E62

Converting From IMS/SMU To RACF Security

Alonia (Lonnie) Coleman, IMS Advanced Technical Support

IMS technical conference

Las Vegas, NV **September 15 - September 18, 2003**

RETURN TO INDEX

- Part 1 -

Converting From IMS Security Maintenance Utility (SMU) to RACF Security

Session E62

All references to RACF are intended to imply either RACF or an equivalent security product

IMS V8 Announcement

IBM United States
Software Announcement 202-229
September 24, 2002

.

.

.

Compatibility: IMS V8 is upwardly compatible from previous versions, allowing existing applications and data to be used without change. Migration and coexistence support is provided for IMS V6 and V7 with V8. Review the Preventative Service Planning (PSP) information for further, current details.

.

.

.

IMS V8 is the last release to support the Security Maintenance Utility (SMU). Customers using SMU should migrate to the Resource Access Control Facility (RACF) or an equivalent product.

.

.

.

Objectives

To convert SMU security to RACF security, you need to

- Know where to look to determine if you use SMU
- Understand which IMS ***resource types*** (e.g. transactions, commands, terminals, etc.) are protected by SMU
- Understand the ***type(s) of protection*** (e.g. password, LTERM based entry restriction, sign on, etc.) that was used to secure each IMS resource

At the end of these two sessions you should be able to

- Determine if your IMS systems use SMU security
- Identify IMS resources which are protected by SMU
- Identify the type(s) of SMU security used to protect IMS resources
- Determine if the SMU security for a resource can be converted to RACF security
- Define the requirements for RACF security for IMS resources

Agenda

Part 1

- IMS security facilities
- SMU security overview

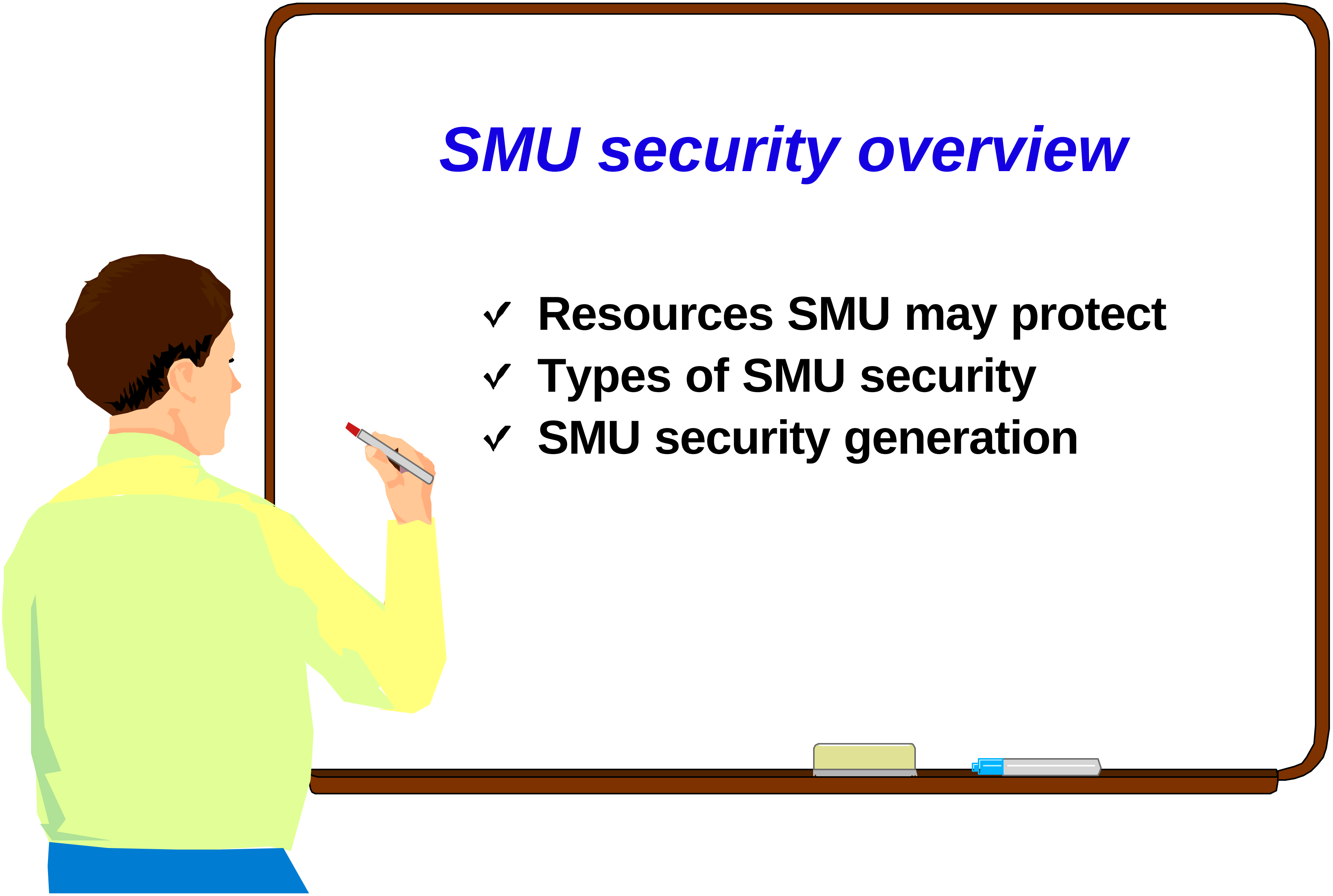
Part 2

- Converting SMU security to RACF security
  - IMS commands
  - IMS transactions
  - IMS databases and data sets
  - Terminals
- Considerations
  - TYPE1 automated operator (AO) programs
  - Application Group Name (AGN) security
    - Start of dependent regions
    - Program Specification Blocks (PSBs)
    - Logical Terminals (LTERMs)
    - Transaction Codes

IMS Security Facilities

IMS provides 5 security facilities/mechanisms to protect resources

1. Default security (for IMS commands only)
2. Security Maintenance Utility (SMU)
3. Program Specification Block (PSB)
   - This is a mechanism that limits an application's view of database segments to only those segments defined in the Program Communications Block (PCB)
4. RACF
5. User/installation exit routines
   - IMS provides samples for some security exits, such as
     - Command Authorization Exit (DFSCCMD0)
     - Transaction Authorization Exit (DFSCTRN0)
     - Security Reverification Exit (DFSBSEX0)
     - Sign On/Sign Off Security Exit (DFSCSGN0)
     - Build Security Exit Routine (DFSBSEX0) - Sample on the web



SMU security overview

- ✓ Resources SMU may protect
- ✓ Types of SMU security
- ✓ SMU security generation

SMU Security Overview

SMU consists of internal IMS modules which provide security for IMS resources

SMU security may be used protect *static* IMS resources

- Commands
- Transactions
- Databases
- Terminals
- Programs/Program Specification Blocks (PSBs)
- Dependent regions

Resources SMU May Protect

IMS Resource Type	SMU may secure if resource is ...
Command	Entered from any of the following sources: Static terminal Time Controlled Operations (TCO) script TYPE 1 automated operator (AO) program
Transaction	Entered from any of the following sources: Static terminal Time Controlled Operations (TCO) script Static Intersystem Communication (ISC) link Multiple Systems Coupling (MSC) logical link
Database	An IMS database
Terminal	A static VTAM or BTAM terminal
Program/Program Specification Block (PSB)	An IMS Program Specification Block (PSB)
Dependent region	Any of the following types of IMS regions: Message Processing Program (MPP) Interactive Fast Path (IFP) Batch Message Program (BMP)
Connection thread	A z/OS address space [e.g. CICS-to-DataBase Control (DBCTL)] that requests connection to the IMS control region

Types of SMU Security

1. **Password security**

2. **Terminal based security**

   – There are 2 types of SMU terminal security

     I. ***LTERM based security***

     - SMU has a limit of 65,535 LTERM definitions

     II. ***Sign on***

     - The terminal user is required to enter:

       /SIGN ON *userid password*

     - SMU has a maximum of 32,767 terminals which may be required to sign on

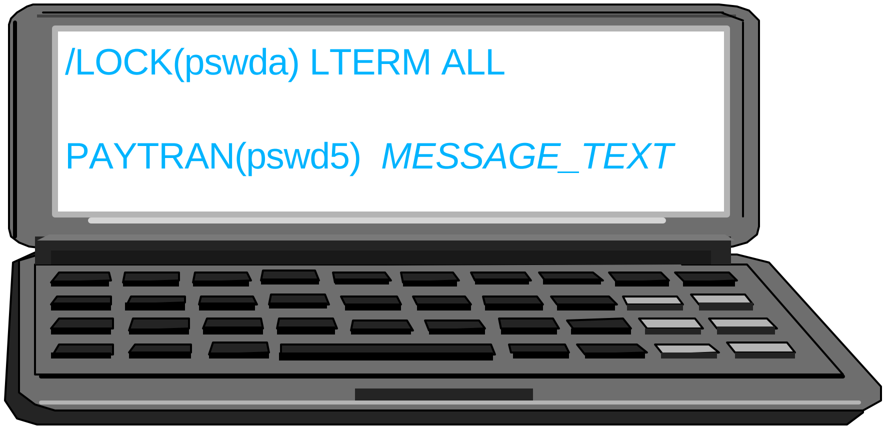
3. **Transaction-command security**

4. **Application group name (AGN) security**

SMU Password Security

Password security may be used to

- Protect IMS commands
  - Passwords may be assigned to commands
- Protect IMS transactions
  - Passwords may be assigned to transactions



```
/LOCK(pswda) LTERM ALL

PAYTRAN(pswd5)  MESSAGE_TEXT
```

- Make some IMS resources (e.g. terminals, programs, transactions, and/or databases) ***unavailable*** or ***available*** for use
  - /LOCK and /UNLOCK commands are used in with resource passwords

```
/LOCK NODE(pswd1)                        /UNLOCK NODE(pswd1)
/LOCK PTERM(pswd2)                       /UNLOCK PTERM(pswd2)
/LOCK LTERM LTERMA(pswd3)                /UNLOCK LTERM LTERMA(pswd3)
/LOCK PROGRAM PAYPGM(pswd4)              /UNLOCK PROGRAM PAYPGM(pswd4)
/LOCK TRANSACTION PAYTRAN(pswd5)         /UNLOCK TRANSACTION PAYTRAN(pswd5)
/LOCK DATABASE PERSNLDB(pswd6)           /UNLOCK DATABASE PERSNLDB(pswd6)
```

- Compliment terminal based security

SMU Password Security Options

SECURITY MACRO

PASSWD=	TERMNL=	SECLVL=	TRANCMD=	TYPE=	SECCNT=	RCLASS=
NO	NO	NOTRAN,NOSIGN	NO		0	IMS
YES	YES	NOTRAN,SIGNON	YES		1	XXXXXXX
FORCE	FORCE	NOTRAN,FORCSIGN	FORCE		2	
		TRANAUTH,SIGNON			3	
		TRANAUTH,FORCSIGN				
		FORCTRAN,FORCSIGN				

NOAGN	NORACTRM	NOTRANEX	NOSIGNEX	NORACFCM
RACFAGN	RACFTERM	TRANEXIT	SIGNEXIT	RACFCOM
AGNEXIT				

/NRE CHECKPOINT 0 **PASSWORD** | /NRE CHECKPOINT 0 **NOPASSWORD**
/ERE COLDSYS FORMAT ALL **PASSWORD** | /ERE COLDSYS FORMAT ALL **NOPASSWORD**

SMU Terminal Based Security

Terminal based security may be used

- To restrict command and/or transaction entry to one or more specific (or authorized) LTERMs
  - Let's call this *'LTERM based'* terminal security
- To require one or more physical terminals/nodes to sign on
  - Let's call this *'user sign on'* security
  - For example, first input from the terminal must be /SIGN ON followed by a userid and password
    - /SIGN ON *ACOLEMAN RACF4ME*
- With or without password security

SMU Terminal Based Security Considerations

Considerations

- SMU modules can ***NOT*** validate the userid provided at sign on
  - The userid may be verified by
    - RACF
    - One or more sign on exit routines

      Sign On Exit Routine (DFSSGNX0)

      Sign On / Sign Off Security Exit Routine (DFSCSGN0)
    - Both RACF and one or more sign on exit routines
- SMU provides terminal based security for ***static*** terminals only
  - The following terminal types are ***not*** supported
    - Extended Terminal Option (ETO)
    - Advanced Program to Program Communications (APPC)
    - TCP/IP
    - Multiple Console Support/Enhanced-Multiple Console Support (MCS/E-MCS)
    - Etc.

LTERM-Based Security Options

SECURITY MACRO

PASSWD=	**TERMNL=**	**SECLVL=**	**TRANCMD=**	**TYPE=**	**SECCNT=**	**RCLASS=**
NO	**NO**	NOTRAN,NOSIGN	NO		0	IMS
YES	YES	NOTRAN,SIGNON	YES		1	XXXXXXX
FORCE	FORCE	NOTRAN,FORCSIGN	FORCE		2	
		TRANAUTH,SIGNON			3	
		TRANAUTH,FORCSIGN				
		FORCTRAN,FORCSIGN				

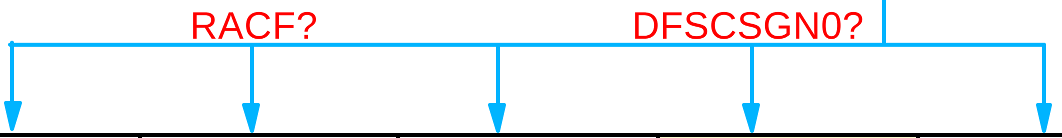
NOAGN	NORACTRM	NOTRANEX	NOSIGNEX	NORACFCM
RACFAGN	RACFTERM	TRANEXIT	SIGNEXIT	RACFCOM
AGNEXIT				

/NRE CHECKPOINT 0 **TERMINAL** | /NRE CHECKPOINT 0 **NOTERMINAL**
/ERE COLDSYS FORMAT ALL **TERMINAL** | /ERE COLDSYS FORMAT ALL **NOTERMINAL**

(User) Sign On Security Options

SECURITY MACRO

PASSWD=	TERMNL=	SECLVL=	TRANCMD=	TYPE=	SECCNT=	RCLASS=
NO	NO	**NOTRAN,NOSIGN**	NO		0	IMS
YES	YES	NOTRAN,SIGNON	YES		1	XXXXXXX
FORCE	FORCE	NOTRAN,FORCSIGN	FORCE		2	
		TRANAUTH,SIGNON			3	
		TRANAUTH,FORCSIGN				
		FORCTRAN,FORCSIGN				



NOAGN	**NORACTRM**	NOTRANEX	**NOSIGNEX**	NORACFCM
RACFAGN	RACFTERM	TRANEXIT	SIGNEXIT	RACFCOM
AGNEXIT				

IMS.PROCLIB(DFSPBxxx)

SGN=N | Y | F
RCF=N | C | S | T | Y | R | B

/NRE CHECKPOINT 0 **USER** | /NRE CHECKPOINT 0 **NOUSER**
/ERE COLDSYS FORMAT ALL **USER** | /ERE COLDSYS FORMAT ALL **NOUSER**

SMU Transaction-command Security

Transaction-command security is

- Also referred to as ***tran-command*** security
- Used to protect IMS commands issued by automated operator (AO) programs that use the ***DL/I CMD*** call
  - AO programs that issue the CMD call are ***TYPE1***

    NOTE: SMU does ***not*** support security for TYPE2 AO programs. TYPE2 AO program use the DL/I ICMD (Issue Command) call to issue IMS commands. Command authorization support for TYPE2 AO programs is provided by RACF and/or Command Authorization Exit.
- Supported in the following environments
  - DB/TM (or DB/DC)
  - DCCTL

Transaction-Command Security Options

SECURITY MACRO

PASSWD=	**TERMNL=**	**SECLVL=**	**TRANCMD=**	**TYPE=**	**SECCNT=**	**RCLASS=**
NO	NO	NOTRAN,NOSIGN	**NO**		0	IMS
YES	YES	NOTRAN,SIGNON	YES		1	XXXXXXX
FORCE	FORCE	NOTRAN,FORCSIGN	FORCE		2	
		TRANAUTH,SIGNON			3	
		TRANAUTH,FORCSIGN				
		FORCTRAN,FORCSIGN				

NOAGN	NORACTRM	NOTRANEX	NOSIGNEX	NORACFCM
RACFAGN	RACFTERM	TRANEXIT	SIGNEXIT	RACFCOM
AGNEXIT				

/NRE CHECKPOINT 0 **TRANCMDS** | /NRE CHECKPOINT 0 **NOTRANCMDS**
/ERE COLDSYS FORMAT ALL **TRANCMDS** | /ERE COLDSYS FORMAT ALL **NOTRANCMDS**

SMU Application Group Name (AGN) Security

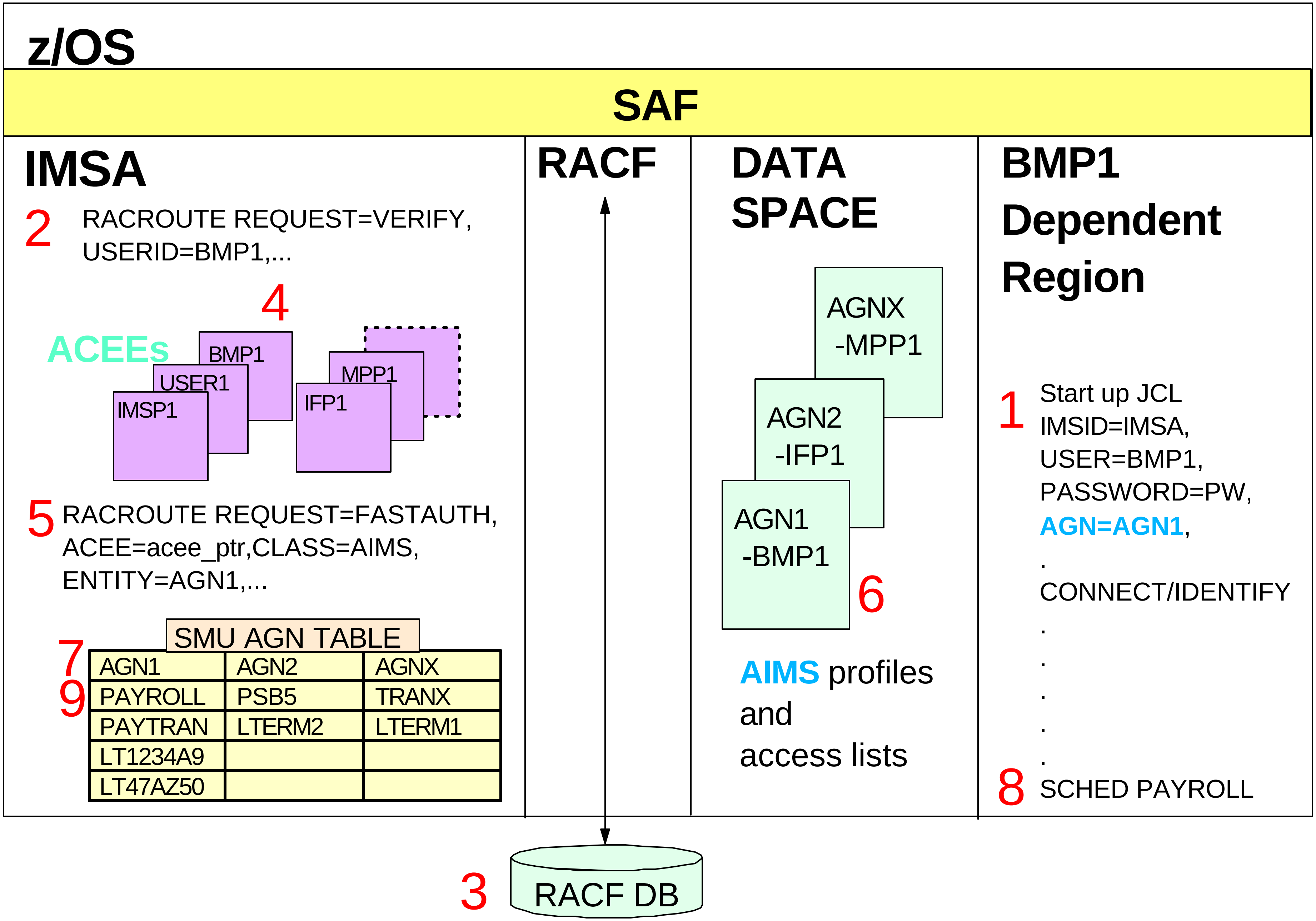
AGN security provides mandatory, 3-part protection

1. Each dependent region/thread must provide an AGN name in either:
   - Startup JCL via the **AGN=***agn_name* specification
   - Database Resource Adapter (DRA) connection request **AGN=***agn_name* specification

2. RACF (or an equivalent product) or the Resource Access Security Exit (DFSISIS0) must authorize the region/thread to the *agn_name* supplied in region/thread JCL at the time the region/thread request a connection to the control region

3. Each *agn_name* and the resources it includes must have been previously defined to IMS via a SMU security generation. IMS validates the *agn_name* exists prior to completion of region/thread initialization

AGN Security Illustration



z/OS

SAF

IMSA

2 RACROUTE REQUEST=VERIFY,
USERID=BMP1,...

4

5 RACROUTE REQUEST=FASTAUTH,
ACEE=acee_ptr,CLASS=AIMS,
ENTITY=AGN1,...

SMU AGN TABLE

7
9

AGN1	AGN2	AGNX
PAYROLL	PSB5	TRANX
PAYTRAN	LTERM2	LTERM1
LT1234A9		
LT47AZ50		

RACF

DATA SPACE

6

AIMS profiles
and
access lists

BMP1 Dependent Region

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

3 RACF DB

AGN Group Resources

Regions/threads are restricted to use of resources in the *agn_name* (or AGN group) supplied at startup/connection

	RESOURCES WHICH MAY BE INCLUDED IN AN AGN GROUP		
Region Type	**PSB(s)**	**Transaction Code(s)**	**LTERM(s)**
BMP Region	✓	✓	✓ **(1)**
MPP Region		✓	
IFP Region	✓		
JMP Region		✓	
JBP Region	✓	✓	✓ **(1)**
CCTL (e.g. CICS-DBCTL)	✓		
z/OS Address Space running Open Database Access (ODBA) program	✓		

Note 1: Logical terminal or transaction code for the OUT=xxxxxxxx specification on the JCL used to start the Batch Message Program (BMP) or the Java Batch Program (JBP).

AGN Security Options

SECURITY MACRO

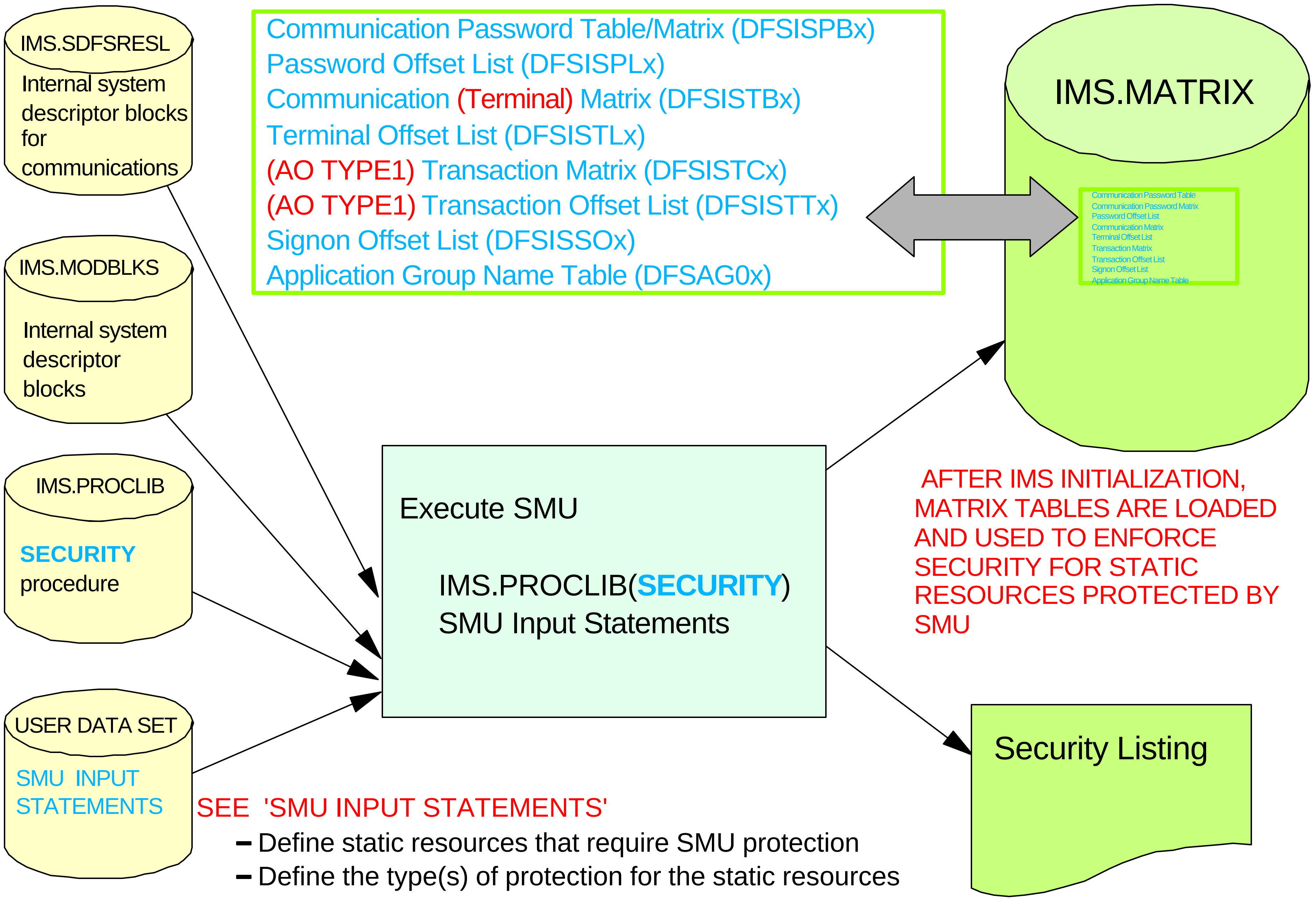
PASSWD=	TERMNL=	SECLVL=	TRANCMD=	TYPE=	**SECCNT=**	**RCLASS=**
NO	NO	NOTRAN,NOSIGN	NO		0	IMS
YES	YES	NOTRAN,SIGNON	YES		1	XXXXXXX
FORCE	FORCE	NOTRAN,FORCSIGN	FORCE		2	
		TRANAUTH,SIGNON			3	
		TRANAUTH,FORCSIGN				
		FORCTRAN,FORCSIGN				

NOAGN	NORACTRM	NOTRANEX	NOSIGNEX	NORACFCM
RACFAGN	RACFTERM	TRANEXIT	SIGNEXIT	RACFCOM
AGNEXIT				

IMS.PROCLIB(DFSPBxxx) ISIS=0 | 1 | 2

ISIS=0 means AGN security is turned *off*. **ISIS=1** means AGN security is turned ***on*** and RACF grants/denies the region/thread request to connect to the IMS control region using the specified AGN (*agn_name*). **ISIS=2** means AGN security is turned ***on*** and the AGN Exit Routine (DFSISIS0, instead of RACF, grants/denies the region/thread request to connect to the IMS control region using the specified AGN (*agn_name*).

SMU Security Generation



IMS.SDFSRESL

Internal system descriptor blocks for communications

IMS.MODBLKS

Internal system descriptor blocks

IMS.PROCLIB

SECURITY procedure

USER DATA SET

SMU INPUT STATEMENTS

Communication Password Table/Matrix (DFSISPBx)
Password Offset List (DFSISPLx)
Communication (Terminal) Matrix (DFSISTBx)
Terminal Offset List (DFSISTLx)
(AO TYPE1) Transaction Matrix (DFSISTCx)
(AO TYPE1) Transaction Offset List (DFSISTTx)
Signon Offset List (DFSISSOx)
Application Group Name Table (DFSAG0x)

IMS.MATRIX

Communication Password Table
Communication Password Matrix
Password Offset List
Communication Matrix
Terminal Offset List
Transaction Matrix
Transaction Offset List
Signon Offset List
Application Group Name Table

Execute SMU

IMS.PROCLIB(**SECURITY**)
SMU Input Statements

AFTER IMS INITIALIZATION, MATRIX TABLES ARE LOADED AND USED TO ENFORCE SECURITY FOR STATIC RESOURCES PROTECTED BY SMU

Security Listing

SEE 'SMU INPUT STATEMENTS'

- Define static resources that require SMU protection
- Define the type(s) of protection for the static resources

SMU Security Listing

```
//       PROC  OPTN=UPDATE,IMS=',0',SOUT=A,SYS2=,RGN=2048K
//S      EXEC  PGM=DFSISMP0,PARM='LIST,0'
//STEPLIB  DD  DSN=IMS.&SYS2 MODBLKS,DISP=SHR
//         DD  DSN=IMS.&SYS2 SDFSRESL,DISP=SHR
//SYSPRINT DD  SYSOUT=&SOUT,DCB=(RECFM=VBA,BLKSIZE=129,LRECL=125)
//SYSPUNCH DD  UNIT=SYSDA,SPACE=(CYL,(2,2)),
//             DCB=(RECFM=FB,LRECL=80,BLKSIZE=400),
//             DISP=(NEW,PASS)
//SYSLIN   DD  UNIT=SYSDA,SPACE=(TRK,(1,1)),
//             DCB=(RECFM=F,BLKSIZE=80),
//             DISP=(NEW,PASS)
//SYSUT1   DD  UNIT=SYSDA,DCB=(BLKSIZE=500,RECFM=FB),
//             SPACE=(CYL,(2,2))
//SYSUT2   DD  UNIT=(SYSDA,SEP=SYSUT1),DCB=*.S.SYSUT1,
//             SPACE=(CYL,(2,2))
//SYSIN    DD  DSN=NO.SYSIN.DD.ASTERISK
//C     EXEC  PGM=ASMA90,PARM='OBJECT,NODECK',COND=(12,LT,S),REGION=&RGN
//SYSLIB   DD  DSN=SYS1.SDFSMAC,DISP=SHR
//SYSPRINT DD  SYSOUT=&SOUT DCB=BLKSIZE=1089;
//SYSLIN   DD  UNIT=(SYSDA,SEP=SYSPRINT),DISP=(,PASS),
//             SPACE=(CYL,(2,2)),
//             DCB=*.S.SYSPUNCH
//SYSUT1   DD  UNIT=SYSDA,SPACE=(CYL,(10,5))
//SYSIN    DD  DSN=*.S.SYSPUNCH,DISP=(OLD,DELETE)
//L      EXEC  PGM=IEWL,PARM=(LIST,NE,OL,'RMODE=ANY'),REGION=&RGN,
//             COND=(4,LT,S)
//SYSPRINT DD  SYSOUT=&SOUT,DCB=(RECFM=FBA,LRECL=121,BLKSIZE=605)
//SYSLMOD  DD  DSN=IMS.&SYS2 MATRIX,DISP=SHR
//INPUT    DD  DSN=*.C.SYSLIN,DISP=(OLD,DELETE)
//SYSUT1   DD  UNIT=(SYSDA,SEP=INPUT),SPACE=(CYL,(5,1))
//SYSLIN   DD  DSN=*.S.SYSLIN,DISP=(OLD,DELETE)
```

RC=16

SMU Input Statements (1)

```
)(  COMMAND DIS
    PASSWORD  SHOWME
```

SMU PASSWORD SECURITY

```
)(  COMMAND STO
    TERMINAL DFSTCFI
```

SMU LTERM BASED TERMINAL SECURITY

```
)(  TRANSACT PAYTRAN
    PASSWORD  IOUMONEY
    TERMINAL LTERM1
```

SMU PASSWORD AND
SMU LTERM BASED TERMINAL SECURITY

```
)(  PASSWORD PEOPLE
    DATABASE CUSTOMER
```

SMU PASSWORD SECURITY

```
)(  AGN ORDERAGN
    AGPSB ORDERPSB
    AGTRAN ORDERTRN
    AGLTERM LTERM2
```

SMU AGN SECURITY

```
)(  SIGN
    STERM ALL
```

SMU (USER) SIGN ON TERMINAL SECURITY

```
)(  SIGN
    STERM NODE1234
    STERM NODE5678
```

SMU (USER) SIGN ON TERMINAL SECURITY

SMU Input Statements (2)

)(CTRANS AOTRAN TCOMMAND STA TCOMMAND STO	SMU TRANSACTION-COMMAND SECURITY
)(TCOMMAND DBR CTRANS OPRNTRAN	SMU TRANSACTION-COMMAND SECURITY
)(DATABASE ACCTSREC PASSWORD UOME	SMU PASSWORD SECURITY
)(PROGRAM BILLING PASSWORD MAIL2YOU	SMU PASSWORD SECURITY
)(PTERM 123 PASSWORD XM2Y3C	SMU PASSWORD SECURITY
)(TERMINAL LTERM5 PASSWORD TPC1MB COMMAND LOC TRANSACT TRAN123	SMU PASSWORD AND SMU LTERM BASED TERMINAL SECURITY
)(TRANSACT MSCTRAN TERMINAL **MSNAME1**	SMU LTERM BASED TERMINAL SECURITY

SMU Input Statements (3)

```
)( TERMINAL DFSTCFI
   COMMAND DIS
   COMMAND STA
   TRANSACT TRANA
   TRANSACT TRANB
```

SMU LTERM BASED TERMINAL SECURITY
[TIME CONTROLLED OPERATIONS (TCO) LTERM]

```
)( TERMINAL DFSTCF
   COMMAND DIS
   COMMAND STA
   TRANSACT TRANA
   TRANSACT TRANB
```

SMU LTERM BASED TERMINAL SECURITY
[TIME CONTROLLED OPERATIONS (TCO) LTERM]

```
)( COMMAND STO
   TERMINAL DFSTCFI
```

SMU LTERM BASED TERMINAL SECURITY
[TIME CONTROLLED OPERATIONS (TCO) LTERM]

```
)( COMMAND STO
   TERMINAL DFSTCF
```

SMU LTERM BASED TERMINAL SECURITY
[TIME CONTROLLED OPERATIONS (TCO) LTERM]

Summary

Objectives

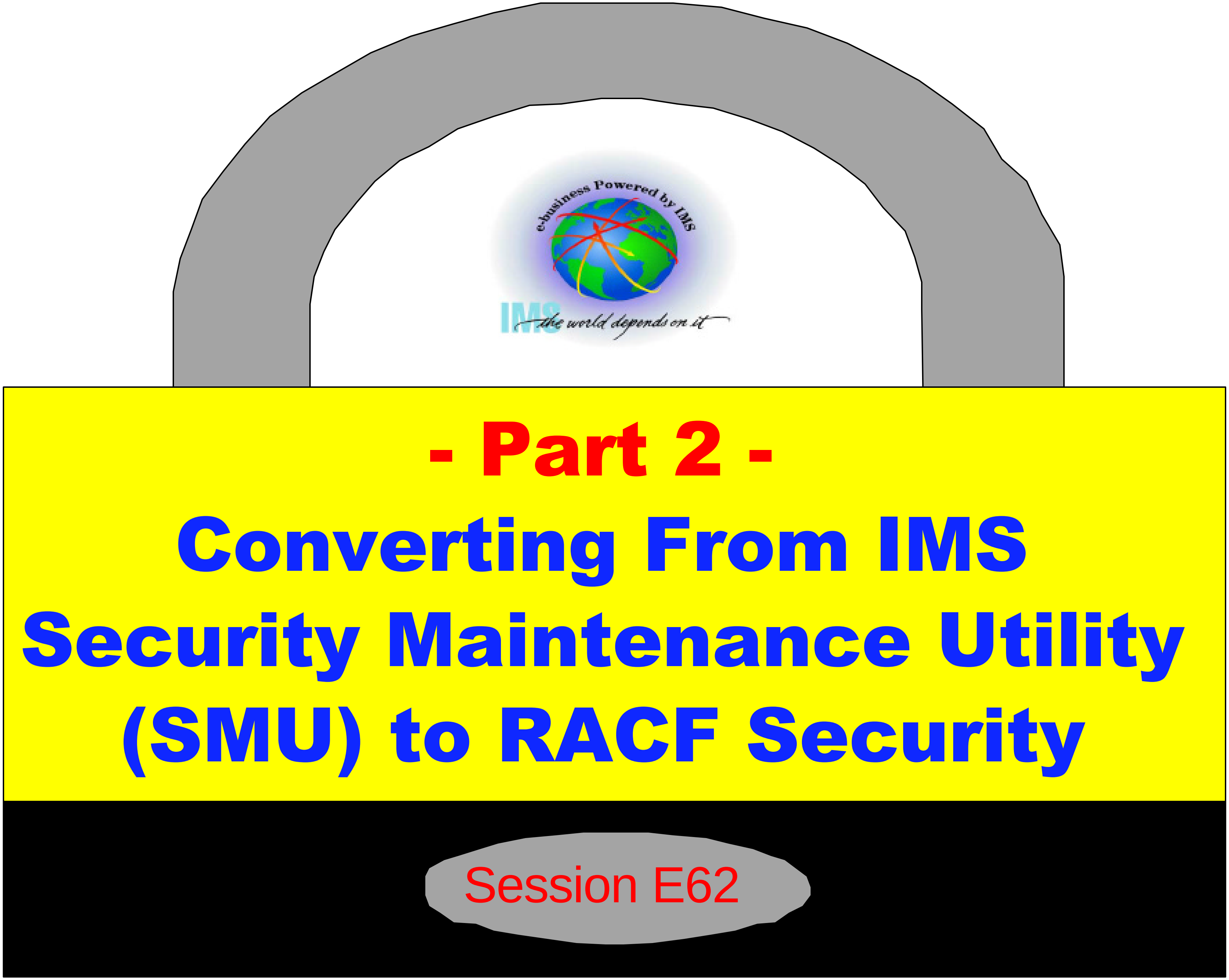
- ✓ Determine if your IMS systems use SMU security
- ✓ Identify IMS resources which are protected by SMU
- ✓ Identify the type(s) of SMU security used to protect IMS resources
- – Determine if the SMU security for a resource can be converted to RACF-provided security NEXT
- – Define the requirements for RACF-provided IMS resource security

✓ **Security facilities**

✓ **SMU security overview**

Converting SMU security to RACF security

- – IMS commands, IMS transactions, IMS databases/data sets, and terminals NEXT
- – Considerations for TYPE1 AO programs and AGNs



- Part 2 -

Converting From IMS Security Maintenance Utility (SMU) to RACF Security

Session E62

Objectives

To convert SMU security to RACF security, you need to

PART 1

- ✓ Know where to look to determine if you use SMU
- ✓ Understand which IMS resource types (e.g. transactions, commands, terminals, etc.) are protected by SMU
- ✓ Understand the type(s) of protection (e.g. password, LTERM based entry restriction, sign on, etc.) SMU uses to secure each IMS resource type

At the end of these two sessions you should be able to

PART 1

- ✓ Determine if your IMS systems use SMU security
- ✓ Identify IMS resources which are protected by SMU
- ✓ Identify the type(s) of SMU security used to protect IMS resources

PART 2

- – Determine if the SMU security for a resource can be converted to RACF security
- – Define the requirements for RACF IMS resource security

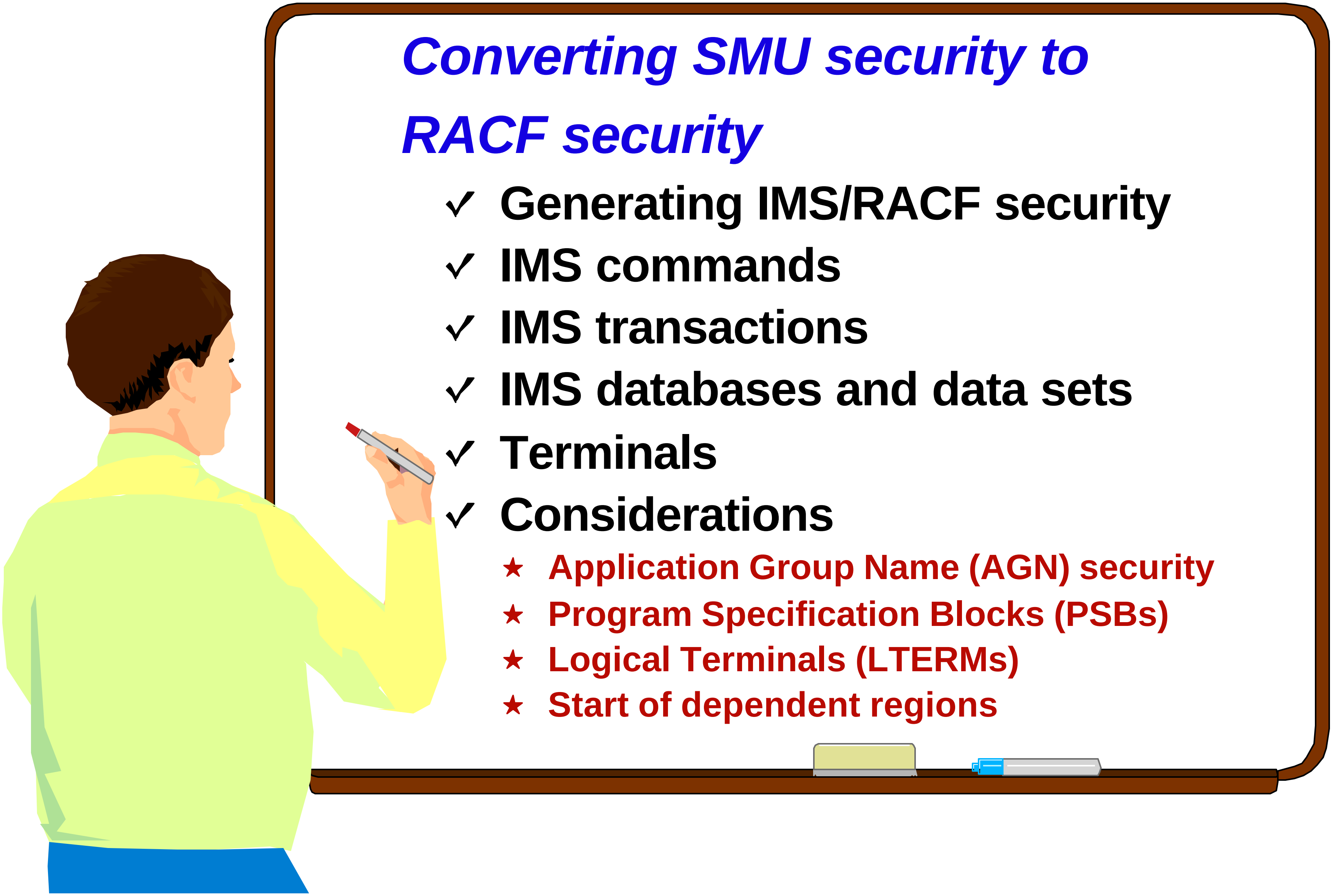
Agenda

Part 1

- IMS security facilities
- SMU security overview

Part 2

- Converting SMU security to RACF security
  - IMS commands
  - IMS transactions
  - IMS databases and data sets
  - Terminals
- Considerations
  - TYPE1 automated operator (AO) programs
  - Application Group Name (AGN) security
    - Start of dependent regions
    - Program Specification Blocks (PSBs)
    - Logical Terminals (LTERMs)
    - Transaction Codes



Converting SMU security to RACF security

- ✓ Generating IMS/RACF security
- ✓ IMS commands
- ✓ IMS transactions
- ✓ IMS databases and data sets
- ✓ Terminals
- ✓ Considerations
  - ★ Application Group Name (AGN) security
  - ★ Program Specification Blocks (PSBs)
  - ★ Logical Terminals (LTERMs)
  - ★ Start of dependent regions

IMS/RACF Overview

RACF security differs from SMU

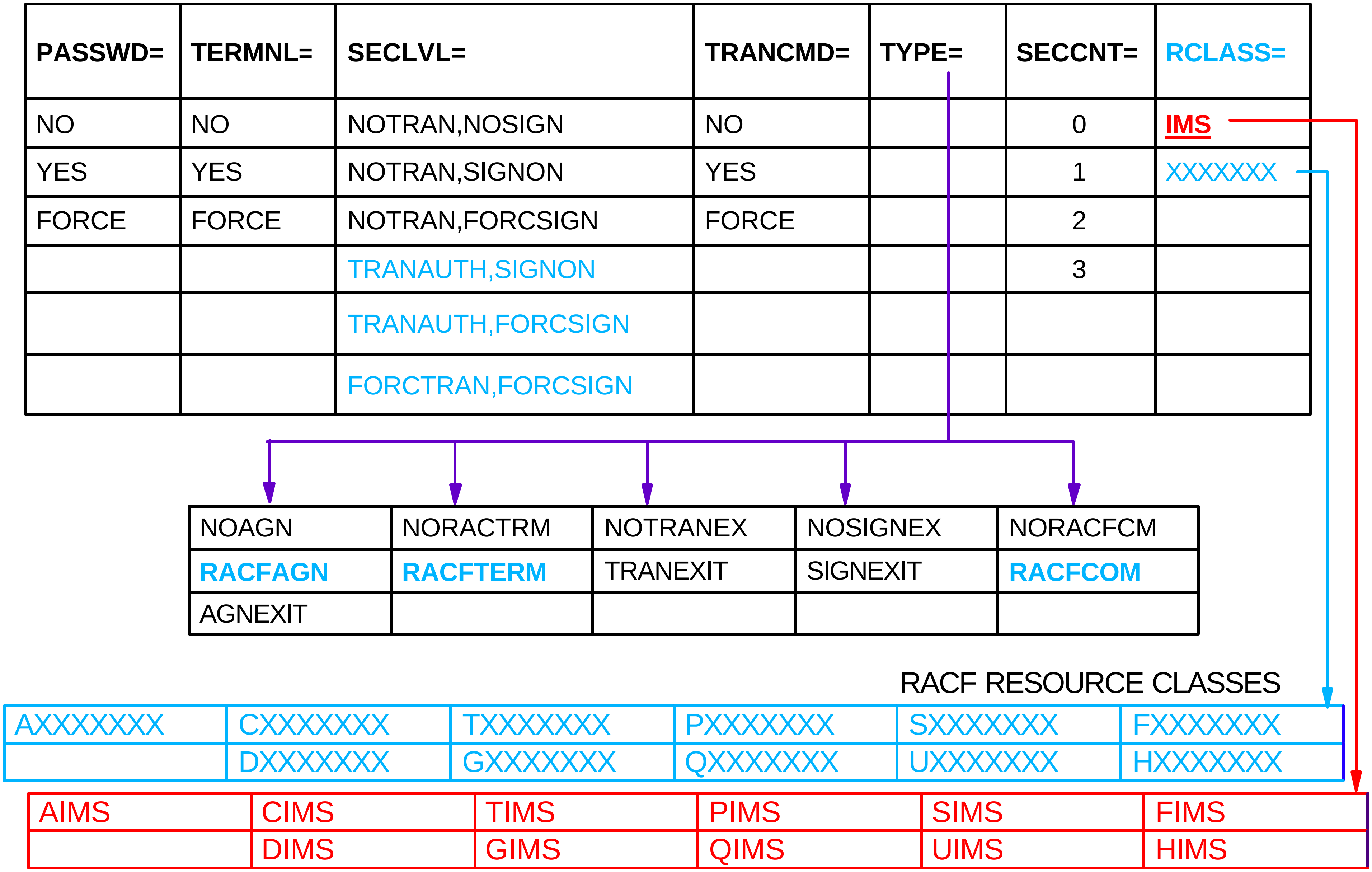
- SMU security is terminal based whereas RACF authorization checking is userid based
  - RACF uses a
    - Unique userid to identify each person
    - Password to authenticate the identity of each person

IMS users

- Are required to sign on when RACF performs user verification and resource authorization checking on behalf of that userid
  - Userid is provided via sign on
    - Userid provided at sign on is used in all subsequent RACF resource authorization checks
- Are people and things, for example
  - Time Controlled Operations (TCO) scripts should be coded to issue: /SIGN ON *userid password*

Generating IMS/RACF Security

SECURITY MACRO



PASSWD=	TERMNL=	SECLVL=	TRANCMD=	TYPE=	SECCNT=	RCLASS=
NO	NO	NOTRAN,NOSIGN	NO		0	IMS
YES	YES	NOTRAN,SIGNON	YES		1	XXXXXXX
FORCE	FORCE	NOTRAN,FORCSIGN	FORCE		2	
		TRANAUTH,SIGNON			3	
		TRANAUTH,FORCSIGN				
		FORCTRAN,FORCSIGN				

NOAGN	NORACTRM	NOTRANEX	NOSIGNEX	NORACFCM
RACFAGN	RACFTERM	TRANEXIT	SIGNEXIT	RACFCOM
AGNEXIT				

RACF RESOURCE CLASSES

AXXXXXXX	CXXXXXXX	TXXXXXXX	PXXXXXXX	SXXXXXXX	FXXXXXXX
	DXXXXXXX	GXXXXXXX	QXXXXXXX	UXXXXXXX	HXXXXXXX

AIMS	CIMS	TIMS	PIMS	SIMS	FIMS
	DIMS	GIMS	QIMS	UIMS	HIMS

IMS RACF Startup Parameters

AOIS=	Issue command (ICMD) security option
CMDMCS=	MCS/E-MCS command option
APPCSE=	APPC security option
OTMASE=	OTMA security option
TRN=	Transaction authorization option
SGN=	Sign on authorization option
ISIS=	Resource Access (AGN) security
RCF=	**RACF security option(s)**
RVFY=	RACF reverify option
RCFTCB=	Number of RACF TCBs

Do not designate the security facility

IMS/RACF Security Options

ISIS=

0 - No resource access security
1 - RACF Resource access (AGN) security
2 - User exit (DFSISIS0) resource access security userid validation

RCF=

N - Do not call RACF for sign on, transaction, or command security checking

C - Call RACF only for command authorization for commands entered from ETO devices

S - Call RACF for command authorization for commands entered from both static and ETO devices

T- Call RACF for sign on and transaction authorization

Y - Call RACF for sign on and transaction authorization as well as for commands authorization for commands entered from ETO devices

A - Call RACF for sign on and transaction authorization as well as for command authorization for commands entered from both static and ETO devices

B - Includes option A, but negates the loading of the sign on verification security table (DFSISSOx) from IMS.MATRIX

R - Includes option S, but negates the loading of the sign on verification security table (DFSISSOx) from IMS.MATRIX

IMS/*RACF* NRE and ERE Restart Options

/NRE -OR- /ERE COLD START KEYWORDS	**DESCRIPTION**
CMDAUTH	RACF command authorization (Static and ETO terminals)
NOCMDAUTH	Deactivate command authorization (Static and ETO terminals)
CMDAUTHE	RACF command authorization (ETO terminals)
NOCMDAUTHE	Deactivate command authorization (Static and ETO terminals)
TRANAUTH	Activate transaction authorization
NOTRANAUTH	Deactivate transaction authorization
USER	Activate userid verification
NOUSER	Deactivate userid validation and verification, transaction authorization and command authorization

- SIGN ON Security must be active for RACF authorization checking
- RACF authorization is USERID based
- The userid is provided at sign on (e.g. /SIGN ON STEVE PASSWD9)

Converting Command Security to RACF

SMU and IMS tasks

- List Matrix data set contents
- Browse SMU input statements
  - Identify commands protected by password security
  - Identify commands protected by LTERM based terminal security
  - Identify commands entered by Time Controlled Operations (TCO)
- Change SMU security definitions
  - SECURITY macro
    - PASSWD=NO
    - TERMNL=NO
    - TYPE=(RACFCOM)
  - Perform SMU generation ???
- *COLD* startup/restart options
  - **RCF=C | S | Y | A | B | R**
  - /NRE and /ERE
    - CMDAUTH or CMDAUTHE
    - NOPASSWORD and NOTERMINAL

RACF tasks

- Create RACF profiles (security definitions)
  - Group (ADDGROUP)
  - User/Userid (ADDUSER)
    - People, TCO, AO programs, etc.
  - Connect Userids to Groups (CONNECT)
  - IMS commands (RDEFINE)
    - CIMS | DIMS
    - CXXXXXXX | DXXXXXXX

      Add installation defined resource classes to Class Descriptor Table (CDT) and RACF Router Table
- Authorize userids/groups to RACF command profiles (PERMIT)
- Activate command resource classes (SETROPTS CLASSACT)

Command Considerations

RACF ***OR*** SMU is invoked for command authorization, not both

Command Authorization Exit (DFSCCMD0)

- Invoked after RACF

IMS command

- Profiles in RACF classes
  - Must be exactly 3 characters, for example
    - DIS, STA, STO, DBR, etc.
  - Grouping class (e.g. DIMS, DXXXXXXX, etc.) profile names may be up to 8 characters
    - Commands protected (ADDMEM) by a grouping profile must be exactly 3 characters
  - Command should be protected in only one resource class
    - Do ***NOT*** protect the same command in CIMS and DIMS
- Passwords
  - RACF 'REVERIFY' option may be used in lieu of SMU password
    - RACF user password must be supplied with command input
  - Requirements for 'REVERIFY' support
    - User must sign on to IMS
    - IMS startup parameters specify ***RVFY=Y***
    - APPLDATA section of command profile contains ***'REVERIFY'***

Sample RACF Commands - IMS Commands

```
=> ADDGROUP IMSGRP1 SUPGROUP(IMSUSERS) OWNER(RACFADMN)
=> ADDUSER IMSUSERA NAME(BILL STILLWELL) PASSWORD(IMSPW99)
   OWNER(RACFADMN) DFLTGRP(IMSGRP1)
=> CONNECT IMSUSERA GROUP(IMSGRP1) AUTHORITY(USE) UACC(NONE)

=> RDEFINE CIMS DIS UACC(NONE)
=> PERMIT DIS CLASS(CIMS) ID(IMSGRP1) ACCESS(READ)
```

3 CHARACTER COMMAND PROFILES

```
=> RDEFINE DIMS DBACMDS ADDMEM(STA STO DBR) UACC(NONE)
=> PERMIT DBACMDS CLASS(DIMS) ID(IMSGRP1) ACCESS(READ)
```

UP TO 8 CHARACTER GROUPING PROFILE

REVERIFY RACF PASSWORD

```
=> RDEFINE CXXXXXXX DIS APPLDATA('REVERIFY') UACC(NONE)
=> PERMIT DIS CLASS(CXXXXXXX) ID(IMSGRP1) ACCESS(READ)

=> RDEFINE DXXXXXXX DBACMDS ADDMEM(STA STO DBR) UACC(NONE)
=> PERMIT DBACMDS CLASS(DXXXXXXX) ID(IMSGRP1 TCOUSID) ACCESS(READ)

=> SETROPTS CLASSACT(CIMS DIMS CXXXXXXX DXXXXXXX)
=> SETROPTS RACLIST(CIMS DIMS CXXXXXXX DXXXXXXX) REFRESH
```

Converting TYPE 1 Automated Operator (AO) Programs to RACF

SMU and IMS tasks

- List Matrix data set contents
- Browse SMU input statements
  - Identify AO command transaction programs/PSBs secured with SMU
    -)(CTRANS *aotran* TCOMMAND DIS
    -)(TCOMMAND DIS CTRANS *aotran*
- Change SMU security definitions
  - SECURITY macro
    - TRANCMD=NO
  - Perform SMU generation
- ***COLD*** startup/restart options
  - /NRE and /ERE
    - NOTRANCMDS

Application tasks

- If you require the protection today
  - Modify applications to issue the DL/I ICMD call (ISSUE COMMAND) in lieu of the CMD (COMMAND) call

Consideration

- May want to wait to see what happens before making application changes!!

RACF tasks

- Same as for commands if AO programs are ***TYPE2 (ICMD call)***
- ***NONE*** if applications are not modified and continue use of CMD call
  - RACF does ***NOT*** currently support CMD call security

Converting Transaction Security to RACF

SMU and IMS tasks

- List Matrix data set contents
- Browse SMU input statements
  - Identify transactions protected by password security
  - Identify transactions protected by LTERM based terminal security
  - Identify transactions entered by Time Controlled Operations (TCO)
- Change SMU security definitions
  - SECURITY macro
    - PASSWD=NO
    - TERMNL=NO
    - TYPE=(RACFTERM)
  - Perform SMU generation
- ***COLD*** startup/restart options
  - **TRN=Y or TRN=F**
  - **RCF=T | Y | A | B | R**
  - /NRE and /ERE
    - TRANAUTH
    - NO PASSWORD and NOTERMINAL

RACF tasks

- Create RACF profiles
  - Group (ADDGROUP)
  - User/Userid (ADDUSER)
    - People, TCO, etc.
  - Connect Userids to Groups (CONNECT)
  - IMS transactions (RDEFINE)
    - TIMS | GIMS
    - TXXXXXXX | GXXXXXXX
      - Add installation defined resource
      - classes to Class Descriptor Table
      - (CDT) and RACF Router Table
- Authorize userids/groups to RACF transaction profiles (PERMIT)
- Activate transaction resource classes (SETROPTS CLASSACT)

Transaction Considerations

SMU password and/or LTERM based terminal security

- Invoked after RACF and/or user exit routines for transactions entered from static terminals
- Should be removed prior to cut over to RACF transaction security

Exit routines

- May need to be coded for non-signed on users and/or back-end (MSC and/or shared queues) systems
  - Transaction authorization (DFSCTRN0 and/or DFSCTSE0)
  - Build Security Environment Exit (DFSBSEX0)

RACF

- Databases on different z/OS system should be synchronized
- Transaction profiles should only be created in 1 resource class
  - Do ***NOT*** create transaction profile in TIMS and GIMS
- 'REVERIFY' may be used in lieu of SMU password security
- Use with installation exit routines
  - May need Build Security Exit Routine (DFSBSEX0)
  - Transaction Authorization Exit (DFSCTRN0) is not invoked if RACF denies authorization to transaction
  - Security Reverification Exit (DFSCTSE0) is invoked unconditionally for transactions requested via
    - CHNG calls and AUTH calls
    - Deferred conversational program to program message switches

Sample RACF Commands - IMS Transactions

```
=> ADDGROUP IMSGRP1 SUPGROUP(IMSUSERS) OWNER(RACFADMN)
=> ADDUSER IMSUSERB NAME(STEVE NATHAN) PASSWORD(IMSPW91)
   OWNER(RACFADMN) DFLTGRP(IMSGRP1)
=> CONNECT IMSUSERB GROUP(IMSGRP1) AUTHORITY(USE) UACC(NONE)

=> RDEFINE TIMS PAYTRAN1 UACC(NONE)
=> PERMIT PAYTRAN1 CLASS(TIMS) ID(IMSGRP1) ACCESS(READ)

=> RDEFINE GIMS PAYTRANS ADDMEM(RAISE AWARD BONUS) UACC(NONE)
=> PERMIT PAYTRANS CLASS(GIMS) ID(IMSGRP1) ACCESS(READ)

=> RDEFINE TXXXXXXX PAYTRAN1 APPLDATA('REVERIFY') UACC(NONE)
=> PERMIT PAYTRAN1 CLASS(TXXXXXXX) ID(IMSGRP1) ACCESS(READ)

=> RDEFINE GXXXXXXX PAYTRANS ADDMEM(RAISE AWARD BONUS)
    UACC(NONE)
=> PERMIT PAYTRANS CLASS(GXXXXXXX) ID(IMSGRP1) ACCESS(READ)

=> SETROPTS CLASSACT(TIMS GIMS TXXXXXXX GXXXXXXX)
=> SETROPTS RACLIST(TIMS GIMS TXXXXXXX GXXXXXXX) REFRESH
```

Converting Database Security to RACF

SMU and IMS tasks

- List Matrix data set contents
- Browse SMU input statements
  - Identify databases protected by password security
- Change SMU security definitions
  - SECURITY macro
    - PASSWD=NO
  - Perform SMU generation
- ***COLD*** startup/restart options
  - **RCF≠N (Any RCF= value except N)**
  - /NRE or /ERE NOPASSWORD

Application tasks

- Modify application to issue DL/I AUTH (authorization) call if needed
- RACF acts as data store for database profiles

RACF tasks

- Create RACF profiles
  - Group (ADDGROUP)
  - User/Userid (ADDUSER)
  - Connect Userids to Groups (CONNECT)
  - IMS databases (RDEFINE)
    - PIMS | QIMS | SIMS | UIMS
      FIMS | HIMS | OIMS | WIMS
    - PXXXXXXX | QXXXXXXX
      SXXXXXXX | UXXXXXXX
      FXXXXXXX | HXXXXXXX
      OXXXXXXX | WXXXXXXX
      - Add installation defined resource
      - classes to Class Descriptor Table
      - (CDT) and RACF Router Table
- Authorize userids/groups to RACF database, segment, field, and/or other profiles (PERMIT)
- Activate transaction resource classes (SETROPTS CLASSACT)

Sample RACF Commands - IMS Databases

```
=> ADDGROUP PERSNL SUPGROUP(SYS1) OWNER(RACFADMN)
=> ADDUSER USERD NAME(RICH LEWIS) PASSWORD(IMSPW75)
   OWNER(RACFADMN) DFLTGRP(PERSNL)
=> CONNECT USERD GROUP(PERSNL) AUTHORITY(USE) UACC(NONE)
=> RDEFINE PIMS EMPLDB UACC(NONE)
=> PERMIT EMPLDB CLASS(PIMS) ID(PERSNL) ACCESS(READ)
=> RDEFINE QIMS COMPDBS ADDMEM(SKILLSDB DEPTDB) UACC(NONE)
=> PERMIT COMPDBS CLASS(QIMS) ID(PERSNL) ACCESS(READ)
=> RDEFINE SIMS NAMESEG UACC(NONE)
=> PERMIT NAMESEG CLASS(SIMS) ID(PERSNL) ACCESS(READ)
=> RDEFINE UIMS EMPLSEGS ADDMEM(EMPNOSEG SALARY) UACC(NONE)
=> PERMIT EMPLSEGS CLASS(UIMS) ID(PERSNL) ACCESS(READ)
=> RDEFINE FIMS PAYFIELD UACC(NONE)
=> PERMIT PAYFIELD CLASS(FIMS) ID(PERSNL) ACCESS(READ)
=> RDEFINE HIMS EMDBFLDS ADDMEM(NAME ADDR) UACC(NONE)
=> PERMIT EMDBFLDS CLASS(HIMS) ID(PERSNL) ACCESS(READ)
=> RDEFINE OIMS DB2VIEW1 UACC(NONE)
=> PERMIT DB2VIEW1 CLASS(OIMS) ID(PERSNL) ACCESS(READ)
=> RDEFINE WIMS DB2VIEWS ADDMEM(DB2VIEW2 DB2VIEW3) UACC(NONE)
=> PERMIT DB2VIEWS CLASS(WIMS) ID(PERSNL) ACCESS(READ)
```

Sample RACF Commands - IMS Databases

```
=> SETROPTS CLASSACT(PIMS QIMS PXXXXXXX QXXXXXXX)
=> SETROPTS CLASSACT(SIMS UIMS SXXXXXXX UXXXXXXX)
=> SETROPTS CLASSACT(FIMS HIMS FXXXXXXX HXXXXXXX)
=> SETROPTS CLASSACT(OIMS WIMS OXXXXXXX WXXXXXXX)
=> SETROPTS RACLIST(PIMS QIMS PXXXXXXX QXXXXXXX) REFRESH
=> SETROPTS RACLIST(SIMS UIMS SXXXXXXX UXXXXXXX) REFRESH
=> SETROPTS RACLIST(FIMS HIMS FXXXXXXX HXXXXXXX) REFRESH
=> SETROPTS RACLIST(OIMS WIMS OXXXXXXX WXXXXXXX) REFRESH
```

Converting Data Set Security to RACF

IMS tasks

- ***COLD*** startup/restart options
  - **RCF≠ N**
    - Any RCF= value except N)

Considerations

- IMS data set and/or database data set may be secured by RACF
- However, authorization checking is performed against the ***DL/I address space userid***
  - May be used to prevent test applications from updating production data

RACF tasks

- Create RACF profiles
  - Group (ADDGROUP)
  - User/Userid (ADDUSER)
  - Connect Userids to Groups (CONNECT)
  - IMS data sets ***(ADDSD)***
    - DATASET
- Authorize userids/groups to RACF data set profiles (PERMIT)
- Activate DATASET resource classes (SETROPTS CLASSACT)

Sample RACF Commands - IMS Data Sets

```
=> ADDGROUP PRODSYS SUPGROUP(SYS1) OWNER(RACFADMN)
=> ADDUSER DLIUSID NAME(DL/I PRODUCTION SYSTEM)
     PASSWORD(DLIPRDA) OWNER(RACFADMN) DFLTGRP(PRODSYS)
=> CONNECT DLIUSID GROUP(PRODSYS)

=> ADDSD 'PARTS.DBDS' UACC(NONE) GENERIC
=> PERMIT  'PARTS.DBDS' ID(PRODSYS DLIUSID) ACCESS(UPDATE)

=> ADDSD 'IMS.TCFSLIB' UACC(NONE) GENERIC
=> PERMIT  'IMS.TCFSLIB' ID(PRODSYS DLIUSID) ACCESS(UPDATE)
```

Converting Terminal Security to RACF

SMU and IMS tasks

- List Matrix data set contents

- Browse SMU input statements
  - Identify terminals protected by password security
  - Identify terminals protected by user sign on terminal security
    -)(SIGN
      STERM ALL
    -)(SIGN
      STERM nodename

- Change SMU security definitions
  - **SECURITY macro**
    - **PASSWD=NO**
    - **TERMNL=NO**
  - **Perform SMU generation**

- ***COLD*** startup/restart options

  - **SGN=Y or SGN=F**

  - **RCF≠N (Any RCF= value except N)**

RACF tasks

- Create RACF profiles
  - Group (ADDGROUP)
  - User/Userid (ADDUSER)
  - Connect Userids to Groups (CONNECT)
  - IMS terminals (RDEFINE)
    - TERMINAL
    - GTERMINL

- Authorize userids/groups to RACF terminal profiles (PERMIT)

- Activate terminal resource classes (SETROPTS CLASSACT)

Sample RACF Commands - IMS Terminals

=> **ADDGROUP** SYSPROG SUPGROUP(SYS1) OWNER(RACFADMN)
=> **ADDUSER** KENNIE NAME(KEN BLACKMAN)
PASSWORD(THEKING) OWNER(RACFADMN) DFLTGRP(SYSPROG)
=> **CONNECT** KENNIE GROUP(SYSPROG)

=>SETROPTS TERMINAL(READ)

=> **RDEFINE** TERMINAL NODE1234 UACC(NONE)
=> **PERMIT** NODE1234 CLASS(TERMINAL) ID(KENNIE) ACCESS(READ)

=> **RDEFINE** GTERMINL IMSNODES UACC(NONE)
=> **PERMIT** IMSNODES CLASS(GTERMINL) ADDMEM(NODEA NODEB NODEC)
ID(KENNIE) ACCESS(READ)

=>SETROPTS CLASSACT(TERMINAL)
=>SETROPTS GENERIC(TERMINAL)
=>SETROPTS RACLIST(TERMINAL)
=>SETROPTS GENERIC(TERMINAL) REFRESH
=>SETROPTS RACLIST(TERMINAL) REFRESH

Converting AGNs to RACF

Consideration

- May want to wait to see what happens before making AGN changes!!
- SMU security required even with RACF

SMU and IMS tasks

- List Matrix data set contents
- Browse SMU input statements
  - Identify AGNs secured using SMU
    -)(AGN agn_name
      AGPSB PSBA
      AGTRAN TRANA
      AGLTERM LTERMA
- Change SMU security definitions
  - SECURITY macro
    - TYPE=RACFAGN
  - Perform SMU generation
- ***COLD*** startup/restart options
  - ISIS=1

RACF tasks

- ***NONE*** if current AGN security continues to be used
- For RACF security checking at region/thread connect time
  - Create RACF profiles
    - Group (ADDGROUP)
    - User/Userid (ADDUSER)
    - Connect Userids to Groups (CONNECT)
    - IMS AGNs (RDEFINE)
      AIMS | AXXXXXXX
  - Authorize userids/groups to RACF AGN profiles (PERMIT)
  - Activate AGN resource classes (SETROPTS CLASSACT)

Sample RACF Commands - IMS AGNs

```
=> ADDGROUP PRODREGS SUPGROUP(SYS1) OWNER(RACFADMN)
=> ADDUSER DEPREG1 NAME(PRODUCTION REGION 1)
    PASSWORD(IMSREG1) OWNER(RACFADMN) DFLTGRP(PRODREGS)
=> CONNECT DEPREG1 GROUP(PRODREGS)

=> RDEFINE AIMS AGN1 UACC(NONE)
=> PERMIT  AGN1 CLASS(AIMS) ID(DEPREG1 PRODREGS) ACCESS(READ)

=> RDEFINE AXXXXXXX AGN2 UACC(NONE)
=> PERMIT  AGN2 CLASS(AXXXXXXX) ID(DEPREG1 PRODREGS) ACCESS(READ)

=>SETROPTS CLASSACT(AIMS AXXXXXXX)
=>SETROPTS RACLIST(AIMS AXXXXXXX)
=>SETROPTS RACLIST(AIMS AXXXXXXX) REFRESH
```

Summary

Objectives

- ✓ Determine if your IMS systems use SMU security
- ✓ Identify the IMS resources which are protected by SMU
- ✓ Identify the type(s) of SMU security used to protect IMS resources
- ✓ Determine if the SMU security for a resource can be converted to RACF-provided security
- ✓ Define the requirements for RACF-provided IMS resource security

- ✓ **Security facilities**

- ✓ **SMU security overview**

- ✓ **Converting SMU security to RACF security**
  - ✓ IMS commands, IMS transactions, IMS databases/data sets, and terminals
  - ✓ Considerations: TYPE 1 AO programs and AGNs
    - ✓ May want to wait before converting to RACF

RETURN TO INDEX