IMS SECURITY

SAF REPLACEMENT FOR SMU

Overview

- **IMS V9 is the last release of IMS that supports SMU**
  - New facilities are introduced
    - All SMU usage can now be replaced with any security product that uses the SAF interface
      - RACF or equivalent
- **Today's presentation:**
  - Considers the 6 SMU facilities that previously had no directly corresponding RACF facilities
  - Explains the corresponding RACF options in IMS Version 9
  - Introduces the new SMU to RACF Conversion Aid

SAF Security before IMS V9

●IMS Security that can be implemented with SAF/RACF

- Sign-On user validation and verification
  - Check user is known
  - Check password is correct
- Terminal Security
  - User v. physical terminal
- IMS System Access Security
  - User v. IMS ID
- Transaction Security
  - User v. Trancode
- Command Security
  - User v. IMS Command in Control Region
  - User v. IMS Command in Operations Manager
- AOI Type2 ICMD Call Security
  - User v. IMS Command
- IMS Data Set Access Security
  - Controls access to DBs and system datasets
- DB Data Access Security – used with DL/1 AUTH call
  - User v. DB Record
  - User v. Segment
  - User v. Field
- PSB Access Security - For ODBA and CPI-C
  - User v. PSBname
- Connection Access Control
  - IMS Connect, CQS, CSL address spaces, etc

IMS V9 Security Enhancements

- Enhancements to the SAF interface to support:
  - Application Group Name (AGN) security
  - Type 1 Automated Operator Interface (AOI)
  - Terminal security for Time-Controlled Operations (TCO)
  - MSC link receive security
  - /LOCK and /UNLOCK commands
  - Signon verification

Last release to support SMU

Resource Access Security (replaces AGN)

Resource Access Security (RAS)

- **Replaces SMU AGN security**

- **Objective of AGN security:**
  - Check at Program Scheduling Time to validate
    - That the resources involved (PSB &/or TRANcode &/or LTERM) are authorized for use by the Dependent Region
  - Primarily used for BMPs, but actually applies to all dependent regions and connecting threads (DRA/CCTL/ODBA

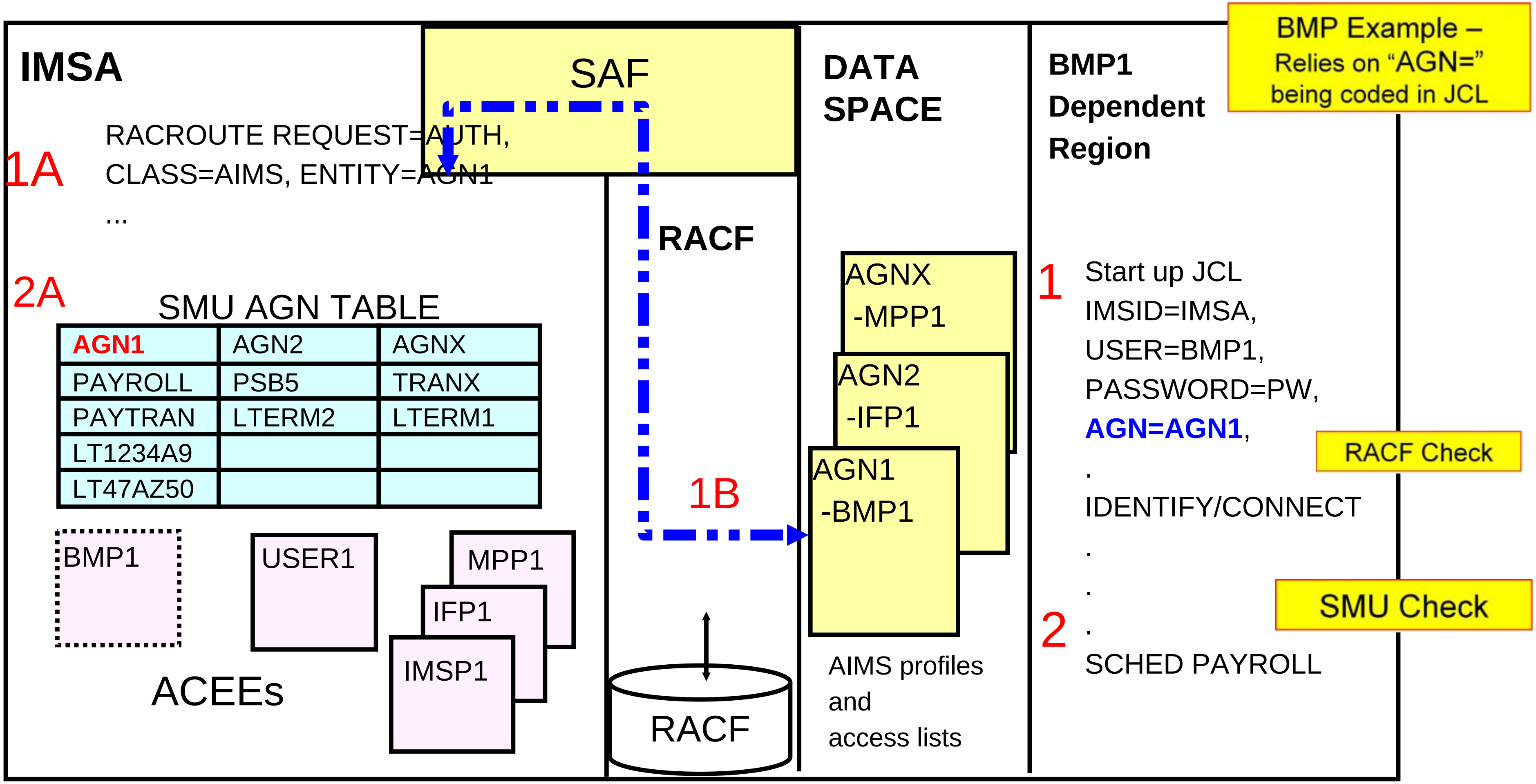
Resource Access Security (RAS) ...

Prior releases - AGN with SMU

- Required elements
  - AGN name defined in SMU
    - A named group that defines the resources that can be accessed
      - PSBs, Transaction Codes, or LTERMs
  - RACF (optional – can alternatively use DFSISIS0 Exit)
    - Defines the AGN in AIMS resource class
    - Permits userids to use AGN
  - Dependent Region JCL
    - Contains AGN= execution parameter
    - Contains USERID that will be used for the security check

Resource Access Security (RAS) ...

•Prior releases - SMU and AGN ...



RACROUTE REQUEST=AUTH,
CLASS=AIMS, ENTITY=AGN1
...

SMU AGN TABLE

AGN1	AGN2	AGNX
PAYROLL	PSB5	TRANX
PAYTRAN	LTERM2	LTERM1
LT1234A9		
LT47AZ50		

Start up JCL
IMSID=IMSA,
USER=BMP1,
PASSWORD=PW,
AGN=AGN1,
.
IDENTIFY/CONNECT
.
.
.
SCHED PAYROLL

An alternative to the use of SAF is the use of the DFSISIS0 exit
(one or the other is called, not both)

Resource Access Security (RAS) ...

- **IMS V9**

  - Provides direct SAF authorization checking of user to IMS resource (TRAN, PSB, LTERM)

  - Supports new RACF security classes for PSBs and LTERMs
    - IIMS: Program Specification Block (PSB)
    - JIMS: Grouping class for PSB
    - LIMS: Logical terminal (LTERM)
    - MIMS: Grouping class for LTERM

  - Invokes existing RACF security classes for Transactions
    - TIMS: Transaction (TRAN)
    - GIMS: Grouping class for Transactions

Resource Access Security (RAS) ...

- **IMS V9 ...**

–**New** specifications in system definiton

•SECURITY ... TYPE = RASRACF | RASEXIT | RAS | NORAS

[| NOAGN | RACFAGN | AGNEXIT]

–**New** specifications during startup

•ISIS = N | R | C | A [| 0 | 1 | 2]

N = No security (turns off both RAS and SMU)
R = RAS security invokes RACF
C = RAS security invokes an IMS user exit (DFSRAS00)
A = RAS security invokes RACF and user exit DFSRAS00

•ISIS =N | 0 turn off both RAS and SMU security checking

Resource Access Security (RAS) ...

- **New user exit (DFSRAS00) is optionally called after SAF**
  - –Provides authorization of IMS resources to IMS dependent regions in a RAS environment
    - •Called to
      - ▪Authorize transaction (MPP, JMP)
      - ▪Authorize PSB (IFP, NMD BMP, JBP, DRA|CCTL|ODBA)
      - ▪Authorize transaction and PSB (MD BMP)
      - ▪Authorize PSB and output LTERM (NMD BMP, JBP)
      - ▪Authorize PSB and output transaction (NMD BMP, JBP)
  - –Available in DCCTL, DB/DC, and DBCTL

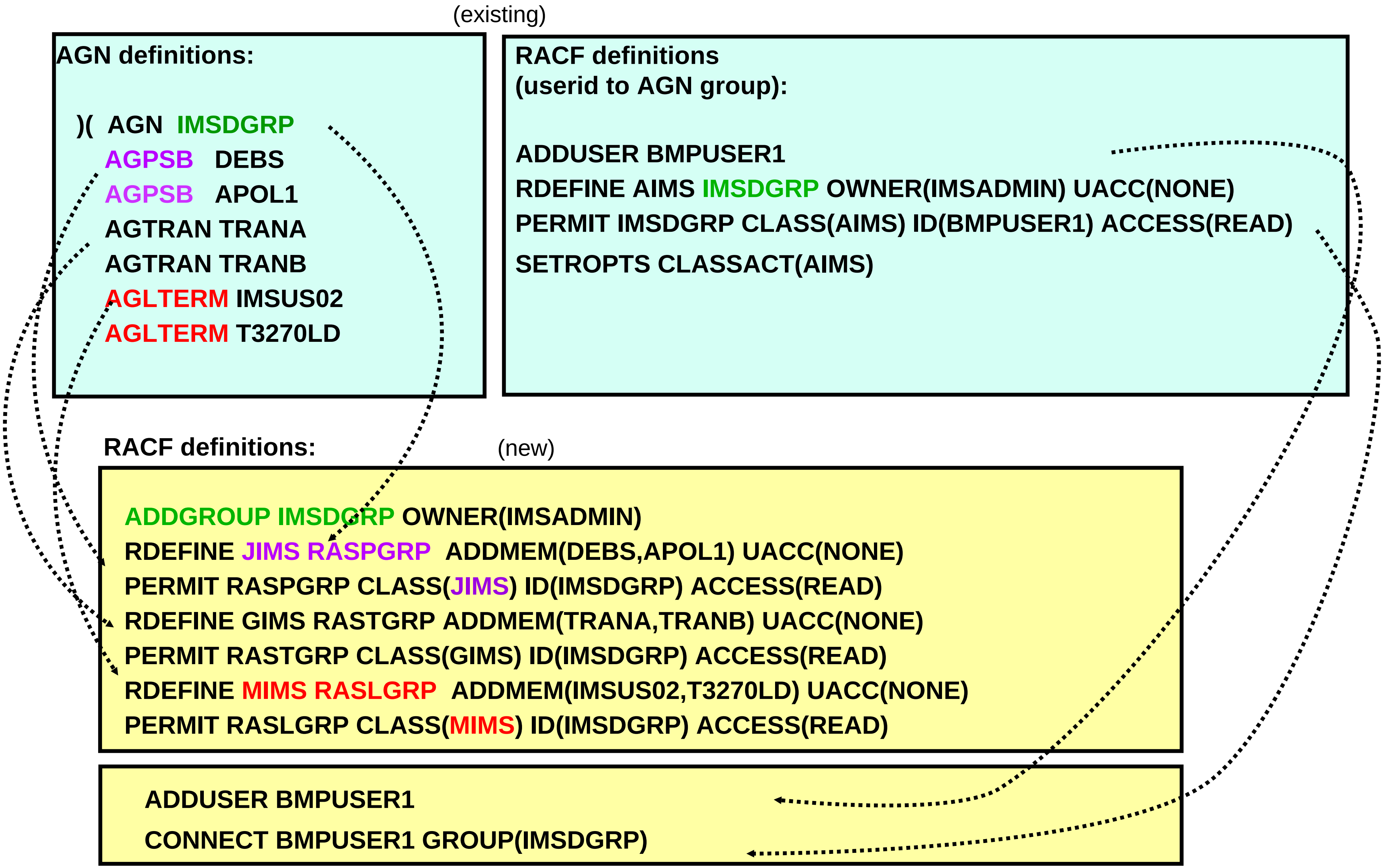
- **DFSISIS0 continues to be used in AGN environment**

Resource Access Security (RAS) ...

- **When RAS is enabled**
  - Check is made at every MPP/JMP/BMP/IFP/JBP pgm schedule using region's userid
  - Check is made at every CICS/DBCTL pgm schedule using CICS region's userid
    - Completely separately, CICS can perform check of terminal user against PSB

RAS Migration Examples

Example 1 - BMP accessing PSB, LTERM resources



(existing)

AGN definitions:

```
)(  AGN  IMSDGRP
    AGPSB   DEBS
    AGPSB   APOL1
    AGTRAN TRANA
    AGTRAN TRANB
    AGLTERM IMSUS02
    AGLTERM T3270LD
```

RACF definitions
(userid to AGN group):

```
ADDUSER BMPUSER1
RDEFINE AIMS IMSDGRP OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSDGRP CLASS(AIMS) ID(BMPUSER1) ACCESS(READ)
SETROPTS CLASSACT(AIMS)
```

RACF definitions:

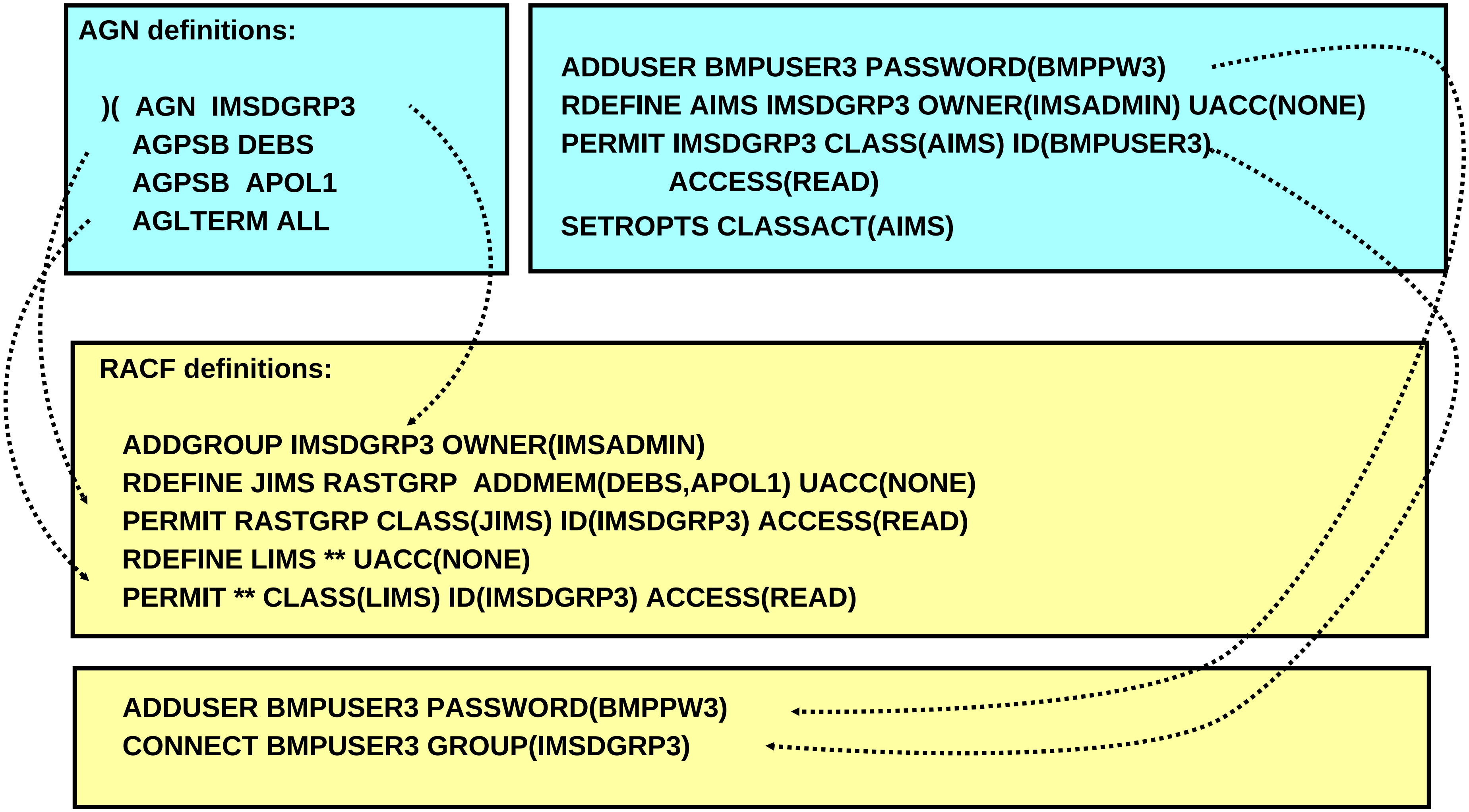
(new)

```
ADDGROUP IMSDGRP OWNER(IMSADMIN)
RDEFINE JIMS RASPGRP  ADDMEM(DEBS,APOL1) UACC(NONE)
PERMIT RASPGRP CLASS(JIMS) ID(IMSDGRP) ACCESS(READ)
RDEFINE GIMS RASTGRP ADDMEM(TRANA,TRANB) UACC(NONE)
PERMIT RASTGRP CLASS(GIMS) ID(IMSDGRP) ACCESS(READ)
RDEFINE MIMS RASLGRP  ADDMEM(IMSUS02,T3270LD) UACC(NONE)
PERMIT RASLGRP CLASS(MIMS) ID(IMSDGRP) ACCESS(READ)
```

```
ADDUSER BMPUSER1
CONNECT BMPUSER1 GROUP(IMSDGRP)
```

RAS Migration Examples ...

Example 2 - combination of resource grouping and generic resources definitions



AGN definitions:

```
)(  AGN  IMSDGRP3
    AGPSB DEBS
    AGPSB  APOL1
    AGLTERM ALL
```

```
ADDUSER BMPUSER3 PASSWORD(BMPPW3)
RDEFINE AIMS IMSDGRP3 OWNER(IMSADMIN) UACC(NONE)
PERMIT IMSDGRP3 CLASS(AIMS) ID(BMPUSER3)
          ACCESS(READ)
SETROPTS CLASSACT(AIMS)
```

RACF definitions:

```
ADDGROUP IMSDGRP3 OWNER(IMSADMIN)
RDEFINE JIMS RASTGRP  ADDMEM(DEBS,APOL1) UACC(NONE)
PERMIT RASTGRP CLASS(JIMS) ID(IMSDGRP3) ACCESS(READ)
RDEFINE LIMS ** UACC(NONE)
PERMIT ** CLASS(LIMS) ID(IMSDGRP3) ACCESS(READ)
```

```
ADDUSER BMPUSER3 PASSWORD(BMPPW3)
CONNECT BMPUSER3 GROUP(IMSDGRP3)
```

Migrating From SMU

- Define AGN resources to RACF in the appropriate classes
- Define region ids as RACF users
  - Permit region ids to access appropriate resources
- Change SECURITY macro to specify RAS and/or

Change ISIS= parameter in DFSPBxxx to specify RAS

- Restart IMS
- When safe, remove SMU definitions

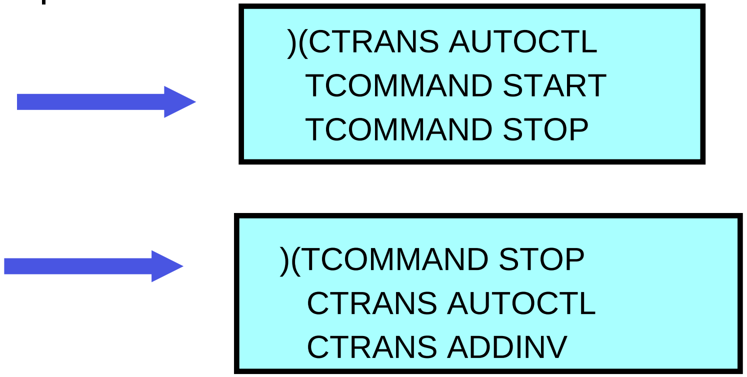
AOI Security

AOI Security

Automated Operator Program commands

- Prior releases
  - Type 1 AOI CMD calls
    - SMU transaction command security
      - SECURITY... TRANCMD = NO | YES | FORCE

        /NRE or /ERE COLDSYS ... TRANCMDS | NOTRANCMDS
    - SMU definitions
      - Which commands can be executed by a specific program
      - Which programs can execute a specific command



```
)(CTRANS AUTOCTL
   TCOMMAND START
   TCOMMAND STOP
```

```
)(TCOMMAND STOP
   CTRANS AUTOCTL
   CTRANS ADDINV
```

AOI Security ...

- IMS V9 enhancements
  - SAF and optionally DFSCCMD0 support extended to Type 1 AOI CMD calls
  - New TRANSACT macro parameter
    - Affects both Type1 and Type2 AOI calls

AOI Security...

- **IMS V9 Enhancement for AOI TYPE 1 CMD calls**
  - Similar to existing SAF support for Type 2 AOI (ICMD)
  - New **startup** parameter to choose type/level of security
    - DFSPBxxx
    - Provides a choice of SMU or SAF/DFSCCMD0
    - AOI1 = A | N | C | R | S

A = Includes options C and R below
N = No authorization security checking is done
C = DFSCCMD0 is called for command authorization
R = RACF is called for command authorization
S = SMU security is called for command authorization

AOI Security ...

Note

- Type 2 AOI (ICMD) calls already have
  - **AOIS** = A | N | C | R | S
  - Same values as with AOI1 …
  - … but some values (N and S) have different meanings

A = Includes options C and R below
N = ICMD calls are not allowed
C = DFSCCMD0 is called for command authorization
R = RACF is called for command authorization
S = Skip - no authorization checking

AOI Security ...

- **New TRANSACT parameter**
  - Applicable to both Type 1 and Type 2 command calls
  - Modifiable by Online Change
  - Specifies whether tran is allowed to process AOI command calls
    - Authorization based on trancode or userid of inputting terminal
  - **AOI** = YES | <u>NO</u> | TRAN | CMD

AOI Security ...

●New TRANSACT parameter

AOI = YES | <u>NO</u> | TRAN | CMD

YES = Requests the userid of the user who entered the transaction be authorized against the command (in the CIMS class)

NO = AOI commands (Type 1 AOI CMD calls) are not allowed
Not relevant for AOI Type 2 ICMD calls - same as YES

TRAN = Requests that the trancode be used for authorization against the command (in the CIMS class)

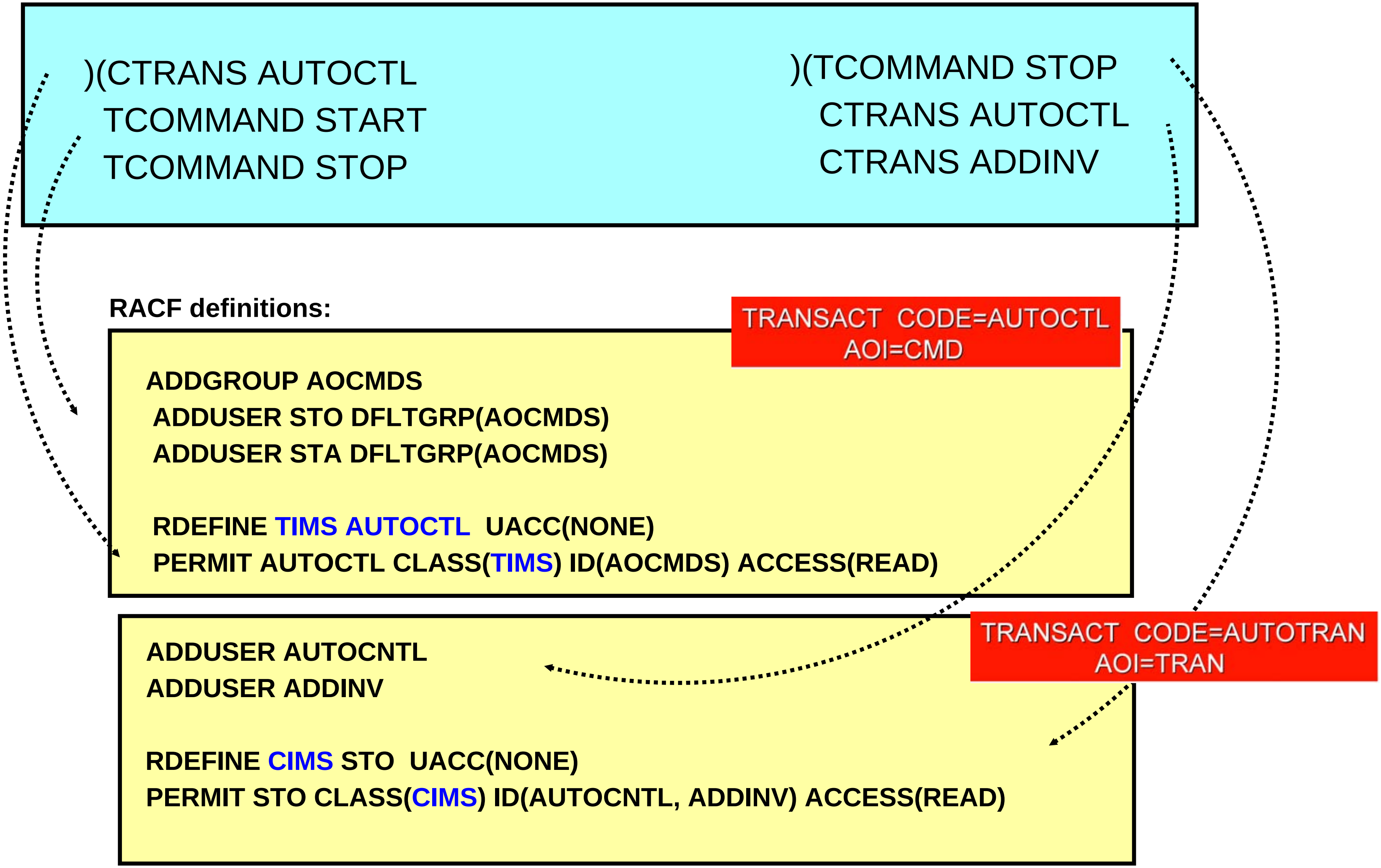
- transactions will have to be defined to the security product as a user

CMD = Requests that the command code (first three characters of the command) be used for authorization against the trancode (in the TIMS class)

- the first three characters of IMS commands will have to be defined to the security product as a user

For Type 1 commands, AOI1=N|S (‘None’ or ‘SMU’) will override TRANSACT AOI=YES|NO

SAF Support for Type 1 AOI (CMD) Example



```
)(CTRANS AUTOCTL
  TCOMMAND START
  TCOMMAND STOP
```

```
)(TCOMMAND STOP
  CTRANS AUTOCTL
  CTRANS ADDINV
```

RACF definitions:

TRANSACT CODE=AUTOCTL AOI=CMD

```
ADDGROUP AOCMDS
 ADDUSER STO DFLTGRP(AOCMDS)
 ADDUSER STA DFLTGRP(AOCMDS)

 RDEFINE TIMS AUTOCTL  UACC(NONE)
 PERMIT AUTOCTL CLASS(TIMS) ID(AOCMDS) ACCESS(READ)
```

TRANSACT CODE=AUTOTRAN AOI=TRAN

```
ADDUSER AUTOCNTL
ADDUSER ADDINV

RDEFINE CIMS STO  UACC(NONE)
PERMIT STO CLASS(CIMS) ID(AUTOCNTL, ADDINV) ACCESS(READ)
```

Specify TRANSACT macro AOI= parameter in IMS definitions

SAF and SMU Coexistence in IMS V9

- **Relevant only to Type 1 AOI (CMD) calls**
  - AOI1=S
    - SMU is invoked (transaction command security)
    - Settings on TRANSACT are ignored
  - AOI1=R|C|A
    - SMU for AOI is ignored, SAF and/or DFSCCMD0 are invoked
    - Settings on TRANSACT are honored
  - AOI1=N (default)
    - No authorization checking is done
    - Settings on TRANSACT are ignored

Migrating From SMU

- **Type 2 (ICMD)**
  - No action needed, but now have choice of what userid to use
- **Type 1 (CMD)**
  - Initially, code AOI1=S or use default (SECURITY macro) value to get SMU security
  - Set up required RACF definitions for type 1 commands
  - Add AOI=value to TRANSACT macros in IMSGEN
    - Can use online change
    - Will be ignored for type 1 commands while AOI1= indicates SMU
  - Change (or add) AOI1=R to DFSPBxxx
  - Restart IMS
  - When safe, remove SMU definitions

TCO Security

SAF Support for TCO

- **Time Controlled Operations (TCO)**
  - IMS capability to execute time-initiated commands and transactions
- **Security support**
  - Authorization of loading of TCO script by an LTERM
    - performed only by DFSTCNT0 exit
  - Resource authorization
    - Commands and Transaction security using SMU
    - Transaction security (only) using RACF
      - Command security can be requested but is not performed

SAF Support for TCO

●Resource authorization - prior releases

–SMU transaction/ command support specifically targeted for the TCO input LTERM, DFSTCFI

```
)( TERMINAL    DFSTCFI
     COMMAND    START
      COMMAND    STOP
       TRANSACT    STATTRN

)( COMMAND    START
    TERMINAL    DFSTCFI

)( COMMAND    STOP
    TERMINAL    DFSTCFI
```

•Followed by optional call to DFSCCMD0 exit

SAF Support for TCO

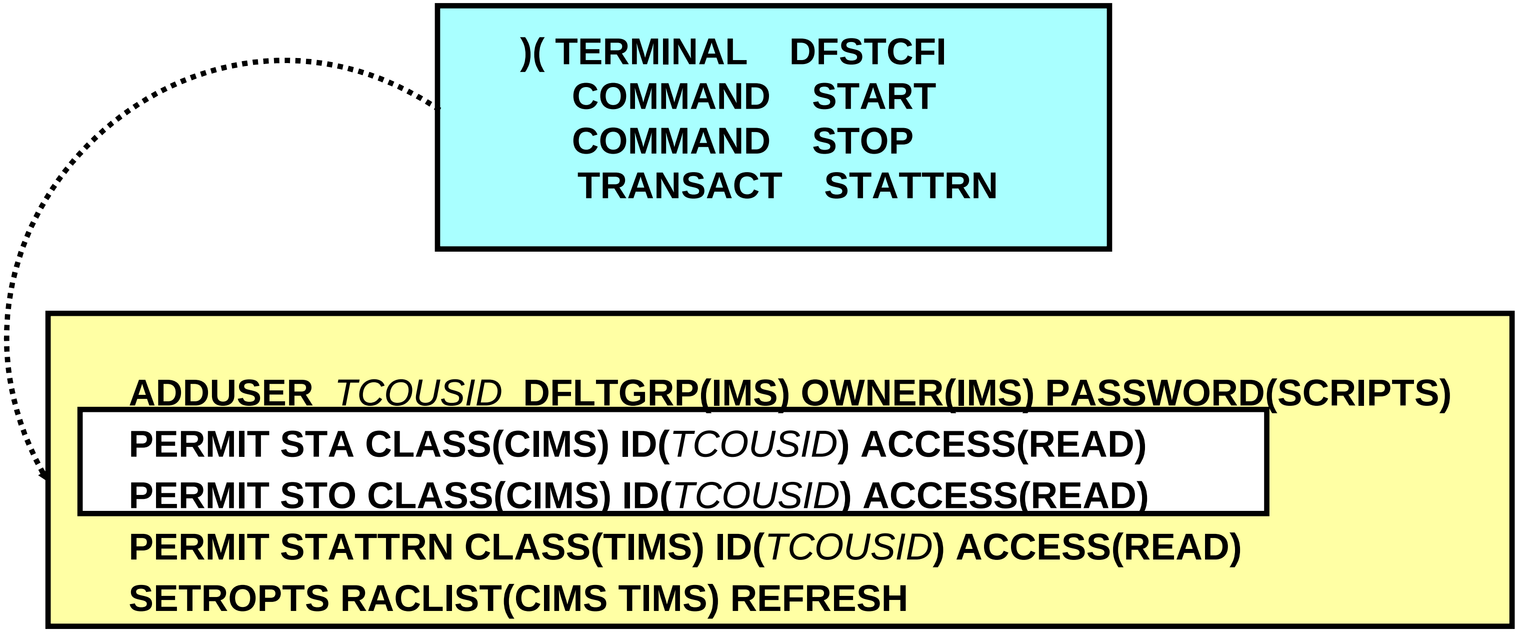
Resource authorization - prior releases ...

- SAF capability
  - Required IMS execution parameter, RCF= A | S | R | B
  - Invoked SAF/RACF for authorization
    - Required a USERID
      - TCO script specification of /SIGN ON tcousid tcopw (and /SIGN OFF)
      - Else used control region userid
  - Only supported authorization for transactions
  - Command security for TCO userid, if specified, was ignored
      - ***TCO was already authorized to issue the same set of commands as the system console and master terminal***
      - DFSCCMD0 always called if available

SAF Support for TCO ...

- **New IMS V9 SAF support**
  - **Introduces new execution parameter: TCORACF = Y | N**
    - Specifies whether or not TCO security supports RACF
  - Requires RCF = A | S | R | B (as previously)
    - SAF is called for TCO security only if TCORACF = Y is also specified
  - Requires a valid USERID
    - TCO script specification of /SIGN ON tcousid tcopw (/SIGN OFF)
      - Else uses control region userid
    - SAF call is used to authorize transactions and/or commands
      - Using TCO USERID
  - DFSCCMD0 will be called if it exists (after SAF call) for command security

SAF Support for TCO ...



```
)( TERMINAL    DFSTCFI
   COMMAND    START
   COMMAND    STOP
   TRANSACT    STATTRN
```

```
ADDUSER  TCOUSID  DFLTGRP(IMS) OWNER(IMS) PASSWORD(SCRIPTS)
PERMIT STA CLASS(CIMS) ID(TCOUSID) ACCESS(READ)
PERMIT STO CLASS(CIMS) ID(TCOUSID) ACCESS(READ)
PERMIT STATTRN CLASS(TIMS) ID(TCOUSID) ACCESS(READ)
SETROPTS RACLIST(CIMS TIMS) REFRESH
```

This example assumes:

- Command and transaction profiles already exist
- The TCO userid (TCOUSID)is connected to a RACF group
- The TCO script issues a /SIGN ON
- RCF= and TCORACF=Y are specified

The above definitions could have been coded in prior releases. If so, authorization for the transaction was done. Command authorization, however, was never invoked.

In IMS V9 (TCORACF=Y), using the same definitions, SAF will be invoked for command authorization.

Migrating From SMU

- **Prerequisite is that RACF or equivalent product is used for command / transaction security**
  - RCF= A | S | R | B
  - Define TCO userid and permissions in RACF
- **Add /SIGN ON (and /SIGN OFF) to all TCO scripts**
- **Add TCORACF=Y to DFSPBxxx**
  - Restart IMS
- **When safe, remove SMU definitions**

MSC Link Receive Security

MSC Link Security

●Prior releases

- Directed Routing*
  - Used RACF, and Transaction Authorization Exit (DFSCTRN0) if defined
  - If DFSMSCE0 exit (link receive entry point) was defined, RACF and DFSCTRN0 were called before and after the call to D

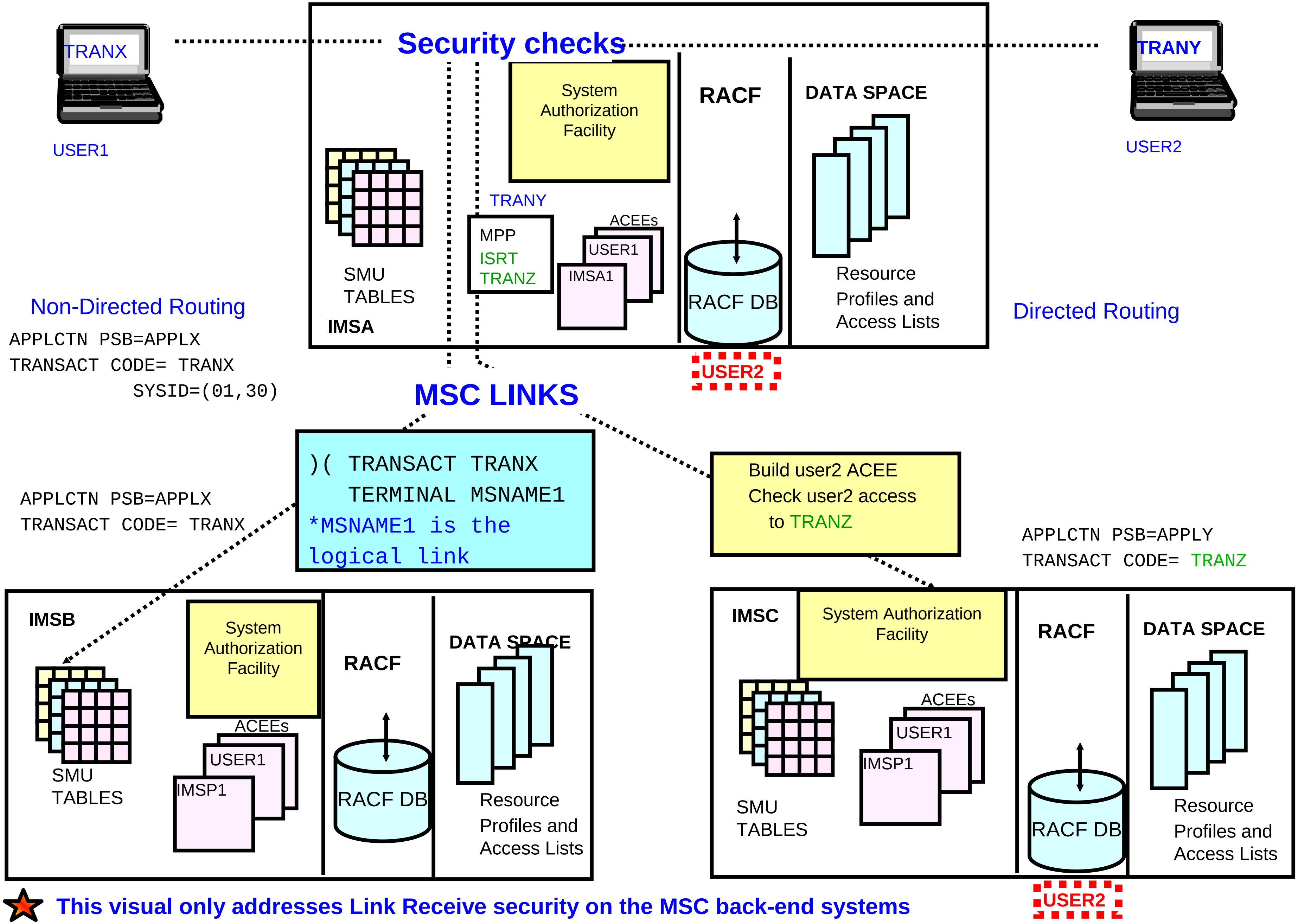
Note that Directed and Non-directed routing use different userids for security

- Non-Directed routing
  - Used SMU (after the DFSMSCE0 call)
    - Normal transaction security used MSName as the LTERMname
  - Note: security checking may also have already taken place in the inputting IMS (terminal security or CHNG call security)

* "Directed Routing" is when application explicitly specifies target location

- Not necessarily defined in IMS GEN

MSC Link Security



```
APPLCTN PSB=APPLX
TRANSACT CODE= TRANX
              SYSID=(01,30)
```

```
)( TRANSACT TRANX
   TERMINAL MSNAME1
*MSNAME1 is the
logical link
```

```
APPLCTN PSB=APPLX
TRANSACT CODE= TRANX
```

```
APPLCTN PSB=APPLY
TRANSACT CODE= TRANZ
```

★ **This visual only addresses Link Receive security on the MSC back-end systems**

IMS V9 MSC Link Security

- **New DFSDCxxx parameter to specify use of RACF / DFSCTRN0**
  - MSCSEC=(parm1, parm2)
    - parm1 : defines types of MSC link-receive usage that require security
      - LRDIRECT | LRNONDR | LRALL | LRNONE
    - parm2 : defines type of security check to be performed
      - CTL | MSN | USER | EXIT | CTLEXIT | MSNEXIT | USREXIT | NONE

MSC Link Security ...

- **MSCSEC=(parm1, …..)**

LRDIRECT = Link Receive directed routing tran security checking
LRNONDR = Link Receive non-directed routing tran security checking
LRALL = LRDIRECT and LRNONDR
LRNONE = No Link Receive security checking

V8 compatibility is provided with LRDIRECT (default)

- SMU security will be used for non-directed routing in V9

– RACF / DFSCTRN0 called once, after DFSMSCE0

– The USERID to be used is defined by MSCSEC parm2 or DFSMSCE0 Exit

MSC Link Security ...

- **MSCSEC=(……., parm2)**
  - Specifies type of security checking
    - MSCSEC=(LRDIRECT | LRNONDR | LRALL | LRNONE ,

      CTL | MSN | USER | EXIT | CTLEXIT | MSNEXIT |

CTL	**=**	**Authorization by CTL address space security**
MSN	**=**	**Authorization by MSNAME**
USER	**=**	**Authorization by userid of inputting terminal**
EXIT	**=**	**Authorization by user exit (DFSCTRN0)**
CTLEXIT	**=**	**Authorization by CTL address space security and by user exit (DFSCTRN0)**
MSNEXIT	**=**	**Authorization by MSNAME and by user exit (DFSCTRN0)**
USREXIT	**=**	**Authorization by userid of inputting terminal and by user exit (DFSCTRN0)**
NONE	**=**	**No Security authorization checking**

Note: with RACF, security environment for control region or MSNAME is built once when first used, and retained. But security environment for an end user is built and deleted for each message.

New Role for DFSMSCE0

- **Traditionally, directed and non-directed routing have used different userids for security**
  - To achieve this in future will require the use of DFSMSCE0 exit
- **Additional data is passed to DFSMSCE0**
  - Userid, Group name, and Userid indicator
  - DFSMSCE0 can override MSCSEC PARM2 value
    - In other words, DFSMSCE0 link receive processing can –
      - Enable or disable security check
      - Enable or disable use of DFSCTRN0
      - Choose what userid to use for RACF security
        - User, control region or MSName

Migrating From SMU

- Specify MSCSEC in DFSDCxxx for directed routing
  - MSCSEC=(LRDIRECT,USER) for compatibility with previous release
    - or authorize control region for transaction execution, and take default MSCSEC values (LRDIRECT,CTL)
- Decide what type of userid to use for directed and non-directed routing
  - Easier when both the same, but can be different
- Update RACF to include new userids (MSNAMEs and Ctl Rgn) if necessary, and grant their access to transactions
- If using two types of userid, code DFSMSCE0 accordingly
- Change DFSDCxxx to include MSCSEC=(LRALL,USER |MSN |CTL)
- Restart IMS
- When safe, remove SMU definitions

/LOCK, /UNLOCK, /SET

/LOCK, /UNLOCK and /SET

- **Password security for certain commands**

```
/LOCK LTERM | DATABASE | PROGRAM | TRANSACTION | NODE | PTERM
    /UNLOCK LTERM | DATABASE | PROGRAM | TRANSACTION | NODE | PTERM
    /SET TRANSACTION
```

- **Prior releases**
  - SMU - provided password security
    - E.g., /LOCK DATABASE payroll (uomecash)
      /UNLOCK DATABASE payroll (uomecash)
      /SET TRANSACTION paytran (uomecash)
    - Definitions
      - SECURITY macro, PASSWD=YES
      - /NRE or /ERE COLDSYS PASSWORD
      - Definitions

Password is associated with specific resource

```
)( DATABASE  PAYROLL
   PASSWORD  UOMECASH
```

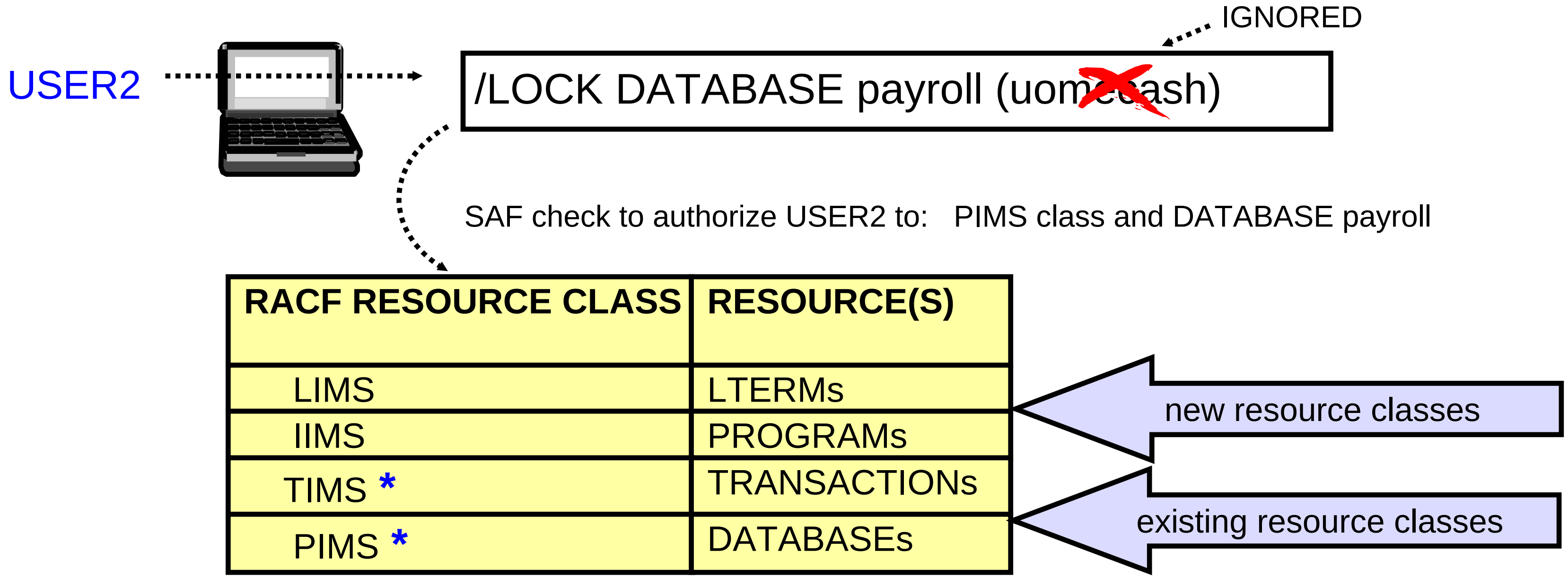
```
)( PASSWORD UOMECASH
   DATABASE PAYROLL
   PROGRAM PAYPROG
   TRANSACT PAYTRAN
```

/LOCK, /UNLOCK and /SET ...

- **IMS V9**
  - SAF Support - New DFSDCxxx parameter
    - Standard command security still applies
- **LOCKSEC = Y | <u>N</u>**
  - N = No authorization checking
  - Y = Calls SAF and DFSCTRN0
    - RACF classes: LIMS, PIMS, IIMS, TIMS
      - If resource is not protected, access is allowed
    - DFS3689W - new message if authorization fails
    - Userid must be authorized to issue /LOCK, /UNLOCK, /SET commands AND must be authorized for use of specific resource

/LOCK, /UNLOCK and /SET ...

- **IMS V9**
  - If the user is authorized to issue the /LOCK, /UNLOCK and /SET commands, another check is made to authorize access to resources



/LOCK DATABASE payroll (uomecash)

SAF check to authorize USER2 to: PIMS class and DATABASE payroll

RACF RESOURCE CLASS	RESOURCE(S)
LIMS	LTERMs
IIMS	PROGRAMs
TIMS *	TRANSACTIONs
PIMS *	DATABASEs

Migrating From SMU

- Create security profiles for all resources that need to be LOCKed or SET
  - LTERMs, DBs, Programs (PSBs), and Transactions
  - Grant authority for using these resources to the appropriate userids
- Add LOCKSEC=Y to DFSDCxxx
- Restart IMS
- When safe, remove SMU definitions
- Inform users that passwords are no longer needed

or ....

Migrating From SMU ...

- **If password security is required, then existing facilities using the reverify capability should be used**
  - Applies to both static and ETO environments
    - Specify RVFY=Y in IMS startup parameters in DFSPBxxx
    - Specify 'REVERIFY' in the APPLDATA section of the RACF profile for the command/transaction
  - Different from SMU password security
    - Password is the same as RACF userid's password

Static Terminal Signon

Signon Verification Security

- **SMU method for static terminal Signon Verification**
  - Defines which terminals have to /SIGN ON

```
–)( SIGN
      STERM TERM1
      STERM TERM2    }     OR        STERM ALL
      STERM TERM3
      ...
```

  - Requires SECURITY SECLVL=SIGNON or FORCSIGN
    - Typically requests RACF verification of userid/password with
      - SECURITY TYPE=RACFTERM

Signon Verification Security ...

- **IMS V9**

  – New startup parameter in DFSDCxxx

    - SIGNON = ALL | <u>SPECIFIC</u>

ALL = All static terminals are required to signon. This is equivalent to the SMU definition of)(SIGN STERM ALL

- Except for 3284/3286, SLU1 (when printer-only device),and MTOs

SPECIFIC = Individual static terminals may be required to signon. This will be based on TYPE/TERMINAL specification or SMU definitions using)(SIGN

Signon Verification Security ...

- Enhancement to the OPTIONS parameter on the TYPE and TERMINAL macros

  - OPTIONS = (...,SIGNON | <u>NOSIGNON</u>)

Migrating From SMU

- **For “ALL”**
  - Add SIGNON=ALL to DFSDCxxx
  - Restart IMS
- **For “SPECIFIC”**
  - Add OPTIONS=(…SIGNON…) for all TERMINALs which currently have an explicit SMU signon requirement
  - Add SIGNON=SPECIFIC to DFSDCxxx
  - Restart IMS
- **When safe, remove SMU definitions**

Note: If a TERMINAL has both a SMU specification (e.g., signon required) and a conflicting OPTIONS=NOSIGNON, then SMU takes precedence

Other Considerations

Considerations - LTERM security

SMU

1. Controls LTERM availability through password security:
   - /LOCK and /UNLOCK LTERM (pswd)

2. Protects which LTERMs can be used in NMD BMP and JBP specification of OUT=
   - AGN definitions

3. Provides additional protection for signed on terminals:
   - requires the user to enter the SMU-defined password that is associated with the transaction or command

SAF / RACF

1. Checks the userid authorization to the resource using:
   - the new resource class LIMS when LOCKSEC=Y

2. Uses RAS security based on SECURITY macro TYPE= RASRACF|RASEXIT|RAS|NORAS or override value of ISIS=N|R|C|A.
   - Checks userid associated with NMD BMP or JBP for authorization to the resource using the new LIMS class

3. Uses the REVERIFY facilities in IMS and RACF by specifying RVFY=Y in IMS and 'REVERIFY' in the APPLDATA section of the RACF profile for the commands and transactions to be protected
   - Requires a signed on user to reenter his/her signon password with the transaction or command input

Considerations - LTERM security

SMU

4. Restricts entry of certain commands to specific static LTERMs

   - SMU definitions

```
e.g., )( COMMAND DIS
            TERMINAL LTERMA

          )( TERMINAL LTERM5
            COMMAND DIS
            TRANSACT TRAN123
```

5. Restricts entry of certain transactions to specific static LTERMs

   - SMU definitions

```
e.g., )(TRANSACT PAYROLL
            TERMINAL LTERMB
```

SAF / RACF

4. Restricts entry based on a combination of RACF and DFSCCMD0. The first check is the SAF call to validate if the userid can enter the command.

   - If DFSCCMD0 exists, it is always invoked and can make the second call. Possible alternatives:

     - Create FACILITY class RACF profiles of command.lterm, e.g., DIS.LTERMA. These would equate to the combinations defined in SMU. In DFSCCMD0, call RACF to authorize userid/groupid to the resource class using the applicable resource combinations.

     - Or, protect all the static LTERMs with the new LIMS resource class. Define the commands (there are about 50) as userids. In the exit, invoke RACF to VERIFY (build the ACEE for the IMS command) as a userid and authorize it against the LTERM name.

5. Similar techniques as described above for restricting commands. DFSCTRN0 is used instead of DFSCCMD0

Migration Considerations

●AOI considerations

- CMD
  - Status code 'CD' is returned on a security failure for a CMD call
    - If AIB is used, the return code is 0900
- ICMD
  - Three new return/reason codes when AOI=CMD:
    - 0110/0054 - Command not authorized to RACF
    - 0110/0058 - Command not authorized to be issued by the transaction
    - 0110/005C - DFSCCMD0 indicated command was not authorized to be issued by the transaction
  - Three new return/reason codes when AOI=TRAN:
    - 0110/0044 - Transaction not authorized to RACF
    - 0110/0048 - Transaction not authorized to issue the command
    - 0110/004C - DFSCCMD0 indicated tran not authorized to issue command

Migration Considerations ...

- Log record X'10'
  - 4 new error codes to describe CMD authorization failures
- Exits
  - DFSRAS00 (new user exit)
    - Replaces DFSISIS0 when using RAS instead of AGN
  - DFSCCMD0
    - Support two new values for the type of caller (CCMD_RQSTTYPE)
      - CMD FOR TRANSACTION and ICMD FOR TRANSACTION
  - DFSISIS0
    - Renamed to Application Group Name (AGN) Security Exit
      - Avoids confusion when referencing DFSRAS00
  - DFSMSCE0
    - Additional information passed to exit
      - Userid, group name, and userid indicator
    - Specification of level of authorization during Link Receive processing

Migration Considerations ...

- **Define new security classes for RACF**
  - IIMS, JIMS, LIMS, MIMS

- **Enable RCF= value to something other than "N"**
  - Requires IMS cold start

- **Specify NORSCCC(MODBLKS) in DFSCGxxx**
  - Turn off resource consistency checking for Matrix data sets in an IMSplex environment

Migration Considerations ...

- Consider possible conflicts of trancodes for AOI and current userids for users
  - Possible MSNAME conflicts also

- Define Matrix data sets
  - Still required, but may be empty

Migration Checklist - SMU to RACF

- **Translate AGN definitions to RACF**
  - –Add the new classes to RACF
  - –Define new RAS parameters
    - SECURITY macro and execution ISIS parameter
  - –Create DFSRAS00 to replace DFSISIS0
  - –Review JCL for AGN= specifications

- **For static terminals required to sign on**
  - –Specify SIGNON=ALL|SPECIFIC parameter in DFSDCxxx
  - –Optionally, specify OPTIONS=SIGNON on applicable TYPE/TERMINAL macros

Migration Checklist - SMU to RACF ...

- **Enable SAF support for TCO command authorization**
  - TCORACF=Y and RCF=A|S|R|B
- **Review AOI requirements**
  - Specify AOI parameter on TRANSACT macro where needed
  - For TYPE 1 CMD security, additionally specify AOI1 = A|N|C|R|S
- **Migrate /LOCK and /UNLOCK security**
  - Specify LOCKSEC=Y in DFSDCxxx

Migration Checklist - SMU to RACF ...

- **Review MSC requirements for link receive security**
  - Specify use of SAF/DFSCTRN0 and level of authorization checking in the new MSCSEC parameter in DFSDCxxx
  - Modify DFSMSCE0 if needed
  - Synchronize RACF profiles on sending and destination systems

- **Determine the need to change or write exit routines**

Conversion Aid

SMU to RACF Conversion Aid

- **PK35433 (UK21894)**
  - **a set of stand-alone programs and sample JCL to aid syntax conversion**
- **PK38522**
  - **enhancements to PK35433**
- **Documentation**
  - **in PSP bucket:**

    upgrade IMS910 subset SMU2RACFCON

SMU to RACF Conversion Aid

AGN

)(AGN

- DFSKAGN0
- Sample JCL in IMS.SDFSISRC(DFSKSMJA)

SMU to RACF Conversion Aid

Type 1 AOI

)(CTRANS and)(TCOMMAND

– DIMS Populator Utility

  – DFSKDIMS

  – Sample JCL in IMS.SDFSISRC(DFSKSMJD

– SMU Command Resource Converter Utility)

  – DFSKCIMS

  – Sample JCL in IMS.SDFSISRC(DFSKSMJC)

– Can optionally update AOI= on TRANSACT macro

SMU to RACF Conversion Aid

LTERM Security

)(TERMINAL and)(COMMAND

- –DIMS Populator Utility
  - – DFSKDIMS
  - – Sample JCL in IMS.SDFSISRC(DFSKSMJD)
- –SMU Command Resource Converter Utility
  - –DFSKCIMS
  - –Sample JCL in IMS.SDFSISRC(DFSKSMJC)

- –Assumes USERID security will replace LTERM

SMU to RACF Conversion Aid

Static terminal sign on

)(SIGN

- STERM Extraction Utility
  - DFSKSMU1
  - Sample JCL in IMS.SDFSISRC(DFSKSMJS)
- STAGE1 Build Utility
  - DFSKSMU2
  - Sample JCL in IMS.SDFISIRC(DFSKSMJS)

And, finally……..

References

IMSV9 System Administration Guide

Chapter 4 (quite comprehensive)

SC18-7807-00 available for viewing or download at http://www.ibm.com/ims

IMS Version 9 Implementation Guide

Chapter 6 Security Consideration with IMS Version 9

SG24-6398 available for viewing or download at http://www.redbooks.ibm.com

We welcome your comments and suggestions!

If you have requests or need additional information or assistance, please send an email to:

maidalee@us.ibm.com