IMS Connect
Security Implementation and Considerations

Alonia (Lonnie) Coleman
IMS Technical Consulting
Dallas Systems Center

Agenda

- **The basics**
  - Accessing IMS from a terminal
  - Open Transaction Manager Access (OTMA)
- **IMS Connect**
  - Primary functions
  - Communications in a sysplex
- **IMS Connect security**
  - Program Properties Table (PPT) entry
  - HWSCFGxx startup/execution parameters
  - Defining IMS Connect's userid and group
  - Supplying and verifying the TCP/IP end user's userid and group
    - IMS Connect
    - Security exit routine
      - IMSLSECX sample
  - Client-bid security

The Basics

- Information Management System (IMS) is
  - A ***t***ransaction ***m***anagement system (IMS-TM)
    - High volume, high performance transaction server
      - With high availability and high reliability
    - Similar to Customer Information Management System (CICS)
  - A ***hierarchical*** ***d***atabase ***m***anagement system (IMS-DB)
    - High volume, high performance database server
      - With high availability and high reliability
    - Database2 (DB2) is a ***relational*** database management system
  - ***Both*** a transaction and database management system
    - IMS-TM and IMS-DB

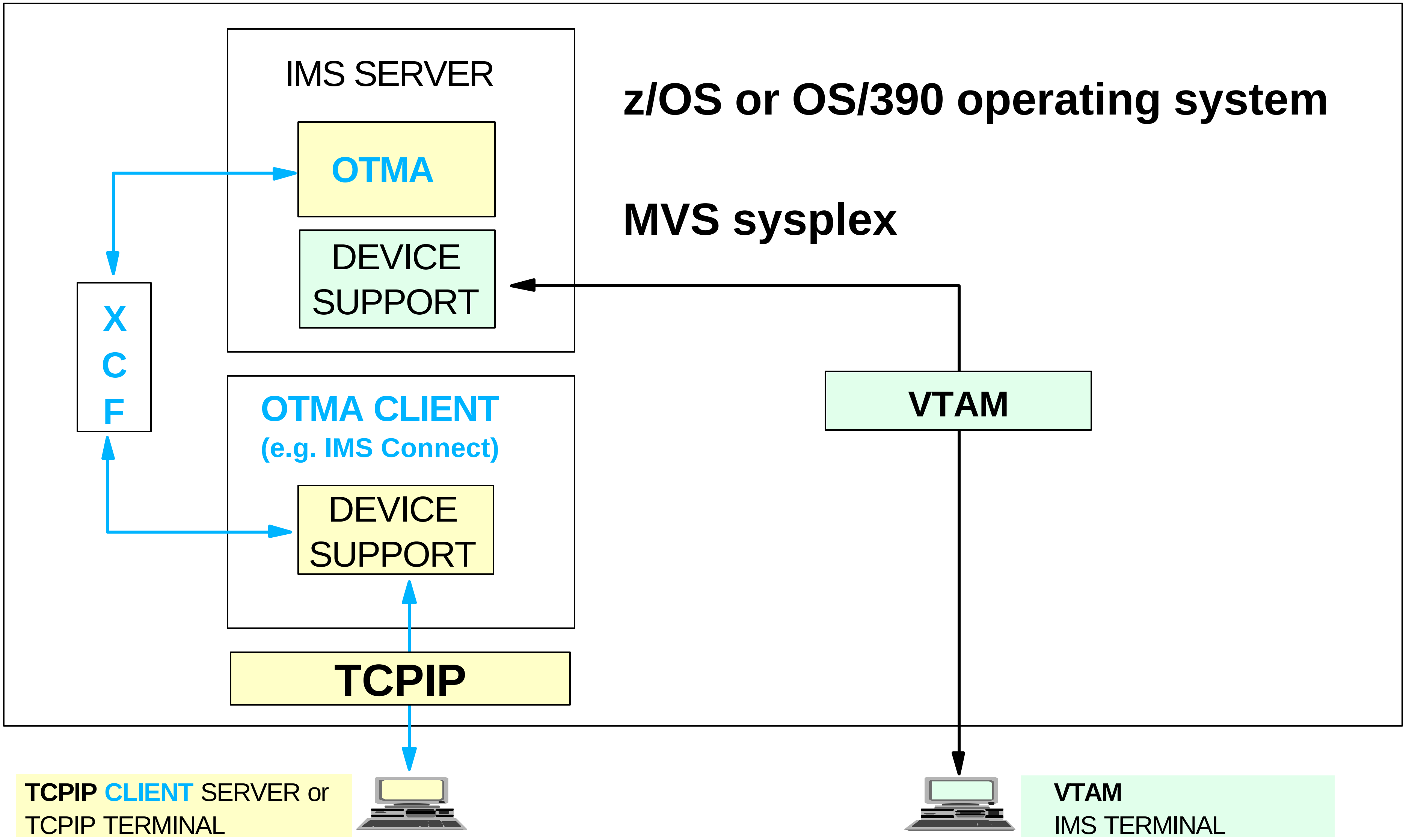
Accessing IMS From a Terminal

- IMS-TM is a VTAM application
  - IMS-TM terminal access is supported through VTAM
- TCP/IP terminal users also wanted to access to IMS
  - IMS transactions and data, IMS commands
    - Protect investment in legacy applications
  - High performance, available, reliable server
- IMS-TM Version 5
  - Announced 4/6/1994, general availability 3/28/1995
  - Introduced a new facility called OTMA
    - Open Transaction Manager Access (OTMA) facility
      - OTMA provides a way for TCP/IP users to access IMS

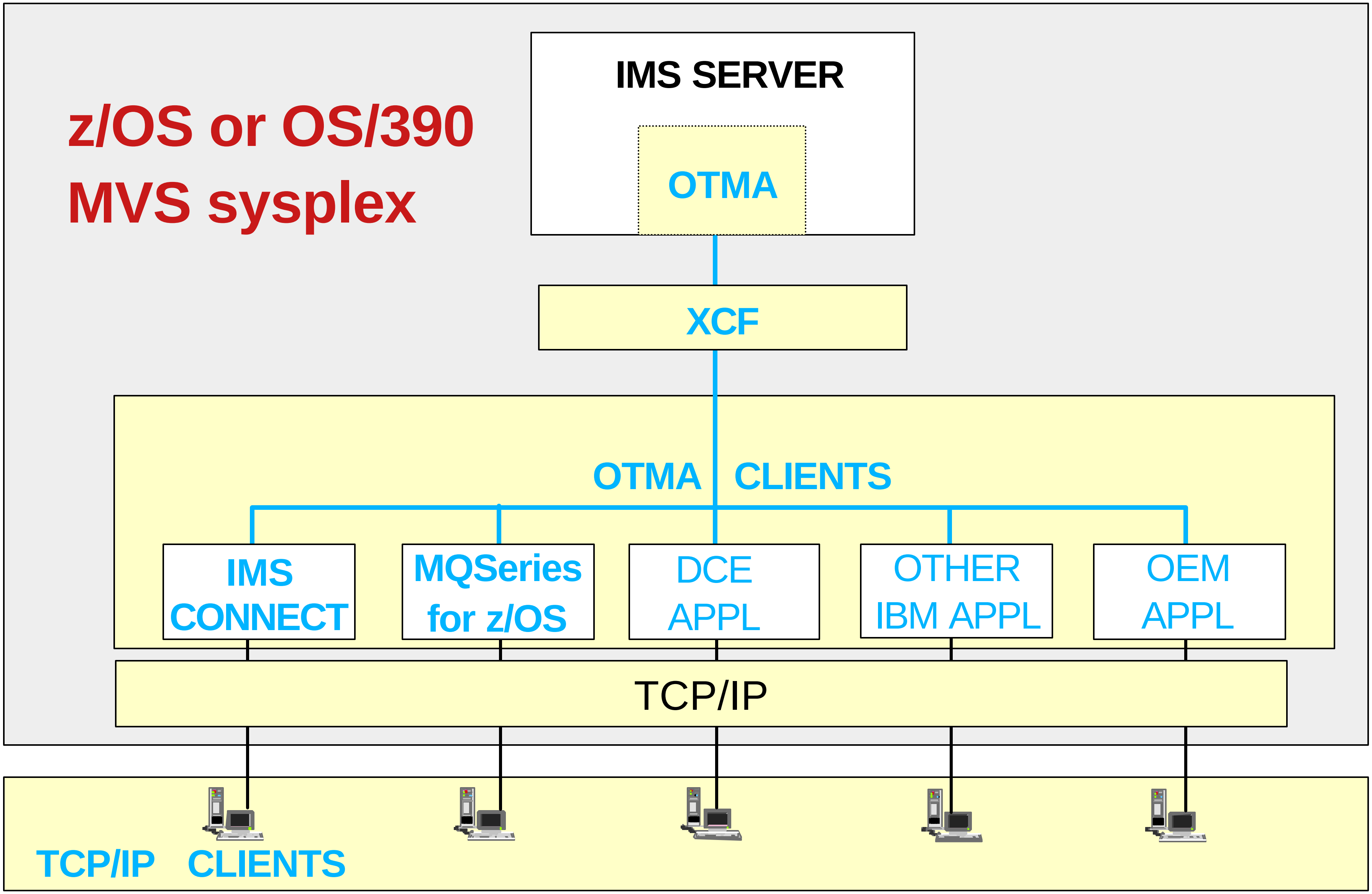
Open Transaction Manager Access (OTMA)

- What Is OTMA?
  - A client-server protocol with the following characteristics
    - ***High performance***
    - Transaction-based
    - ***Connectionless***
  - A gateway for transactions outside IMS to enter IMS
- OTMA
  - Uses MVS Cross-System Coupling Facility (**XCF**) services
    - Facilitates communications between OTMA and OTMA clients
  - Allows ***MVS programs*** **(called OTMA clients)** to access IMS applications

OTMA Connection -vs- IMS Connection



An OTMA Client - Any MVS Application



IMS Connect - Primary Functions

- Sends/receives messages to/from IMS-OTMA
  - Input messages
    - Remove TCP/IP headers
    - Translate ASCII to EBCDIC
    - Build OTMA headers
  - Output messages
    - Remove OTMA headers
    - Translate EBCDIC to ASCII
    - Build TCP/IP headers
- Userid validation and password verification
- Provides support for
  - TCP/IP client applications
  - WebSphere on z/OS (OS/390) running IMS Connector for JAVA

IMS Connect - Software Requirements

OS/390 V2.7 or higher

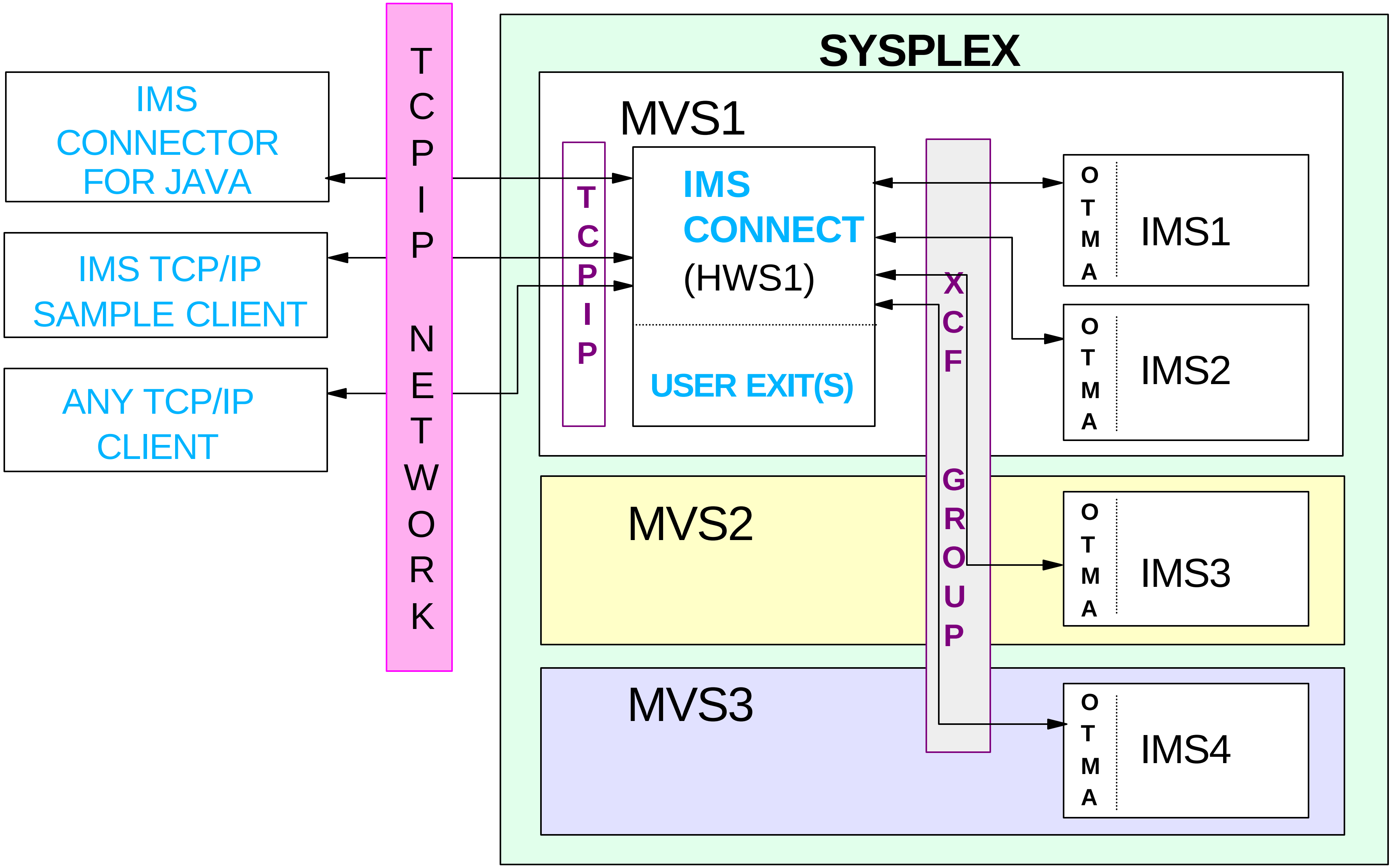
OS/390 V2.8 or higher for WebSphere '***local option***'

TCP/IP V3.2 or TCP/IP V3.4 or higher

Plus APARs PQ13154 and PQ38814

RACF V1.9.2 or higher (or equivalent OEM product)

XCF Communications In a SYSPLEX



IMS Connect Security

- Runtime libraries must be APF authorized
- MVS Program Properties Table (PPT) must allow IMS Connect to use
  - Supervisor state
  - Key 7 storage
- IMS Connect
  - Startup parms are in HWSCFGxx file
  - Can call RACF for ***end user*** userid and password security checking
    - UTOKEN
      - Returned for valid RACF userid
      - Passed to IMS
  - Should have a valid RACF **userid** and **group** for client-bid security checking

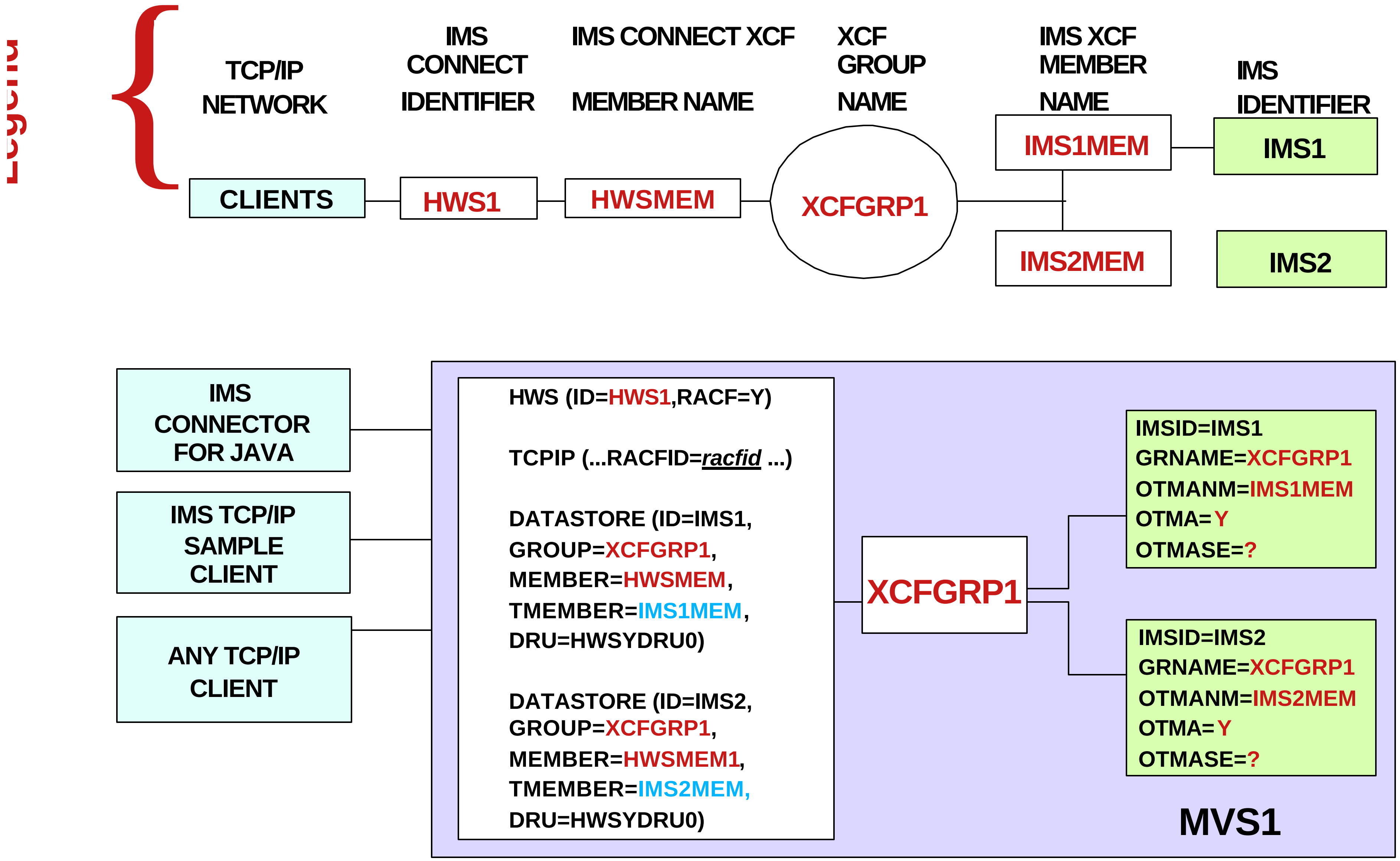
```
PPT PGMNAME(HWSHWS00)     /* PROGRAM NAME = HWSHWS00                         */
KEY(7)                    /* PROTECT KEY ASSIGNED IS 7                       */
PASS                      /* CANNOT BYPASS DATASET PASSWORD PROTECTION       */
SYST                      /* PROGRAM IS A SYSTEM TASK   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

MVS PPT

HWSCFGxx

```
HWS (ID=HWS1,RACF=Y)
TCPIP (...RACFID=default_userid,EXIT=(HWSIMSO0,HWSJAVA0,...)
DATASTORE (ID=IMS1,GROUP=XCFGRP1,MEMBER=HWSMEM,TMEMBER=IMS1MEM,DRU=HWSYDRU0)
DATASTORE (ID=IMS2,GROUP=XCFGRP1,MEMBER=HWSMEM1,TMEMBER=IMS2MEM,DRU=HWSYDRU0)
...
```

Startup Parameters

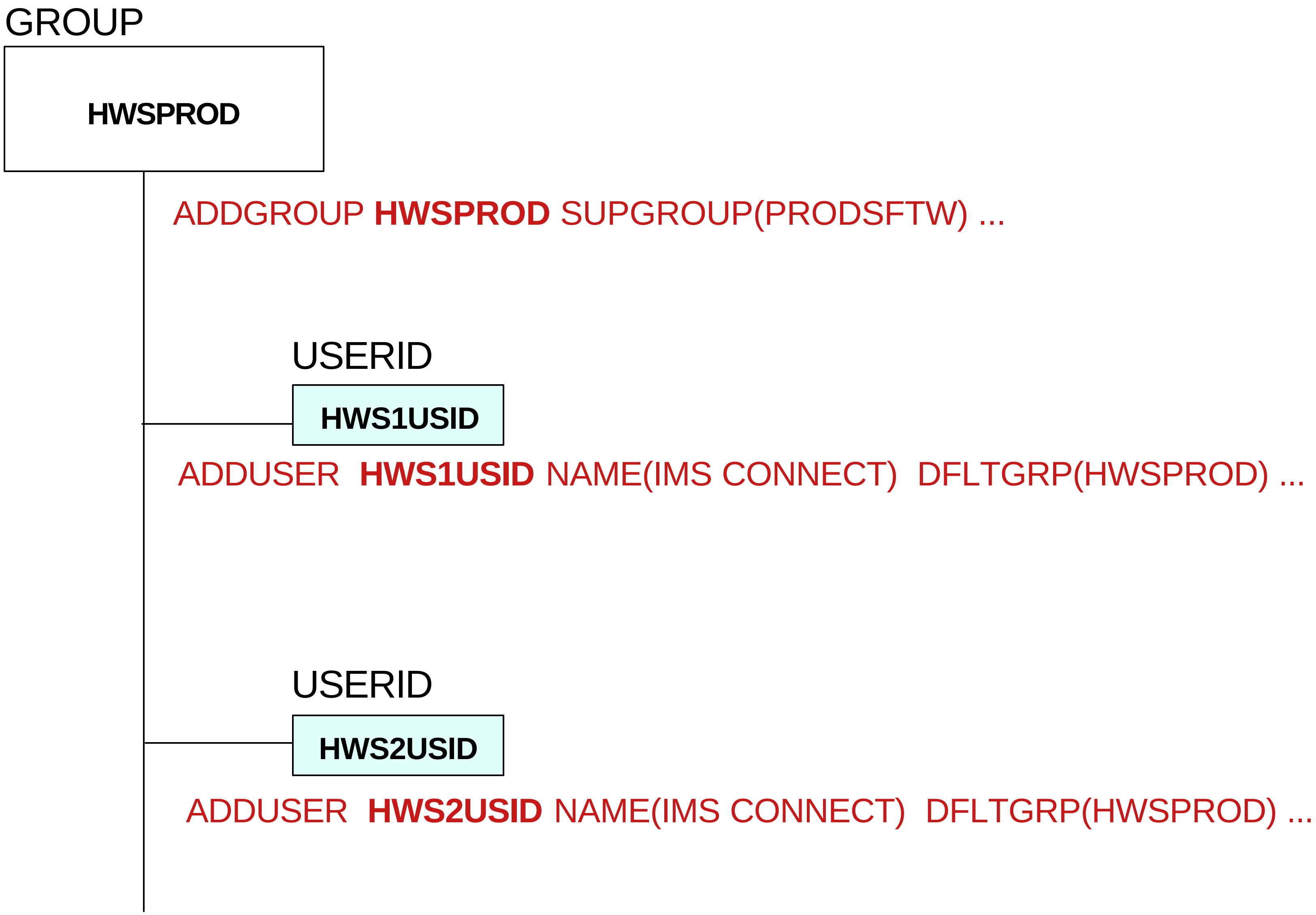


```
HWS (ID=HWS1,RACF=Y)

TCPIP (...RACFID=racfid ...)

DATASTORE (ID=IMS1,
GROUP=XCFGRP1,
MEMBER=HWSMEM,
TMEMBER=IMS1MEM,
DRU=HWSYDRU0)

DATASTORE (ID=IMS2,
GROUP=XCFGRP1,
MEMBER=HWSMEM1,
TMEMBER=IMS2MEM,
DRU=HWSYDRU0)
```

```
IMSID=IMS1
GRNAME=XCFGRP1
OTMANM=IMS1MEM
OTMA=Y
OTMASE=?
```

```
IMSID=IMS2
GRNAME=XCFGRP1
OTMANM=IMS2MEM
OTMA=Y
OTMASE=?
```

Defining IMS Connect's Userid and Group



GROUP

HWSPROD

ADDGROUP **HWSPROD** SUPGROUP(PRODSFTW) ...

USERID

HWS1USID

ADDUSER **HWS1USID** NAME(IMS CONNECT) DFLTGRP(HWSPROD) ...

USERID

HWS2USID

ADDUSER **HWS2USID** NAME(IMS CONNECT) DFLTGRP(HWSPROD) ...

IMS Connect's Userid Association

- Started procedure
  - RACF STARTED Class
    - Associate IMS Connect userid with procedure

```
RDEF STARTED HWSPROC STDATA(USER(HWS1USID) GROUP(HWSPROD)...
```

- Started Procedure Table (SPT)
  - Code entry table to associate userid with started procedure

- JOB card USERID= parameter

```
//HWS01  JOB  ...,USERID=HWS1USID,...
```

- Use STARTED Class and SPT
  - STARTED Class to avoid IPL
  - Update SPT during scheduled IPL

End User Userid/Password Verification

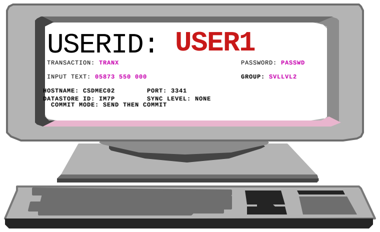
- Verification may be performed by
  - IMS Connect user security exit
  - IMS Connect
  - IMS/OTMA
    - IMS/OTMA verifies userid and group only; ***not*** user password
  - Combination

- Activating IMS Connect userid/password verification
  - **RACF=Y** in HWSCFGxx file or **SETRACF ON** command

- When RACF=N and IMS Connect security exit not used
  - Password is not sent to IMS
  - Potential security exposure in IMS (no password verification)

En User's Userid Passed To IMS

- Userid used for authorizations originates from
  - Client
    - Passed in security data (SE)
    - section of the message prefix



```
USERID: USER1
TRANSACTION: TRANX                              PASSWORD: PASSWD
INPUT TEXT: 05873 550 000                       GROUP: SVLLVL2
HOSTNAME: CSDMEC02        PORT: 3341
DATASTORE ID: IM7P        SYNC LEVEL: NONE
  COMMIT MODE: SEND THEN COMMIT
```

  - 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=(HWSIMSO0,HWSJAVA0,...)
```

  - Default RACFID=*xxxxxxxx*, *racfid* is the default if not specified

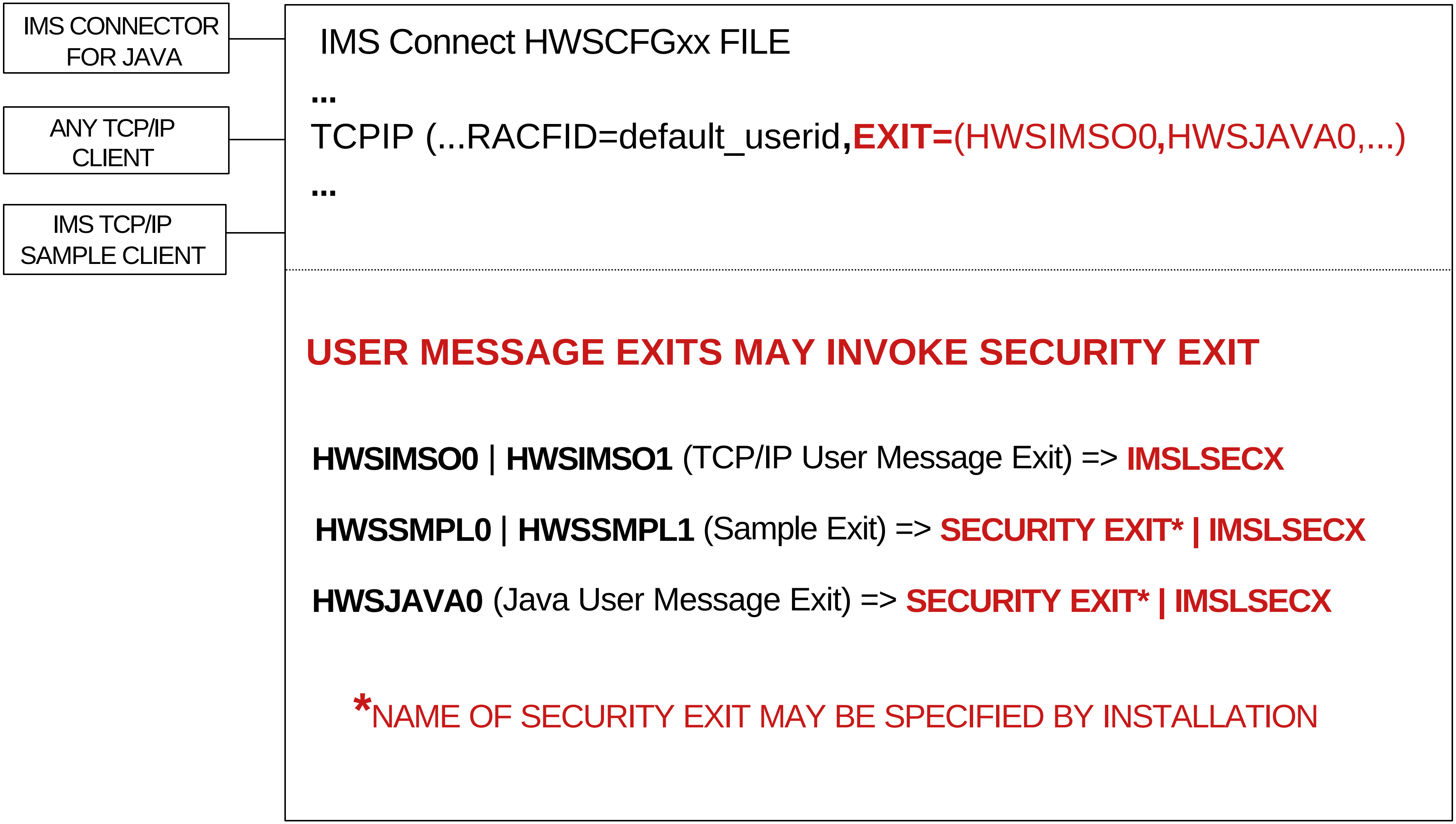
```
IMS Connect HWSCFGxx FILE
TCPIP (...RACFID=default_racf_userid,EXIT=(HWSIMSO0,HWSJAVA0,...)
```

User Message Exit Routines

- Security exit may be called by user message exits
  - Message exit **HWSIMSO0 | HWSIMSO1**
    - Security exit must be named ***IMSLSECX***
      - Sample provided by TCP/IP
  - Message exit **HWSSMPL0 | HWSSMPL1**
    - Security exit name may be supplied by the user
  - Message exit **HWSJAVA0**
    - Security exit name may be supplied by the user

- IMS Connect allows up to 15 user exits in HWSCFGxx
  - TCPIP statement EXIT= keyword names exits

User Message Exit Routines Illustration



IMS CONNECTOR FOR JAVA

ANY TCP/IP CLIENT

IMS TCP/IP SAMPLE CLIENT

IMS Connect HWSCFGxx FILE

```
...
TCPIP (...RACFID=default_userid,EXIT=(HWSIMSO0,HWSJAVA0,...)
...
```

USER MESSAGE EXITS MAY INVOKE SECURITY EXIT

HWSIMSO0 | **HWSIMSO1** (TCP/IP User Message Exit) => **IMSLSECX**

HWSSMPL0 | **HWSSMPL1** (Sample Exit) => **SECURITY EXIT* | IMSLSECX**

HWSJAVA0 (Java User Message Exit) => **SECURITY EXIT* | IMSLSECX**

*NAME OF SECURITY EXIT MAY BE SPECIFIED BY INSTALLATION

TCP/IP Provided Exit IMSLSECX

- 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*

Use exit to verify

*IRM - IMS Request Message

Security Exit *Not Invoked* By User Exit

USERID PASSED

USERID FIELD IN IRM?	IRM USERID FIELD BLANKS/NULLS?	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 USERID FIELD BLANKS/NULLS?	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

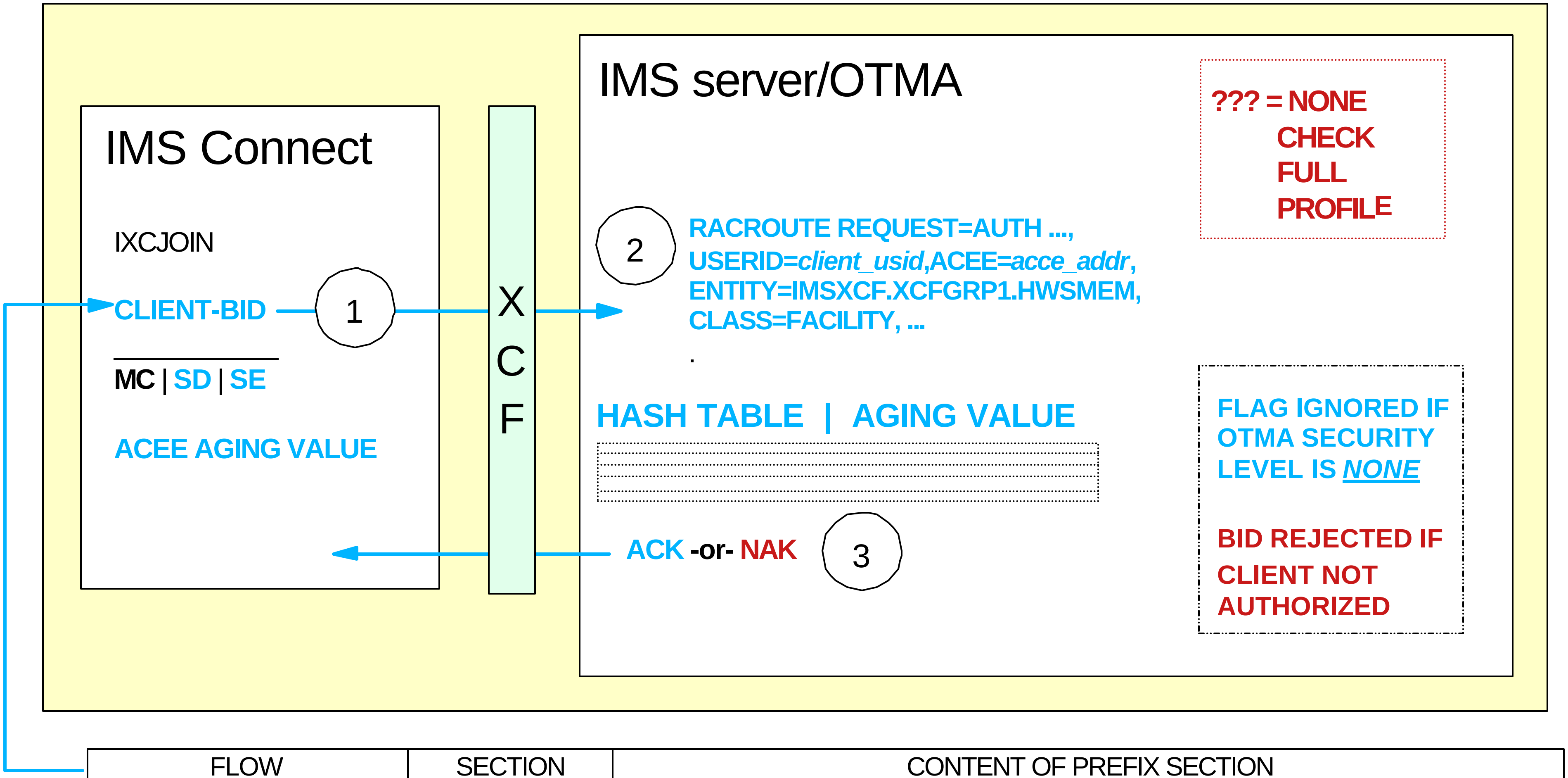
GROUPID FIELD IN IRM?	IRM GROUPID FIELD BLANK/NULL?	GROUPID RETURNED BY SECURITY EXIT?	RESULTS PASSED TO IMS IN OTMA SECURITY HEADER
YES	YES	NO	**BLANK GROUPID**
YES	YES	YES	**SECURITY EXIT RETURNED GROUP NAME**
YES	NO	NO	**BLANK GROUPID**
YES	NO	YES	**SECURITY EXIT RETURNED GROUP NAME**
NO	N/A	NO	**BLANK 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 GROUPID returned by the exit is ***not*** used.

Communicating With OTMA

- IMS Connect
  - Joins the same XCF group as IMS/OTMA
  - Sends a client-bid message to OTMA
- After successful client-bid, IMS Connect
  - Can invoke IMSLSECX (or other user security exit) from the message exit for userid/password security checking for messages received from TCP/IP clients
  - Can perform userid and password verification security itself
  - Processes and sends input messages to IMS
  - Processes and sends output messages to TCP/IP clients
- To cause OTMA client hash table (with userid entries) to be rebuilt
  - *nn*STOPDS IMS1 and *nn*OPENDS IMS1
    - *Where nn* is the reply number of the outstanding reply message
    - Only affects OTMA hash table for IMS Connect !! (This is GOOD)

IMS Connect Client-Bid



IMS Connect

IXCJOIN

CLIENT-BID

MC | SD | SE

ACEE AGING VALUE

IMS server/OTMA

RACROUTE REQUEST=AUTH ...,
USERID=*client_usid*,ACEE=*acce_addr*,
ENTITY=IMSXCF.XCFGRP1.HWSMEM,
CLASS=FACILITY, ...

.

??? = NONE
CHECK
FULL
PROFILE

HASH TABLE | AGING VALUE

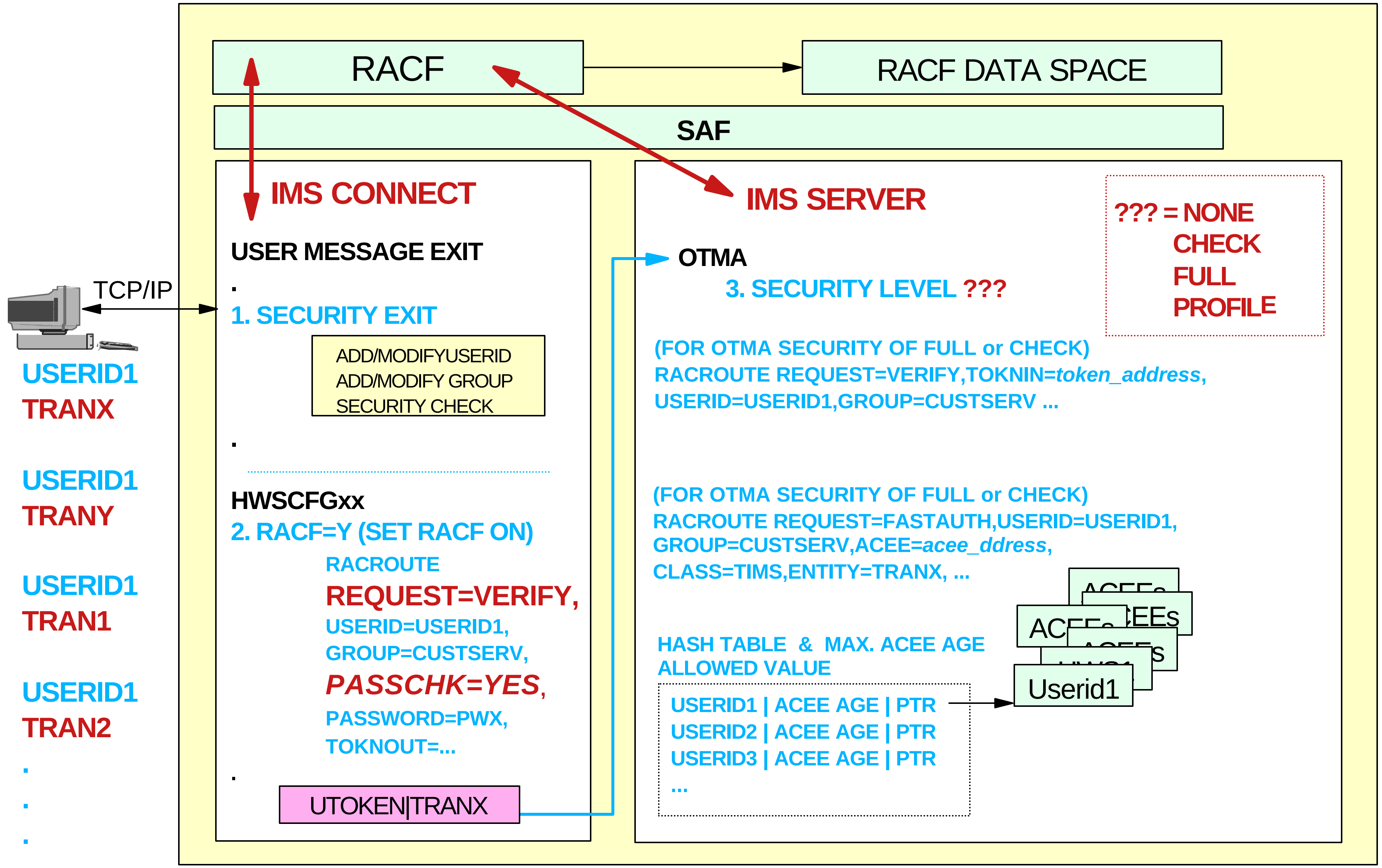
FLAG IGNORED IF OTMA SECURITY LEVEL IS *NONE*

BID REJECTED IF CLIENT NOT AUTHORIZED

ACK -or- NAK

FLOW	SECTION	CONTENT OF PREFIX SECTION
CLIENT-BID MESSAGE	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

IMS Connect - Transmitting User Messages



TCP/IP

USERID1
TRANX

USERID1
TRANY

USERID1
TRAN1

USERID1
TRAN2

.
.
.

RACF

RACF DATA SPACE

SAF

IMS CONNECT

USER MESSAGE EXIT

.

1. SECURITY EXIT

ADD/MODIFYUSERID
ADD/MODIFY GROUP
SECURITY CHECK

.

HWSCFGxx

2. RACF=Y (SET RACF ON)

RACROUTE
REQUEST=VERIFY,
USERID=USERID1,
GROUP=CUSTSERV,
PASSCHK=YES,
PASSWORD=PWX,
TOKNOUT=...

.

UTOKEN|TRANX

IMS SERVER

OTMA

3. SECURITY LEVEL ???

??? = NONE
CHECK
FULL
PROFILE

(FOR OTMA SECURITY OF FULL or CHECK)
RACROUTE REQUEST=VERIFY,TOKNIN=*token_address*,
USERID=USERID1,GROUP=CUSTSERV ...

(FOR OTMA SECURITY OF FULL or CHECK)
RACROUTE REQUEST=FASTAUTH,USERID=USERID1,
GROUP=CUSTSERV,ACEE=*acee_ddress*,
CLASS=TIMS,ENTITY=TRANX, ...

HASH TABLE & MAX. ACEE AGE
ALLOWED VALUE

USERID1 | ACEE AGE | PTR
USERID2 | ACEE AGE | PTR
USERID3 | ACEE AGE | PTR
...

ACEEs

ACEEs

Userid1

RACF ACEE Caching Facility

- IMS Connect does not cache ACEEs
  - VLF ACEE caching may enhance IMS Connect VERIFY processing performance
    - RACF can save ACEEs in VLF (***V***irtual ***L***ookaside ***F***acility)
      - VLF data space searched for ACEE before I/O to RACF database
- Performance improvement may be attained through
  - Path length reduction
  - Elimination of I/O to the RACF database
    - For VERIFY requests for multiple input messages from the same userid
- Amount of performance improvement related to
  - How often RACF finds information in VLF

Implementing VLF ACEE Caching

- For RACF to begin saving and retrieving ACEEs
  - Activate VLF using the MVS **START** command

```
S VLF,SUB=MSTR
```

  - Update the COFVLFxx of SYS1.PARMLIB
    - Include the VLF class name (e.g. IRRACEE)
    - Updating COFVLFxx member activates IRRACEE class

```
SYS1.PARMLIB(COFVLF00)
    CLASS NAME(IRRACEE)       /* RACF ACEE Data in Memory    */
    EMAJ (ACEE)               /* Major name = ACEE           */
```

  - Invokers, such as IMS Connect, may benefit from use of ACEEs cached in VLF

VLF - Software Requirements

- Software prerequisites
  - RACF 1.9.2 or higher
  - z/OS Version 1 Release 2 or higher
    - APAR OW46269 must be installed on all down level systems in sysplexes running in sysplex communication mode
  - MVS Cross System Coupling Facility (XCF)
    - If your installations uses sysplex communications

IMS Connect Security Summary

- Each OTMA client must perform a client-bid before user messages can be transmitted to IMS
  - The client-bid process may be secured by specifying an OTMA security level of CHECK or FULL
- IMS Connect is an OTMA client
- Security options are available
  - User security exit
  - IMS Connect userid validation and password verification
    - Userid/password supplied by end user
    - Userid/password supplied by message/security exit
    - Default racfid