E37

IMS/OTMA Security Considerations Part 1 of 2

Alonia (Lonnie) Coleman

IMS Technical Conference

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

RETURN TO INDEX

Agenda

- Part 1
  - Open Transaction Manager Access (OTMA)
    - Overview
    - Security overview
    - Security levels
      - NONE
      - CHECK
      - FULL
      - PROFILE
    - Callable Interface (OTMA CI)
    - Security enhancements update
  - Summary
  - Additional information and Attachments

OTMA Overview

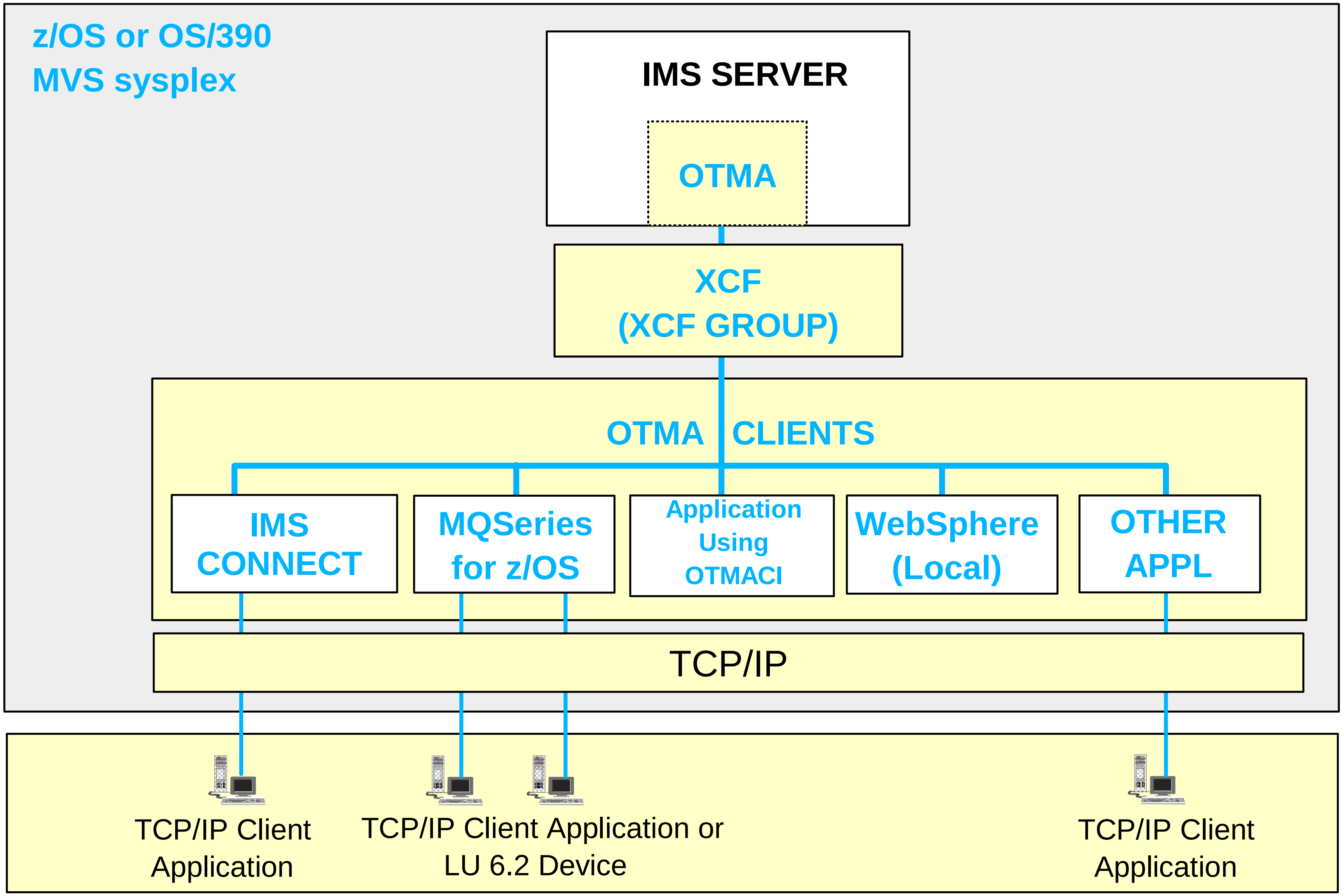
- What Is OTMA?
  - A client-server protocol that
    - Has high performance
    - Is transaction-based
    - Is connectionless

- OTMA
  - Provides a gateway for transactions outside IMS to enter IMS
  - Allows MVS (z/OS and OS/390) programs to access IMS
    - These MVS programs are called OTMA clients
  - Uses MVS Cross-System Coupling Facility (XCF) services
    - XCF facilitates communications between OTMA and OTMA clients

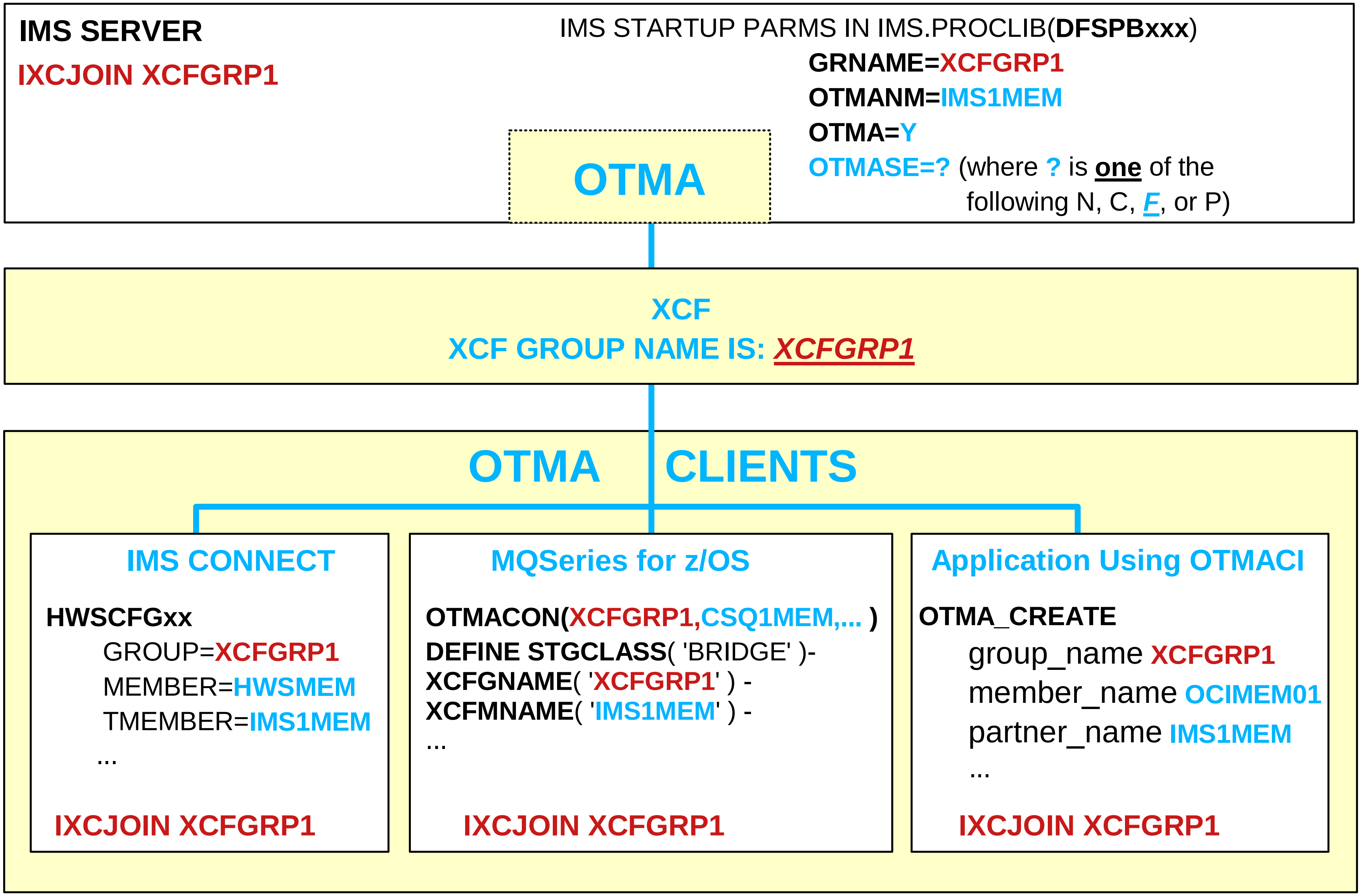
OTMA Clients

- OTMA clients
  - Format and send input messages to OTMA
    - Remove TCP/IP headers
    - Translate ASCII to EBCDIC
    - Build OTMA headers
    - Perform userid validation and password verification
  - Format output messages from OTMA and transmit to clients
    - Remove OTMA headers
    - Translate EBCDIC to ASCII
    - Build TCP/IP headers
    - Transmit output response message to TCP/IP client
  - Must be authorized to connect to OTMA if OTMA security is activated

OTMA Clients In An XCF Group



Joining The Same XCF Group



IMS SERVER

IXCJOIN XCFGRP1

IMS STARTUP PARMS IN IMS.PROCLIB(**DFSPBxxx**)

```
GRNAME=XCFGRP1
OTMANM=IMS1MEM
OTMA=Y
OTMASE=? (where ? is one of the
          following N, C, F, or P)
```

OTMA

XCF

XCF GROUP NAME IS: ***XCFGRP1***

OTMA CLIENTS

IMS CONNECT

```
HWSCFGxx
     GROUP=XCFGRP1
     MEMBER=HWSMEM
     TMEMBER=IMS1MEM
     ...
```

IXCJOIN XCFGRP1

MQSeries for z/OS

```
OTMACON(XCFGRP1,CSQ1MEM,... )
DEFINE STGCLASS( 'BRIDGE' )-
XCFGNAME( 'XCFGRP1' ) -
XCFMNAME( 'IMS1MEM' ) -
...
```

IXCJOIN XCFGRP1

Application Using OTMACI

```
OTMA_CREATE
     group_name XCFGRP1
     member_name OCIMEM01
     partner_name IMS1MEM
     ...
```

IXCJOIN XCFGRP1

Messages Destined For OTMA

- The client-bid message
  - Sent by OTMA client to OTMA
    - Requests a connection to OTMA
    - Must be the 1st message sent to OTMA
  - Contains security info

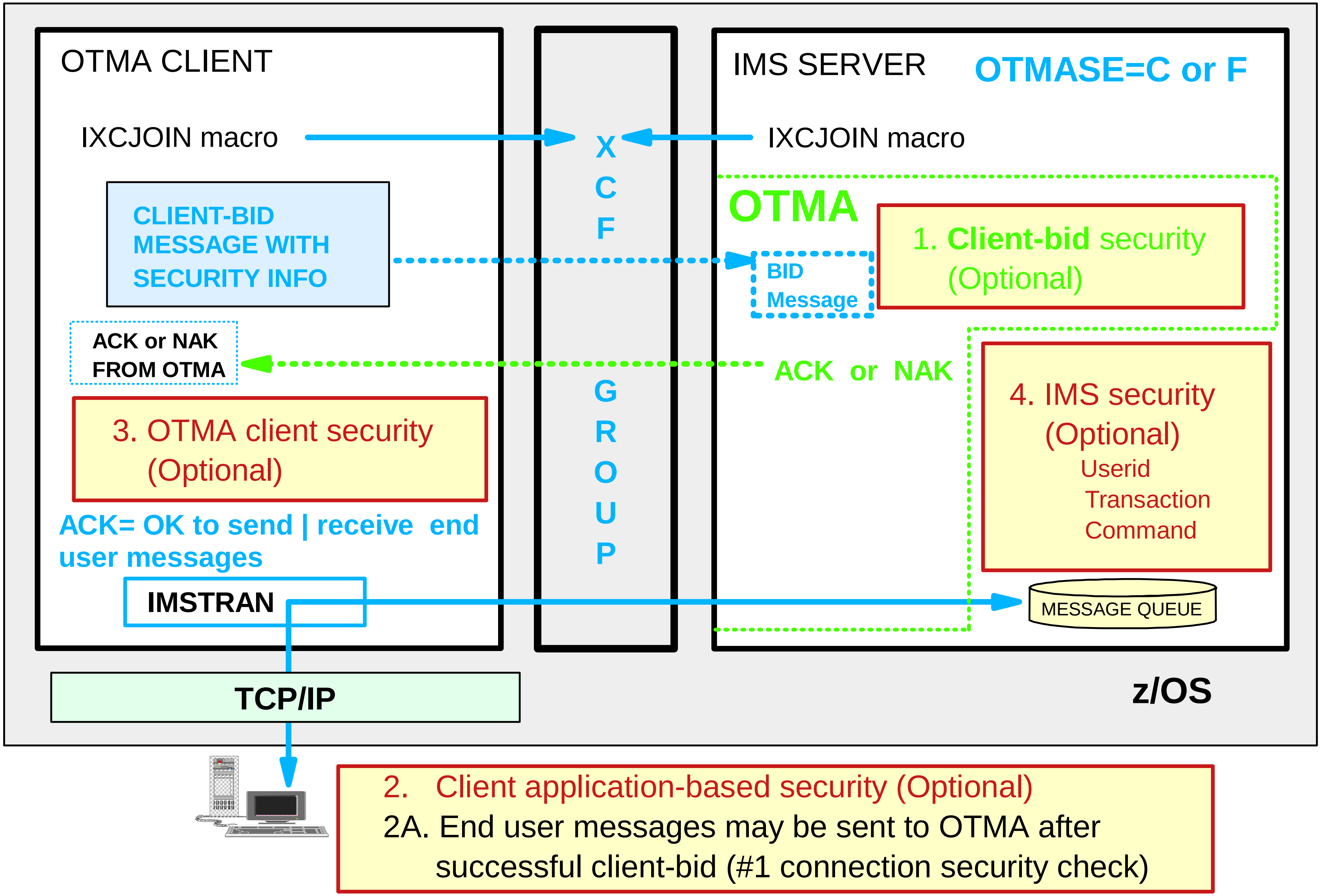
- End user messages
  - Sent to the OTMA client for formatting and transmission to OTMA
  - May be sent to OTMA by the OTMA client only after a successful client-bid
  - Contain security info

OTMA MESSAGE PREFIX	**MESSAGE TYPE**	
MESSAGE CONTROL INFORMATION (MCI)	**CLIENT-BID**	**END USER** TRANSACTION OR COMMAND
STATE DATA (SD)	**ACEE AGING VALUE, ...**	
SECURITY DATA (SE)	**SECURITY FLAG (N / C / F)** **UTOKEN** **USERID** **SAF PROFILE**	**SECURITY FLAG (N / C / F)** **UTOKEN** **USERID** **SAF PROFILE**
APPLICATION DATA		TRANSACTION CODE -OR- COMMAND

OTMA Security Overview

- A number of security checking options are available for OTMA environments
  1. OTMA client-bid security checking (optional)
     - Performed by OTMA and RACF
  2. Client-based security checking (optional)
     - Performed by TCP/IP client application
  3. OTMA client (e.g. IMS Connect or WebSphere MQ-IMS Bridge) userid validation and optionally, password verification
     - Performed by the OTMA client
  4. IMS and OTMA security (optional)
     - OTMA end user userid validation (password is not verified)
       - Performed by OTMA and RACF
     - IMS command authorization
       - Performed by RACF, user-written exit, or both
     - IMS transaction authorization
       - Performed by RACF, user-written exits, or both

End-To-End Security Options



OTMA CLIENT

IXCJOIN macro

CLIENT-BID
MESSAGE WITH
SECURITY INFO

ACK or NAK
FROM OTMA

3. OTMA client security
(Optional)

ACK= OK to send | receive end user messages

IMSTRAN

X
C
F

G
R
O
U
P

IMS SERVER

OTMASE=C or F

IXCJOIN macro

OTMA

BID
Message

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

ACK or NAK

4. IMS security
(Optional)
Userid
Transaction
Command

MESSAGE QUEUE

TCP/IP

z/OS

2. Client application-based security (Optional)

2A. End user messages may be sent to OTMA after
successful client-bid (#1 connection security check)

OTMA Security Options

- The security options available to OTMA users are
  - **No security at all** for messages received via OTMA
  - **No RACF security** for messages received via OTMA
  - **RACF security** for messages received via OTMA
  - **User-written security exit** routine(s)may be used to secure IMS commands and transactions received via OTMA
  - **Both RACF and user-written exit** routines may be used to secure messages received via OTMA
- If OTMA security is desired, **RACF** authorization (or validation) checking is performed for ***all*** of the following
  - Client-bid connection requests
  - Userid validation, IMS command authorization, and IMS transaction authorization

OTMA Security Levels

- There are four OTMA security levels
  - NONE
  - CHECK
  - FULL
  - PROFILE

- One OTMA security level may used at a time

- An OTMA security level may be set by either an
  - IMS execution parameter
    - OTMASE=N, OTMASE=C, OTMASE=***F***, or OTMASE=P
  - IMS command
    - /SECURE OTMA NONE, /SECURE OTMA CHECK, ***/SECURE OTMA FULL***, or /SECURE OTMA PROFILE

OTMA Security Level NONE

- RACF is ***not*** invoked by OTMA for
  - ***Client-bids*** which results in all bids being allowed
  - ***Command authorization***
    - However IMS does enforce '***default security***' if the Command Authorization Exit Routine (DFSCCMD0) is not invoked
  - ***Transaction authorization***

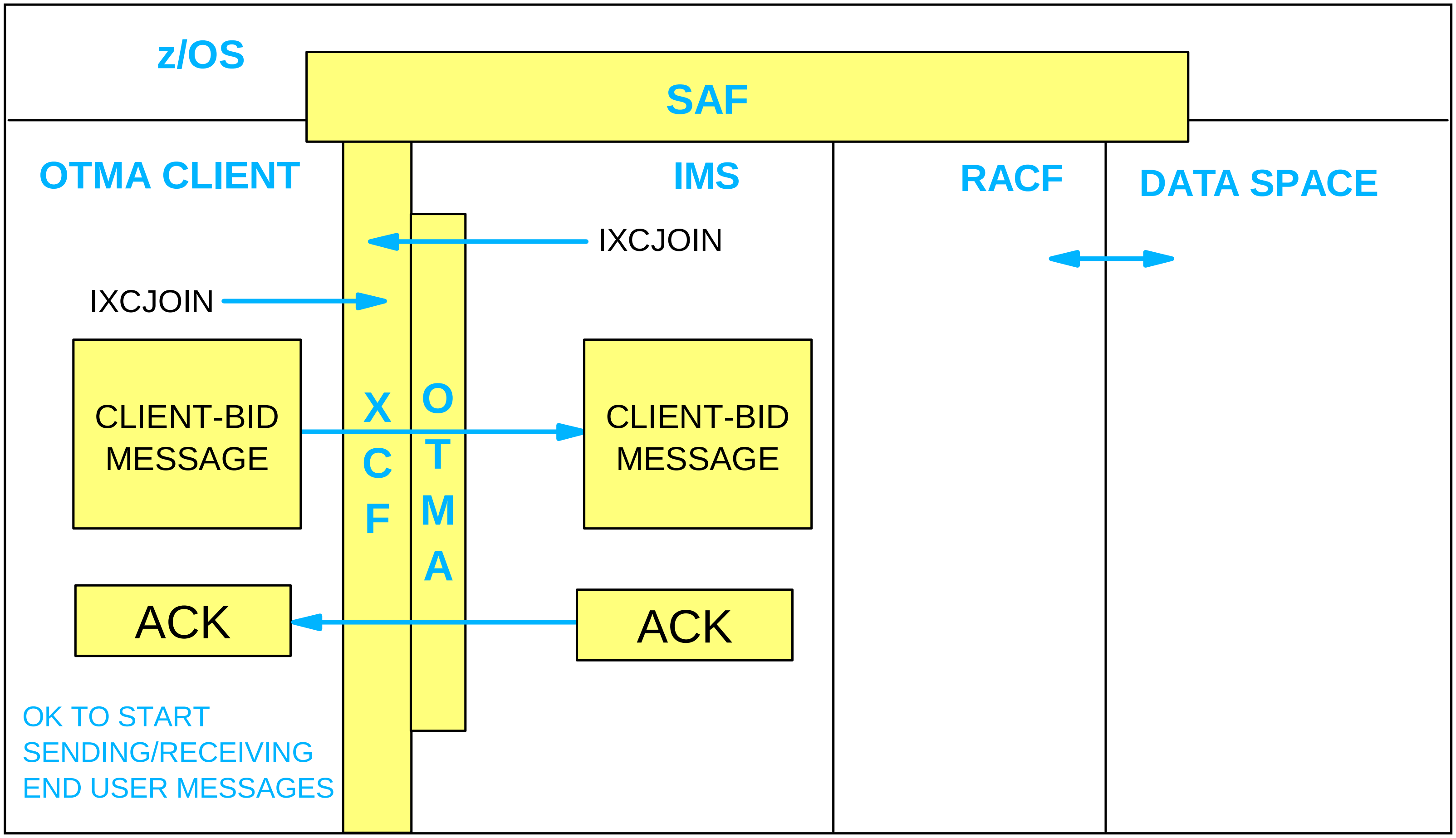
Exception: RACF ***may be*** invoked for resources (transaction codes, databases, segments, fields, or other database resources) requested by application programs which issue CHNG calls, AUTH calls, and/or perform deferred conversational program-to-program message switches. To disable the calls to RACF apply the following maintenance:

APAR PQ02865/PTF UQ05169 and APAR PQ33602/PTF UQ41660 for IMS V6
APAR PQ33603/PTF UQ41663 for IMS V7

- User written security exit routines ***are*** invoked
  - Command Authorization Exit ***(DFSCCMD0)***
  - Transaction Authorization Exit ***(DFSCTRN0)***
  - Security Reverification Exit ***(DFSCTSE0)***

/SEC OTMA NONE or OTMASE=N

For Client-Bid Requests



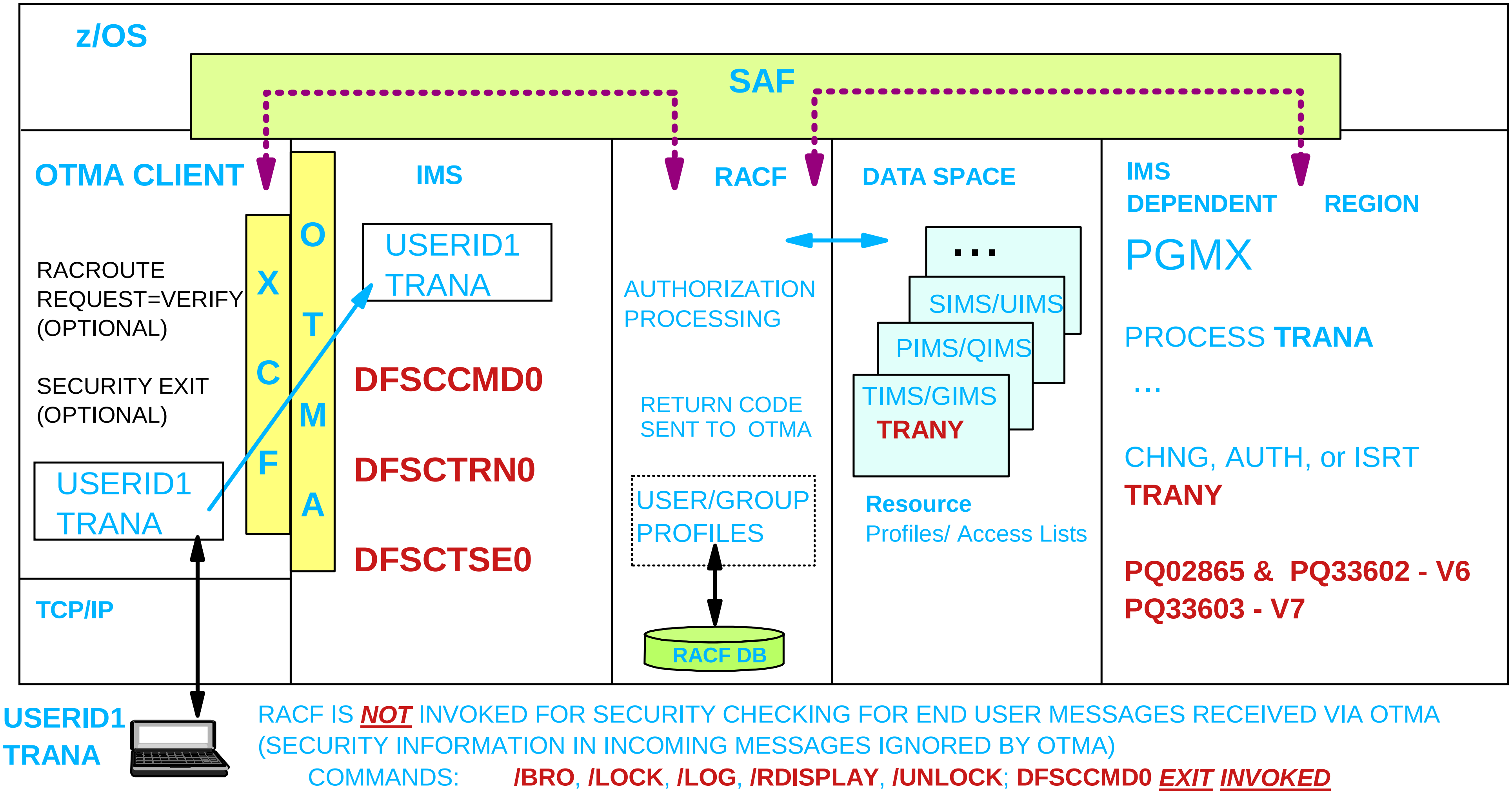
RACF IS NOT CALLED BY OTMA FOR CLIENT-BID CONNECTION SECURITY CHECKING

AS A RESULT, ALL CLIENT-BID CONNECTION REQUESTS ARE ALLOWED

SECURITY FLAG AND OTHER SECURITY INFO IN CLIENT-BID MESSAGE IGNORED BY OTMA

/SEC OTMA NONE or OTMASE=N

For End User Messages



RACF IS ***NOT*** INVOKED FOR SECURITY CHECKING FOR END USER MESSAGES RECEIVED VIA OTMA (SECURITY INFORMATION IN INCOMING MESSAGES IGNORED BY OTMA)

COMMANDS: **/BRO**, **/LOCK**, **/LOG**, **/RDISPLAY**, **/UNLOCK**; **DFSCCMD0** ***EXIT INVOKED***

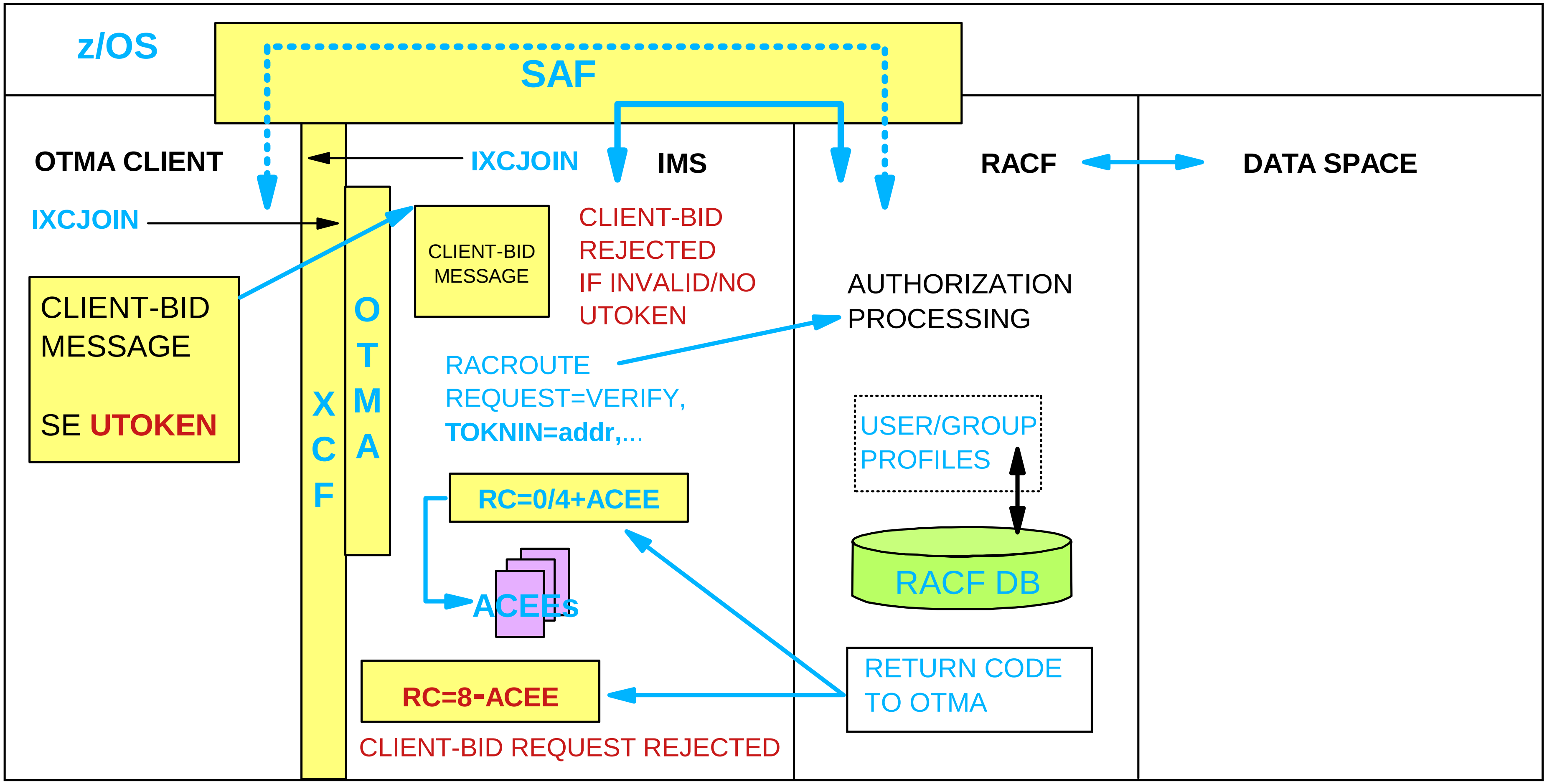
TRANSACTIONS: RACF NOT INVOKED UNLESS APARS ARE NOT INSTALLED; **DFSCTRN0** AND **DFSCTSE0** EXITS ***ARE INVOKED***

OTMA Security Level CHECK

- RACF ***is*** invoked by OTMA for
  - ***Client-bid*** security checking
    - Bid must contain valid ***UTOKEN*** for authorized OTMA client, otherwise bid is rejected
  - ***Userid validation*** for client-bid and end user messages
    - ACEE (RACF security control block) is built in the control region only
  - ***Command authorization***
    - CIMS | DIMS resource classes (or equivalent) are used by RACF
      - OTMA allows access to commands that are not protected by a RACF profile
  - ***Transaction authorization***
    - TIMS | GIMS resource classes (or equivalent) are used by RACF
      - OTMA allows access to transactions that are not protected by a RACF profile
- User written security exit routines ***may be*** invoked
  - Command Authorization Exit ***(DFSCCMD0) is*** invoked
  - Transaction Authorization Exit ***(DFSCTRN0) is only invoked*** when the RACF return code (RC) is '**0**' or '**4**'
  - Security Reverification Exit ***(DFSCTSE0) is*** invoked

/SEC OTMA CHECK or OTMASE=C

For Client-Bid Requests (Part 1)



RACF ***IS*** INVOKED BY OTMA FOR CLIENT-BID CONNECTION SECURITY CHECKING

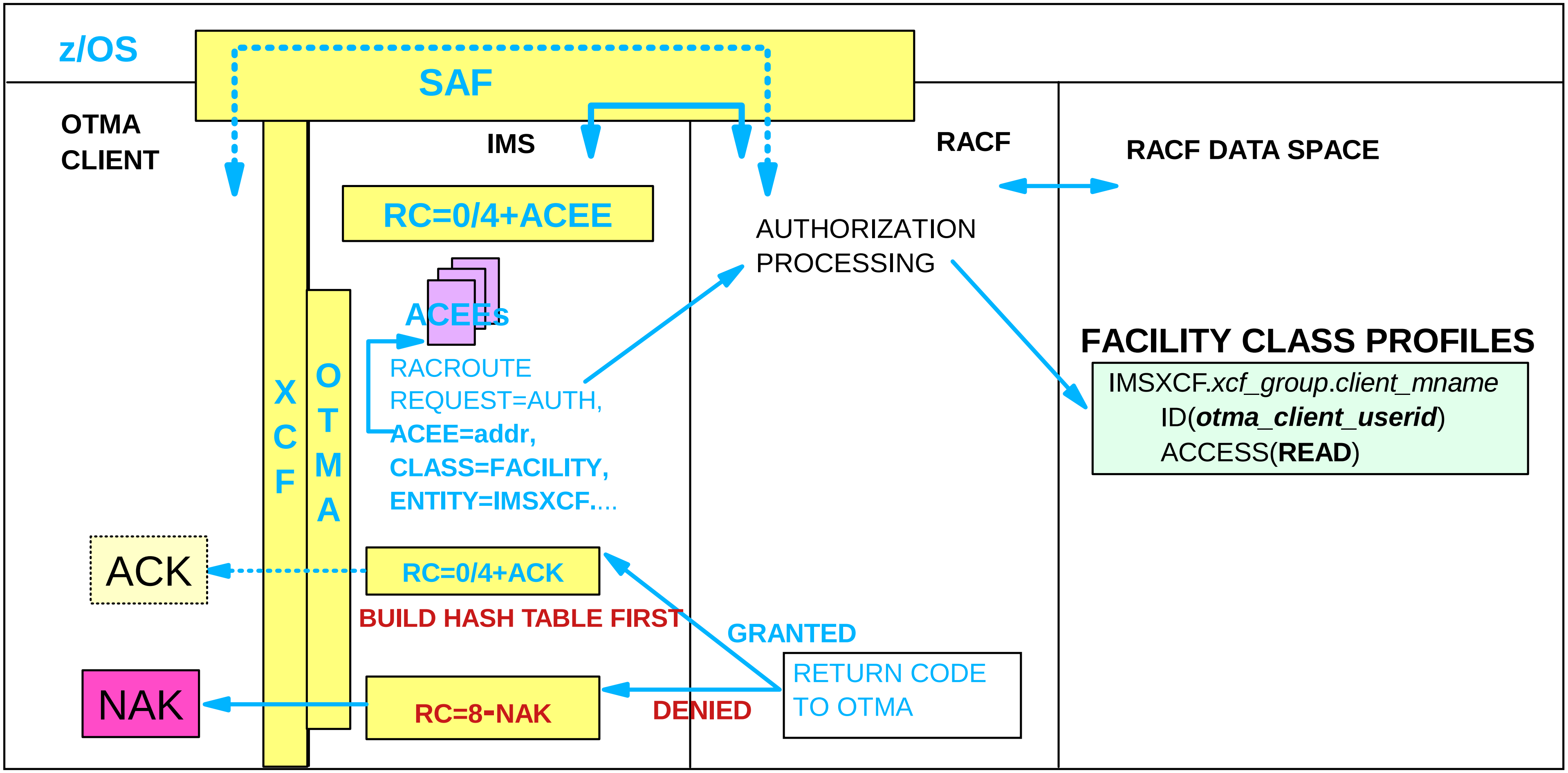
a. TO VERIFY THAT THE SECURITY INFO IN THE UTOKEN IS VALID; **UTOKEN IS REQUIRED FOR AUTHORIZED OTMA CLIENT OR CLIENT-BID IS REJECTED**

b. TO RETURN AN ACEE FOR THE OTMA CLIENT IF THE USERID (AND OPTIONALLY, GROUP) IS VALID

c. TO CHECK THE APPROPRIATE FACILITY CLASS PROFILE TO DETERMINE IF THE OTMA CLIENT CAN CONNECT TO OTMA

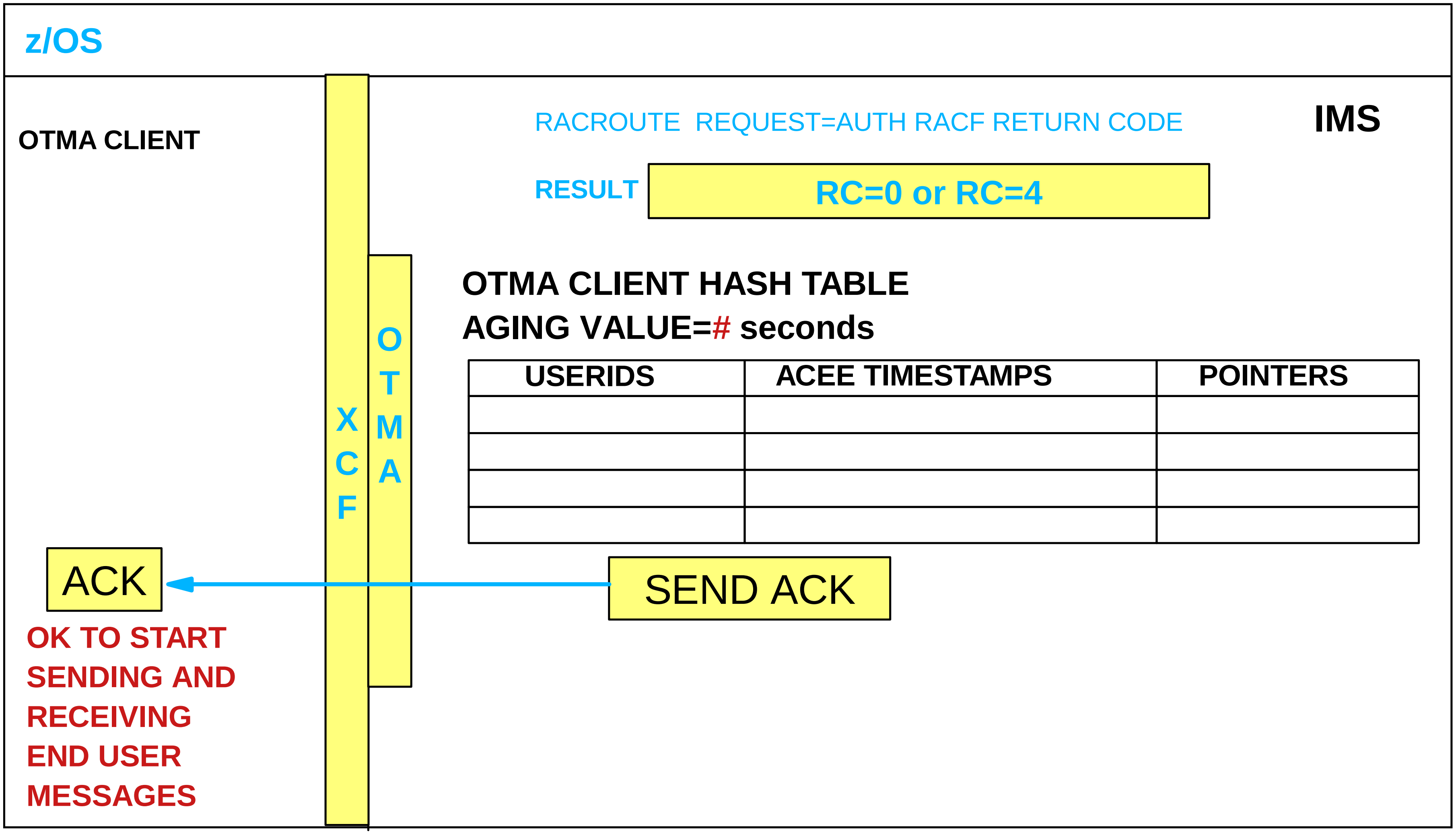
/SEC OTMA CHECK or OTMASE=C

For Client-Bid Requests (Part 2)



/SEC OTMA CHECK or OTMASE=C

A Successful Client-Bid (Part 3)



z/OS

OTMA CLIENT

IMS

RACROUTE REQUEST=AUTH RACF RETURN CODE

RESULT

RC=0 or RC=4

OTMA CLIENT HASH TABLE

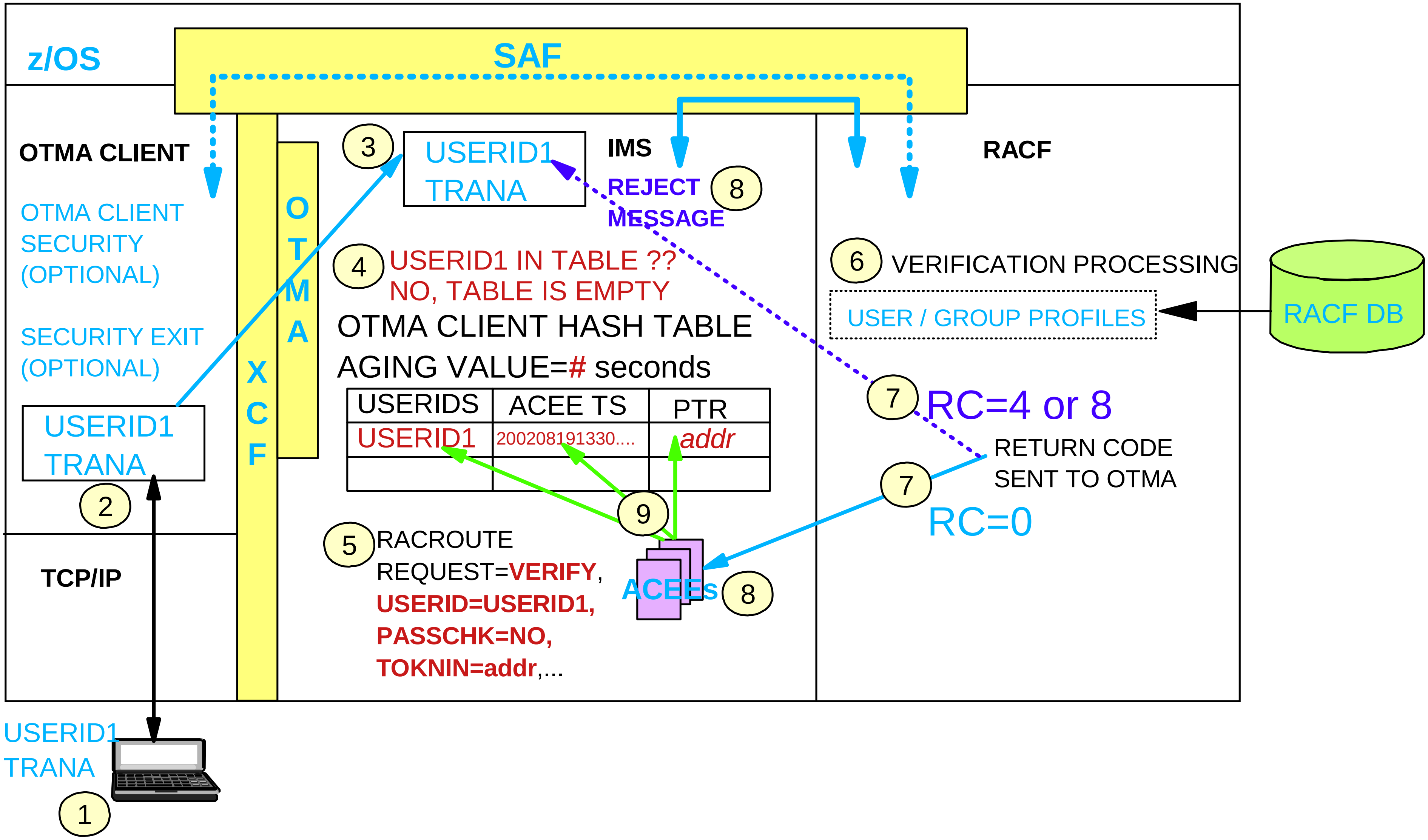
AGING VALUE=# seconds

USERIDS	ACEE TIMESTAMPS	POINTERS

OK TO START SENDING AND RECEIVING END USER MESSAGES

/SEC OTMA CHECK or OTMASE=C

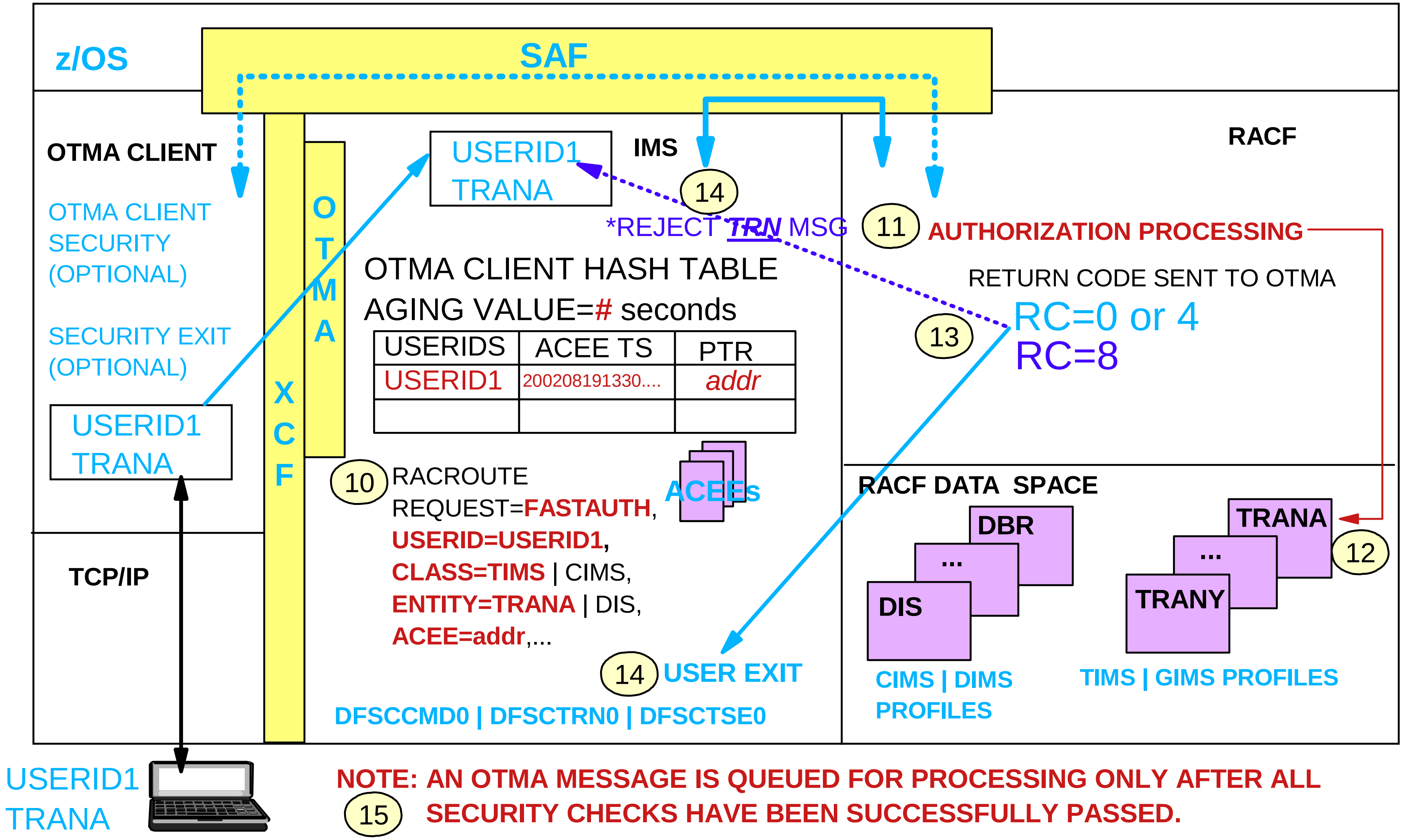
For End User Messages (Part 1A)



USERIDS	ACEE TS	PTR
USERID1	200208191330....	addr

/SEC OTMA CHECK or OTMASE=C

For End User Messages (Part 1B)



z/OS

SAF

OTMA CLIENT

OTMA CLIENT SECURITY (OPTIONAL)

SECURITY EXIT (OPTIONAL)

USERID1
TRANA

TCP/IP

XCF

OTMA

USERID1
TRANA

IMS

14 *REJECT ~~TRN~~ MSG

OTMA CLIENT HASH TABLE

AGING VALUE=# seconds

USERIDS	ACEE TS	PTR
USERID1	200208191330....	*addr*

10 RACROUTE
REQUEST=**FASTAUTH**,
USERID=USERID1,
CLASS=TIMS | CIMS,
ENTITY=TRANA | DIS,
ACEE=addr,...

ACEEs

14 **USER EXIT**

DFSCCMD0 | DFSCTRN0 | DFSCTSE0

RACF

11 **AUTHORIZATION PROCESSING**

RETURN CODE SENT TO OTMA

13 RC=0 or 4
RC=8

RACF DATA SPACE

DBR

...

DIS

CIMS | DIMS PROFILES

TRANA 12

...

TRANY

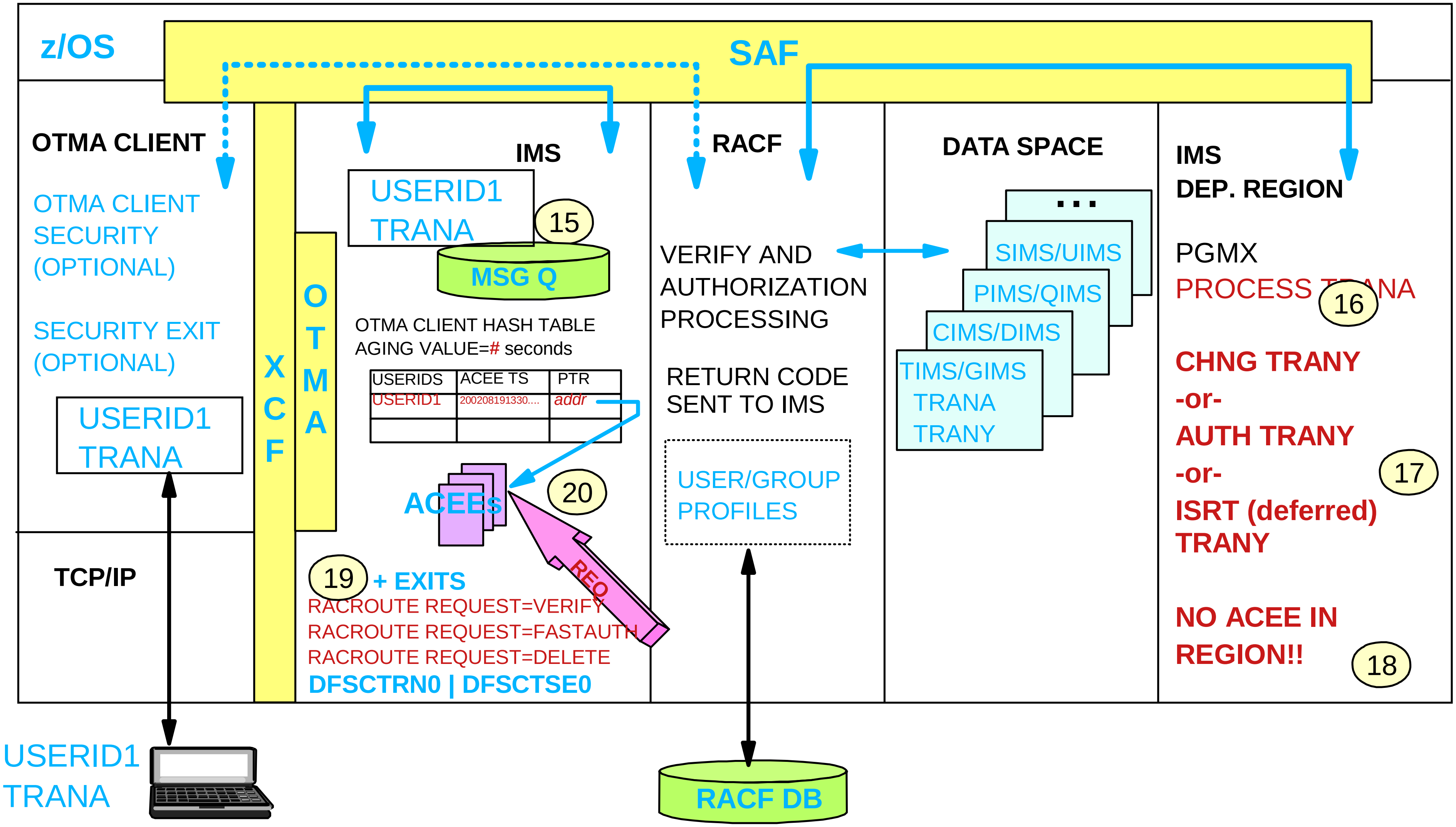
TIMS | GIMS PROFILES

USERID1
TRANA

NOTE: AN OTMA MESSAGE IS QUEUED FOR PROCESSING ONLY AFTER ALL
15 **SECURITY CHECKS HAVE BEEN SUCCESSFULLY PASSED.**

/SEC OTMA CHECK or OTMASE=C

Processing End User Transactions



z/OS

SAF

OTMA CLIENT

OTMA CLIENT SECURITY (OPTIONAL)

SECURITY EXIT (OPTIONAL)

USERID1
TRANA

TCP/IP

USERID1
TRANA

XCF

OTMA

IMS

USERID1
TRANA

15

MSG Q

OTMA CLIENT HASH TABLE
AGING VALUE=# seconds

USERIDS	ACEE TS	PTR
USERID1	200208191330....	*addr*

ACEEs

20

REQ

19 + EXITS

RACROUTE REQUEST=VERIFY
RACROUTE REQUEST=FASTAUTH
RACROUTE REQUEST=DELETE

DFSCTRN0 | DFSCTSE0

RACF

VERIFY AND AUTHORIZATION PROCESSING

RETURN CODE SENT TO IMS

USER/GROUP PROFILES

RACF DB

DATA SPACE

. . .

SIMS/UIMS

PIMS/QIMS

CIMS/DIMS

TIMS/GIMS
TRANA
TRANY

IMS
DEP. REGION

PGMX
PROCESS TRANA

16

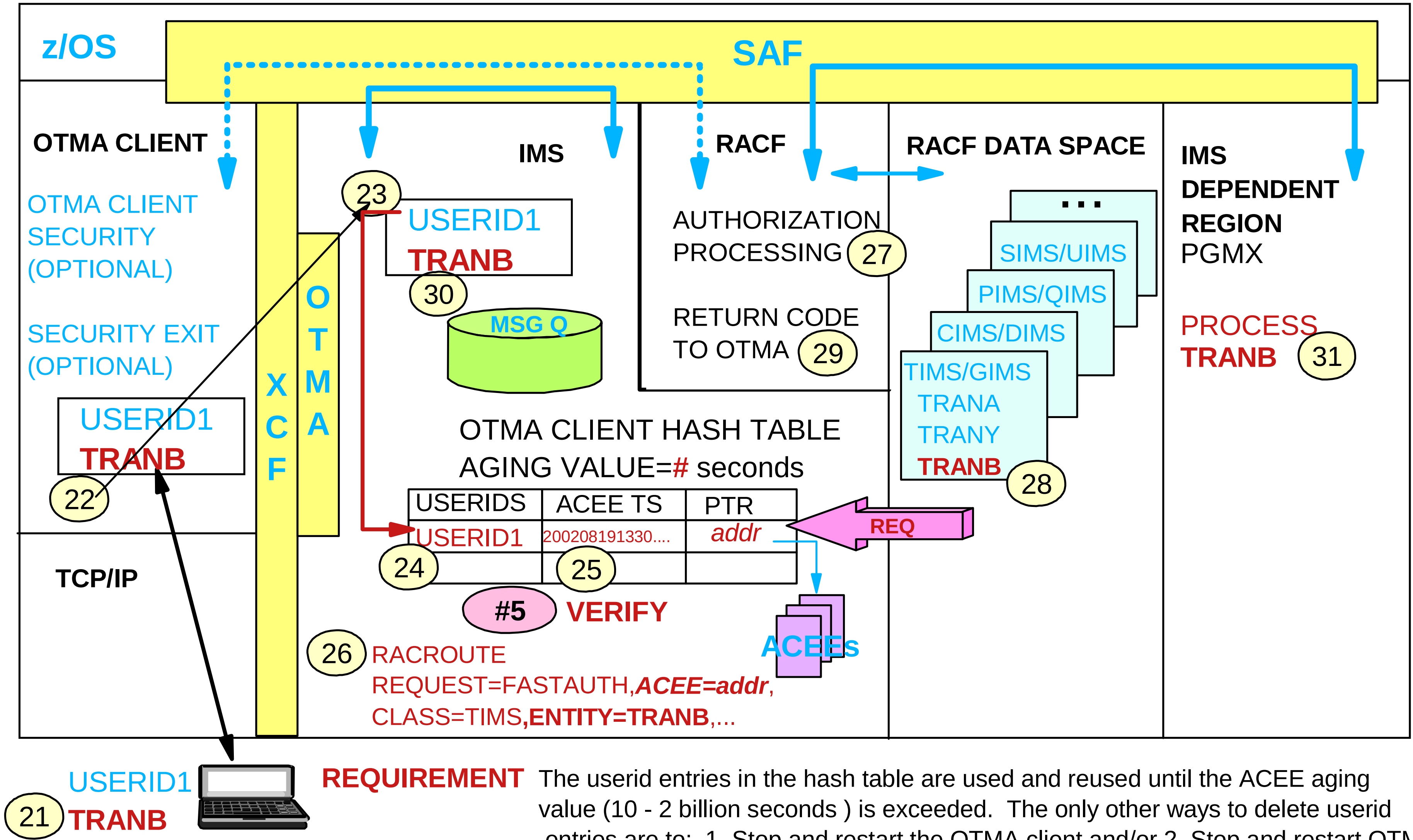
CHNG TRANY
-or-
AUTH TRANY
-or-
ISRT (deferred)
TRANY

17

NO ACEE IN REGION!!

18

Hash Table Use



USERIDS	ACEE TS	PTR
USERID1	200208191330....	addr

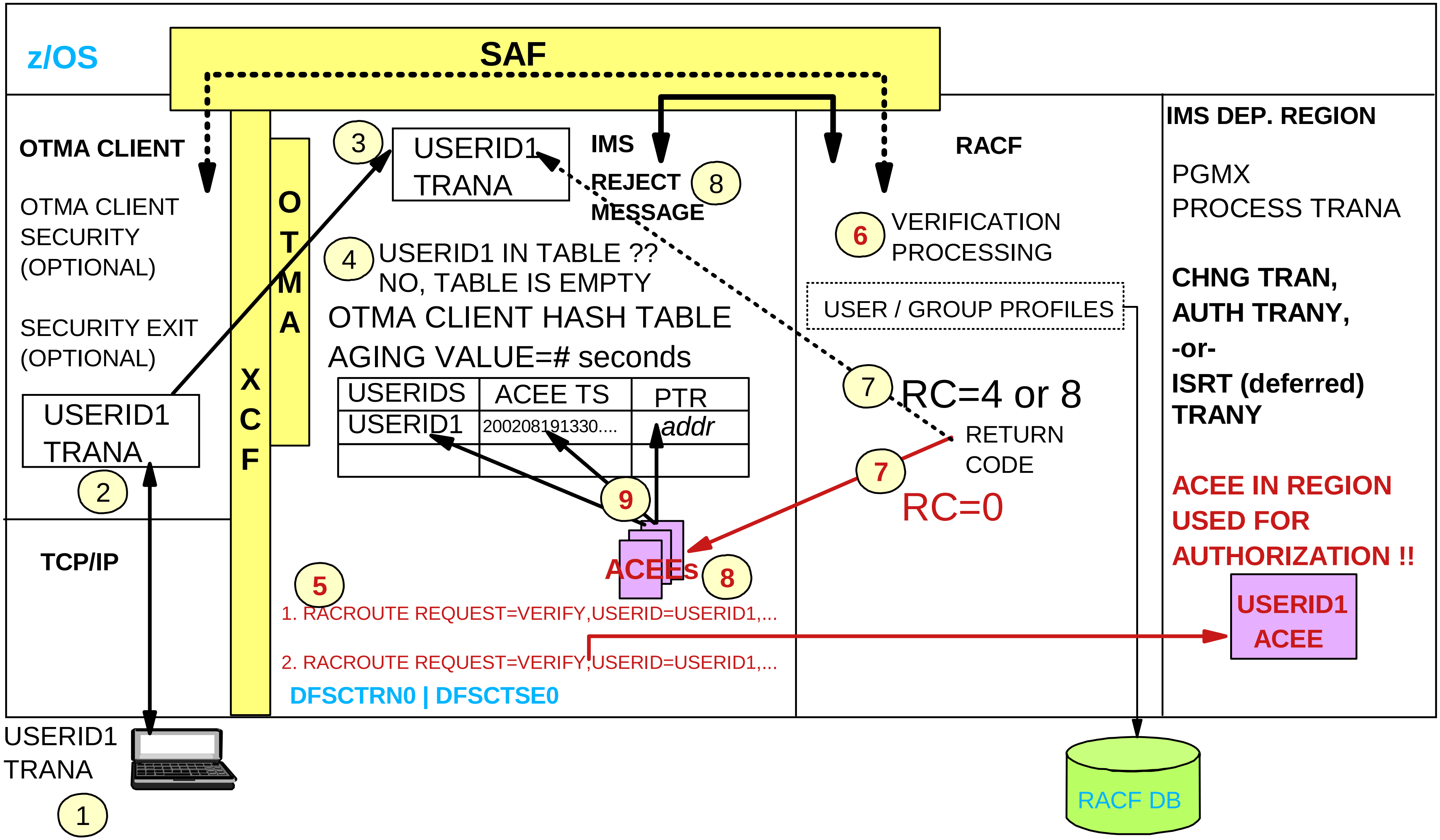
RACROUTE
REQUEST=FASTAUTH,***ACEE=addr***,
CLASS=TIMS,**ENTITY=TRANB**,...

REQUIREMENT The userid entries in the hash table are used and reused until the ACEE aging value (10 - 2 billion seconds) is exceeded. The only other ways to delete userid entries are to: 1. Stop and restart the OTMA client and/or 2. Stop and restart OTMA.

OTMA Security Level FULL

- When an OTMA security level of ***FULL*** is used
  - OTMA and RACF processing
    - For ***client-bid*** security checking is ***identical*** to the processing performed for OTMA security level **CHECK**
    - For ***command authorization*** checking is ***identical*** to the processing performed for OTMA security level **CHECK**
    - Are done in a ***different*** manner for ***both*** of the following
      1. ***Userid validation*** for an ***end user***
         - Two ACEEs are build during VERIFY processing (one for the control region plus a second ACEE for the dependent region)
      2. ***RACF transaction authorization***
         - The ACEE built in the dependent region is used for transaction authorization and/or database resource authorization
         - The transaction or database resource is requested by one of the following: CHNG call, AUTH call, and/or deferred conversational program-to-program message switch
  - DFSCCMD0, DFSCTRN0, and DFSCTSE0 exit routines are invoked in the same manner as for OTMA security level **CHECK**
  - The OTMA client's hash table is used the same way for incoming messages as is done for the OTMA security level **CHECK**

/SEC OTMA FULL or OTMASE=F
For End User Messages



z/OS

SAF

OTMA CLIENT

OTMA CLIENT SECURITY (OPTIONAL)

SECURITY EXIT (OPTIONAL)

USERID1
TRANA

2

TCP/IP

XCF

OTMA

3 USERID1
TRANA

IMS REJECT MESSAGE 8

4 USERID1 IN TABLE ??
NO, TABLE IS EMPTY

OTMA CLIENT HASH TABLE

AGING VALUE=# seconds

USERIDS	ACEE TS	PTR
USERID1	200208191330....	*addr*

9

ACEEs 8

5
1. RACROUTE REQUEST=VERIFY,USERID=USERID1,...
2. RACROUTE REQUEST=VERIFY,USERID=USERID1,...

DFSCTRN0 | DFSCTSE0

RACF

6 VERIFICATION PROCESSING

USER / GROUP PROFILES

7 RC=4 or 8

RETURN CODE

7 RC=0

RACF DB

IMS DEP. REGION

PGMX
PROCESS TRANA

CHNG TRAN,
AUTH TRANY,
-or-
ISRT (deferred)
TRANY

ACEE IN REGION USED FOR AUTHORIZATION !!

USERID1 ACEE

USERID1
TRANA

1

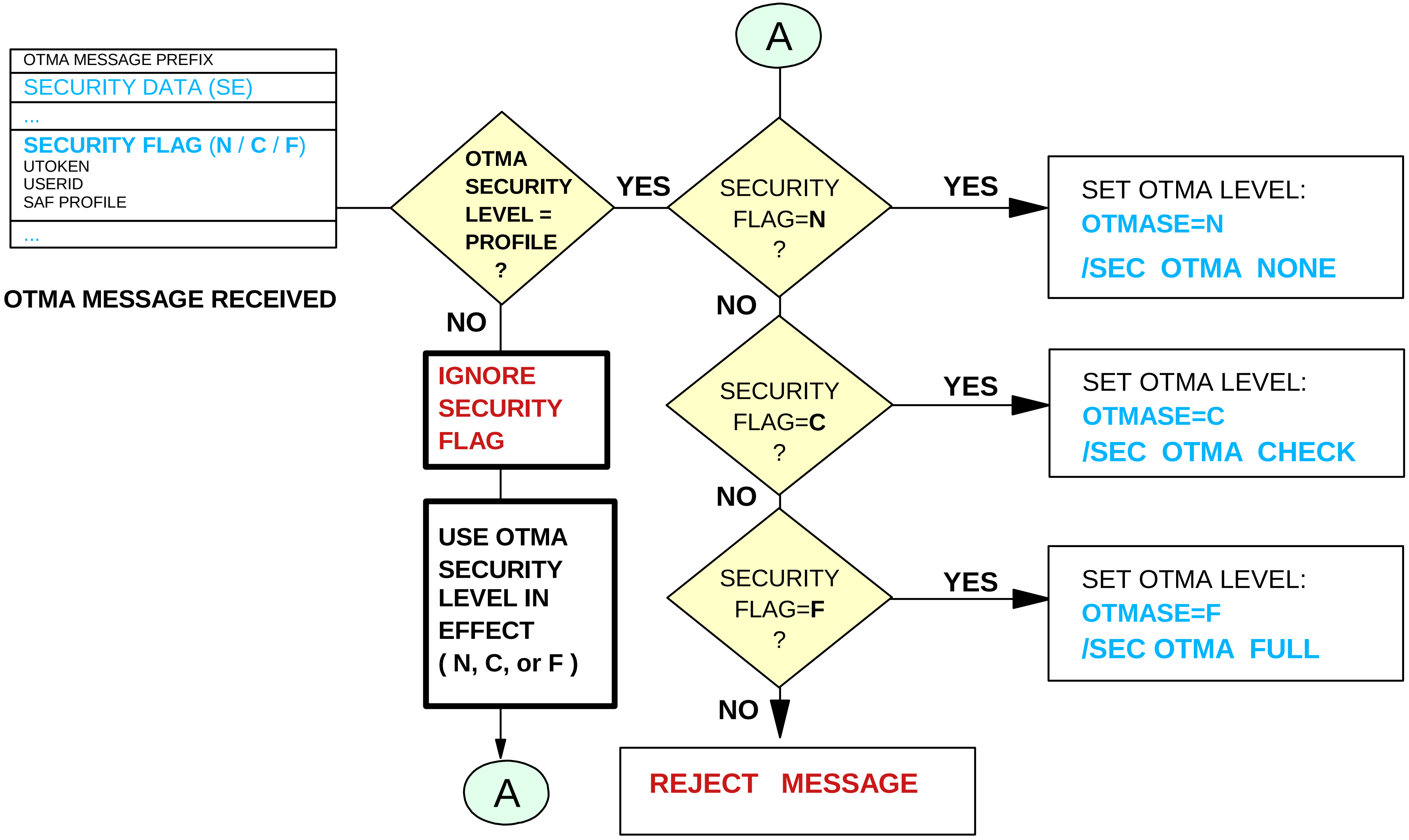
Impact of 2nd ACEE In Resource Authorization Processing

MAXIMUM NUMBER OF TIMES RACF INVOKED FOR OTMA SECURITY LEVEL	**FULL**	**CHECK**
RACROUTE **REQUEST=VERIFY,ENVIR=CREATE**,... (BUILD ACEE IN CONTROL REGION UPON RECEIPT OF INITIAL INPUT MESSAGE)	1	1
RACROUTE **REQUEST=VERIFY,ENVIR=CREATE**,... (BUILD ACEE IN DEPENDENT REGION FOR VERIFIED USERID)	1	0 (NA)
RACROUTE **REQUEST=FASTAUTH,ACEE=*acee_address***,CLASS=TIMS,ENTITY=TRANX... (TRANSACTION AUTHORIZATION CHECK FOR TRANSACTION REQUESTED IN INITIAL MESSAGE)	1	1
APPLICATION PROGRAM ISSUES 30 CHNG CALLS, EACH REQUESTING AN IMS TRANSACTION CODE		
RACROUTE **REQUEST=VERIFY,ENVIR=CREATE**,**USERID=*user_id*,**.... [VERIFY AND BUILD SECURITY CONTROL BLOCK (ACEE) FOR USERID IN IOPCB OF INITIAL MESSAGE]	0 (NA)	30
RACROUTE REQUEST=FASTAUTH,ACEE=acee_address,CLASS=TIMS,ENTITY=TRANY,... (TRANSACTION AUTHORIZATION CHECK FOR TRANSACTION REQUESTED VIA CHNG CALL)	30	30
RACROUTE **REQUEST=VERIFY,ENVIR=DELETE**,**USERID=user_id**,**ACEE=acee_address**,... (DELETE ACEE WHEN NO LONGER REQUIRED)	1	30
TOTAL NUMBER OF TIMES RACF INVOKED	**34**	**92**

OTMA Security Level PROFILE

- Using security level PROFILE, security checking done on a ***message-by-message*** level
  - The other levels are ***IMS-wide*** (rather than message-by-message) for all client-bid and end user messages
    - Provides ***flexibility*** for varying security requirements
- Considerations for using PROFILE
  - PROFILE is ***not*** supported for use with the OTMA Callable Interface
  - The application ***programmer*** sets the 1-byte security flag in each message to determine whether RACF is invoked
    - Flag contains one of three possible values: N, C , or F
  - Security flag is used by OTMA ***only*** when the OTMA security level is PROFILE
    - Flag is ignored by OTMA when level is NONE, CHECK, or FULL

PROFILE Logic Flow



OTMA MESSAGE PREFIX
SECURITY DATA (SE)
...
SECURITY FLAG (N / C / F)
UTOKEN
USERID
SAF PROFILE
...

OTMA MESSAGE RECEIVED

OTMA SECURITY LEVEL = PROFILE ?

NO

IGNORE SECURITY FLAG

USE OTMA SECURITY LEVEL IN EFFECT (N, C, or F)

A

YES

A

SECURITY FLAG=**N** ?

YES

SET OTMA LEVEL:
OTMASE=N
/SEC OTMA NONE

NO

SECURITY FLAG=**C** ?

YES

SET OTMA LEVEL:
OTMASE=C
/SEC OTMA CHECK

NO

SECURITY FLAG=**F** ?

YES

SET OTMA LEVEL:
OTMASE=F
/SEC OTMA FULL

NO

REJECT MESSAGE

EXIT IS INVOKED -or- EXIT MAY BE INVOKED

DFSCCMD0, DFSCTRN0, and DFSCTSE0

OTMA Callable Interface (OTMA C/I)

- OTMA C/I
  - Was introduced in IMS V6 via APARs PQ17203 and PQ32398
    - Requires OS/390 V1R3 or higher
  - Provides an interface for access to IMS from C/C++ applications running on z/OS or OS/390
  - Does not provide support for OTMA security level PROFILE
    - OTMASE=P and /SECURE OTMA PROFILE are ***not*** supported

OTMA C/I ...

- OTMA C/I is an
  - Application Programming Interface (API) that may be used by
    - Authorized programs
      - ***Client-bid security*** is ***not*** performed for ***authorized callers*** which use the API
    - Unauthorized programs
      - ***Client-bid security*** ***is*** performed for ***unauthorized callers*** which use the API
        - Security provided by RACF and '*IMSXCF.OTMACI*' FACILITY class profile
        - Userid of program must have **READ** access level or higher

See '*RACF Command Examples*' in this handout

OTMA Security Enhancements Update

ITEM	DESCRIPTION	ORIGINAL PLAN DATE	PTF DATE - CURRENT OUTLOOK
Improve the performance of security checking for transactions and/or other database resources that are set as the destination on CHNG calls and/or specified as the resource on AUTH calls *SEE NOTE BELOW	Use the existing OTMA ACEE that was built for inbound messages security check in the control region to be used for the AUTH and/or *CHNG calls * SEE NOTE BELOW	09/30/2002	**08/30/2002** APAR NUMBERS **IMS V8 PQ61405** **IMS V7 PQ60233**
Enhance IMS to keep track of previous combinations of userid-transaction verification.	This function would eliminate (or significantly minimize) userid-to-transaction verifications. IMS/OTMA would not have to reissue the RACROUTE request for the same userid-transaction combination.	This function will not be provided because it would introduce security exposures.	N/A
Enhance the /SECURE OTMA command to support the TMEMBER keyword.	This would provide greater granularity on security checking performed for IMS commands and IMS transactions received from a TMEMBER rather than from an OTMA client. As an OTMA client, IMS Connect may communicate with one or more IMS/OTMA datastores and it is desirable to specify security options by individual datastores.	09/30/2002	09/30/2002

* APARs PQ61405 and PQ60233 resolve the issue for AUTH calls only at this time. It is possible that AUTH call and CHNG call security logic take the same path through the IMS code, in which case the APARs may resolve the problems for both calls. However, the tests have ***not*** been completed to determine if the security code path is identical for both calls

OTMA Security Enhancements Update ...

ITEM	DESCRIPTION	ORIGINAL PLAN DATE	PTF DATE - CURRENT OUTLOOK
Increase the size of the OTMA hash tables used for OTMA clients, or provide a mechanism to support a user-defined client hash table size.	There is an existing restriction that limits the hash table size to 5,000 entries. Additionally, there is no existing mechanism to request a 'cast-out' of specific entries. This causes the ACEEs for some userids to be reused indefinitely.	12/31/2002	**11/30/2002**
Enhance the /SEC OTMA command to allow the aging value to be refreshed on a tmember basis	Provide a mechanism for dynamically changing the ACEE aging value associated with a client's hash table on a TMEMBER basis without having to recycle OTMA or the OTMA client. This capability already exist if using IMS Connect. It is a problem for the MQSeries-IMS Bridge.	12/31/2002	**09/30/2002**
Enhance the Build Security Environment Exit (DFSBSEX0) interface to support transaction input from OTMA and APPC environments.	DFSBSEX0 will not be enhanced for this purpose because the exit will not be needed for APPC and/or OTMA environment because the problem is solved by **APARS PQ61405 / PQ60233** and any subsequent APARs that may be needed for the CHNG call security processing.	N/A	N/A

OTMA Security Enhancements Update ...

ITEM	DESCRIPTION	ORIGINAL PLAN DATE	PTF DATE - CURRENT OUTLOOK
Change the way RACF-protected IMS data set security is implemented for dependent regions in OTMA environments.	When the OTMA security level is FULL, if a transaction that originates from an OTMA client accesses a RACF-protected OS data set in a dependent region, the userid used in security checking is that associated with the end user (rather than the userid associated with the dependent region). This requires the security administrator to authorize many different userids/groups access to the data sets.	NOT ESTABLISHED	NOT ESTABLISHED

Detailed information on OTMA enhancements, security-related as well as non-security-related enhancements may be found in the '*Security Options and Considerations*' white paper.

Summary

- IMS communications
  - There are many ways to communicate with IMS, one of which is OTMA
- OTMA
  - Overview
  - Security overview
    - OTMA security is optional, but if security is desired, it may be provided by: RACF, user written exit routines, or a combination of both
  - Security levels
    - Determine how much, if any, ***RACF*** authorization checking will be performed
      - NONE | CHECK | ***FULL (the default)*** | PROFILE
  - Callable Interface (OTMA CI)
  - Security enhancements update
    - IMS Development management & developers are committed to meeting customer requirements and continue to provide outstanding responsiveness

Additional Information

'*OTMA Guide and Reference*' manual

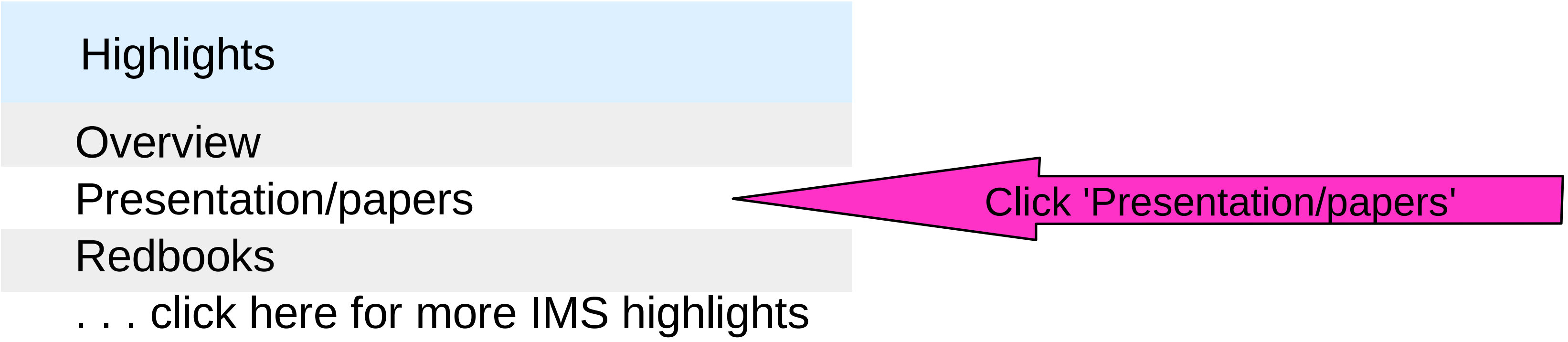
'*Security Options and Considerations*'

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

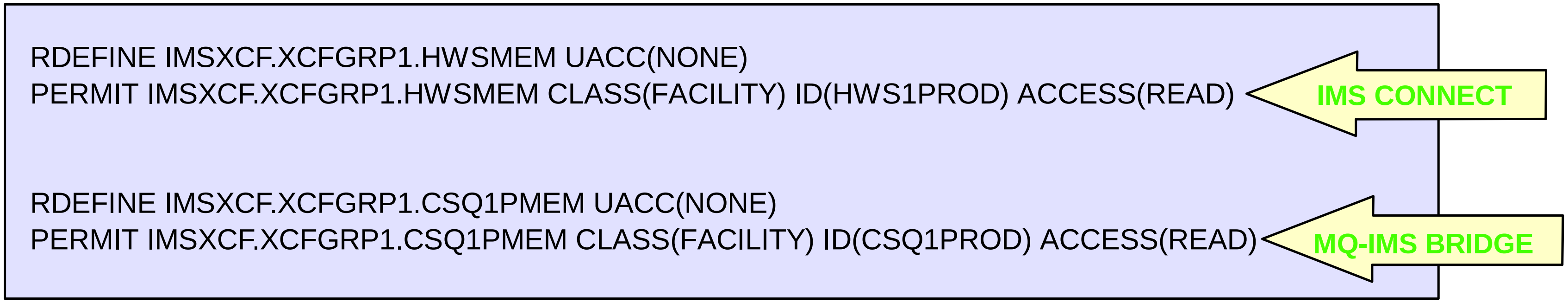
Redbooks

. . . click here for more IMS highlights

Click 'Presentation/papers'

RACF Command Examples

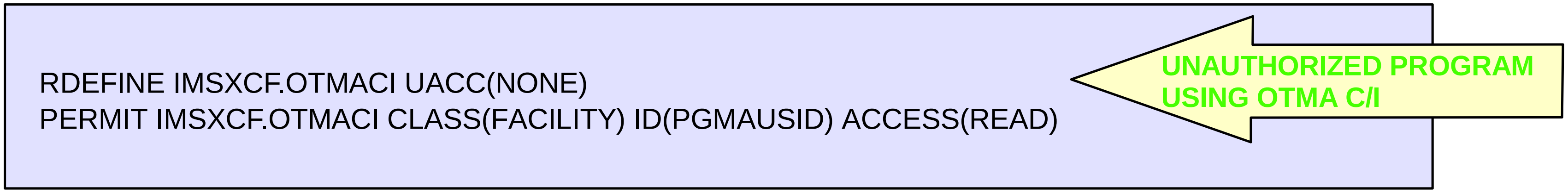
- Sample RACF commands are shown to secure
  - The ***client-bid*** process
    - For OTMA client subsystems (i.e. IMS Connect and MQSeries-IMS Bridge)



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

RDEFINE IMSXCF.XCFGRP1.CSQ1PMEM UACC(NONE)
PERMIT IMSXCF.XCFGRP1.CSQ1PMEM CLASS(FACILITY) ID(CSQ1PROD) ACCESS(READ)
```

- Non-authorized programs using the OTMA callable interface



```
RDEFINE IMSXCF.OTMACI UACC(NONE)
PERMIT IMSXCF.OTMACI CLASS(FACILITY) ID(PGMAUSID) ACCESS(READ)
```

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)
```

RETURN TO INDEX