B52

IMS Version 8 and Version 9 Security Enhancements

Geoff Nicholls

Certified Senior IT Specialist

IMS

Technical Conference

Sept. 27-30, 2004

Orlando, FL

RETURN TO INDEX

DBRC - Command Authorization

Security support for DBRC commands

- Commands can be authorized
  - At the *command verb* level
    - For example, the **CHANGE** command
  - At the *verb + resource type* level
    - For example, the **CHANGE.DB** command
  - At the *verb + resource type + resource name* level
    - For example, the **CHANGE.DB** DBD(**ACCTDB**) command
- Security is invoked only for commands issued from
  - DBRC Utility (DSPURX00) -or-
  - HALDB Partition Definition Utility (DSPXDL00)
  - Use IMS command security for /RMx commands
- Security profiles may differ for different RECONs

DBRC - Command Authorization ...

Invoking Command Authorization

- Activate using DBRC command

CHANGE.RECON CMDAUTH(SAF|EXIT|BOTH|NONE,safhlq)

  - SAF - invoke security product (e.g. RACF)
  - EXIT - invoke DBRC Command Authorization exit routine (DSPDCAX0)
  - BOTH - invoke both security product and exit routine
  - NONE - do not invoke command authorization

  - safhlq - RECON high level qualifier (e.g. IMSP)
    - To distinguish between different RECONs in RACF
    - 1 to 8 characters
    - Must be specified with SAF, EXIT, or BOTH
    - Cannot be specified with NONE

- LIST.RECON displays current settings

DBRC - Command Authorization ...

Resource Name Table

- Contains list of resources which may be protected
  - List cannot be modified
- Example entries:
  - CHANGE .PRILOG .OLDS
  - CHANGE .PRILOG .RLDS
  - CHANGE .DB .ALL
  - CHANGE .DB .dbname
  - GENJCL .RECOV .dbname
  - GENJCL .RECOV .grpname
- Entries are prefixed by RECON qualifier for authorization processing
- See *DBRC Guide and Reference*, Appendix C, for complete list

DBRC - Command Authorization ...

RACF Definitions

- Uses FACILITY resource class
  - RDEFINE FACILITY *resource* UACC(NONE)
    - *resource* is *safhlq.command-verb.resource-type.resource-name*

- Users must be given READ access to command resource
  - PERMIT resource CLASS(FACILITY) ID(user_id) ACCESS(READ)

Example

```
RDEFINE FACILITY IMSP.GENJCL.RECOV.ACCTDB UACC(NONE)

PERMIT IMSP.GENJCL.RECOV.ACCTDB CLASS(FACILITY)
            ID(LONNIE) ACCESS(READ)
```

DBRC - Command Authorization ...

Equivalent HALDB partition definition commands

HALDB request	Master or Partition	Equivalent DBRC command
Query	Master	LIST.DB DBD(master db)
Set	Master	INIT.DB DBD(master db)
Set	Partition	INIT.PART DBD(master db)
Change	Master	CHANGE.DB DBD(master db)
Change	Partition	CHANGE.PART DBD(master db)
Delete	Master	DELETE.DB DBD(master db)
Delete	Partition	DELETE.PART DBD(master db)

DBRC - Command Authorization ...

If authorization denied by security product

```
DSP1157I USER userid NOT AUTHORIZED FOR COMMAND
RESOURCE NAME=resource-name SAF RC=rc RACF
RC=racfrc RACF REASON=racfrsn

DSP0209I  PROCESSING TERMINATED WITH CONDITION
CODE = 12
```

DBRC - Command Authorization ...

DBRC Command Authorization Exit (DSPDCAX0)

- Optional
- May deny authorization

```
DSP1154I   DBRC COMMAND AUTHORIZATION DENIED
BY DSPDCAX0 FOR USER userid
RESOURCE NAME = hlq.verb.type.name  RC = rc

DSP0209I  PROCESSING TERMINATED WITH CONDITION
CODE = 12
```

- May be used with security product (RACF, etc.)
  - Security product is invoked first
  - SAF return code and RACF return code/reason code are passed to exit routine
  - Exit may override security product

DBRC - Command Authorization ...

DBRC Command Authorization Exit (DSPDCAX0) ...

- Sample exit routine is provided in SDFSSMPL

- Input includes:
  - Address/Length of resource name
    - Address/Length of high level qualifier
    - Address/Length of command verb
    - Address/Length of command qualifier (resource type)
    - Address/Length of command modifier (resource name)
  - Userid
  - Flags (security product called?)
  - SAF return code
  - RACF return code and reason code
  - Address/Length of 1024-byte user area

- Returns:
  - DSPDCAX0 return code
    - 0 - authorization given
    - non-0 - authorization denied

DBRC - Command Authorization ...

All resources are uniquely defined

For example ...

- If user is permitted to use LIST.DB ALL command

```
RDEF FACILITY IMSP.LIST.DB.ALL UACC(NONE)
PERMIT IMSP.LIST.DB.ALL CLASS (FACILITY)
ID(LONNIE) ACCESS=(READ)
```

- User LONNIE *is not* automatically permitted to use

```
LIST.DB TYPHALDB
LIST.DB DBD(ACCTDB)
```

DBRC Command Authorization

Wildcard usage in resource names

- Wildcard ('*') may be used in definitions

```
RDEF FACILITY IMSP.LIST.DB.* UACC(NONE)
PERMIT IMSP.LIST.DB.* CLASS(FACILITY)
ID(LONNIE) ACCESS(READ)
```

- User LONNIE *is* permitted to use

```
LIST.DB TYPHALDB
LIST.DB DBD(ACCTDB)
```

DBRC - Command Authorization ...

Wildcard usage in resource names

- Unique resource definitions may disable a wildcard

```
RDEF FACILITY IMSP.LIST.DB.* UACC(NONE)
PERMIT IMSP.LIST.DB.* .... ID(LONNIE) ...
RDEF FACILITY IMSP.LIST.DB.ACCTDB UACC(NONE)
PERMIT IMSP.LIST.DB.ACCTDB ... ID(SUZIE) ...
```

- LONNIE *cannot* use
  `LIST.DB DBD(ACCTDB)`
- LONNIE *can* list database ACCTDB by using
  `LIST.DB ALL`

DBRC - Command Authorization ...

LIST.RECON

- Shows current setting for command authorization

```
RECON
 RECOVERY CONTROL DATA SET, IMS V8R1
 DMB#=7                                  INIT TOKEN=01225F2206572F
 NOFORCER  LOG DSN CHECK=CHECK17         STARTNEW=NO
 TAPE UNIT=3400       DASD UNIT=3400        TRACEOFF    SSID=IMSA
 LIST DLOG=NO                      CA/IC/LOG DATA SETS CATALOGED=NO
 MINIMUM VERSION = 8.1
 LOG RETENTION PERIOD=00.001 00:00:00.0
 COMMAND AUTH=SAF    HLQ=IMSP
 SIZALERT DSNUM=366       VOLNUM=999     PERCENT= 3
 LOGALERT DSNUM=52        VOLNUM=999
```

IMS Version 9 Security Enhancements

Security Enhancements

- **Enhancements to the SAF interface to support:**
  - Application Group Name (AGN) security
  - Type 1 and Type 2 Automated Operator Interface (AOI)
  - Terminal security for Time-Controlled Operations (TCO)
  - MSC link receive security
  - /LOCK and /UNLOCK commands
  - Signon verification

- **Benefits**
  - Overcomes limitations that prevent migration from SMU

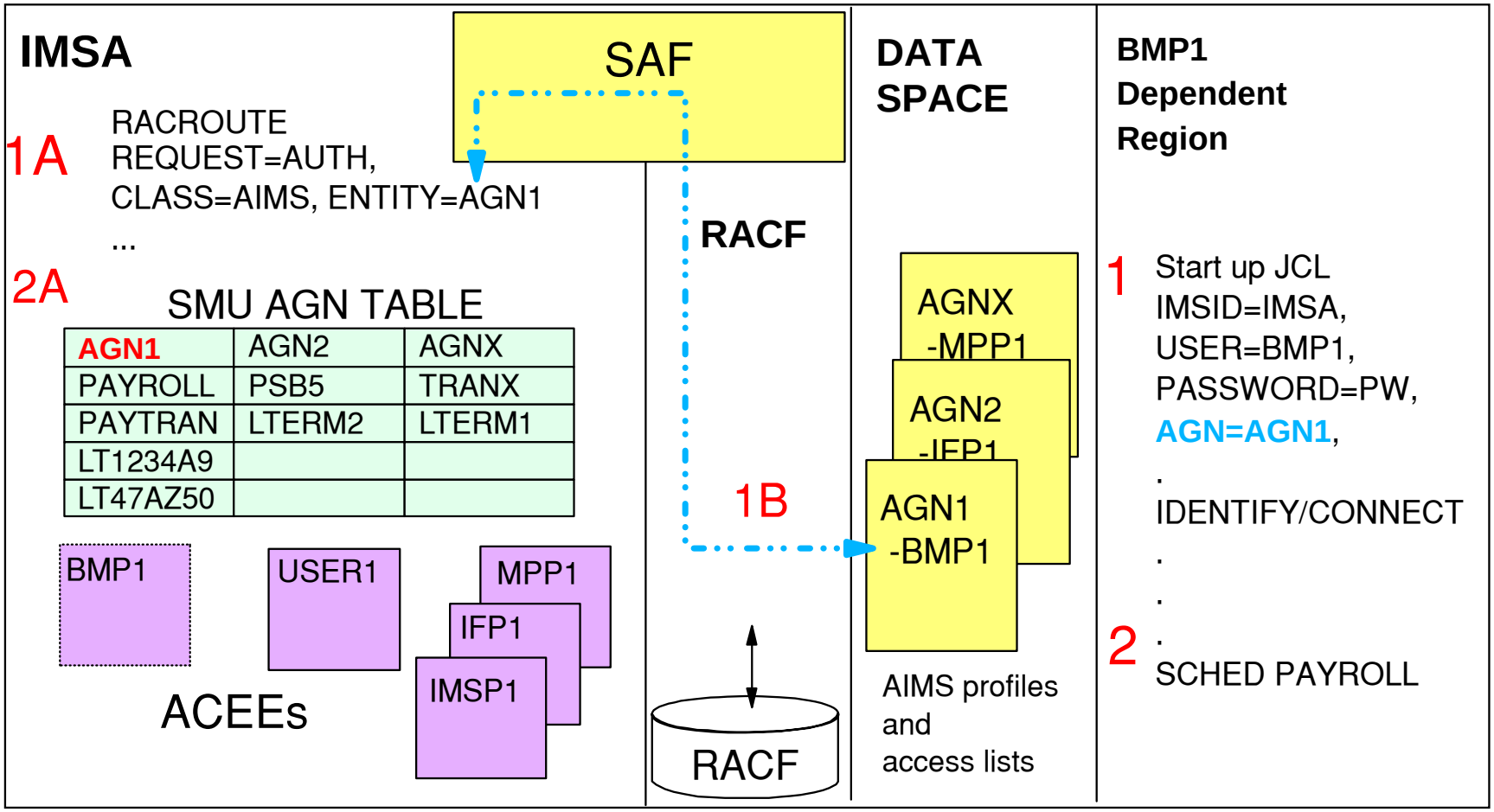
Resource Access Security (RAS)

- **Replaces SMU AGN security**
  - Also called resource access security

- **Prior releases - SMU and AGN**
  - Application Group Name (AGN)
    - Name associated with a group of resources
      - PSBs, Transactions, LTERMs
  - Security check for a region to access the resources
    - Region's userid to the AGN name
      - SAF or DFSISIS0
    - Access to the resources in the group
      - SMU

Resource Access Security (RAS) ...

- Prior releases - SMU and AGN ...



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 Version 9**
  - Provides direct SAF authorization checking of user to IMS resource (TRAN, PSB, LTERM)
    - Versus AGN (userid to AGN group, AGN group to resources)
  - 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 Version 9 ...**
  - **New** specifications in system definiton
    - SECURITY ... TYPE = RASRACF | RASEXIT | RAS | NORAS
      [| NOAGN | RACFAGN | AGNEXIT]

RASRACF = RAS security invokes RACF
RASEXIT = RAS security invokes an IMS user exit (DFSRAS00)
RAS = RAS security invokes RACF and user exit DFSRAS00
NORAS = No security (turns off both RAS and SMU)

  - **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 securityinvokes RACF and user exit DFSRAS00

defaults to SECURITY ... TYPE= specification

    - 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**

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 PASSWORD(BMPPW1)
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(GIM) ID(IMSDGRP) ACCESS(READ)
RDEFINE MIMS RASLGRP  ADDMEM(IMSUS02,T3270LD) UACC(NONE)
PERMIT RASLGRP CLASS(MIMS) ID(IMSDGRP) ACCESS(READ)
```

```
ADDUSER BMPUSER1 PASSWORD(BMPPW1)
CONNECT BMPUSER1 GROUP(IMSDGRP)
```

RAS Migration Examples ...

Example 2 - AGN name with access to all entities of a particular resource

AGN definitions:

```
)( AGN  IMSDGRP2
   AGPSB   ALL
   AGTRAN  ALL
```

in RACF, generic resource definitions can be used

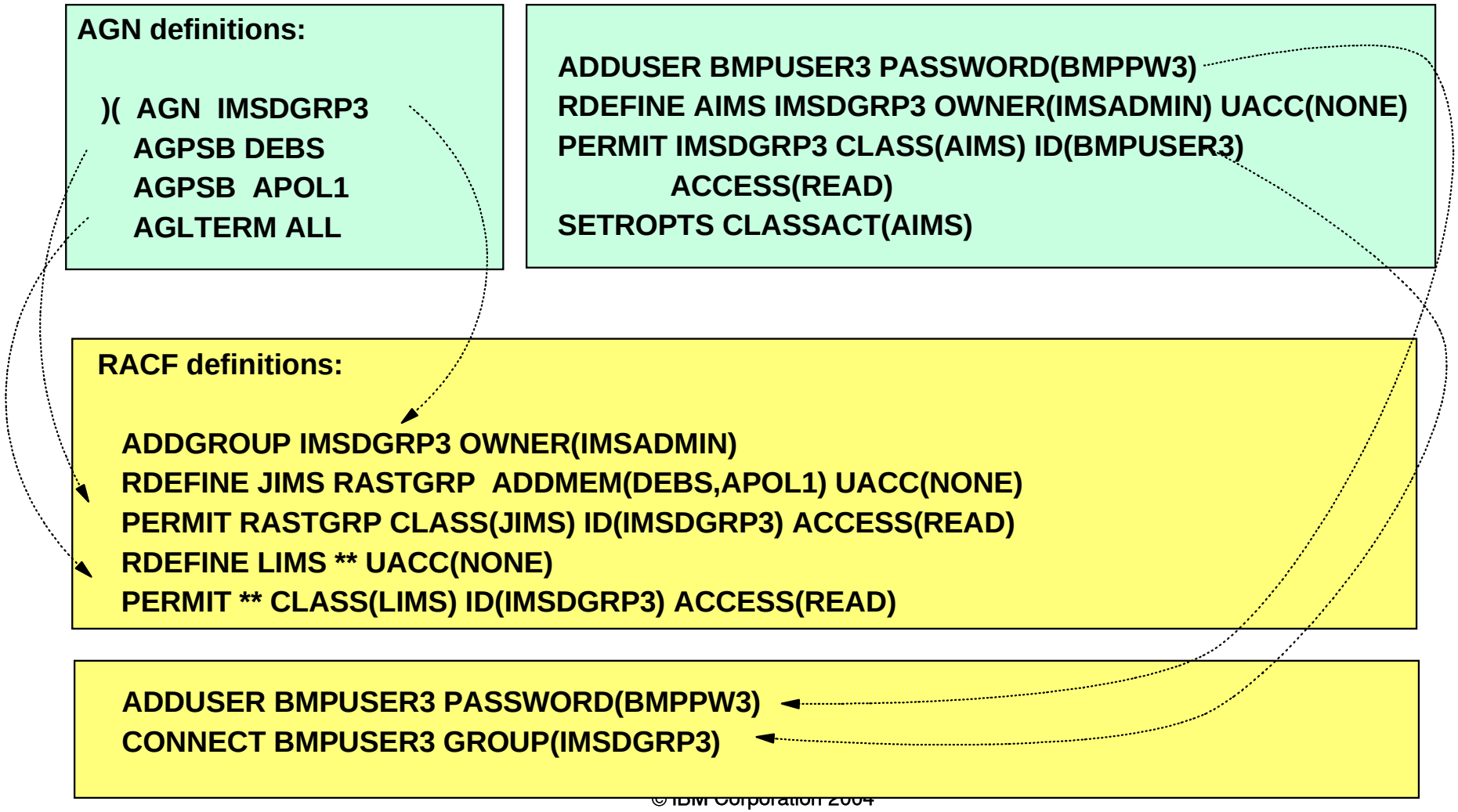
RACF definitions:

```
ADDGROUP IMSDGRP2 OWNER(IMSADMIN)
RDEFINE JIMS ** UACC(NONE)
PERMIT ** CLASS(JIMS) ID(IMSDGRP2) ACCESS(READ)
RDEFINE TIMS ** UACC(NONE)
PERMIT ** CLASS(TIMS) ID(IMSDGRP2) ACCESS(READ)
```

```
ADDUSER BMPUSER2 PASSWORD(BMPPW2)
CONNECT BMPUSER2 GROUP(IMSDGRP2)
```

RAS Migration Examples ...

Example 3 - combination of resource grouping and generic resources definitions



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

```
)(CTRANS AUTOCTL
  TCOMMAND START
  TCOMMAND STOP

)(TCOMMAND STOP
  CTRANS AUTOCTL
  CTRANS ADDINV
```

    - Type 2 AOI ICMD calls
      - SAF security
      - Checks userid access to CIMS class resources

AOI Security ...

- **IMS Version 9 enhancements**
  - SAF support for Type 1 AOI CMD calls
  - New TRANSACT macro parameter
    - Affects both Type1 and Type2 AOI calls

SAF Support for Type 1 AOI (CMD)

- **IMS Version 9 Enhancement**
  - 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. SAF (RACF) is called first then DFSCCMD0
      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
    - Defaults to system definition specification on SECURITY macro
  - Can be overriden by /NRE or /ERE ... TRANCMDS | NOTRANCMDS

SAF Support for Type 1 AOI (CMD) ...

- **New TRANSACT parameter**
  - Modifiable by Online Change
  - Specifies whether transaction is allowed to process AOI CMD calls
    - Authorization based on trancode or userid of inputting terminal
  - **AOI** = YES | NO | TRAN | CMD

YES = Requests the userid of the user who entered the transaction be used to determine authorization of the commands for the CMD call issued by the transaction

NO = No authorization checking is done

TRAN = Similar to YES but requests that the trancode be used instead of userid for authorization

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

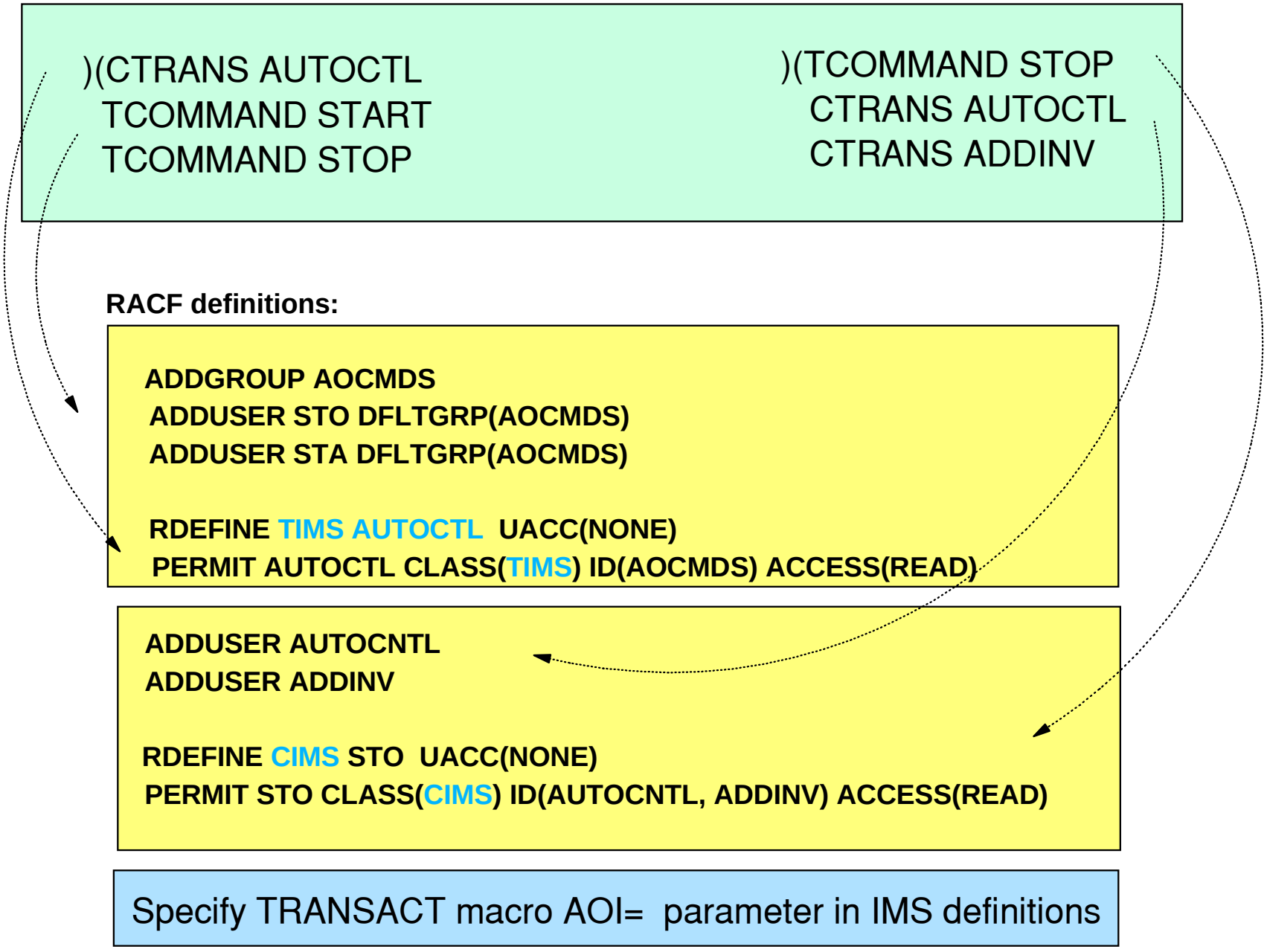
)(TCOMMAND STOP
CTRANS AUTOCTL

CMD = Similar to YES but requests that the command code (first three characters of the command) be used instead of the userid for authorization

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

)(CTRANS AUTOCTL
TCOMMAND START

SAF Support for Type 1 AOI (CMD) ...



SAF Support for Type 1 AOI (CMD) ...

- **Interaction between AOI1 on startup and AOI on TRANSACT macro**
  - 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
- **Final override**
  - /NRE or /ERE ... TRANCMDS|NOTRANCMDS

SAF Support for Type 2 AOI (ICMD)

- **Already supports a SAF interface**
  - AOIS = A | C | N | R | S
    - Execution parameter
- **New TRANSACT parameter**
  - Applies to both Type 1 and Type 2 AOI
  - **AOI** = YES | NO | TRAN | CMD
    - AOI=YES
      - Does not apply to Type 2 AOI (already uses userid checking)
    - AOI=NO is not enforced
      - If specified or defaulted,
        - Transaction still allowed to use Type 2 AOI and issue ICMD
    - AOI=TRAN | CMD
      - Requests authorization similar to what used to be provided with SMU

SAF Support for TCO

- **Time Controlled Operations (TCO)**
  - IMS capability to execute time-initiated commands and transactions
- **Security support**
  - Loading of TCO scripts
  - Resource authorization
    - Commands
    - Transactions

SAF Support for TCO ...

- **Loading of TCO scripts**
  - Restricts who can load a TCO script
  - Checked by the TCO CNT Edit Exit (DFSTCNT0)
    - No change from previous release

SAF Support for TCO

- **Resource authorization**
  - Prior releases
    - SMU support of the DFSTCFI LTERM authorization

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

)( COMMAND   START
        TERMINAL   DFSTCFI

)( COMMAND   STOP
     TERMINAL   DFSTCFI
```

    - SAF support
      - TCO script specification of /SIGN ON *tcousid tcopw*
        - Created ACEE
        - Available for SAF authorization to the transaction
        - But **NO** SAF authorization for commands

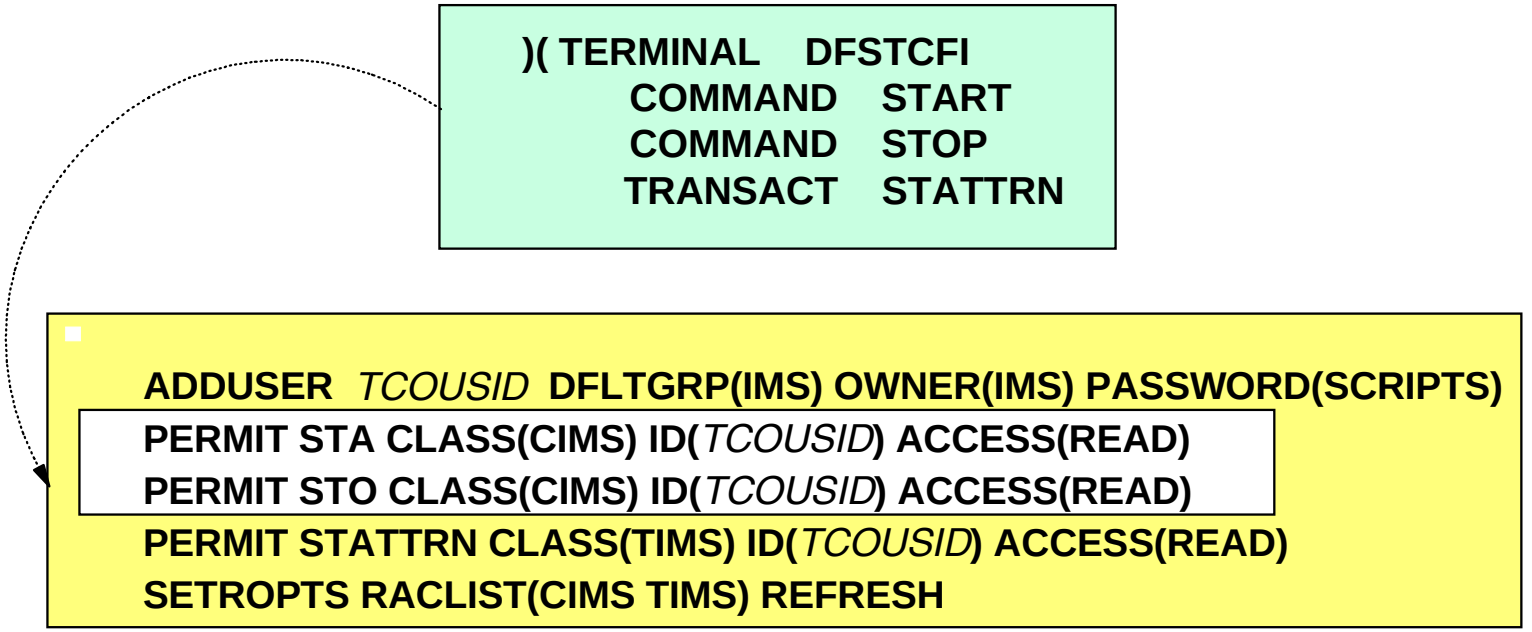
SAF Support for TCO ...

- **Resource authorization ...**
  - Prior releases - command authorization
    - With RCF = A | S | R | B (only calls DFSCCMD0)
    - Could specify /SIGN ON in TCO script to define userid
    - But since TCO was authorized to issue the same set of commands as the system console and master terminal
      - **SAF not called for command authorization**
      - **DFSCCMDO could make final decision**

SAF Support for TCO ...

- **Command authorization ...**
  - IMS Version 9
    - New execution parameter TCORACF = Y | N
      - DFSPBxxx
      - Specifies whether or not TCO security supports SAF
    - With RCF = A | S | R | B, SAF and DFSCCMD0 are called
      - SAF is called only if TCORACF = Y is specified
      - Can use /SIGN ON in TCO script to define userid for command authorization
        - **Assumes userid is valid**

SAF Support for TCO ...



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

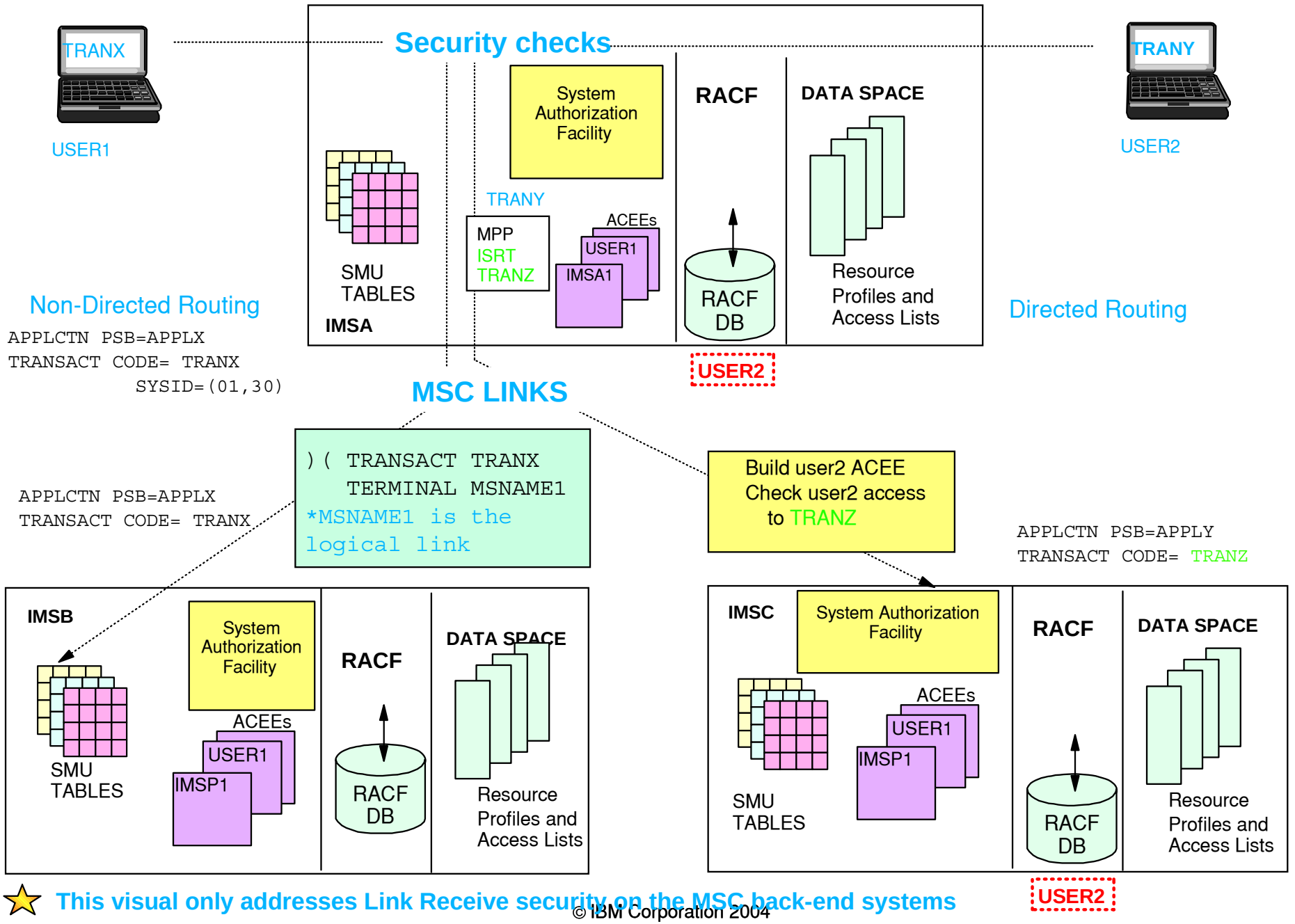
The above definitions could have been coded in prior releases. If so, authorization for the transaction was done. Command authorization, however, was never invoked.

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

MSC Link Security

- **Prior releases**
  - Directed routing
    - Used SAF and DFSCTRN0 before and after DFSMSCE0 call
  - Non-Directed routing
    - Used SMU after the DFSMSCE0 call

MSC Link Security



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

MSC Link Security ...

- **IMS Version 9**
  - New parameter in DFSDCxxx to specify use of SAF/DFSCTRN0
    - **MSCSEC**=(<LRDIRECT | LRNONDR | LRALL | LRNONE >)
      < , CTL | MSN | USER | EXIT | CTLEXIT |
      MSNEXIT | USREXIT | NONE>)
      - First value:

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

MSC Link Security ...

- **IMS Version 9 considerations**
  - Possible call to SMU security
    - If MSCSEC=LRNONDR is not specified
  - Link Receive processing
    - No SAF/DFSCTRN0 call prior to DFSMSCE0 call
    - Level of authorization checking controlled by DFSMSCE0
    - SAF/ DFSCTRN0 call after DFSMSCE0
  - Additional data is passed to DFSMSCE0
    - Userid, Group name, and Userid indicator
  - RACF profiles should be kept synchronized on sending and receiving systems

MSC Link Security ...

- **DFSMSCE0 can control level of authorization during Link Receive processing**
  - Authorization by MSNAME
    - ACEE dynamically created for first authorization
  - Authorization by CTL address space security
  - Authorization by userid of inputting terminal
    - ACEE dynamically created and deleted for each authorization
  - Authorization by user exit (DFSCTRN0)
  - No Security authorization checking

MSC Link Security ...

- **Second value in the MSCSEC parameter**
  - Specifies level of authorization similar to that in DFSMSCE0
    - MSCSEC=(<LRDIRECT | LRNONDR | LRALL | LRNONE>
      < , CTL | MSN | USER | EXIT | CTLEXIT |
      MSNEXIT | USREXIT | NONE>)

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**

/LOCK and /UNLOCK

- **Commands to make resources unavailable or available to all users**

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

- **Prior releases**

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

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

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

/LOCK and /UNLOCK ...

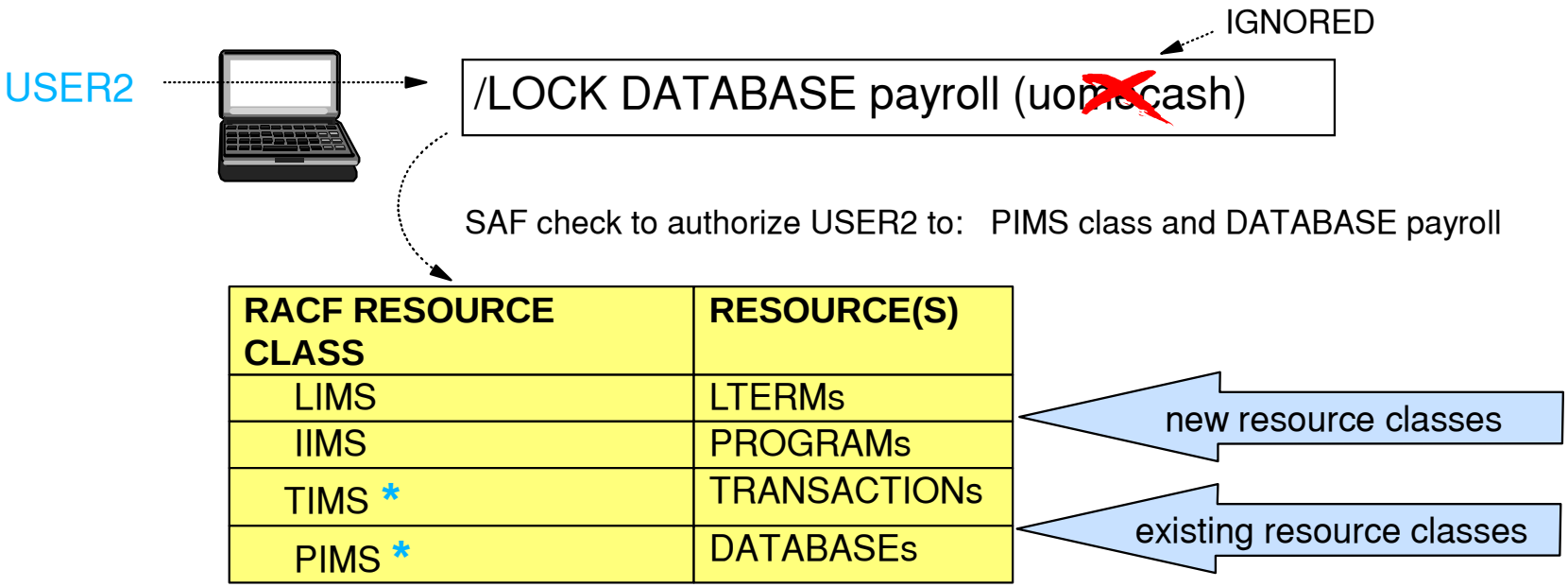
- **IMS Version 9**
  - SAF Support - New DFSDCxxx parameter
  - LOCKSEC = Y | N
    - N = No authorization checking
    - Y = Calls SAF and DFSCTRN0
      - RACF classes: LIMS, PIMS, IIMS, TIMS
      - DFS3689W - new message if authorization fails

- SAF security is based on userid

Supports:
/LOCK and /UNLOCK LTERM | DATABASE | PROGRAM | TRANSACTION

/LOCK and /UNLOCK ...

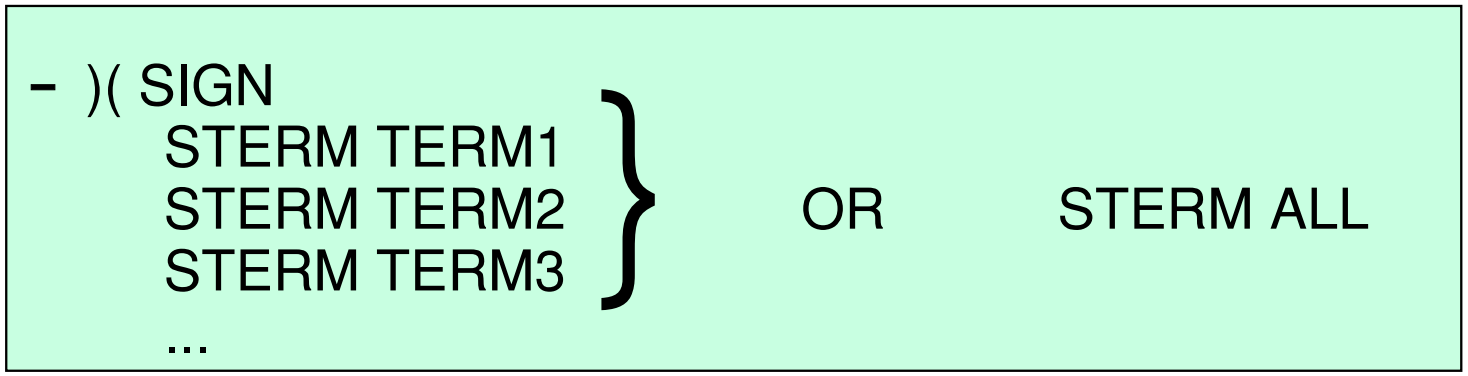
- **IMS Version 9**
  - If the user is authorized to issue the /LOCK and /UNLOCK commands, another check is made to authorize access to resources



Note: No SAF call made for /LOCK and /UNLOCK NODE | PTERM
Protection of VTAM nodes and BTAM terminals relies on the use of RACF TERMINAL|GTERMINAL support

Signon Verification Security

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



Signon Verification Security ...

- **IMS Version 9**
  - New startup parameter in DFSDCxxx
    - SIGNON = ALL | SPECIFIC

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 | NOSIGNON)
  - VTAM
    - Specification on TERMINAL macro overrides TYPE
    - No specification on the TERMINAL macro defaults to TYPE macro
  - BTAM
    - Specification only applies to TERMINAL macro
      - Not available on LINEGRP or LINE macros

Performance and Operational Considerations

- **Performance**
  - Characteristics
    - SAF calls versus SMU matrix table authorizations
  - Consideration
    - For MSC link security, options control security impact
- **Operations**
  - DFS066 (password security violation) and DFS067 (terminal security violation)
    - No longer displayed, instead ICH408I RACF messages
  - IVP
    - Supports the use of RACF or SMU and AGN security

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**

RETURN TO INDEX