RSM PARTNERS

RACF For Dummies

Presented by a Dummy

World Class, Full Spectrum, z Services

RACF For Dummies

Presented By A Dummy

Leanne Wilson
RSM Partners

Agenda

- Introductions
- Overview
- User & Group Profiles
- Dataset & General Resource Profiles
- Access Granted! Access Denied!
- Summary

Introduction

- Wil
- n se
- r 4 y
- curit

What is RACF?

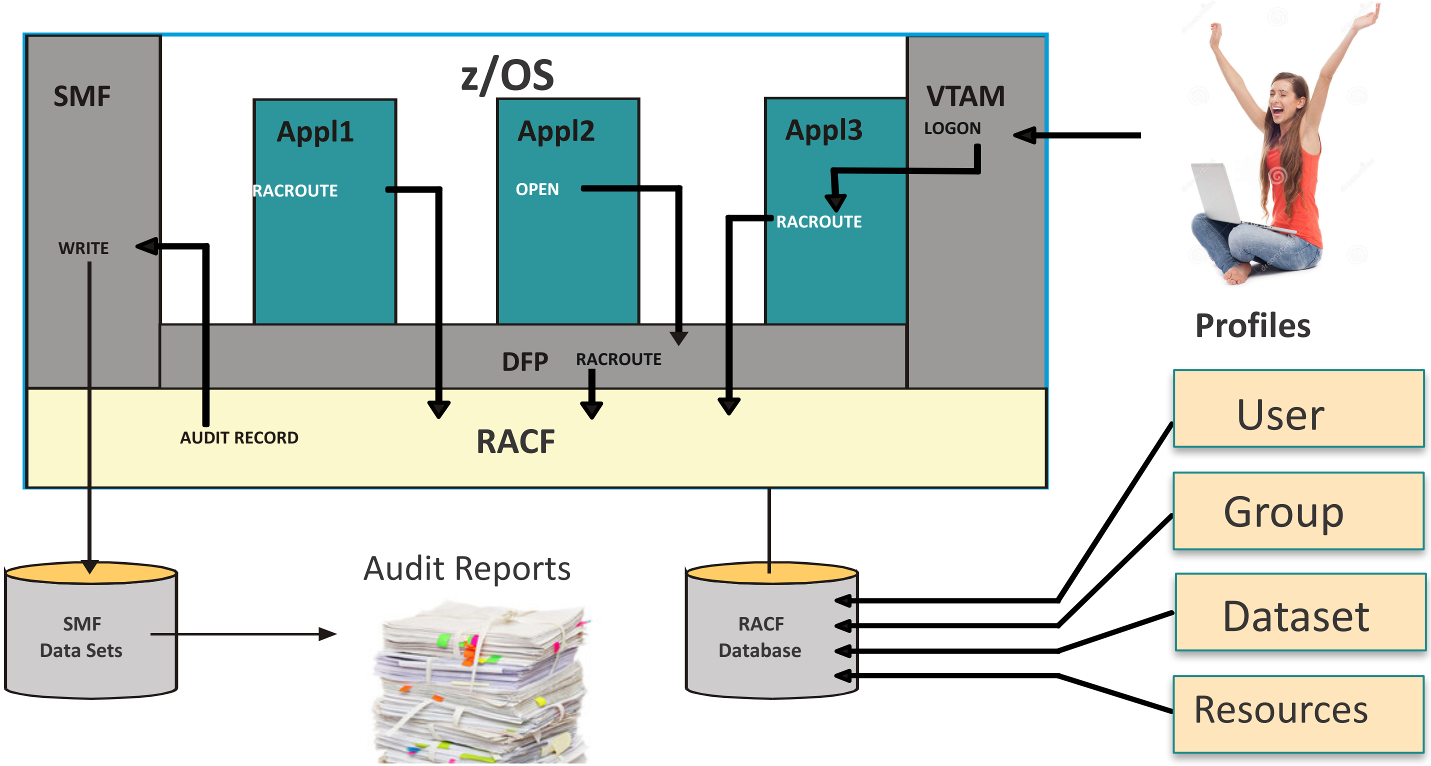
R ESOURCE

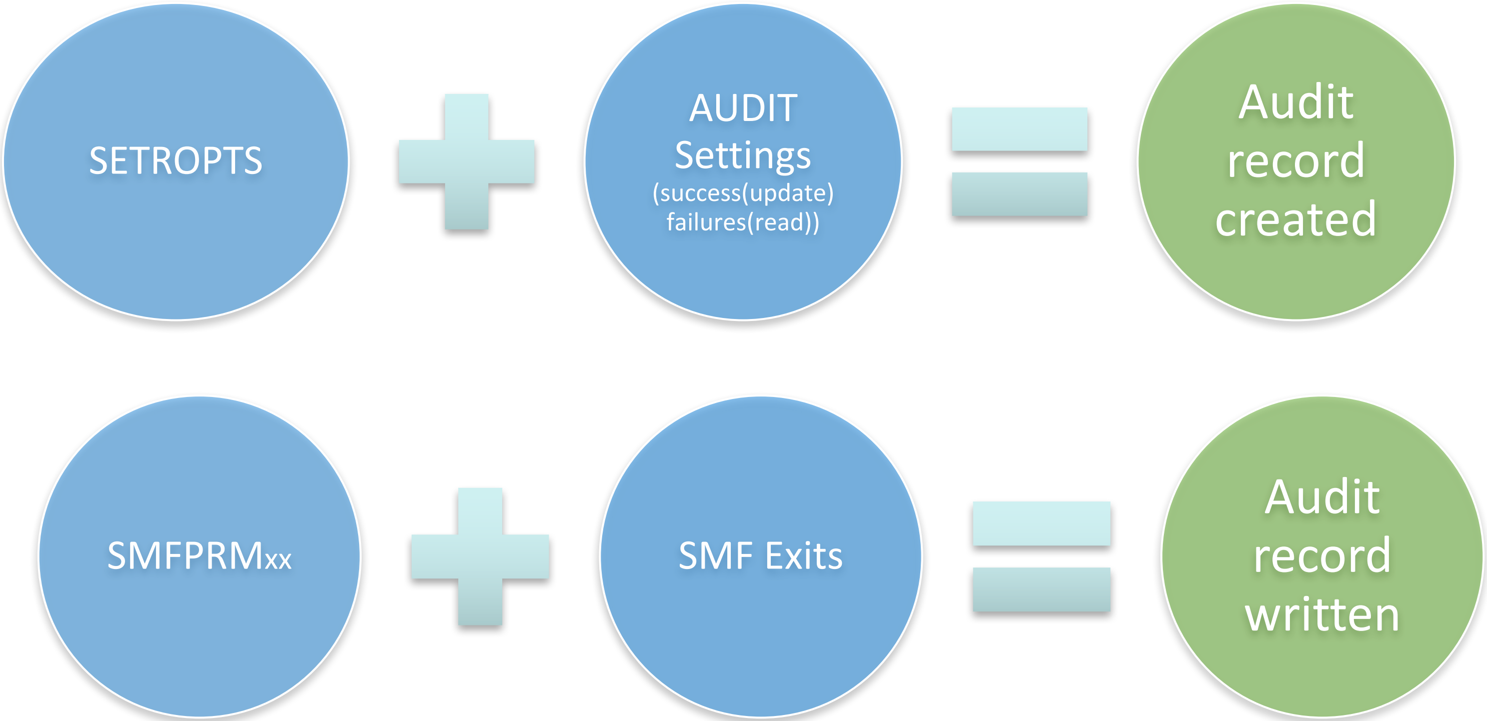
A ACCESS

C ONTROL

F ACILITY

How RACF works

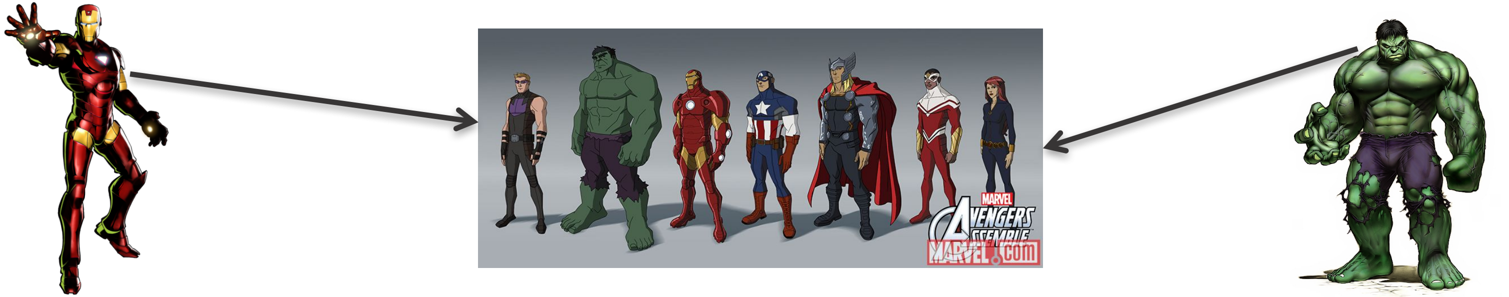




SETROPTS + AUDIT Settings (success(update) failures(read)) = Audit record created

SMFPRMxx + SMF Exits = Audit record written

How Can RACF Help?



User Profiles

Group Profiles

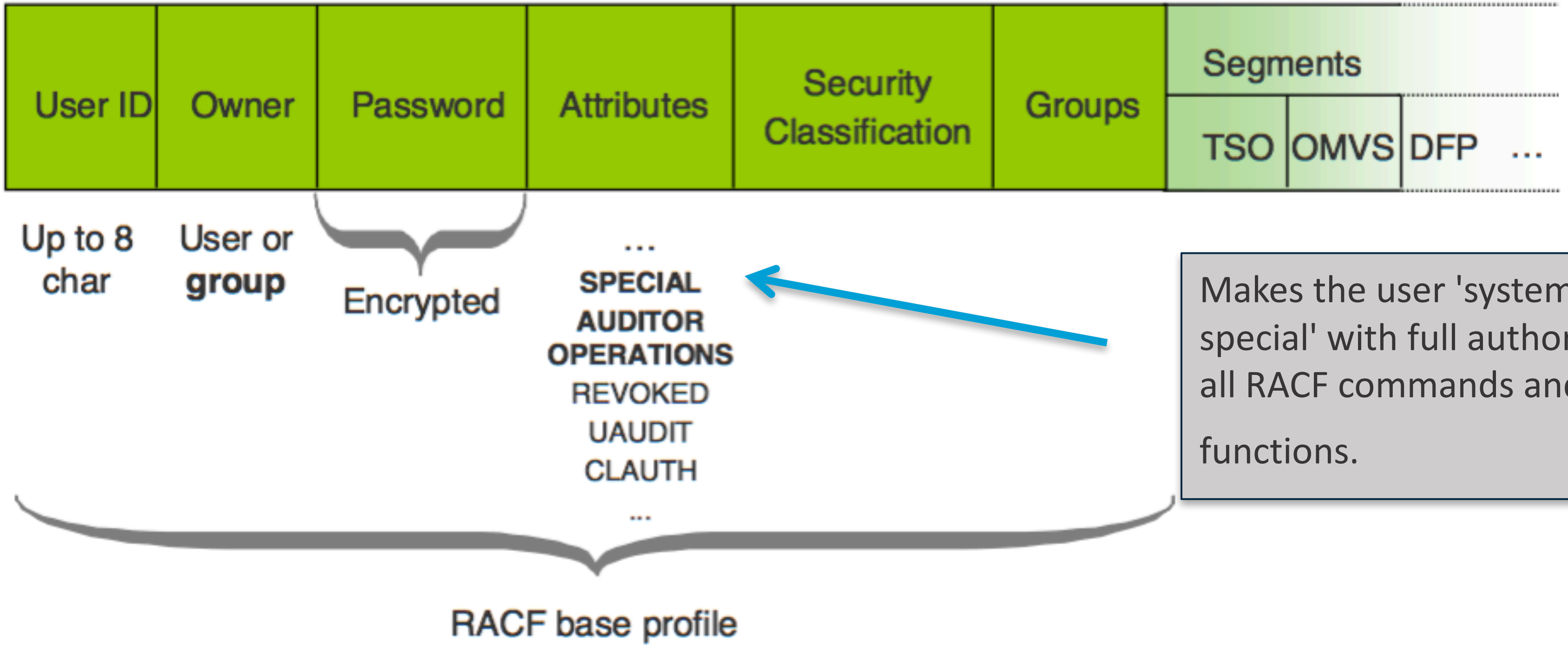
User Profiles

Dataset Profiles

Resource Profiles

User Profiles

User Profile



User ID | Owner | Password | Attributes | Security Classification | Groups | Segments

TSO | OMVS | DFP …

Up to 8 char

User or group

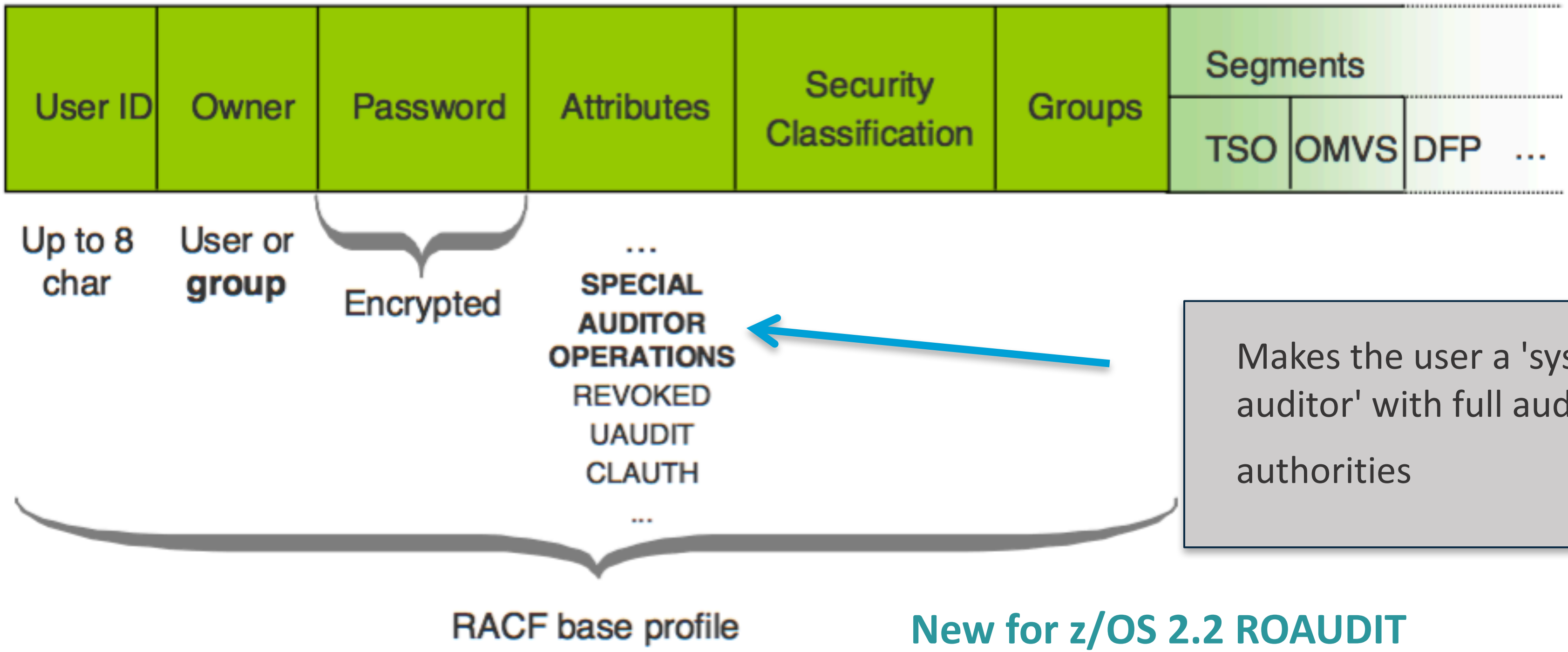
Encrypted

…
SPECIAL
AUDITOR
OPERATIONS
REVOKED
UAUDIT
CLAUTH
...

RACF base profile

Makes the user 'system special' with full authority to all RACF commands and functions.

User Profile



User ID | Owner | Password | Attributes | Security Classification | Groups | Segments: TSO | OMVS | DFP …

Up to 8 char

User or **group**

Encrypted

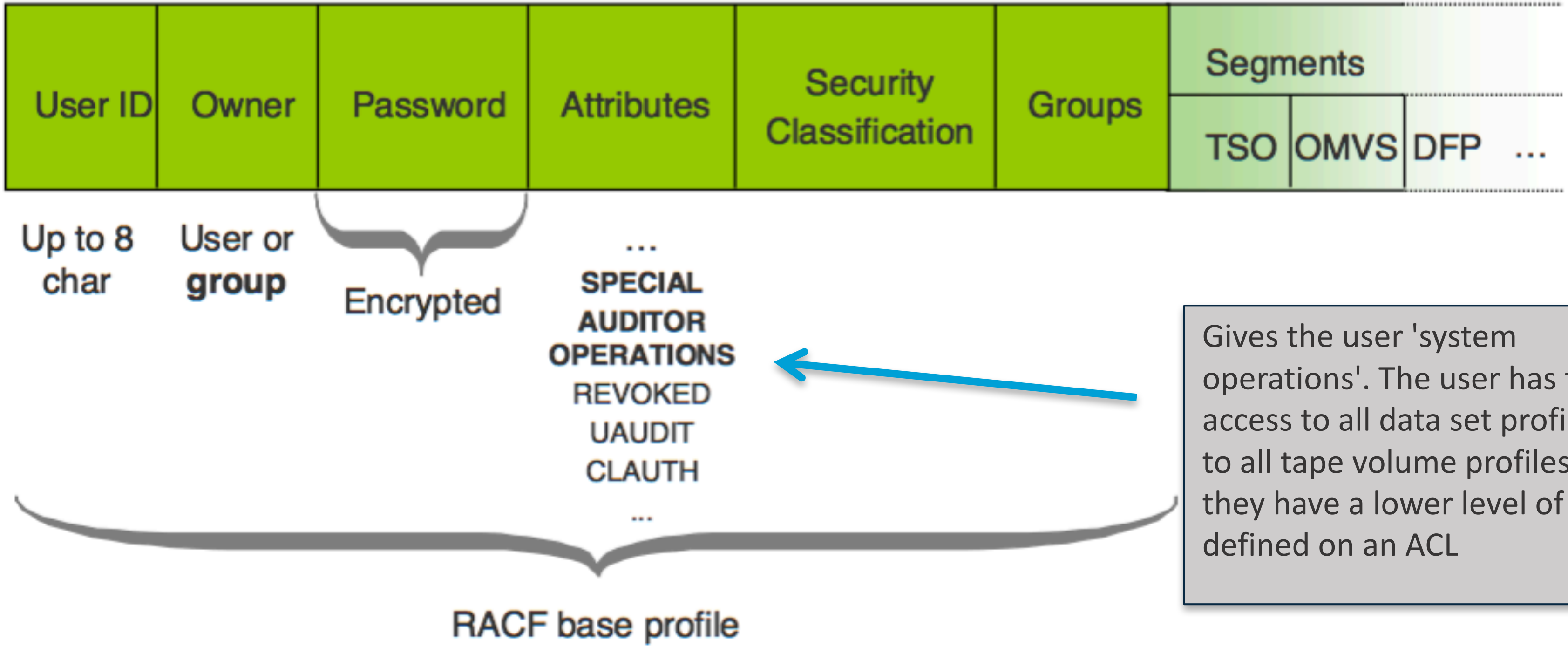
…
SPECIAL
AUDITOR
OPERATIONS
REVOKED
UAUDIT
CLAUTH
...

RACF base profile

Makes the user a 'system auditor' with full auditing authorities

New for z/OS 2.2 ROAUDIT

User Profile



User ID | Owner | Password | Attributes | Security Classification | Groups | Segments

TSO | OMVS | DFP ...

Up to 8 char

User or group

Encrypted

...

SPECIAL

AUDITOR

OPERATIONS

REVOKED

UAUDIT

CLAUTH

...

RACF base profile

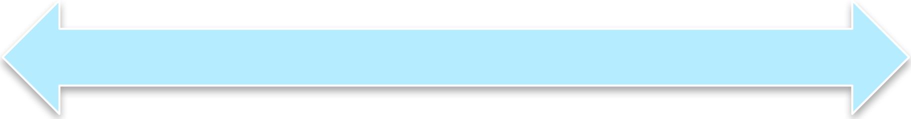
Gives the user 'system operations'. The user has full access to all data set profiles and to all tape volume profiles. Unless they have a lower level of access defined on an ACL

Group Profiles

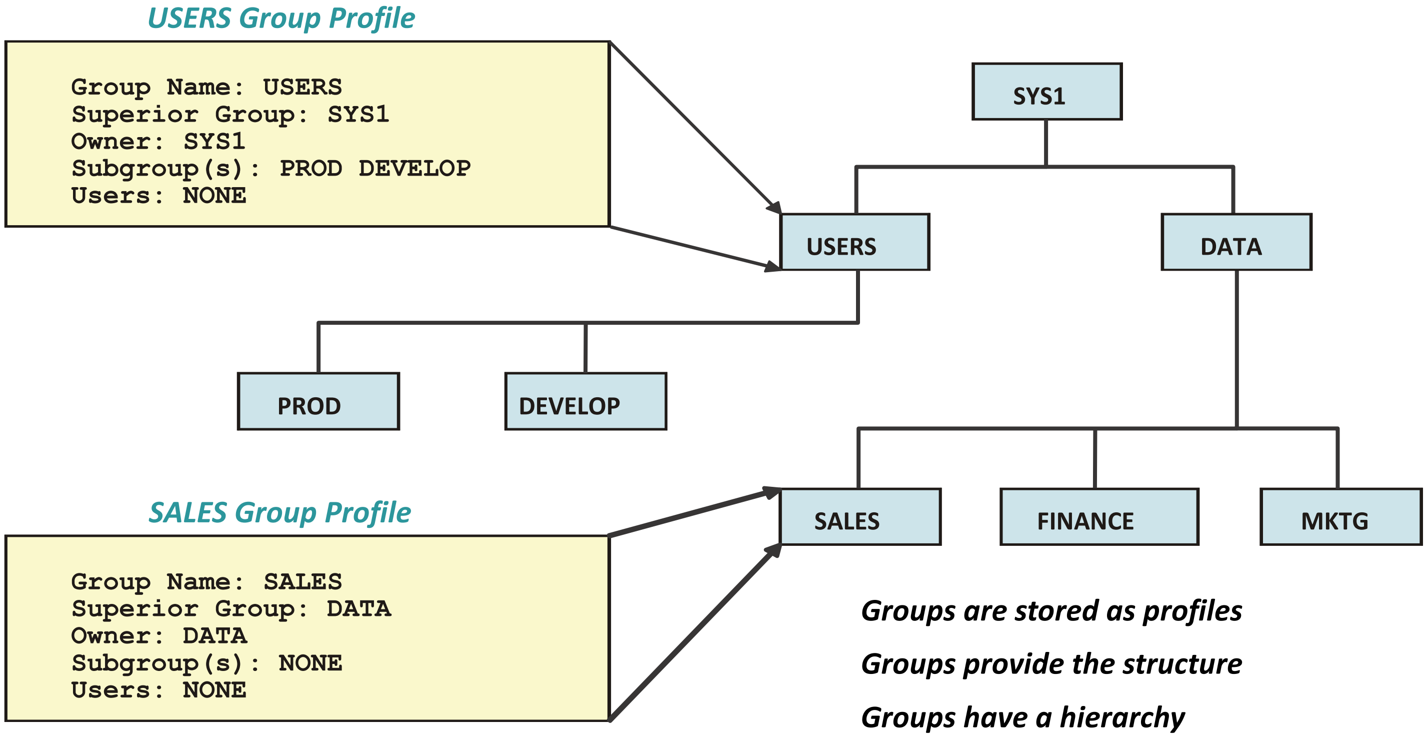
Group Profile

Group Name	Owner	Supgroup	Data	Segments
Unique, up to 8 chars	User or group			**OMVS** **CSDATA** **....**

RACF base profile



What are groups?



USERS Group Profile

```
Group Name:  USERS
Superior Group:  SYS1
Owner:  SYS1
Subgroup(s):  PROD DEVELOP
Users:  NONE
```

SALES Group Profile

```
Group Name:  SALES
Superior Group:  DATA
Owner:  DATA
Subgroup(s):  NONE
Users:  NONE
```

Groups are stored as profiles

Groups provide the structure

Groups have a hierarchy

Grouping resources and users

Group resources together:

Used by the same users

Have the same owner

Are logically connected

Connected to the RACF group structure

Group users together:

Using the same resources

Have the same manager

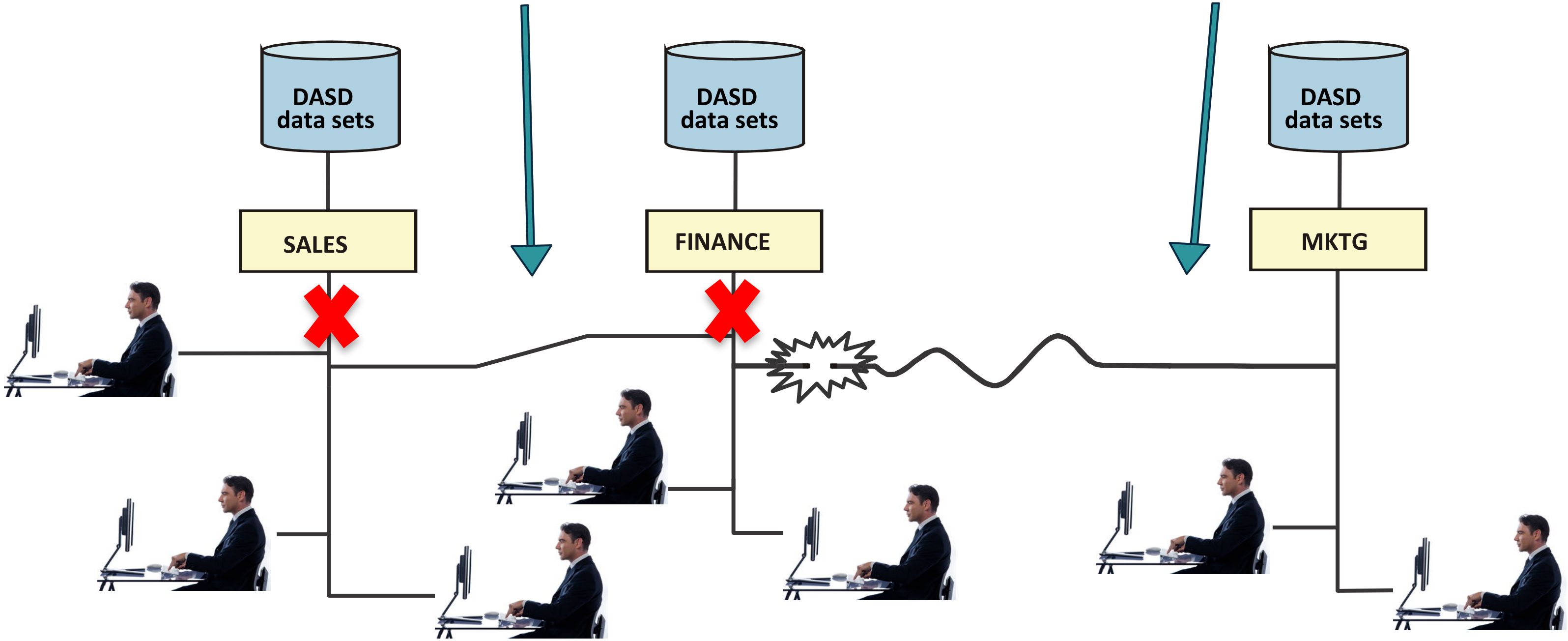
Belong to the same department

Do the same job

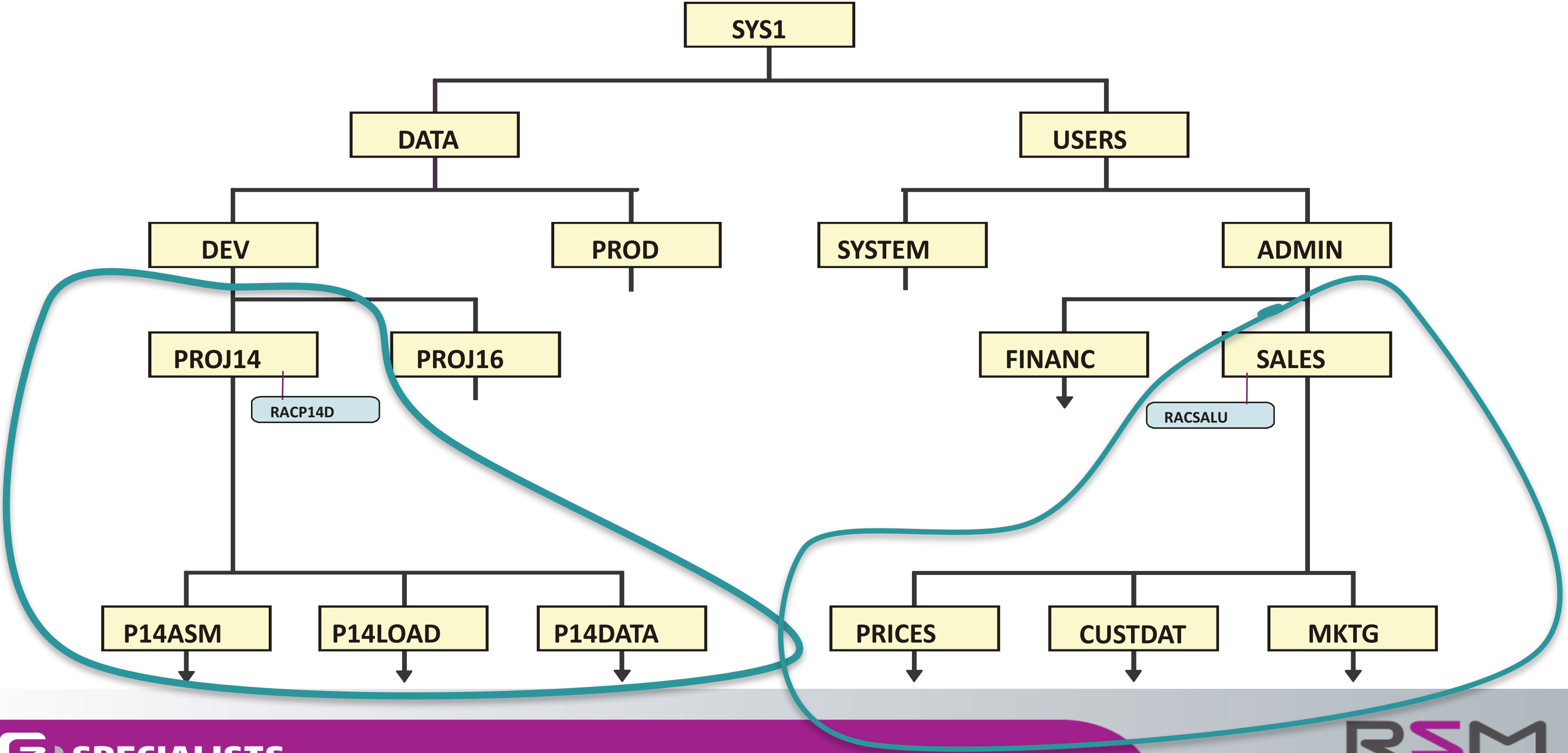
Users and groups

Users who are connected to multiple groups, get access to all resources to which the groups have access

A user who has been disconnected from a group immediately ceases to have access to group resources



Group Level Attributes



Dataset Profiles

Dataset Profile

Profile	Owner	UACC	Warning	Erase	Auditing	ACL	Segments
							……..
44 chars							

RACF base profile

Discrete Profiles	Generic Profiles
Protects one dataset	Protects multiple datasets Use of 3 wildcard characters % , * , ** Use of ** requires EGN activated in SETROPTS
Not possible to create a discrete profile unless a data set of the same name already exists	A generic profile can be created even if no data set matching the name exists
If a data set protected by a discrete profile is deleted then RACF will unconditionally delete the profile	When a data set protected by a generic profile is deleted the profile is not

How to Protect Resources

Generic Profiles

- TSGLW.J*.**
- TSGLW.J%.**

Discrete Profiles

- TSGLW.JCL.CNTL

All examples are listed as if EGN is activated

TSGLW.JCL.CNTL
TSGLW.JCL.CNTL.BACKUP
TSGLW.JA.WORK
TSGLW.JB.WORK.OLD

Generic wildcard characters:

%	**Matches with any single character**
*	**Matches with any number of characters in the qualifier**
**	**Matches with any number of characters and qualifiers**

<u>Can not be in HLQ!</u>

Generic Wildcard Characters

Profile Name: TSGLW.D%TAKEY.**

Dataset Names:

TSGLW.DATAKEY.NEW	YES
TSGLW.DETAKEY	YES
TSGLW.DATAKE	NO
TSGLW.DETAKEY.OLD	YES

Generic Wildcard Characters

Profile Name:	TSGLW.R%%%.C*	
Dataset Names:	TSGLW.RACF.CODE	YES
	TSGLW.RACF2.CODE	NO
	TSGLW.REXX.CODE.V2	NO
	TSGLW.REXX.CODE	YES
Profile Name:	TSG%%.JCL.**	NO

Auditing Attributes

Profile	Owner	UACC	Warning	Erase	Auditing	ACL	Segments
							....

```
ADDSD ‘TSGLW.JCL.C*’
UACC(NONE)
AUDIT(success(update) failures(read))
```

Auditing Attributes

- The types of auditing required are:

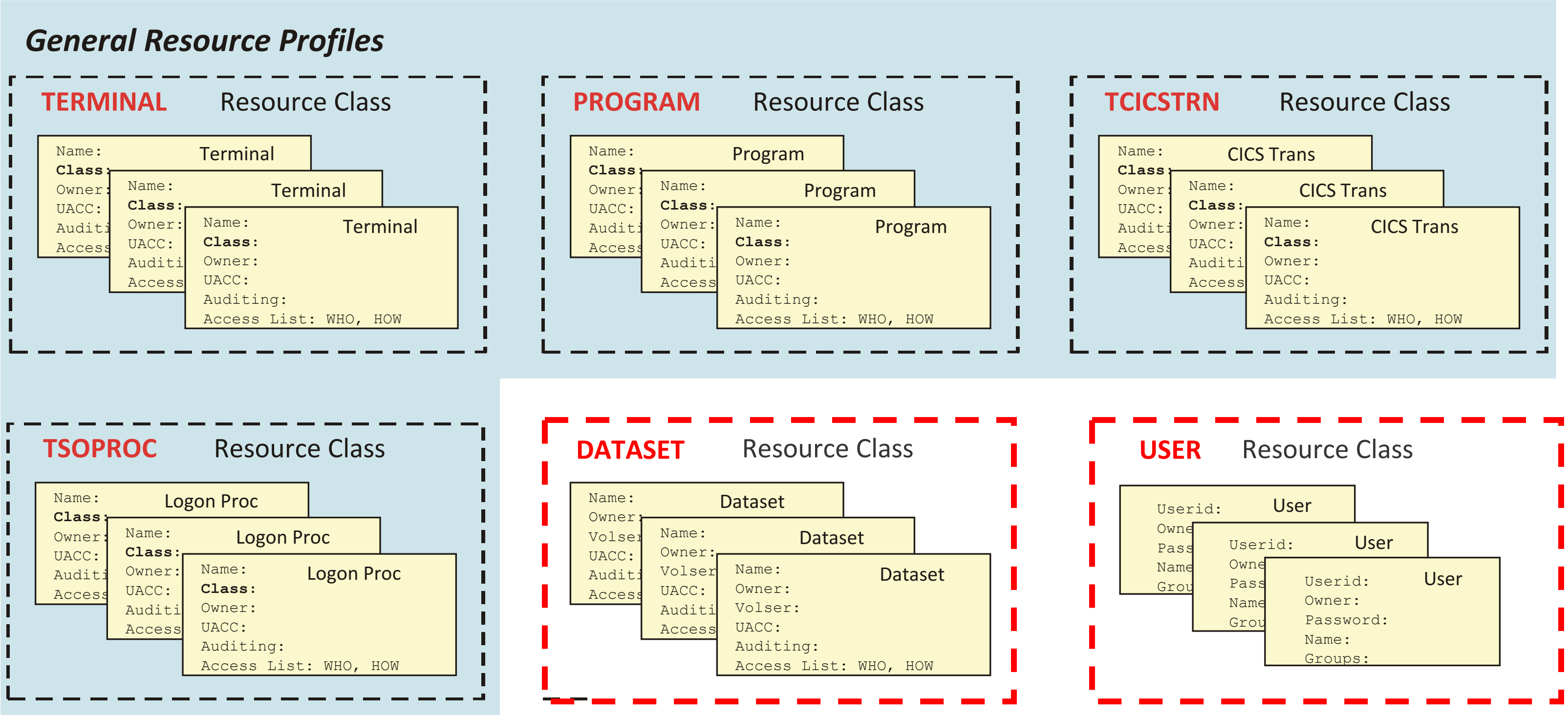
ALL, FAILURES, SUCCESS, and NONE

- Then the access level:
  - READ
  - UPDATE
  - CONTROL
  - ALTER

- The default, if AUDIT is not specified, is FAILURES(READ)

General Resource Profiles

Resource classes



General Resource Profiles

TERMINAL Resource Class

Name: Terminal
Class:
Owner:
UACC:
Auditi
Access

Name: Terminal
Class:
Owner:
UACC:
Auditi
Access

Name: Terminal
Class:
Owner:
UACC:
Auditing:
Access List: WHO, HOW

PROGRAM Resource Class

Name: Program
Class:
Owner:
UACC:
Auditi
Access

Name: Program
Class:
Owner:
UACC:
Auditi
Access

Name: Program
Class:
Owner:
UACC:
Auditing:
Access List: WHO, HOW

TCICSTRN Resource Class

Name: CICS Trans
Class:
Owner:
UACC:
Auditi
Access

Name: CICS Trans
Class:
Owner:
UACC:
Auditi
Access

Name: CICS Trans
Class:
Owner:
UACC:
Auditing:
Access List: WHO, HOW

TSOPROC Resource Class

Name: Logon Proc
Class:
Owner:
UACC:
Auditi
Access

Name: Logon Proc
Class:
Owner:
UACC:
Auditi
Access

Name: Logon Proc
Class:
Owner:
UACC:
Auditing:
Access List: WHO, HOW

DATASET Resource Class

Name: Dataset
Owner:
Volser
UACC:
Auditi
Access

Name: Dataset
Owner:
Volser
UACC:
Auditi
Access

Name: Dataset
Owner:
Volser:
UACC:
Auditing:
Access List: WHO, HOW

USER Resource Class

Userid: User
Owne
Pass
Name
Grou

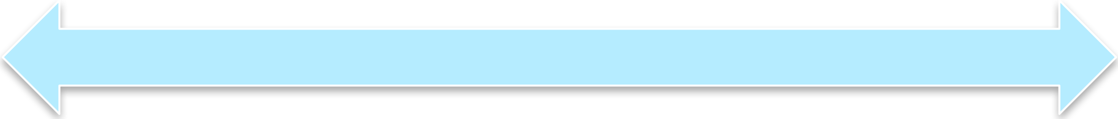
Userid: User
Owne
Pass
Name
Grou

Userid: User
Owner:
Password:
Name:
Groups:

General Resource Profile

Profile	Class	Owner	UACC	Warning	Erase	Auditing	ACL	Segments
256 chars								....

RACF base profile



General Resource Profiles

- Protect everything else!
- Both generic and discrete general resource profiles are allowed
- Wildcard characters can be used in any qualifier position
- Have to specify a CLASS
- Profiles are grouped by this CLASS
- Auditing attribute applies

Access Granted!
Access Denied!

Example ACL

User Profiles

Group Profiles

User Profiles

Dataset Profiles

Resource Profiles

Example ACL

Dataset Profiles

Resource Profiles

TSGLW.JCL.**

Avengers	READ
Thor	UPDATE
Loki	ALTER

Class OPERCMDS
MVS.SETPROG.**

Avengers	UPDATE

Access lists

- Conditional access lists have additional restrictions on the access

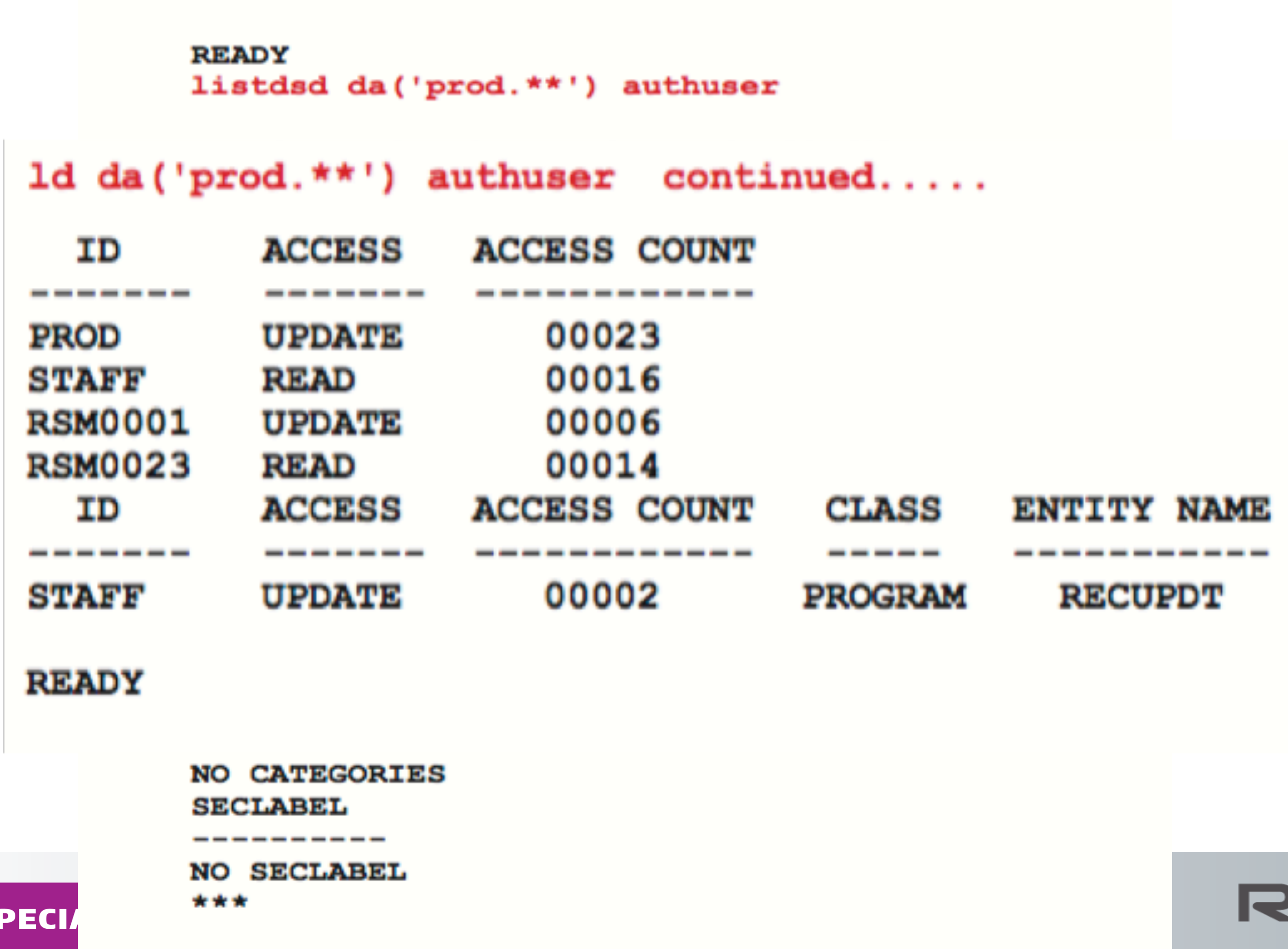
- For example: You can require that

  - a user be logged onto a particular terminal
  - when executing a particular program

Access lists

- Access permissions are specified in three ways:
  - Standard Access List
  - Conditional Access List
  - Universal Access (UACC) - default access granted to anyone

- Access can be permitted to:
  - USERID
  - Group
  - ID(*) - Grants access to all RACF- defined users
  - Granted by attribute OPERATIONS



```
READY
listdsd da('prod.**') authuser
```

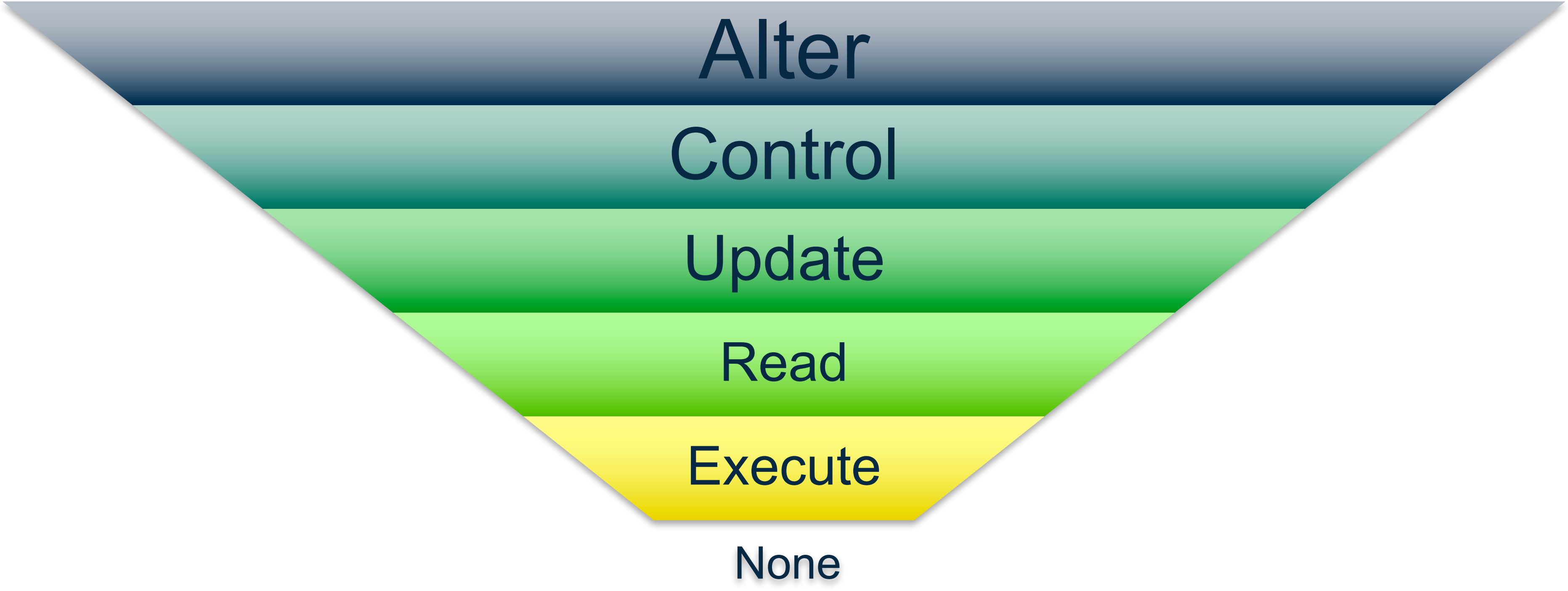
```
ld da('prod.**') authuser  continued.....

  ID        ACCESS    ACCESS COUNT
--------   --------   ------------
PROD        UPDATE        00023
STAFF       READ          00016
RSM0001     UPDATE        00006
RSM0023     READ          00014
  ID        ACCESS    ACCESS COUNT    CLASS     ENTITY NAME
--------   --------   ------------    -----     -----------
STAFF       UPDATE        00002      PROGRAM      RECUPDT

READY
```

```
NO CATEGORIES
SECLABEL
----------
NO SECLABEL
***
```

Access levels



Alter

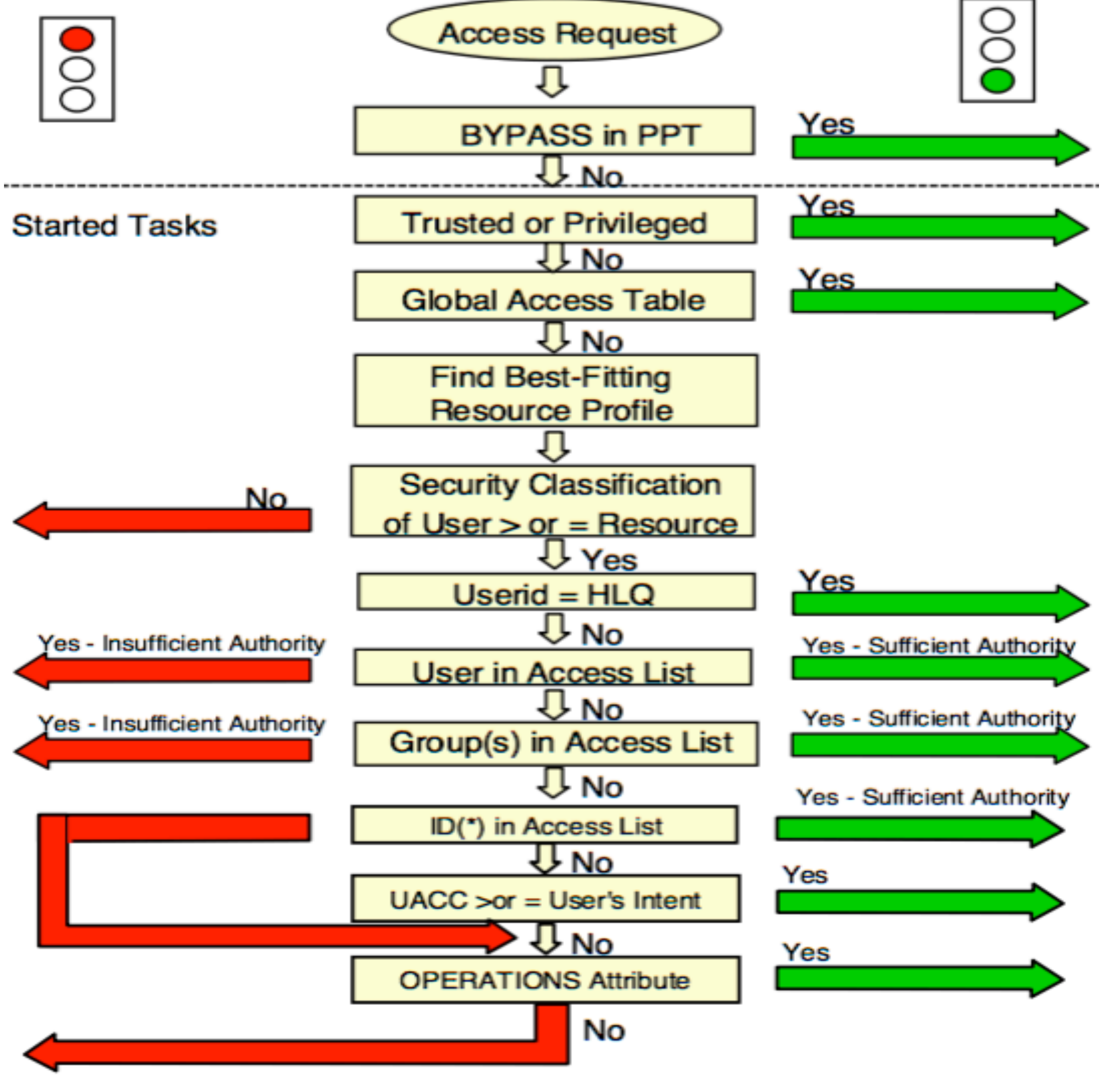
Control

Update

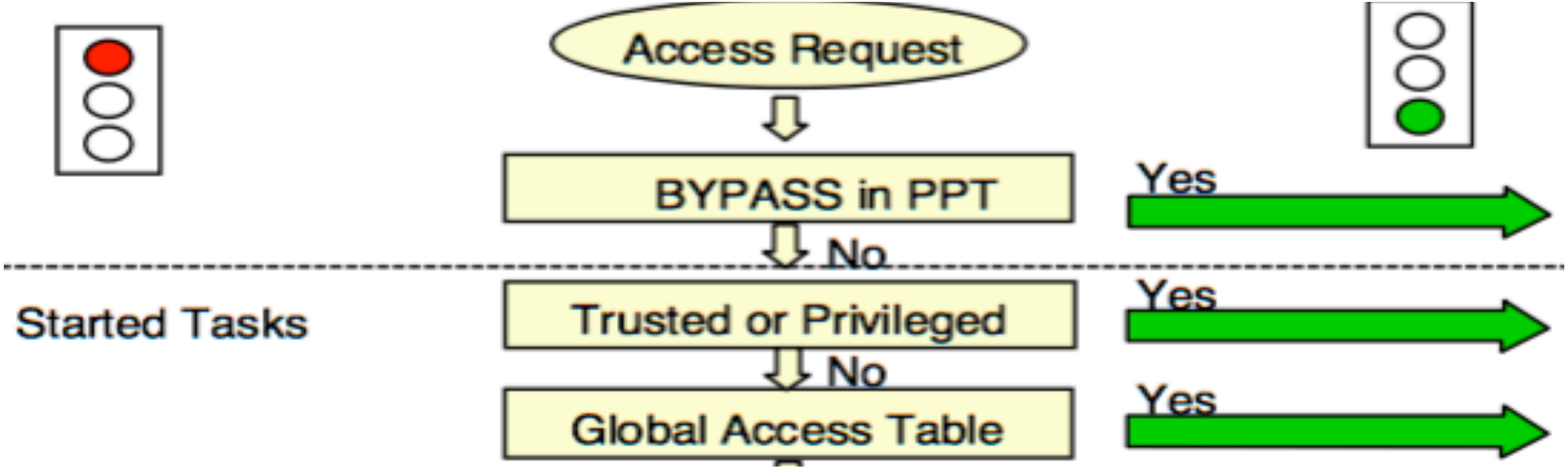
Read

Execute

None



Access Request
BYPASS in PPT
Yes
No
Started Tasks
Trusted or Privileged
Yes
No
Global Access Table
Yes
No
Find Best-Fitting Resource Profile
Security Classification of User > or = Resource
No
Yes
Userid = HLQ
Yes
No
Yes - Insufficient Authority
User in Access List
Yes - Sufficient Authority
No
Yes - Insufficient Authority
Group(s) in Access List
Yes - Sufficient Authority
No
ID(*) in Access List
Yes - Sufficient Authority
No
UACC >or = User's Intent
Yes
No
OPERATIONS Attribute
Yes
No



Access Request

BYPASS in PPT

Yes

No

Started Tasks

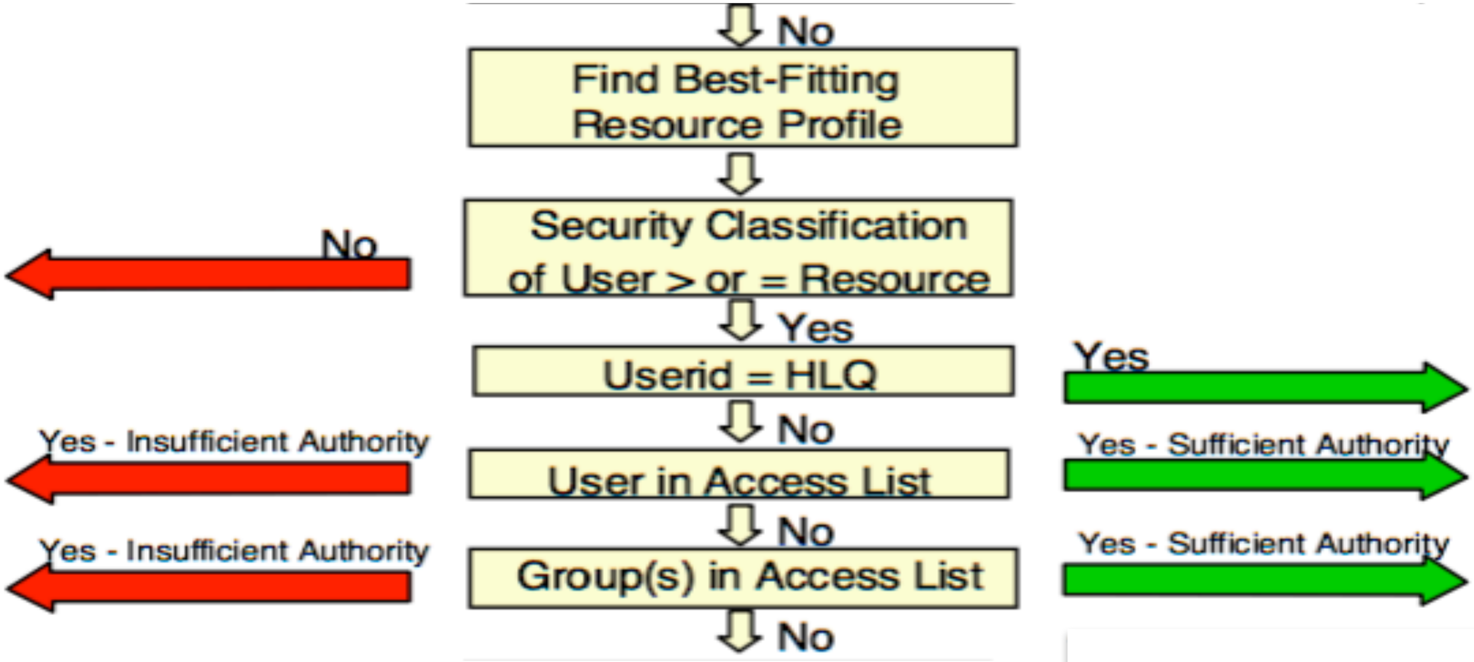
Trusted or Privileged

Yes

No

Global Access Table

Yes



No

Find Best-Fitting Resource Profile

Security Classification of User > or = Resource

No

Yes

Userid = HLQ

Yes

No

User in Access List

Yes - Insufficient Authority

Yes - Sufficient Authority

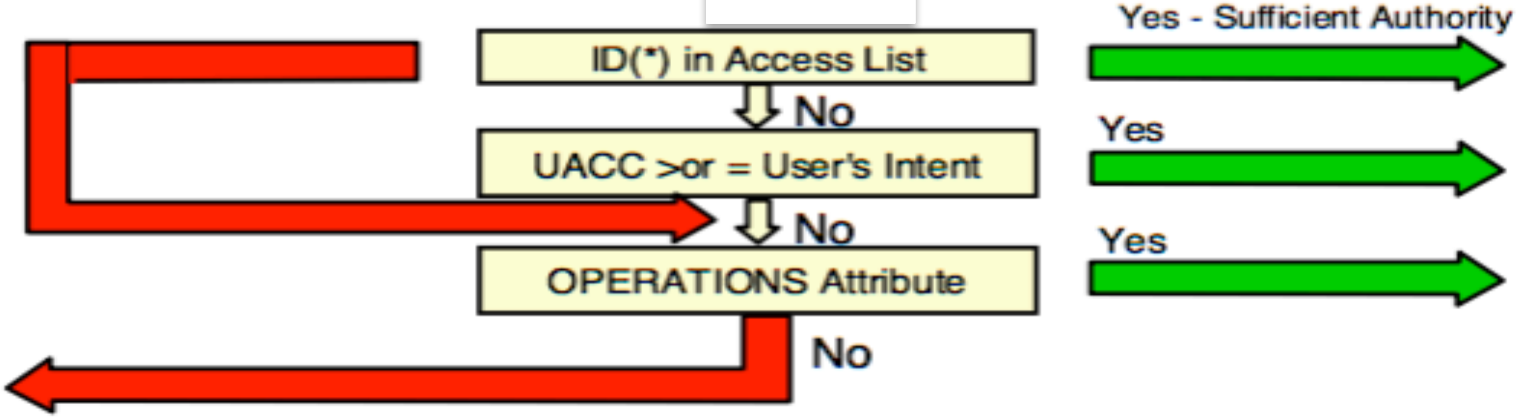
No

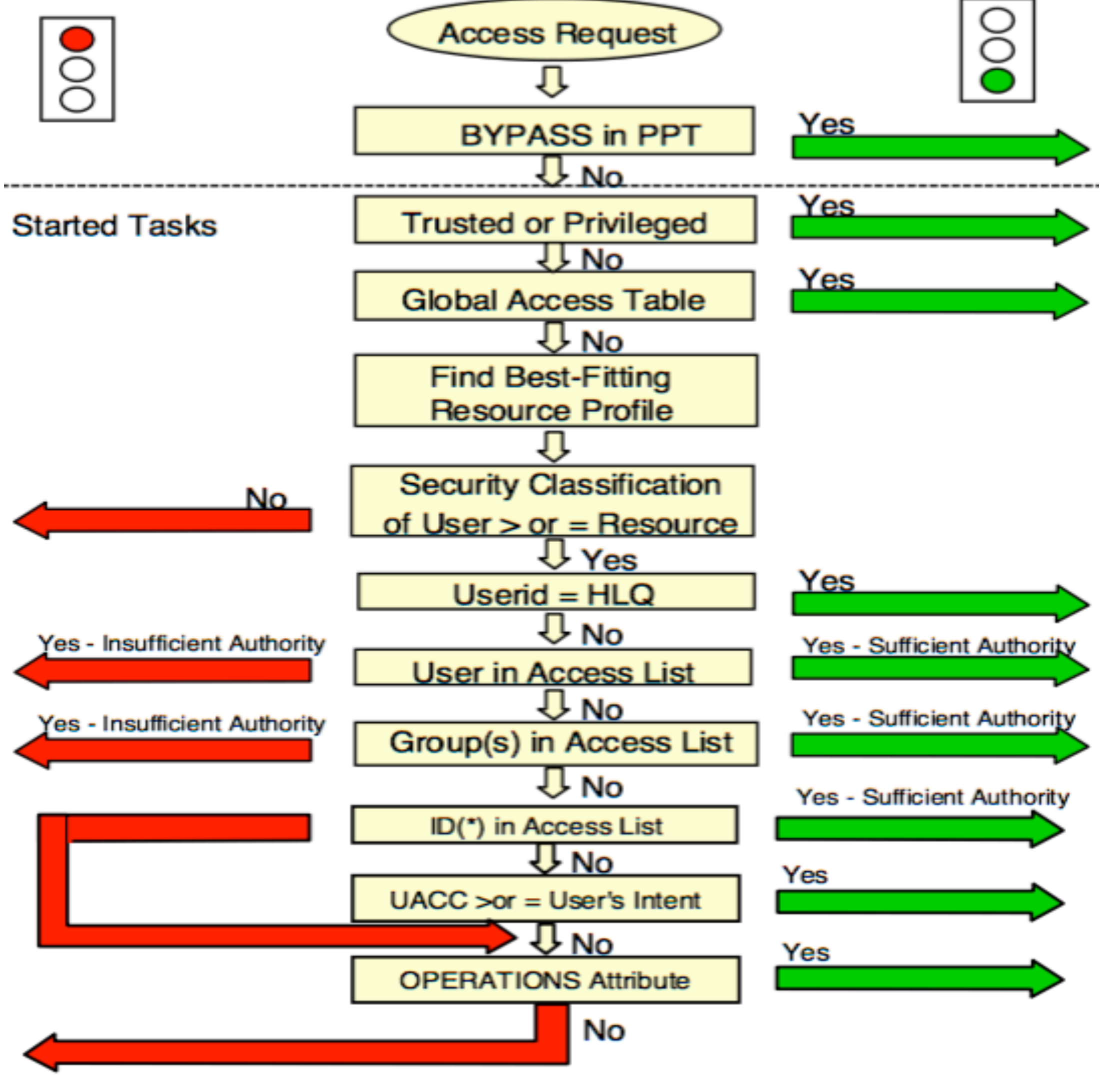
Group(s) in Access List

Yes - Insufficient Authority

Yes - Sufficient Authority

No


Yes - Sufficient Authority
ID(*) in Access List
No
Yes
UACC >or = User's Intent
No
Yes
OPERATIONS Attribute
No



Access Request

BYPASS in PPT

Started Tasks

Trusted or Privileged

Global Access Table

Find Best-Fitting Resource Profile

Security Classification of User > or = Resource

Userid = HLQ

User in Access List

Group(s) in Access List

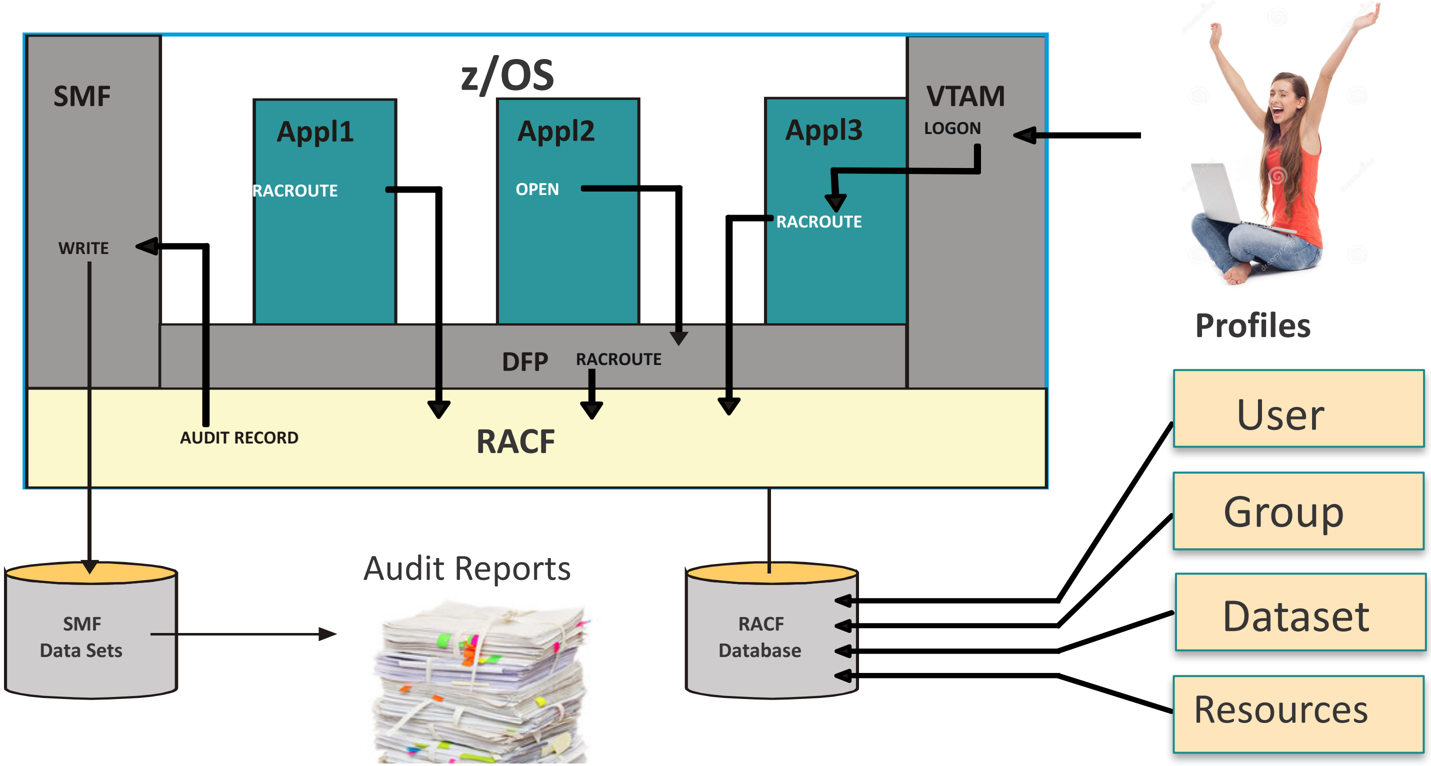
ID(*) in Access List

UACC >or = User's Intent

OPERATIONS Attribute

Yes
No
Yes
No
Yes
No
No
Yes
Yes
No
Yes - Insufficient Authority
Yes - Sufficient Authority
No
Yes - Insufficient Authority
Yes - Sufficient Authority
No
Yes - Sufficient Authority
No
Yes
No
Yes
No

Summary


z/OS
SMF
WRITE
Appl1
RACROUTE
Appl2
OPEN
Appl3
RACROUTE
VTAM
LOGON
DFP
RACROUTE
AUDIT RECORD
RACF
Profiles
User
Group
Dataset
Resources
SMF
Data Sets
Audit Reports
RACF
Database

Summary

- The bigger picture – subsystem & application configuration, SETROPTS, auditing, SMF configuration, exits
- A profile is just a list of protection parameters for a specific resource, and a list of users who can access the resource
- Resources are grouped together by class
- Be mindful of privileged user attributes

Questions