E38

IMS Connect Security Considerations

Alonia (Lonnie) Coleman

IMS Technical Conference

St. Louis, MO **Sept. 30 - Oct. 3, 2002**

RETURN TO INDEX

Agenda

- Part 2
  - OTMA overview
  - IMS Connect
    - Overview
    - Security
  - Planned security enhancements for IMS Connect
  - Additional information
  - Summary

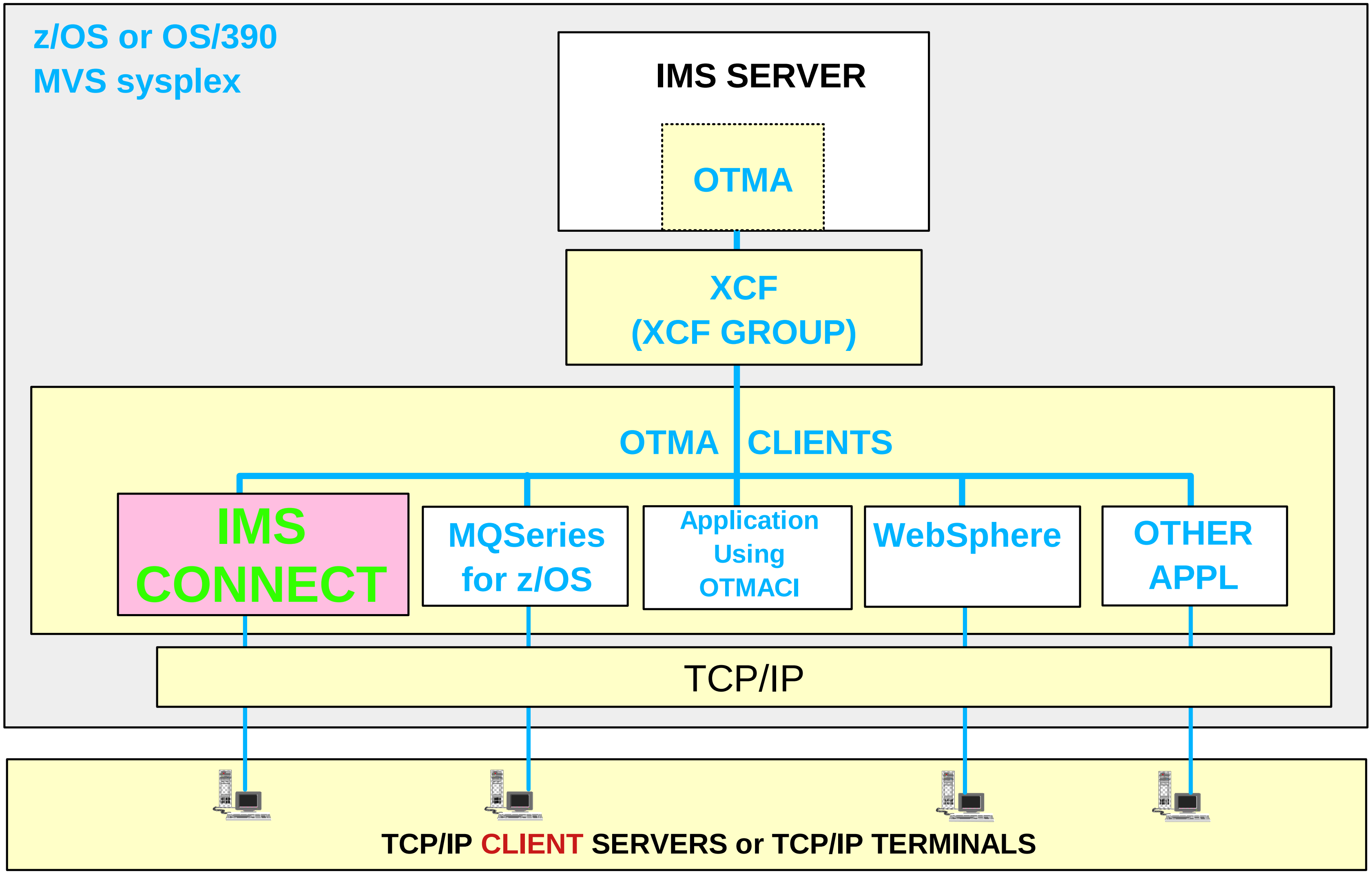
- Attachments to read at your convenience
  - Acronyms
  - RACF command examples
  - Virtual Lookaside Facility (VLF) ACEE caching information

OTMA Overview

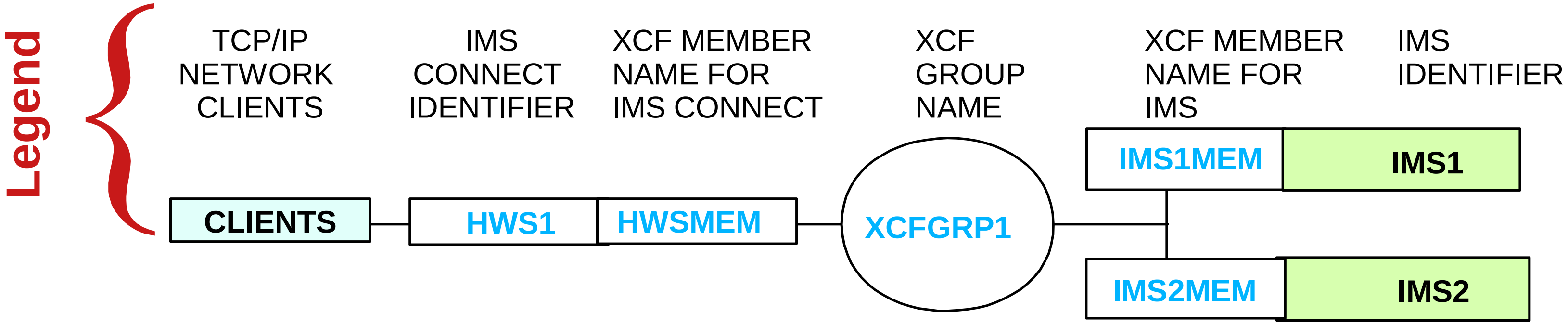
- What Is OTMA?
  - A client-server protocol that
    - *Has high performance*
    - *Is transaction-based*
    - *Is connectionless*
    - Provides a gateway for transactions outside IMS to enter IMS

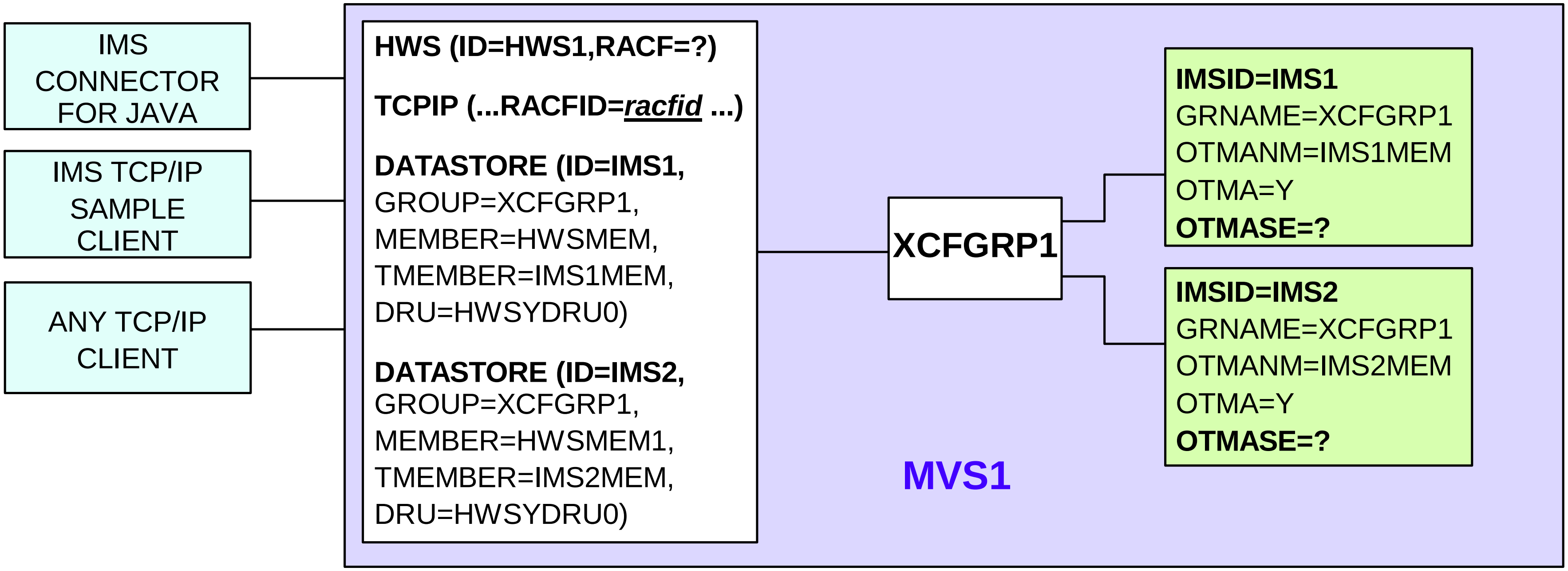
- OTMA
  - Allows z/OS and OS/390 programs to access IMS
    - These MVS programs are called ***OTMA clients***
  - Uses MVS ***Cross-System Coupling Facility (XCF)*** services
    - Facilitates communications between OTMA and OTMA clients

An XCF Group and OTMA Clients



IMS Connect & IMS Startup Parameters





HWS (ID=HWS1,RACF=?)

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=?

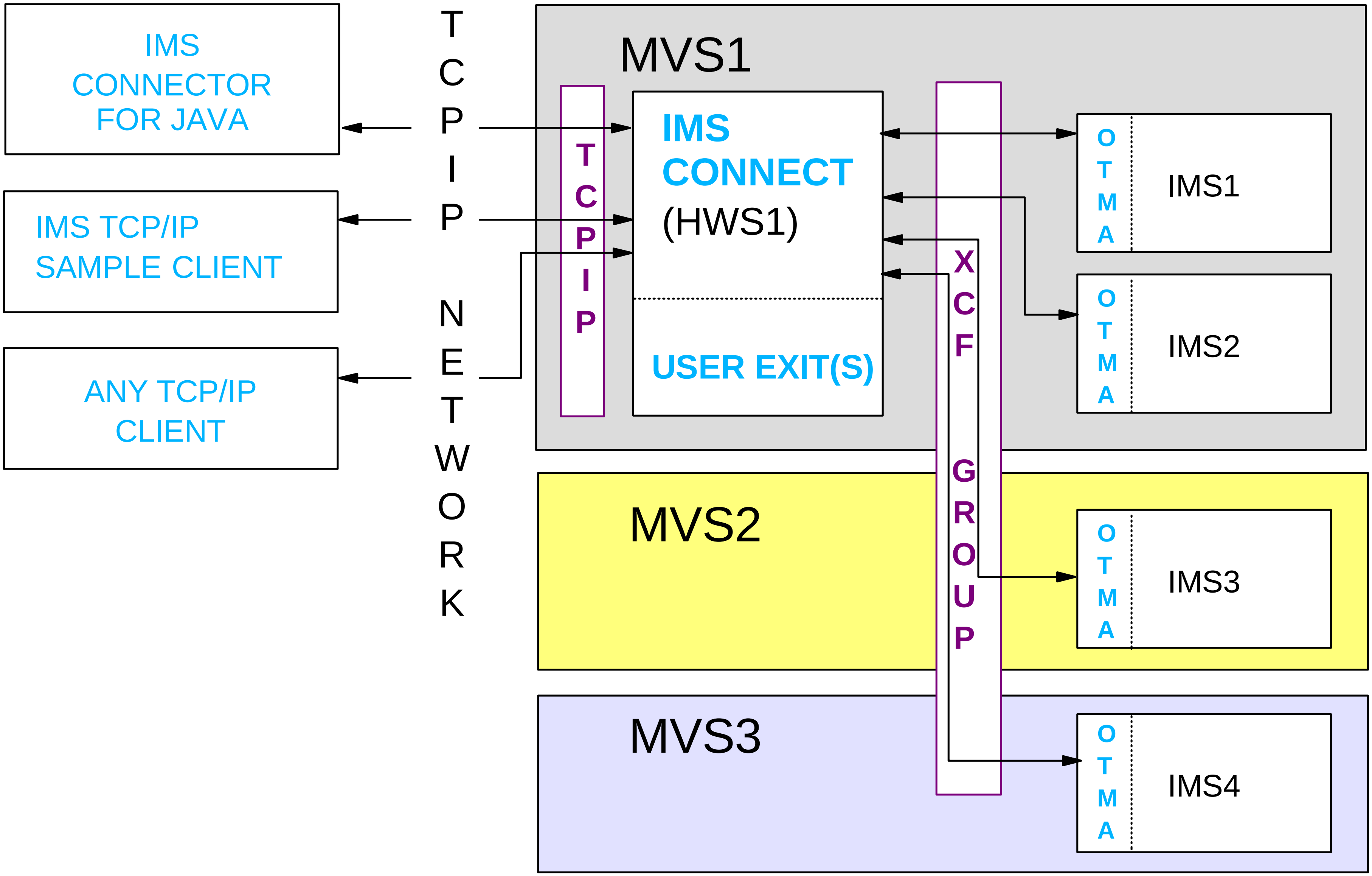
IMS Connect Overview

- Primary functions are
  - To send/receive messages to/from OTMA
    - For input messages
      - Remove TCP/IP headers
      - Translate ASCII to EBCDIC
      - Build OTMA headers
      - Userid validation ***and*** password verification
    - For output messages
      - Remove OTMA headers
      - Translate EBCDIC to ASCII
      - Build TCP/IP headers
- Provides support for
  - TCP/IP client applications
  - WebSphere on z/OS or OS/390 running IMS Connector for JAVA (local option)

USERID VALIDATION ONLY

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)

Communications In the SYSPLEX



IMS CONNECTOR FOR JAVA

IMS TCP/IP SAMPLE CLIENT

ANY TCP/IP CLIENT

TCP/IP NETWORK

MVS1

TCP/IP

IMS CONNECT (HWS1)

USER EXIT(S)

XCF GROUP

OTMA IMS1

OTMA IMS2

MVS2

OTMA IMS3

MVS3

OTMA IMS4

IMS Connect PPT Entry

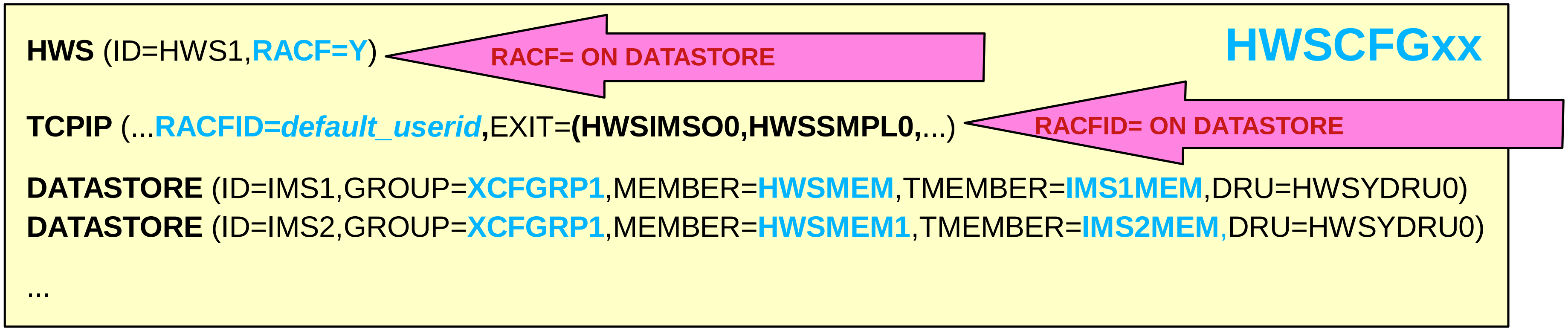
- IMS Connect runtime libraries must be APF authorized
- MVS Program Properties Table (PPT) must contain an entry for IMS Connect

```
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 Program Properties Table (PPT)

IMS Connect Security

- IMS Connect needs a valid RACF **userid** and **group**
- IMS Connect security
  - Is optional
    - Choices are: no userid validation, exit routine userid validation, RACF userid validation
  - May be used to invoke RACF for end user userid and password security checking
    - UTOKEN is returned for valid RACF userid with correct password
      - UTOKEN is passed to OTMA in the OTMA message prefix



HWSCFGxx

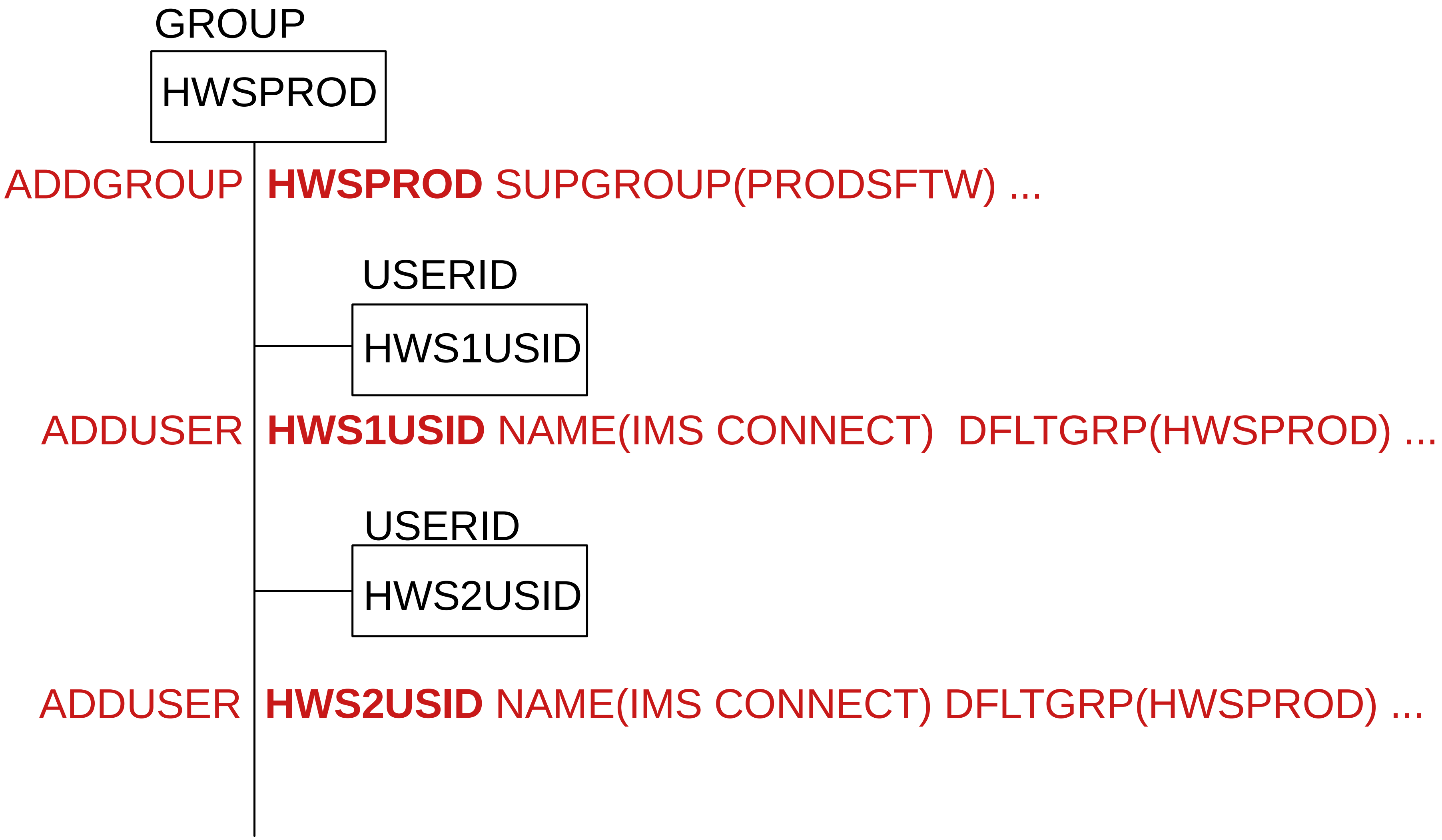
```
HWS (ID=HWS1,RACF=Y)

TCPIP (...RACFID=default_userid,EXIT=(HWSIMSO0,HWSSMPL0,...)

DATASTORE (ID=IMS1,GROUP=XCFGRP1,MEMBER=HWSMEM,TMEMBER=IMS1MEM,DRU=HWSYDRU0)
DATASTORE (ID=IMS2,GROUP=XCFGRP1,MEMBER=HWSMEM1,TMEMBER=IMS2MEM,DRU=HWSYDRU0)

...
```

Creating the RACF Userid & Group For IMS Connect



GROUP

HWSPROD

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

USERID

HWS1USID

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

USERID

HWS2USID

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

Associating the IMS Connect Userid With A Started Procedure or Job

- There are several ways to associate IMS Connect's userid with the started procedure or job used to start IMS Connect
  - Define a profile in the RACF STARTED Class

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

  - Code an entry in the RACF Started Procedure Table (SPT)

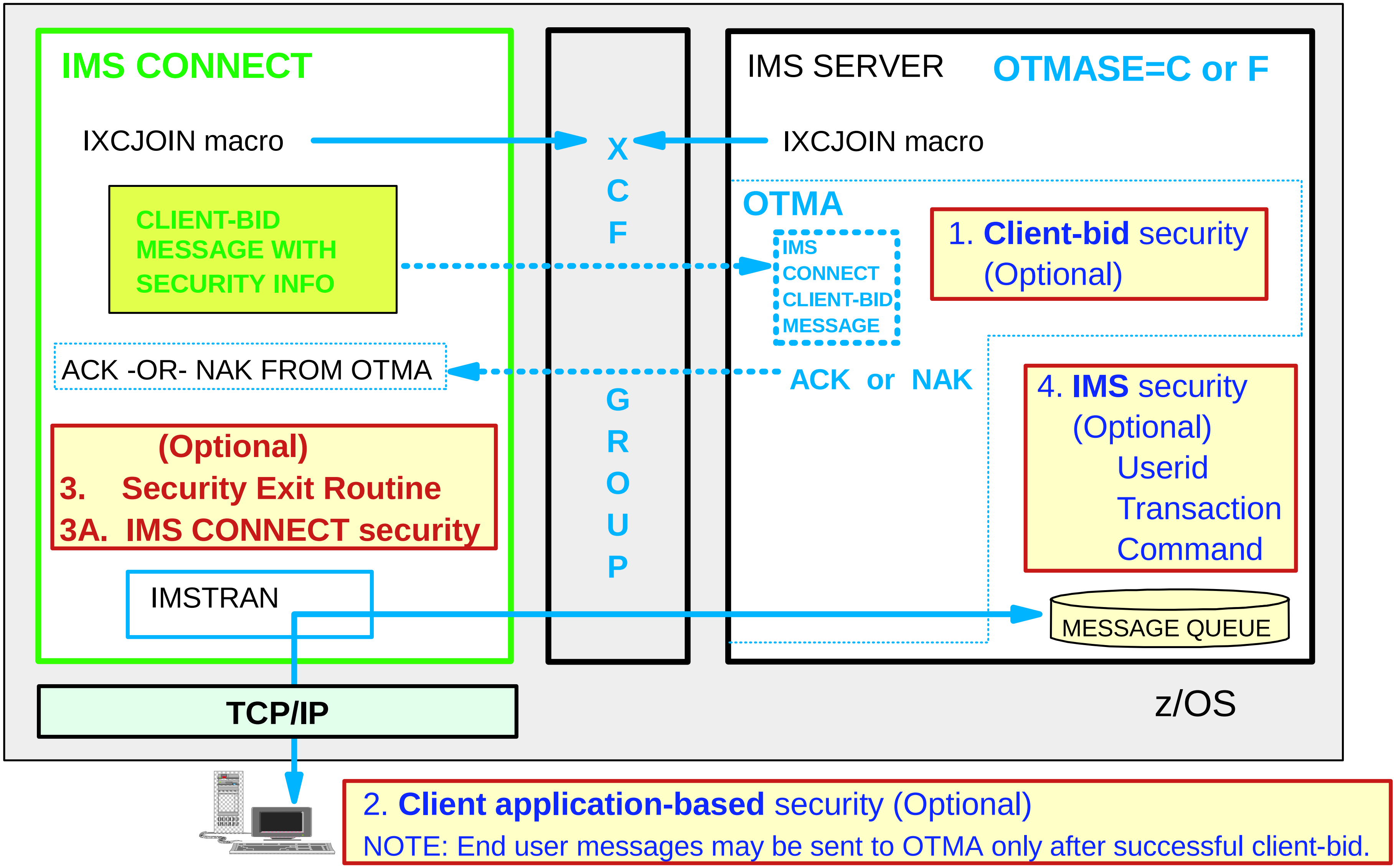
ICHRIN03	CSECT	
...		
ENTRY	EQU	*
PROC	DC	HWSPROC
USERID	DC	HWS1USID
GROUP	DC	HWSPROD
FLAGS	DC	XL1'00'
	DC	XL7'00'
...		

RECOMMENDATION: USE THE STARTED CLASS TO AVOID AN IPL (WHICH IS REQUIRED FOR CHANGING THE SPT) AND ALSO PLACE AN ENTRY IN THE SPT (DURING SCHEDULED IPL) FOR BACKUP PURPOSES

  - Supply a value for the IMS Connect userid on the JOB card of the job submitted to start IMS Connect

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

IMS Connect Security Options



1. **Client-bid** security (Optional)

(Optional)
3. **Security Exit Routine**
3A. **IMS CONNECT security**

4. **IMS** security (Optional)
Userid
Transaction
Command

2. **Client application-based** security (Optional)
NOTE: End user messages may be sent to OTMA only after successful client-bid.

Userid/Password Verification

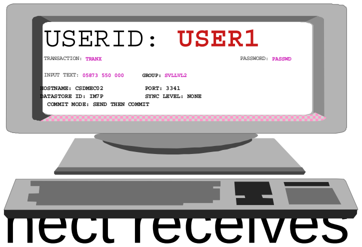
- Verification may be performed by
  1. An IMS Connect user written security exit
  2. IMS Connect
     - Verifies both userid ***and*** password
  3. IMS/OTMA
     - Verifies userid, and optionally, group name; does ***not*** verify user password
  4. Combination of the above

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

- A potential security exposure exists in IMS when all of the following are true:
  - Client-based userid and password verification is ***not*** done
  - IMS Connect
    - Security exit is ***not*** used and
    - **RACF=N** is specified

Userid Sources

- Userid used for authorizations may originate 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
      - For example, exit may be coded to generate userid when no client userid passed to it

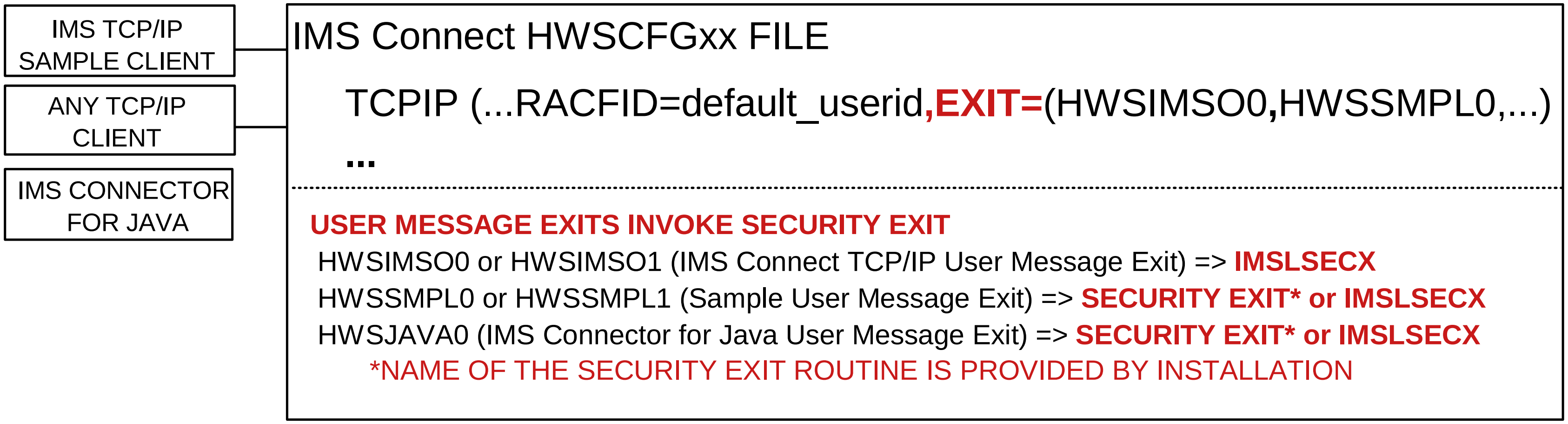
IMS Connect **HWSCFGxx** FILE
TCPIP (...RACFID=default_userid**,EXIT=**(HWSIMSO0**,**HWSSMPL00,...)

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

IMS Connect **HWSCFGxx** FILE
TCPIP (...**RACFID=*default_racf_userid*,**EXIT=(HWSIMSO0,HWSSMPL0,...)

User Message Exit Routine

- Security exit may be invoked by (link-edited with) the user message exit
  - 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 HWSCFGxx FILE

```
TCPIP (...RACFID=default_userid,EXIT=(HWSIMSO0,HWSSMPL0,...)
...
```

USER MESSAGE EXITS INVOKE SECURITY EXIT

HWSIMSO0 or HWSIMSO1 (IMS Connect TCP/IP User Message Exit) => **IMSLSECX**

HWSSMPL0 or HWSSMPL1 (Sample User Message Exit) => **SECURITY EXIT* or IMSLSECX**

HWSJAVA0 (IMS Connector for Java User Message Exit) => **SECURITY EXIT* or IMSLSECX**

*NAME OF THE SECURITY EXIT ROUTINE IS PROVIDED BY INSTALLATION

TCP/IP Provided Sample Exit

- IMSLSECX is a sample exit provided by TCP/IP
- IMSLSECX may be invoked from any of the message exits
- Parameter list passed to exit includes addresses of
  - Client's IP address and port number
  - IMS transaction code
  - Data type setting
    - 0=ASCII or 1=EBCDIC
  - Length of user data
  - User-supplied data
  - RACF USERID, password, and GROUPID
    - Depend on value specified in IRM*

*IRM - IMS Request Message

Userid/Group Used - NO Security Exit

- The tables illustrate how IMS Connect determines the userid (and optionally, the group) that is placed in the message destined for OTMA ***when a security exit is not invoked***

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**

PASSWORD IS ***NOT*** PASSED

PASSWORD FIELD IN IRM?	IRM PASSWORD FIELD BLANKS/NULLS?	RESULTS PASSED TO IMS IN OTMA SECURITY HEADER
YES	YES	**N/A**
YES	NO	**N/A** **NOTE: IRM PASSWORD IS USED IN IMS CONNECT VERIFY CALL**
NO	N/A	**N/A**

GROUP NAME PASSED

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

Userid/Group Used - *Security Exit* Invoked

USERID PASSED

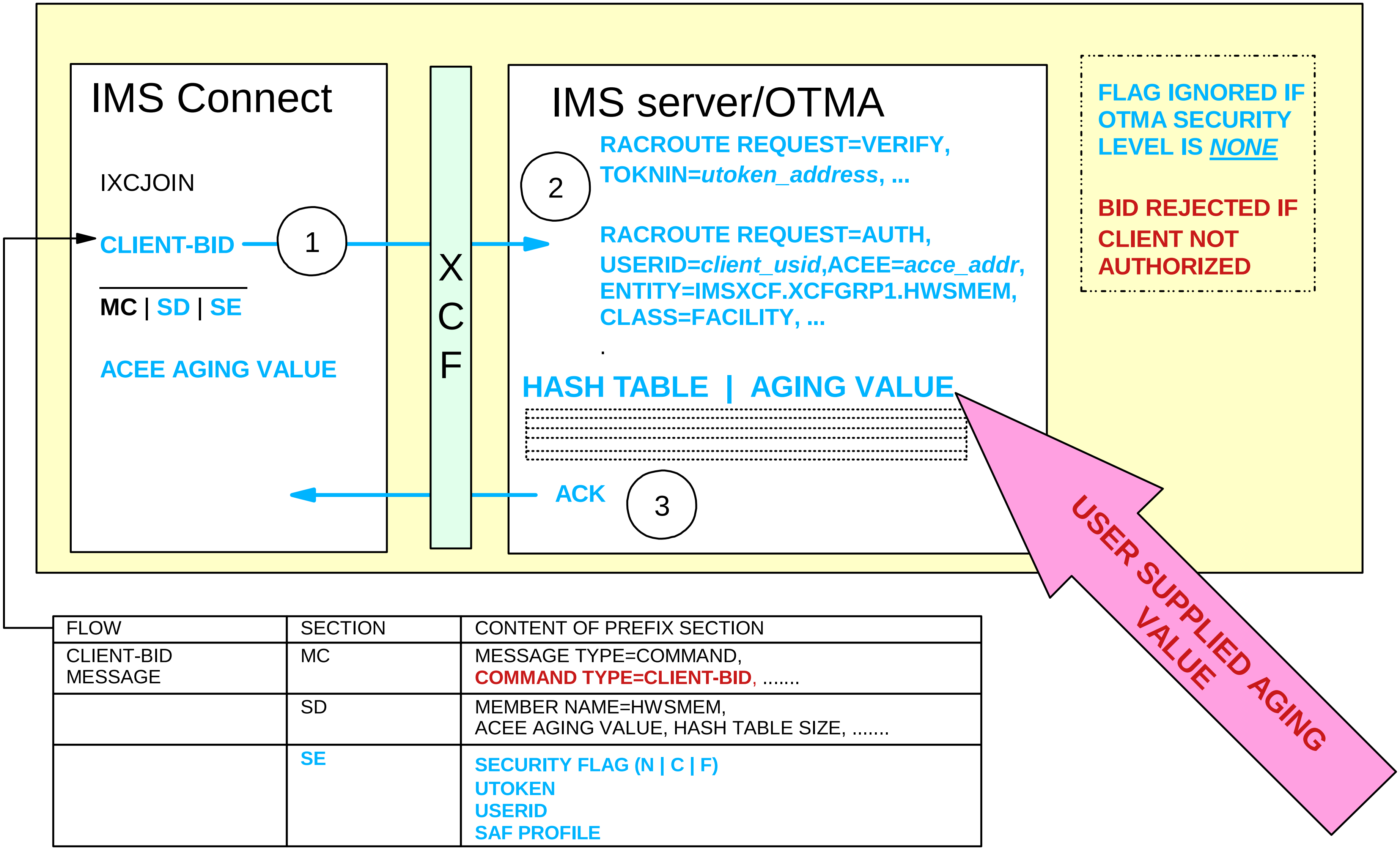
USERID FIELD IN IRM?	IRM USERID FIELD BLANK/NULL?	USERID RETURNED BY SECURITY EXIT?	RESULTS PASSED TO IMS IN OTMA SECURITY HEADER
YES	YES	NO	**DEFAULT RACFID USERID**
YES	YES	YES	**SECURITY EXIT RETURNED USERID**
YES	NO	NO	**USERID PASSED IN IRM**
YES	NO	YES	**SECURITY EXIT RETURNED USERID**
NO	N/A	NO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

IMS Connect Client-Bid

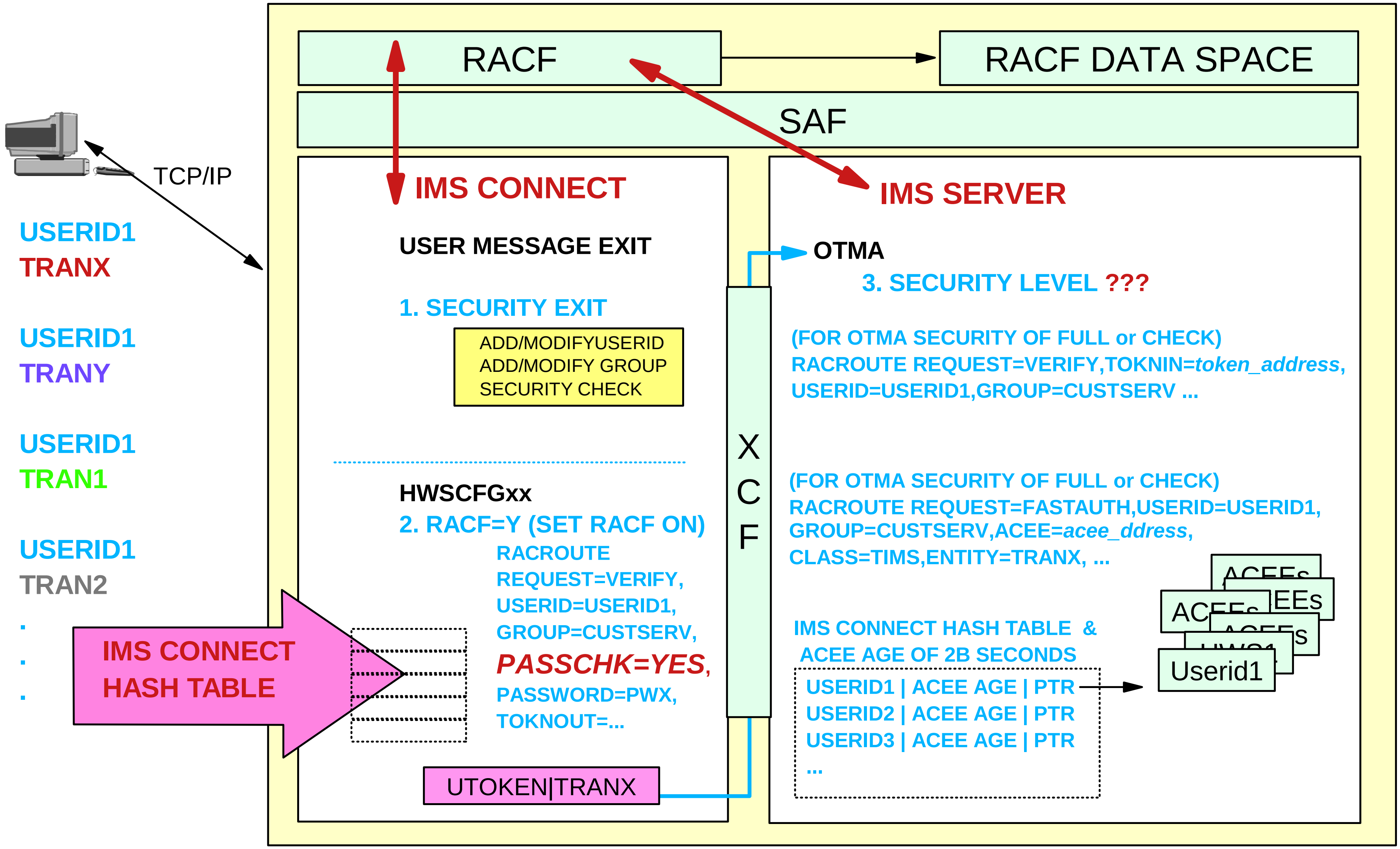


FLAG IGNORED IF OTMA SECURITY LEVEL IS *NONE*

BID REJECTED IF CLIENT NOT AUTHORIZED

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 Security Recap



RACF

RACF DATA SPACE

SAF

TCP/IP

USERID1
TRANX

USERID1
TRANY

USERID1
TRAN1

USERID1
TRAN2

.
.
.

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=...

IMS CONNECT
HASH TABLE

UTOKEN|TRANX

X
C
F

IMS SERVER

OTMA

3. SECURITY LEVEL ???

(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, ...

IMS CONNECT HASH TABLE &
ACEE AGE OF 2B SECONDS

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

Rebuilding the Hash Table in OTMA

- Security administrators could make significant changes to RACF information
  - User profiles
  - Group profile
  - Resource (transaction, data, command, etc.) profiles
- To cause OTMA client hash table for IMS Connect to be rebuilt, issue the STOPDS and OPENDS commands
  - *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 a GOOD thing !!

Customer Requests for 'Security' Enhancements

- IMS Connect customers have requested the following ***security*** enhancements

1. IMS Connect RACF userid validation only, no RACF password verification
2. Ability for user to specify ACEE aging value on client-bid
   - Use default ACEE aging value if not specified
3. Use of ACEE caching scheme, for example an IMS Connect hash table
4. Ability to specify values for *RACF=* and *RACFID=* on the DATASTORE statement
   - To override corresponding values on the HWS and TCP/IP statements respectively
     - Would support different IMS Connect security options for each target IMS

Customer Requests for 'Security' Enhancements ...

- IMS Connect customers have requested the following ***security*** enhancements **...**

5. Enhance IMS Connect to provide support for a 'password change'
   and a 'new password reverify' function
6. Enhance IMS Connect to support all of the following
   - Secure Socket Layer (SSL)
   - PassTickets
   - Digital certificates
7. Allow all message exits that are shipped with IMS Connect and associated connector products to invoke user-written security exit routines
   - HWSJAVA does not call the security exit

IMS Development Response To Customer Requests

- IMS development plans to address customer requests for IMS Connect ***security*** enhancements as follows

1. IMS Connect RACF userid validation only, no RACF password verification
   - ***Planned*** for delivery by December 31, 2002, via the service process

2. Ability for user to specify ACEE aging value on client-bid
   - ***Planned*** for delivery by December 31, 2002, via the service process

IMS Development Response To Customer Requests ...

3. Use of ACEE caching scheme, for example an IMS Connect hash table
   - ACEE caching scheme is already available for use by IMS Connect through the RACF Virtual Lookaside Facility (VLF) ACEE caching mechanism
     - VLF ACEE caching facility is deemed to be more appropriate and may be used in lieu of a 'hash table' scheme implementation in IMS Connect
     - z/OS 1.2 with APAR OW46269

4. Ability to specify values for *RACF=* and *RACFID=* on the DATASTORE statement
   - Enhancement is ***planned*** for delivery by allowing the user message exit routine to override the options
   - ***Planned*** for delivery by December 31, 2002, via the service process

IMS Development Response To Customer Requests ...

5. Enhance IMS Connect to provide support for a 'password change' and a 'new password reverify' function

   - Requirement may be met by the 'trusted user' support described in the '*IMS Connect RACF userid validation only, no RACF password verification*' enhancement

     - The IRM format enhancement to allow the IMS Connect client to set an 'already verified' flag to indicate that only the userid is to be verified (no password authentication)

     - When IMS Connect detects that the 'already verified' flag has been set in an incoming message, IMS Connect could invoke RACF with a PASSCHK=NO specification on the RACROUTE REQUEST=VERIFY macro

IMS Development Response To Customer Requests ...

6. Enhance IMS Connect to support SSL, PassTickets, and digital certificates
   - PassTicket support - APAR PQ48862
   - ***Planned*** for delivery by December 31, 2002, via the service process

7. Allow all message exits that are shipped with IMS Connect (e.g. HWSJAVA) and associated connector products to invoke user-written security exit routines
   - This is an existing capability
   - HWSJAVA0 and the related macros are shipped as source code
     - So the installation may modify the message exit and do security checking simply by
       - Providing the name of a security exit called by HWSJAVA0
(E.g. IMSLSECX may be invoked or an installation-provided exit name)
       - Defining the exit in the HWSJAVA0 message exit

Special Thanks To ...

- Customers
  - **Steve Nathan,** Telcordia
  - **Dave Cameron,** Royal Bank of Canada
    Ralph Spadafora, Royal Bank of Canada
    Greg Ross, Royal Bank of Canada
  - **Wang Chen,** Toronto Dominion Bank
  - **Jean Rollet**, AGF-French Insurance Group
  - **Nancy Hemmerly**, Bank One
- IBM
  - **Bob Gilliam**, Silicon Valley Lab, IMS Family Product Manager
    - **Jack Yuan**, Silicon Valley Lab, IMS Developer
    - **Gerald Hughes**, Silicon Valley Lab, IMS Developer and IMS Connect Developer
  - **Suzie Wendler**, IMS Technical Support, Dallas Systems Center

Additional Information

'*OTMA Guide and Reference*' manual

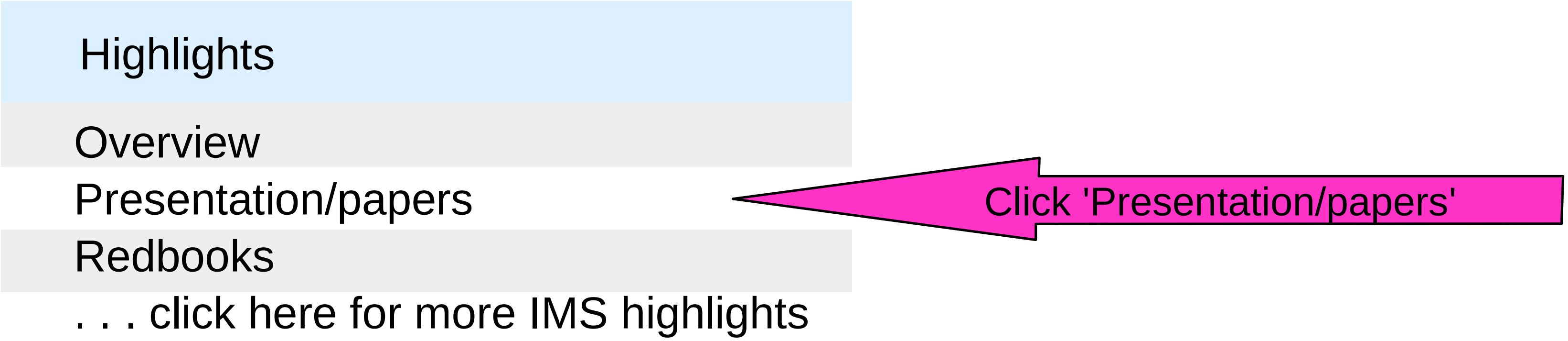
'*Security Options and Considerations*'

Abstract: A white paper detailing the security options for IMS/Open Transaction Manager (OTMA), IMS Connect, and the MQSeries-IMS Bridge Application

WEB sites

Exact page: http://www-3.ibm.com/software/data/ims/shelf/presentations/

From IMS home page: http://www-3.ibm.com/software/data/ims/



Highlights

Overview

Presentation/papers

Redbooks

. . . click here for more IMS highlights

Click 'Presentation/papers'

Summary

- Part 2
  - OTMA overview
  - IMS Connect
    - Overview
    - Security
  - Planned security enhancements for IMS Connect
    - IMS Development management & developers are committed to meeting customer requirements and continue to provide outstanding responsiveness
  - Additional information
    - Found in IMS Connect and IMS publications
    - Web site

Acronyms

- Cross-System Coupling Facility **(XCF)**
- IMS Request Message **(IRM)**
- Information Management System (IMS)
  - Open Transaction Manager Access **(OTMA)**
- Multiple Virtual Systems **(MVS)**
- Operating System/390 **(OS/390)**
- Program Properties Table **(PPT)**
- Resource Access Control Facility (**RACF)**
- System Authorization Facility **(SAF)**
- Transmission Control Protocol/Internet Protocol **(TCP/IP)**
- Virtual Telecommunications Access Method **(VTAM)**
- zSeries/Operating System **(z/OS)**

RACF Command Examples

- Sample RACF commands are shown

  - ► To secure the ***client-bid*** process for IMS Connect
    - – The check is actually performed by OTMA in the IMS subsystem

```
RDEFINE IMSXCF.XCFGRP1.HWSMEM UACC(NONE)
PERMIT IMSXCF.XCFGRP1.HWSMEM CLASS(FACILITY) ID(HWS1PROD) ACCESS(READ)
```

IMS CONNECT

  - ► To create a RACF group for IMS Connect

```
ADDGROUP  HWSPROD SUPGROUP(PRODSFTW) ...
```

  - ► To create a RACF userid for IMS Connect

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

RACF Command Examples ...

- Sample RACF commands are shown to secure

  - ***IMS commands*** entered by end users

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

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

  - ***IMS transactions*** entered by end users

```
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 OTMAUSRS) ACCESS(READ)
```

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

RETURN TO INDEX