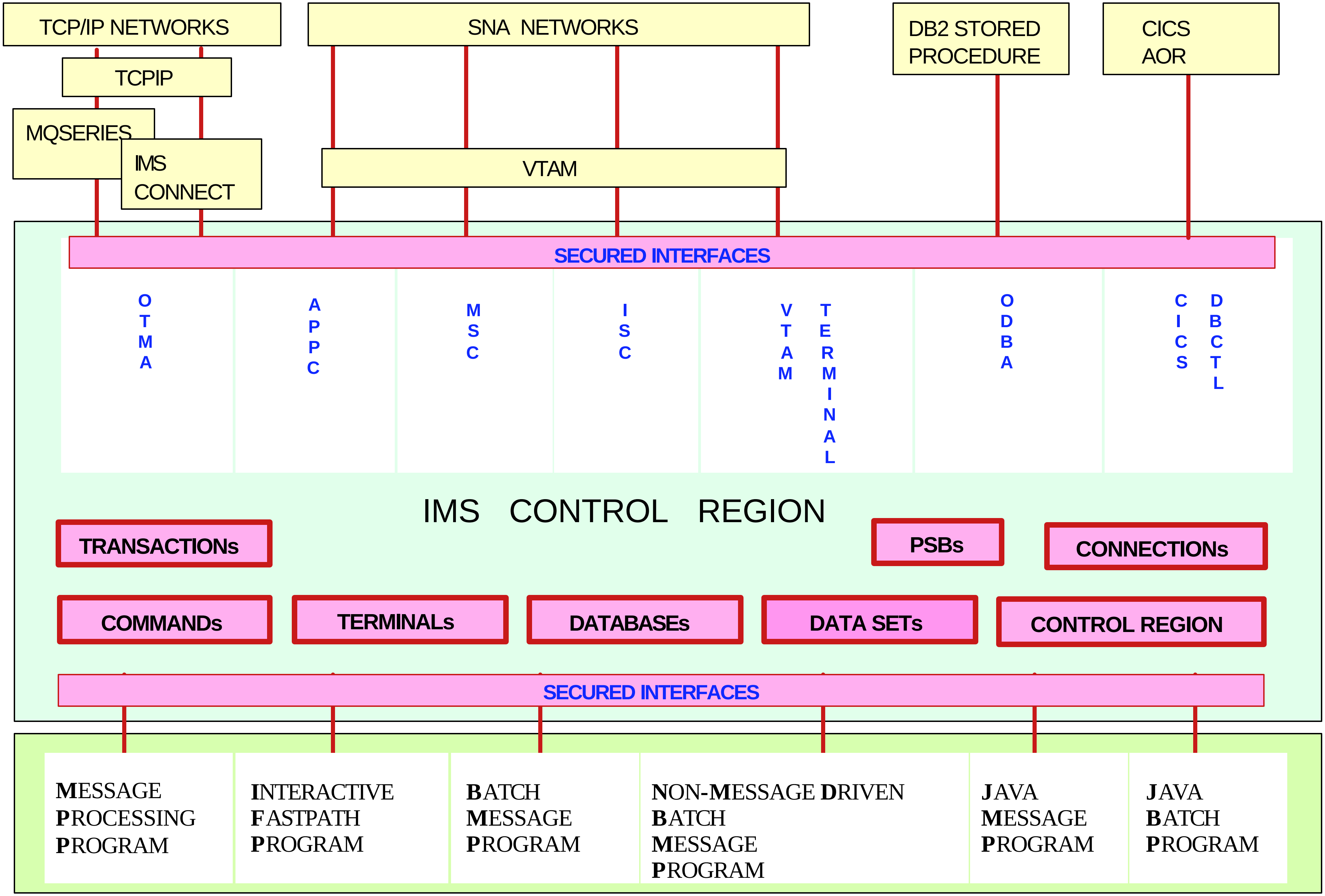
- **IMS acronyms**
  - Information Management System (IMS)
    - Extended Terminal Option (ETO)
    - InterSystems Communications (ISC)
    - Multiple Systems Coupling (MSC)
    - Open Database Access (ODBA)
    - Open Transaction Manager Access (OTMA)
    - Security Maintenance Utility (SMU)
    - Time Controlled Operations (TCO)
    - Program specification block (PSB)
    - Program communications block (PCB)
  - IMS configuration options
    - Database Control (DBCTL)
    - Database/Transaction Manager (DB/TM)
    - Data Communications Control (DCCTL)
  - IMS dependent region types
    - Message processing program (MPP) region
    - Interactive Fas Path (IFP) region
    - Batch Message Processing (BMP) region

- **Other acronyms**
  - Advanced Program-to-Program Communications (APPC)
    - Common Programming Interface for Communications (CPIC)
  - Customer Information Control System (CICS)
  - Resource Access Control Facility (RACF)
  - Virtual Telecommunications Access Method (VTAM)
  - Cross System Coupling Facility (XCF)
  - System Authorization Facility (SAF)

Accessing IMS



IMS Resources That May Be Secured



TCP/IP NETWORKS

TCPIP

MQSERIES

IMS CONNECT

SNA NETWORKS

VTAM

DB2 STORED PROCEDURE

CICS AOR

SECURED INTERFACES

OTMA

APPC

MSC

ISC

VTAM TERMINAL

ODBA

CICS DBCTL

IMS CONTROL REGION

TRANSACTIONs

PSBs

CONNECTIONs

COMMANDs

TERMINALs

DATABASEs

DATA SETs

CONTROL REGION

SECURED INTERFACES

MESSAGE PROCESSING PROGRAM

INTERACTIVE FASTPATH PROGRAM

BATCH MESSAGE PROGRAM

NON-MESSAGE DRIVEN BATCH MESSAGE PROGRAM

JAVA MESSAGE PROGRAM

JAVA BATCH PROGRAM

Source Of Input

- The type of protection available to secure an IMS resource depends on
  - The source of the input of the command, transaction, etc.

- Examples
  - Commands
    - Static terminals, TCO scripts, ETO terminals, OTMA clients, APPC devices, etc.
  - Transactions
    - Static terminals, TCO scripts, ETO terminals, OTMA clients, APPC devices, CHNG call, AUTH call, etc.

Security Facilities Used By IMS

- RACF or equivalent product
  - This presentation focuses on RACF-based security

- Security Maintenance Utility (SMU)

- Installation coded exit routines
  - Command Authorization Exit Routine (DFSCCMD0)
  - Transaction Authorization Exit Routine (DFSCTRN0)
    - Security Reverification Exit Routine (DFSCTSE0)
  - Build Security Environment Exit Routine (DFSBSEX0)

- Security facilities may be used in combination
  - Examples
    - RACF and Command Authorization Exit
    - RACF and Transaction Authorization Exit

- IMS default '**command**' security

IMS Command Sources

- Terminal-entered commands
  - Static terminals
    - And Time Controlled Operations (TCO) scripts
  - ETO terminals

- Automated operator (AO) program-entered commands
  - Two types of AO programs that issue IMS commands
    - Type 1 uses DL/I **CMD** (command) call
      - Must use SMU security
    - Type 2 uses DL/I **ICMD** (issue command) call

- APPC devices

- OTMA clients

- MCS/E-MCS terminals
  - Multiple Console Support / Extended-Multiple Console Support

Securing Terminal-Entered Commands

SECURITY **TYPE=RACFCOM** * Static and ETO *

IMS.PROCLIB(**DFSPBxxx**)

RCF=**C**	* ETO *
RCF=**S**	* Static and ETO *
RCF=**Y**	* ETO, transaction *
RCF=**A**	* Static, ETO, transaction *
RCF=**R**	* RCF=S option without Matrix tables *
RCF=**B**	* RCF=A option without Matrix tables *

/NRE CHECKPOINT 0 **CMDAUTH**	* Static and ETO *
/NRE CHECKPOINT 0 **CMDAUTHE**	* ETO *

/STA**(user_password)** DB PAYDB

IMS.PROCLIB(DFSPBxxx) **RVFY=Y**

'REVERIFY' in APPLDATA section of RACF profile

Securing AO Type 2 Commands

- Automated operator (AO) program that uses DL/I ICMD call
  - IMS type 2 AO programs
  - CICS DBCTL environments
  - ODBA DBCTL environments
- RACF command authorization specified by
  - IMS.PROCLIB(DFSPBxxx) **AOIS=** startup parameter

```
IMS.PROCLIB(DFSPBxxx)
AOIS=R          * RACF for commands issued by AO pgm ICMD call *
AOIS=A          * RACFand Command Authorization Exit *
```

Securing APPC-Entered Commands

- RACF command authorization specified by
  - IMS.PROCLIB(DFSPBxxx) **APPCSE=** startup parameter
  - /SECURE APPC command

IMS.PROCLIB(**DFSPBxxx**)

APPCSE=C

APPCSE=***F***

APPCSE=P with security flag in message set to 'C' or 'F'

/SECURE APPC CHECK

/SECURE APPC ***FULL***

/SECURE APPC PROFILE with security flag in message set to 'C' or 'F'

- Commands executed in IMS control region, only needs CHECK

Securing OTMA Client-Entered Commands

- RACF command authorization specified by
  - IMS.PROCLIB(DFSPBxxx) **OTMASE=** startup parameter
  - /SECURE OTMA command

IMS.PROCLIB(**DFSPBxxx**)
OTMASE=C
OTMASE=***F***
OTMASE=P with security flag in message set to 'C' or 'F'

/SECURE OTMA CHECK
/SECURE OTMA ***FULL***
/SECURE OTMA PROFILE with security flag in message set to 'C' or 'F'

- Commands executed in IMS control region, only needs CHECK

Securing MCS/E-MCS-Entered Commands

- Commands issued from SDSF consoles
- RACF command authorization specified by
  - IMS.PROCLIB(DFSPBxxx) **CMDMCS=** startup parameter

```
IMS.PROCLIB(DFSPBxxx)
CMDMCS=R    * RACF for commands issued by MCS/E-MCS consoles *
CMDMCS=B    * RACF and Command Authorization Exit *
```

Command Security Considerations

- RACF ***cannot*** be used to secure Type 1 AO program issued commands
  - DL/I **CMD** (command) call

- RACF may be used to secure command verbs only for IMS V7 (or lower) systems

- RACF command resource classes may contain 3 character command profiles
  - Examples: DIS, STA, STO, DBR, ...

- Command Authorization Exit invoked (if included in system) after RACF for
  - Terminal-entered commands
  - APPC-entered commands
  - OTMA-entered commands
  - MCS/E-MCS-entered commands
  - Type 2 AO ICMD call issued commands

IMS Default Security

- Default command security automatically provided by IMS
  - When security facility is not specified for commands entered from each command input source (e.g. terminal, OTMA, Type 2 AO program, etc.
  - Limits commands that may be entered to IMS command subset
    - Subset for each source listed in *'Command Reference'* manual
  - Can be deactivated by using RACF (and/or a user exit) to secure commands from that source

RACF Command Examples

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

```
RDEF DIMS IMSUSER ADDMEM(DIS STA) OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSUSER CLASS(DIMS)  ACCESS(READ)
ID(GROUPY MCSUSRS TCOUSID CICSUSID ODBAUSID OTMAUSRS APPCUSRS)
```

```
RDEFINE DIMS AOCMDS ADDMEM(ASS CHA) OWNER(IMSADMIN) UACC(NONE)
PERMIT AOCMDS CLASS(DIMS) ID(T2AOUSID GROUPZ) ACCESS(READ)
```

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

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

IMS Transaction Sources

- Terminal-entered transaction codes
  - Static terminals
    - And Time Controlled Operations (TCO) scripts
  - ETO terminals
- APPC devices
- OTMA clients
- Application programs

DL/I **CHNG call** destination is a transaction code
DL/I **AUTH call** CLASSNAME specified as TRAN and RESOURCE is a transaction code
DL/I **ISRT call** when scratch pad area (SPA) is inserted for a conversational transaction

- Transaction code specified on an IMS command
  - **SMU** password security (rather than RACF) used to secure transactions referenced by the following commands

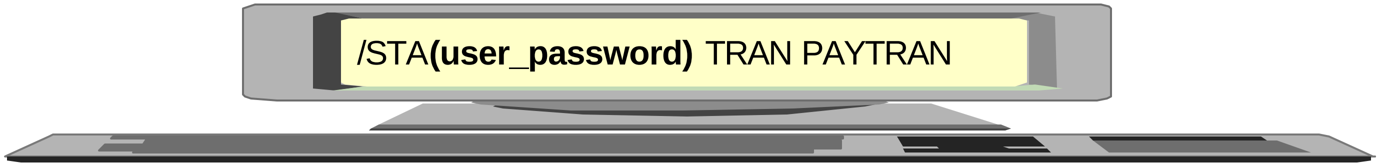
```
/SET TRANSACTION trancode (password)
/LOCK TRANSACTION trancode (password)
/UNLOCK TRANSACTION trancode (password)
```

Securing Terminal-Entered Transactions

```
SECURITY RCLASS=xxxxxxx
         SECLVL=TRANAUTH * (or SECLVL=FORCTRAN) *
         TYPE=RACFTERM
```

```
IMS.PROCLIB(DFSPBxxx)

TRN=Y or TRN=F or TRN=E or TRN=X
RCF=T          * Transaction *
RCF=Y          * Transaction, ETO commands *
RCF=A          * Transaction*, static and ETO commands *
RCF=B          * RCF=A option without Matrix tables *
```

```
/NRE CHECKPOINT 0 TRANAUTH        * Transaction *
```



```
/STA(user_password) TRAN PAYTRAN
```

IMS.PROCLIB(DFSPBxxx) **RVFY=Y**
'REVERIFY' in APPLDATA section of RACF profile

Securing APPC-Entered Transactions

- RACF transaction authorization specified by
  - IMS.PROCLIB(DFSPBxxx) **APPCSE=** startup parameter
  - /SECURE APPC command

IMS.PROCLIB(**DFSPBxxx**)
APPCSE=C
APPCSE=***F***
APPCSE=P with security flag in APPC message set to 'C' or 'F'

/SECURE APPC CHECK
/SECURE APPC ***FULL***
/SECURE APPC PROFILE with security flag in APPC message set to 'C' or 'F'

Securing OTMA Client-Entered Transactions

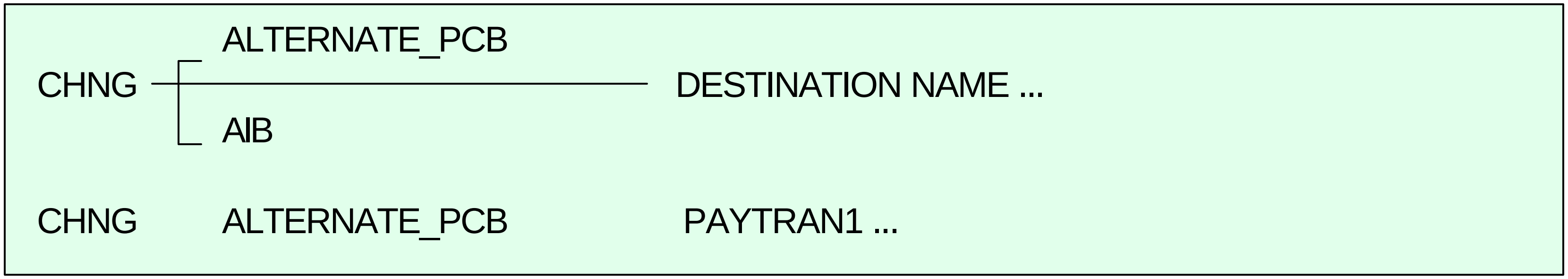
- RACF transaction authorization specified by
  - IMS.PROCLIB(DFSPBxxx) **OTMASE=** startup parameter
  - /SECURE OTMA command

IMS.PROCLIB(**DFSPBxxx**)
OTMASE=C
OTMASE=***F***
OTMASE=P with security flag in OTMA message set to 'C' or 'F'

/SECURE OTMA CHECK
/SECURE OTMA ***FULL***
/SECURE OTMA PROFILE with security flag in OTMA message set to 'C' or 'F'

Application Program-Entered Transactions

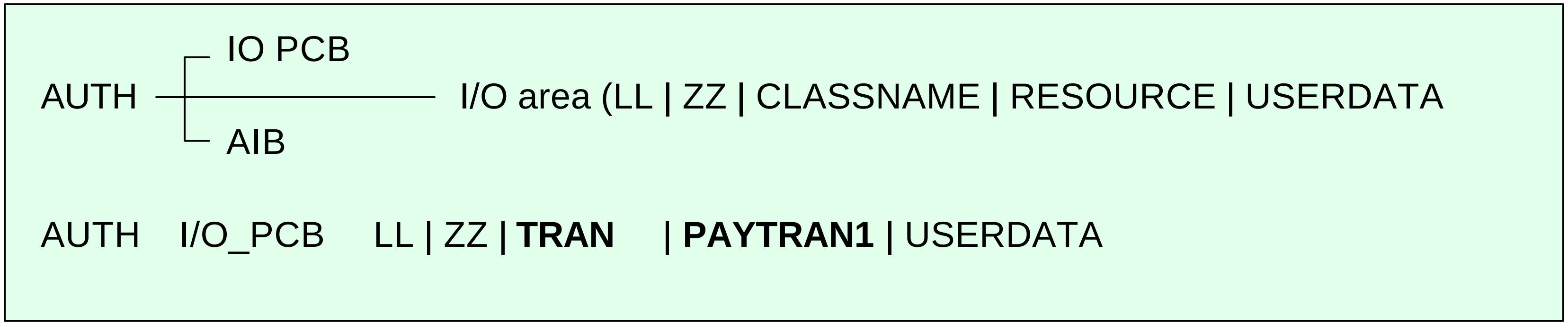
- Applications running in dependent regions may issue 1 or more
  - **CHNG** calls with transaction code set as the destination name



CHNG ALTERNATE_PCB | AIB DESTINATION NAME ...

CHNG ALTERNATE_PCB PAYTRAN1 ...

  - **AUTH** calls with CLASSNAME specified as TRAN and RESOURCE specifies transaction code



AUTH IO PCB | AIB I/O area (LL | ZZ | CLASSNAME | RESOURCE | USERDATA

AUTH I/O_PCB LL | ZZ | **TRAN** | **PAYTRAN1** | USERDATA

  - SPA **ISRT** for conversational program-to-program switches that occur to a transaction code

Securing Appl Program-Entered Transactions

- Security specified the same way as for terminal-entered transactions
  - Exception
    - Password 'REVERIFY' not applicable

```
SECURITY RCLASS=xxxxxxx
                  SECLVL=TRANAUTH * (or SECLVL=FORCTRAN) *
                  TYPE=RACFTERM
```

```
IMS.PROCLIB(DFSPBxxx)
TRN=Y or TRN=F or TRN=E or TRN=X
RCF=T          * Transaction *
RCF=Y          * Transaction, ETO commands *
RCF=A          * Transaction*, static and ETO commands *
RCF=B          * RCF=A option without Matrix tables *
```

```
/NRE CHECKPOINT 0 TRANAUTH          * Transaction *
```

Transaction Security Considerations

- Application programs that process transactions from APPC and/or OTMA sources may issue DL/I CHNG and/or AUTH calls
  - The APPC and/or OTMA security level may impact performance for request to RACF to perform security checking
  - Consideration should be given to whether a security level of CHECK -versus- FULL -versus- PROFILE is more appropriate

CHECK may be most appropriate if CHNG | AUTH calls ***not*** issued by most application programs

FULL may be most appropriate if CHNG | AUTH calls ***are*** issued by most application programs

PROFILE may be most appropriate if there is a ***mixture***

Some applications do not issue CHNG nor AUTH calls

Some applications issue CHNG and/or AUTH calls

Some transactions received from APPC and/or OTMA do not require transaction authorization checking and a security level of **NONE** is desired for these transactions

Examples: Transaction received from a trusted source
Transaction security is not desired

Transaction Security Considerations ...

- OTMA security level NONE
  - APARs needed to disable transaction security checking resulting from CHNG and/or AUTH call
    - APARs PQ02865 and PQ33602
- Installation coded transaction security exit routines are invoked
  - Unconditionally when RACF (or equivalent) is not used
  - After RACF when used in conjunction with RACF
    - Transaction Authorization Exit (DFSCTRN0)
      - Called prior to queuing message to message queue
      - Called for CHNG calls, AUTH calls, and deferred conversational program-to-program message switches
      - Exception: Not invoked if RACF denies access to transaction
    - Security Reverification Exit Routine (DFSCTSE0)
      - Called for CHNG and AUTH calls regardless of RACF return code
    - Exits are passed RACF return code and may override RACF decision to grant/deny access to the requested transaction

RACF Transaction Examples

```
RDEFINE TIMS TRANA  UACC(NONE)
PERMIT TRANA CLASS(TIMS) ID(OTMAUSRS APPCUSRS GROUPX) ACCESS(READ)

RDEFINE GIMS PAYTRANS  ADDMEM(PAYRAISE,PAYDECR,PAYROLL) UACC(NONE)
PERMIT PAYTRANS CLASS(GIMS)  ID(GROUPY TCOSUID) ACCESS(READ)

RDEFINE TIMS TRANB APPLDATA('REVERIFY') UACC(NONE)
PERMIT DEBSTRN2 CLASS(TIMS) ID(GROUPZ) ACCESS(READ)
```

Securing IMS Terminals

- IMS terminal types

VTAM nodes **ETO terminals** **Static terminals**	**BTAM terminals**	**Logical terminals (LTERMs)**

- RACF
  - May be used to secure VTAM nodes and BTAM terminals
  - Uses profiles in the **TERMINAL** and **GTERMINL** resources classes in terminal authorization checking
    - Terminal profile names must match
      - Node names (VTAM ETO and static terminals)
      - Line and terminal combination (BTAM terminals)
  - Terminal authorization checking performed during
    - Logon to TSO and/or sign on to IMS
- To activate RACF terminal security checking

SECURITY SECLVL=(...,SIGNON) or SECURITY SECLVL=(...,FORCSIGN), **TYPE=(...,RACFTERM)**
IMS.PROCLIB(DFSPBxxx) SGN=Y (or F, Z, G, W, X, D, or E) **RCF=T (or Y, A, or B)**

Terminal Security Considerations

- RACF provides 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.

RACF Terminal Examples

```
RDEFINE TERMINAL NODE1234 UACC(NONE)
PERMIT NODE1234 CLASS(TERMINAL) ID(GROUP01 GROUP02) ACCESS(READ)

RDEFINE TERMINAL NODE2345 UACC(NONE)
PERMIT NODE2345 CLASS(TERMINAL) ID(GROUP01 GROUP02) ACCESS(READ)
      WHEN(DAYS(WEEKDAYS))
```

Securing the IMS Control Region

- RACF may be used to secure access to the IMS control region
- Use the RACF **APPL** class to
  - Restrict access to IMS to authorized users
  - Restrict access to specific terminals (optional)
  - Control ATTACH requests
    - Protect conversations between partner LUs
    - Access is granted or denied based on userid and origin LU

RACF Control Region Examples

```
RDEFINE APPL IMSA OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSA CLASS(APPL) ID(GROUP1,GROUP2) ACCESS(READ)
```

```
RDEF APPL  IMSA OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSA CLASS(APPL)  ID(USERID1) ACCESS(READ)
         WHEN(TERMINAL(NODE1234))
```

```
RDEFINE APPL  local_LU_name  UACC(NONE)
PERMIT local_LU_name  CLASS(APPL)
           ID(GROUP1) ACCESS(READ)
            WHEN(APPCPORT(partner_LU_name))
```

```
IMSCTRL SYSTEM=(VS/2,(ALL,DB/DC),390),
IRLM=YES,
IRLMNM=IRLM,
CMDCHAR=,
DBRC=(YES,YES),
DBRCNM=IMS8DBRC,
DLINM=IMS8DLI,
DCLWA=YES,
IMSID=IMSA,
NAMECHK=(YES,S1),
MAXREGN=(15,512K,A,A),
MCS=(2,7),
DESC=7,
ETOFEAT=(YES,YES,ALL),
MAXCLAS=016
```

NOTE: APPL profile names match value specified on **IMSID=** keyword

Securing IMS Data Sets

- IMS data sets may be secured using RACF
  - Database data sets
  - IMS system libraries
    - IMS.JOBS
    - IMS.TCFSLIB
    - IMS.RECON# (where # is 1, 2, and/or 3)
  - User program libraries

- Data set profiles are created in the RACF DATASET class
  - Authorize the userid/group of
    - The IMS control region
    - DL/I address space
    - Or both of the above

RACF Data Set Examples

```
ADDSD  'IMS.JOBS'  UACC(NONE) GENERIC
PERMIT 'IMS.JOBS'  ID(IMSUSRID DLIUSRID) ACCESS(UPDATE)

ADDSD  'IMS.TCFSLIB'  UACC(NONE) GENERIC
PERMIT 'IMS.TCFSLIB'  ID(IMSUSRID GROUPB) ACCESS(UPDATE)

ADDSD  'IMS.RECON1'  UACC(NONE) GENERIC
PERMIT 'IMS.RECON1'  ID(IMSUSRID DBRCUSID DLIUSRID) ACCESS(UPDATE)

ADDSD  'PARTS.DBDS'  UACC(NONE) GENERIC
PERMIT 'PARTS.DBDS'  ID(GROUPA DLIUSRID) ACCESS(UPDATE)
```

NOTE:

The ADDSD (add data set descriptor) command is used to create data set profiles in the DATASET class.

Securing IMS Databases

- IMS database security is provided by RACF in conjunction with the DL/I **AUTH** (authorization) call.

- RACF resource classes used for IMS database security include the following:

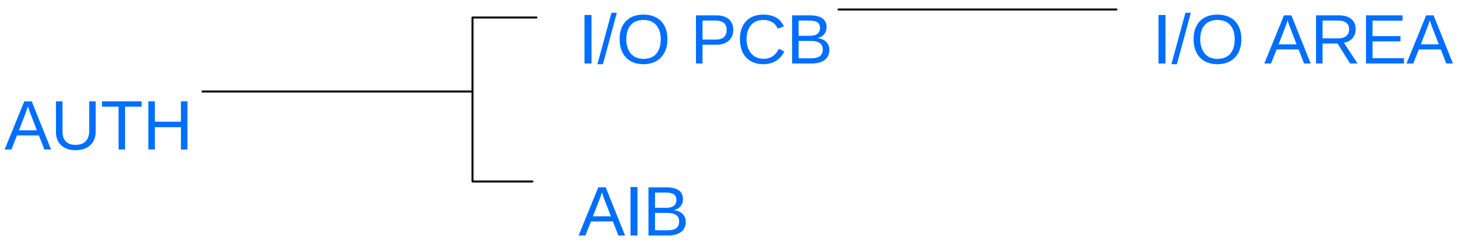
PIMS	QIMS	Database classes
SIMS	UIMS	Segment classes
FIMS	HIMS	Field classes
OIMS	WIMS	Other classes

  - These classes are used in application based security checking
    - An application program issues the DL/I AUTH call to request information in
      - Profiles in the above resource classes
      - The ACEE that was created for a userid

- The application program grants or denies access to the data
  - Based on the userid of the user that entered the transaction

DL/I AUTH Call

- Application program's I/O area ***before*** AUTH call is issued



AUTH

I/O PCB

I/O AREA

AIB

LL (2)	##
ZZ (8)	00
CLASSNAME (8)	DATABASE
RESOURCE (8)	PAYDB___
USERDATA (8)	USERDATA

DL/I AUTH Call ...

- Application program's I/O area ***after*** AUTH call is issued
  - Application program uses installation data returned by AUTH call to decide whether to grant or deny authorization

DESCRIPTION OF CONTENTS OF I/O AREA AFTER AUTH CALL

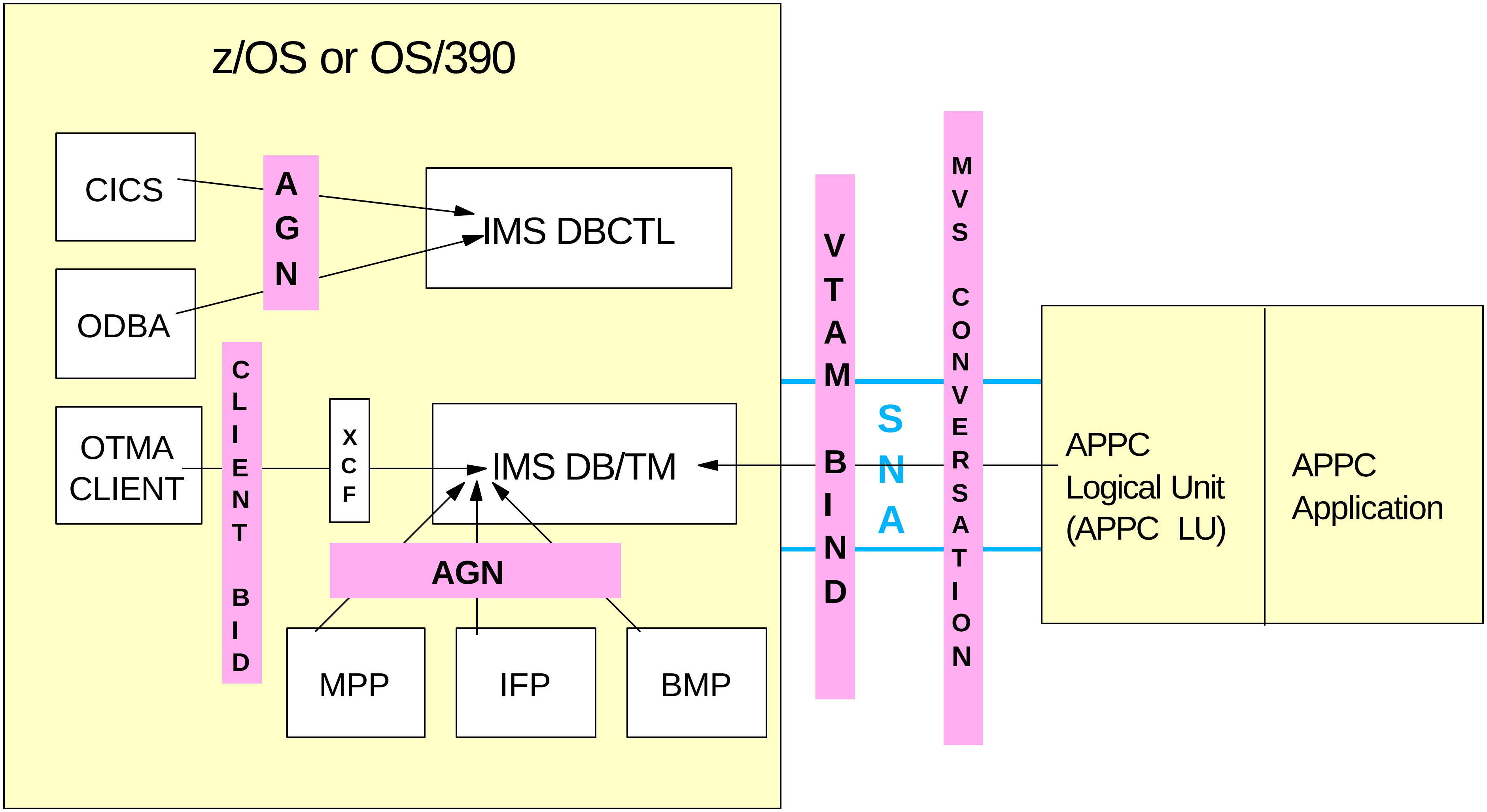
LL	1054	
ZZ	00	
FEEDBACK	00 04 08 0C 10	RACF RETURN CODE: USERID IS AUTHORIZED RESOURCE OR CLASS NOT DEFINED USERID IS NOT AUTHORIZED RACF IS NOT ACTIVE INVALID INSTALLATION OR EXIT RETURN CODE
EXITRC	NEGATIVE (0) 4 8	RETURN CODE FROM LAST EXIT (DFSCTRN0 OR DFSCTSE0) ENTERED: USERID IS AUTHORIZED RESOURCE IS NOT PROTECTED USERID IS NOT AUTHORIZED
STATUS	00 04 08 0C 10 14 18	INSTALLATION DATA STATUS RACF INSTALLATION DATA PRESENT IN I/O AREA DFSCTRN0/DFSCTSE0 INSTALLATION DATA PRESENT IN I/O AREA USERID IS NOT CURRENTLY SIGNED ON USERID IS NOT AUTHORIZED - INSTALLATION DATA NOT RETURNED, OR USERID IS AUTHORIZED - BUT INSTALLATION DATA NOT DEFINED USERID IS AUTHORIZED - BUT INSTALLATION DATA NOT REQUESTED USERDATA EXCEEDS PSBWORK AREA LENGTH RACF NOT ACTIVE AND TRN=N HAS BEEN SPECIFIED
RESERVED	0000000000000000	
UL	00	2-BYTE FIELD THAT SPECIFIES LENGTH OF THE INSTALLATION DATA, INCLUEING LENGTH OF THE UL PARAMETER
USERDATA		UP TO 1026 BYTES OF INSTALLATION DATA: FROM THE ACEE FOR THE USERID RETURNED BY DFSCTRN0 OR DFSCTSE0

RACF IMS Database Example

```
RDEFINE PIMS PAYDB DATA('PAYROLL DATABASE RECORDS') UACC(NONE)
PERMIT PAYDB CLASS(PIMS) ID(GROUPX) ACCESS(READ)

RDEFINE SIMS SALARY DATA('SALARY SEGMENT') UACC(NONE)
PERMIT SALARY CLASS(SIMS) ID(GROUPY) ACCESS(READ)

RDEFINE FIMS HOURLY DATA('HOURLY WAGE FIELD') UACC(NONE)
PERMIT HOURLY CLASS(FIMS) ID(GROUPX) ACCESS(READ)

RDEFINE OIMS DB2VIEW DATA('OTHER - DB2 TABLE VIEW') UACC(NONE)
PERMIT DB2VIEW CLASS(OIMS) ID(GROUPY) ACCESS(READ)
```

Connection Requests

- Requests to connect to IMS are made from several sources



Types of Security For Connection Requests

- Application Group Name (AGN)

- Client-bid

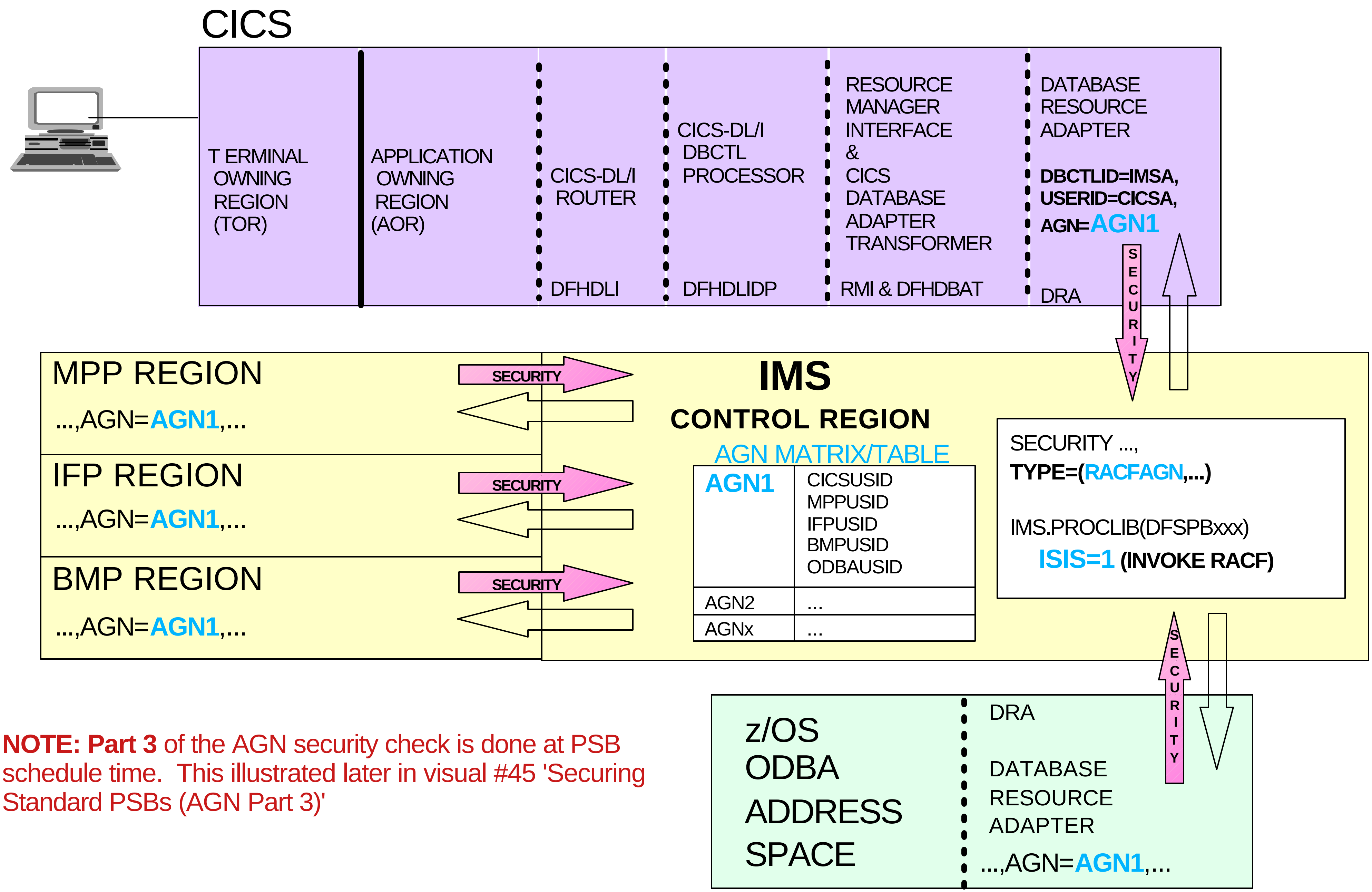
- VTAM session bind and/or APPC/MVS conversational-levels
  - Too many options to cover in this presentation
  - If you require additional information
    - Refer to
      - APPC/VTAM manuals
      - z/OS or OS/390 APPC/MVS manuals
      - Contact IBM

AGN Security

- **Application Group Name (AGN) security is**
  - A three-part security check, where all 3 checks are required
    1. Connection security check
    2. AGN *'name validation'* check
    3. PSB schedule security check
  - Used for connection requests from
    - IMS dependent regions accessing IMS TM system
      - MPPs, IFPs, and BMPs
    - CICS application owning regions accessing DBCTL
    - z/OS and OS/390 ODBA address spaces accessing DBCTL
  - Provided by RACF (or user exit) ***and*** SMU AGN table/matrix
  - Activated by

```
SECURITY TYPE=(RACFAGN,...) or SECURITY TYPE=(AGNEXIT,...)
IMS.PROCLIB(DFSPBxxx) ISIS=1 or ISIS=2
```

AGN Security (Parts 1 and 2)



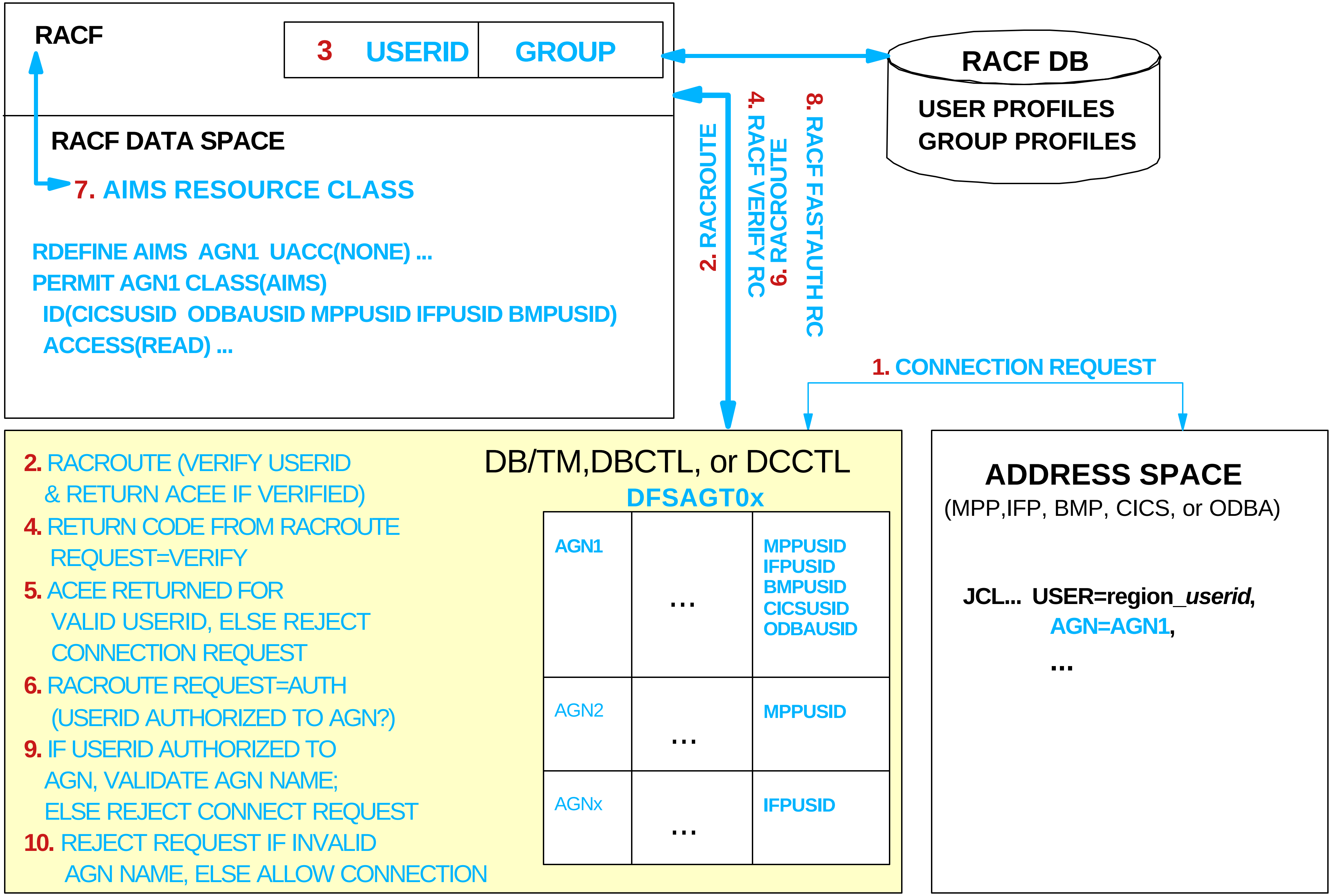
AGN1	CICSUSID MPPUSID IFPUSID BMPUSID ODBAUSID
AGN2	...
AGNx	...

SECURITY ...,
TYPE=(RACFAGN,...)

IMS.PROCLIB(DFSPBxxx)
ISIS=1 (INVOKE RACF)

NOTE: Part 3 of the AGN security check is done at PSB schedule time. This illustrated later in visual #45 'Securing Standard PSBs (AGN Part 3)'

AGN (Parts 1 and 2) and RACF Processing



RACF

3 USERID GROUP

RACF DB

USER PROFILES
GROUP PROFILES

RACF DATA SPACE

7. AIMS RESOURCE CLASS

```
RDEFINE AIMS  AGN1  UACC(NONE) ...
PERMIT AGN1 CLASS(AIMS)
  ID(CICSUSID  ODBAUSID MPPUSID IFPUSID BMPUSID)
  ACCESS(READ) ...
```

2. RACROUTE

4. RACF VERIFY RC

6. RACROUTE

8. RACF FASTAUTH RC

1. CONNECTION REQUEST

DB/TM,DBCTL, or DCCTL

2. RACROUTE (VERIFY USERID
& RETURN ACEE IF VERIFIED)
4. RETURN CODE FROM RACROUTE
REQUEST=VERIFY
5. ACEE RETURNED FOR
VALID USERID, ELSE REJECT
CONNECTION REQUEST
6. RACROUTE REQUEST=AUTH
(USERID AUTHORIZED TO AGN?)
9. IF USERID AUTHORIZED TO
AGN, VALIDATE AGN NAME;
ELSE REJECT CONNECT REQUEST
10. REJECT REQUEST IF INVALID
AGN NAME, ELSE ALLOW CONNECTION

DFSAGT0x

AGN1	...	MPPUSID IFPUSID BMPUSID CICSUSID ODBAUSID
AGN2	...	MPPUSID
AGNx	...	IFPUSID

ADDRESS SPACE
(MPP,IFP, BMP, CICS, or ODBA)

```
JCL... USER=region_userid,
       AGN=AGN1,
       ...
```

Client-Bid Security

- Controls/secures connection requests to IMS/OTMA from OTMA clients such as IMS Connect and MQSeries-IMS Bridge
  - IMS/OTMA security level of **CHECK** or **FULL** activates security

/SECURE OTMA **FULL** -or- IMS.PROCLIB(DFSPBxxx) **OTMASE=F**

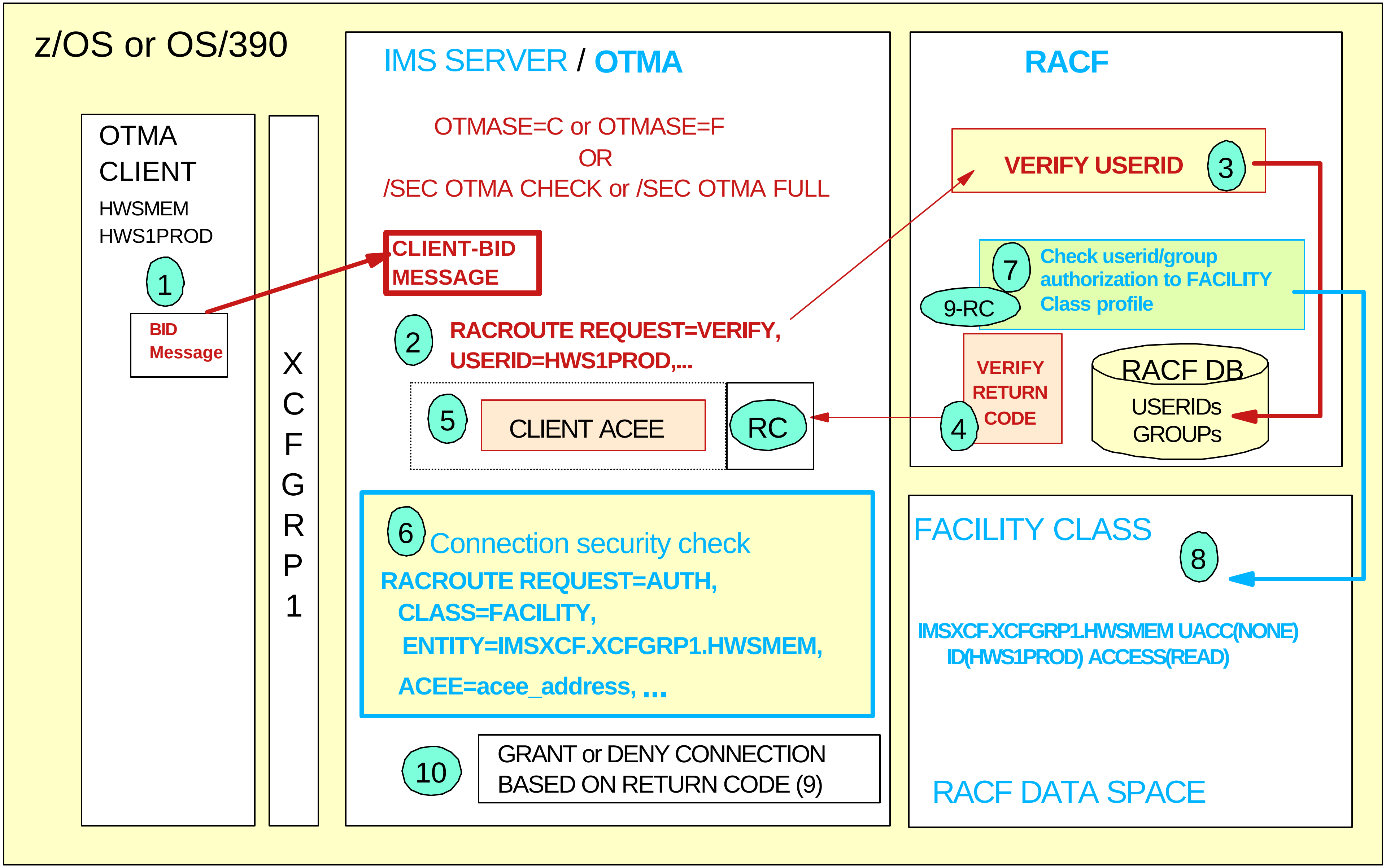
/SECURE OTMA **CHECK** -or- IMS.PROCLIB(DFSPBxxx) **OTMASE=C**

/SECURE OTMA PROFILE -or- IMS.PROCLIB(DFSPBxxx) **OTMASE=P**
AND THE SECURITY FLAG BYTE CONTENT OF '**C**' -or- '**F**'

- IMS/OTMA invokes RACF upon receipt of client-bid (connection request) message
- RACF profile(s) created in the FACILITY resource class
  - Profile naming convention is used

IMSXCF.*xcf_group_name*.*xcf_member_name_of_OTMA_client*

Client-Bid Authorization Checking



z/OS or OS/390

OTMA CLIENT

HWSMEM

HWS1PROD

1

BID Message

XCFGRP1

IMS SERVER / **OTMA**

OTMASE=C or OTMASE=F
OR
/SEC OTMA CHECK or /SEC OTMA FULL

CLIENT-BID MESSAGE

2 **RACROUTE REQUEST=VERIFY, USERID=HWS1PROD,...**

5 CLIENT ACEE

RC

6 Connection security check

RACROUTE REQUEST=AUTH,
CLASS=FACILITY,
ENTITY=IMSXCF.XCFGRP1.HWSMEM,
ACEE=acee_address, ...

10 GRANT or DENY CONNECTION
BASED ON RETURN CODE (9)

RACF

VERIFY USERID 3

7 **Check userid/group authorization to FACILITY Class profile**

9-RC

VERIFY RETURN CODE 4

RACF DB

USERIDs

GROUPs

FACILITY CLASS 8

IMSXCF.XCFGRP1.HWSMEM UACC(NONE)
ID(HWS1PROD) ACCESS(READ)

RACF DATA SPACE

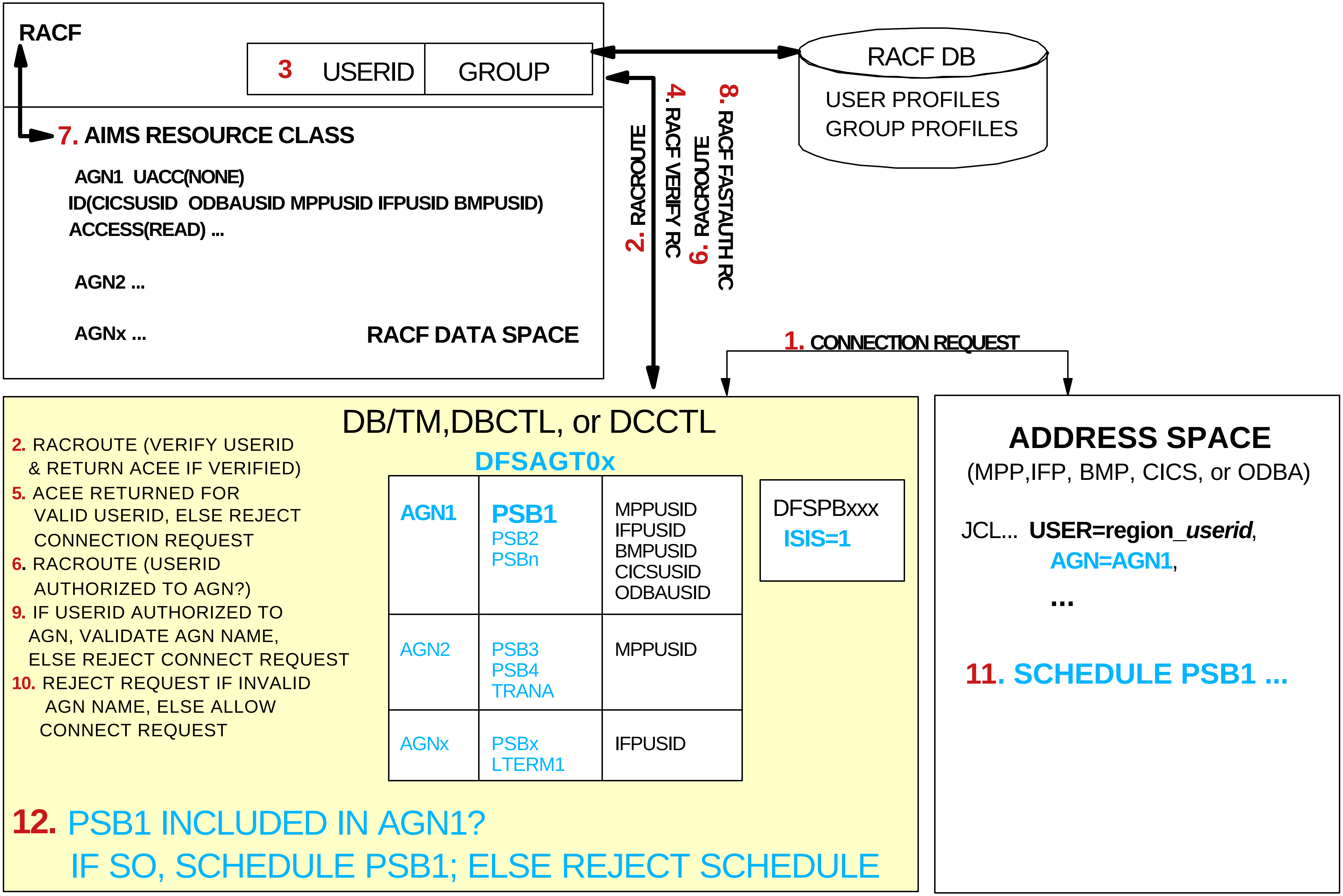
IMS PSB Types

- IMS has two types of program specification blocks (PSBs)
  - Standard PSBs
  - CPIC-driven PSBs
    (Common Programming Interface for Communications)
    - APPC/IMS applications

- Standard PSBs are secured using SMU security
  - PSB is secured in AGN using AGN security
    - Part 3 of the AGN security checking process

- CPIC-driven PSBs are secured using APSB - SAF security
  - Allocate PSB - System Authorization Facility (APSB-SAF) security is provided by RACF

Securing Standard PSBs (AGN Part 3)



RACF

3 USERID | GROUP

7. AIMS RESOURCE CLASS

AGN1 UACC(NONE)
ID(CICSUSID ODBAUSID MPPUSID IFPUSID BMPUSID)
ACCESS(READ) ...

AGN2 ...

AGNx ...

RACF DATA SPACE

RACF DB

USER PROFILES
GROUP PROFILES

2. RACROUTE

4. RACF VERIFY RC

6. RACROUTE

8. RACF FASTAUTH RC

1. CONNECTION REQUEST

DB/TM,DBCTL, or DCCTL

2. RACROUTE (VERIFY USERID
& RETURN ACEE IF VERIFIED)
5. ACEE RETURNED FOR
VALID USERID, ELSE REJECT
CONNECTION REQUEST
6. RACROUTE (USERID
AUTHORIZED TO AGN?)
9. IF USERID AUTHORIZED TO
AGN, VALIDATE AGN NAME,
ELSE REJECT CONNECT REQUEST
10. REJECT REQUEST IF INVALID
AGN NAME, ELSE ALLOW
CONNECT REQUEST

DFSAGT0x

AGN1	PSB1 PSB2 PSBn	MPPUSID IFPUSID BMPUSID CICSUSID ODBAUSID
AGN2	PSB3 PSB4 TRANA	MPPUSID
AGNx	PSBx LTERM1	IFPUSID

DFSPBxxx
ISIS=1

12. PSB1 INCLUDED IN AGN1?
IF SO, SCHEDULE PSB1; ELSE REJECT SCHEDULE

ADDRESS SPACE
(MPP,IFP, BMP, CICS, or ODBA)

JCL... USER=region_*userid*,
AGN=AGN1,
...

11. SCHEDULE PSB1 ...

Securing CPIC-Driven PSBs

- Allocate PSB (APSB) call is used to allocate CPIC-driven programs
  - The PSB controls access to IMS databases and alternate PCBs

- APSB-SAF security is
  - Used to secure access to PSBs for CPIC-driven applications
  - Activated by

SECURITY TYPE=(RACFAGN,RACFTERM,...)
AND
IMS.PROCLIB(DFSPBxxx) ISIS=1, RCF≠N, & APPCSE=F
(the equivalent command /SEC APPC FULL)

SECURITY CHECKING FOR ALL CPIC PSBs

SECURITY TYPE=(RACFAGN,RACFTERM,...)
AND
IMS.PROCLIB(DFSPBxxx) ISIS=1, RCF≠N, & APPCSE=P
(the equivalent command /SEC APPC PROFILE) plus security flag value of 'F'

SECURITY CHECKING ON A TRANSACTION BY TRANSACTION BASIS

Securing CPIC-Driven PSBs Using RACF

- RACF profiles created in the AIMS (or equivalent) resource class
  - Authorization checking based on the userid of end user who submitted CPIC transaction

- AIMS resource class is used for both AGN security and CPIC PSB security
  - Make sure CPIC PSB profile name do not conflict with AGN profile names

RACF CPIC PSB Example

```
RDEFINE AIMS CPICPSB1 OWNER(IMSADMIN) UACC(NONE)

PERMIT CPICPSB1 CLASS(AIMS) ID(GROUPX GROUPY) ACCESS(READ)

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

Summary

- **Accessing IMS**
- **Key concepts**
  - IMS resources that may be secured
  - Source of input
  - Security facilities used to secure IMS resources
  - IMS resources that may be secured using RACF
- **IMS-RACF security**
  - Commands
  - Transactions
  - Terminals
  - Control region
  - Data sets
  - Databases
  - Connections to control region
  - Program specification blocks