



IBM IT Education Services

R05

Peggy LaBelle, IBM Corporation

RACF Features for Everyone!

Secureworld Conference

August 25-29, 2003 | Miami Beach, FL

© 2003 IBM Corporation

Disclaimer

The information contained in this document is distributed on an "as is" basis without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that customers using the information or techniques will obtain the same or similar results in their own operational environments.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed programs may be used. Functionally equivalent programs may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

Trademarks

- **The following are trademarks or registered trademarks of the International Business Machines Corporation in the United States, other countries, or both:**
 - ▶ AIX
 - ▶ DB2
 - ▶ eServer
 - ▶ OS/400
 - ▶ pSeries
 - ▶ RACF
 - ▶ xSeries
 - ▶ z/OS
 - ▶ zSeries
- **The Open Group:**
 - ▶ UNIX is a registered trademark of The Open Group in the United States and other countries
- **Other company, product or service names may be trademarks or service marks of others.**

Agenda

■ RACF 2.1

- ▶ Dynamic Started Procedures Table
- ▶ SMF Data Unload Utility
- ▶ RACROUTE REQUEST=LIST,GLOBAL=YES

■ RACF 2.2

- ▶ Program Control Enhancement
- ▶ Remove ID Utility
- ▶ Enhanced PassTickets
- ▶ Unloading SETROPTS and RVARY with IRRADU00
- ▶ Remote Sharing Facility
- ▶ Year 2000

■ OS/390 Release 3 Security Server

- ▶ Command Exit
- ▶ Prevent Automatic Addition of Creator
- ▶ Controlling Program Access by SMF System ID
- ▶ Password Reset Only

Agenda...

- **OS/390 Release 4 Security Server**
 - ▶ RACF Control of DB2 Objects
 - ▶ Password History Enhancement
 - ▶ Default UID and GID for OpenEdition
 - ▶ Support for Digital Certificates
- **OS/390 Release 6 Security Server**
 - ▶ Networked Qualified Names
- **OS/390 Release 8 Security Server**
 - ▶ Protected User IDs
 - ▶ UNIX System Services SuperUser Granularity
 - ▶ Certificate name filtering
 - ▶ Restricted user ids
 - ▶ Mixed case profiles

Agenda...


- **OS/390 Release 10 Security Server**
 - ▶ Program control usability enhancement
 - ▶ Application Identity Mapping
 - ▶ Network Authentication Services (Kerberos)
- **z/OS Version 1 Release 2 Security Server**
 - ▶ UNIVERSAL groups
 - ▶ SAF Trace
- **z/OS Version 1 Release 3 Security Server**
 - ▶ UNIX File Security Enhancements
- **z/OS Version 1 Release 4 Security Server**
 - ▶ UID/GID enhancements
 - ▶ PADS
 - ▶ UNIX access enhancements

RACF 2.1

Started Procedures Table - Before

SYS1.LPALIB(ICHRIN03)

- What is a started procedure table - ICHRIN03
- Assembled and linked into LPA
- Problems:
 - Requires an IPL to change
 - Strict format requirements
 - Must run DSMON to see what is in use



```
ICHRIN03 CSECT
          Title 'ICHRIN03'
          DC XL2'800B'
          *-----*
          DC CL8 'JES2   '
          DC CL8 'JES2   '
          DC CL8 'STCGRP '
          DC XL1 '40'
          DC XL7 '00'
          *-----*
          DC CL8 'CICS   '
          DC CL8 'CicsProd'
          DC XL1 '80'
          DC CL8 'STCGRP '
          DC XL7 '00'
```


Dynamic Started Procedures Table

■ Advantages:

- ▶ Ability to use STARTED class or ICHRIN03
- ▶ Easier to define
- ▶ Allows changes to security definitions for stated tasks without an IPL
- ▶ Supports MVS 5.1 START command enhancements
- ▶ Better generic support than ICHRIN03
- ▶ Easier to see what is being used

RLIST STARTED * STDATA

A new class - STARTED

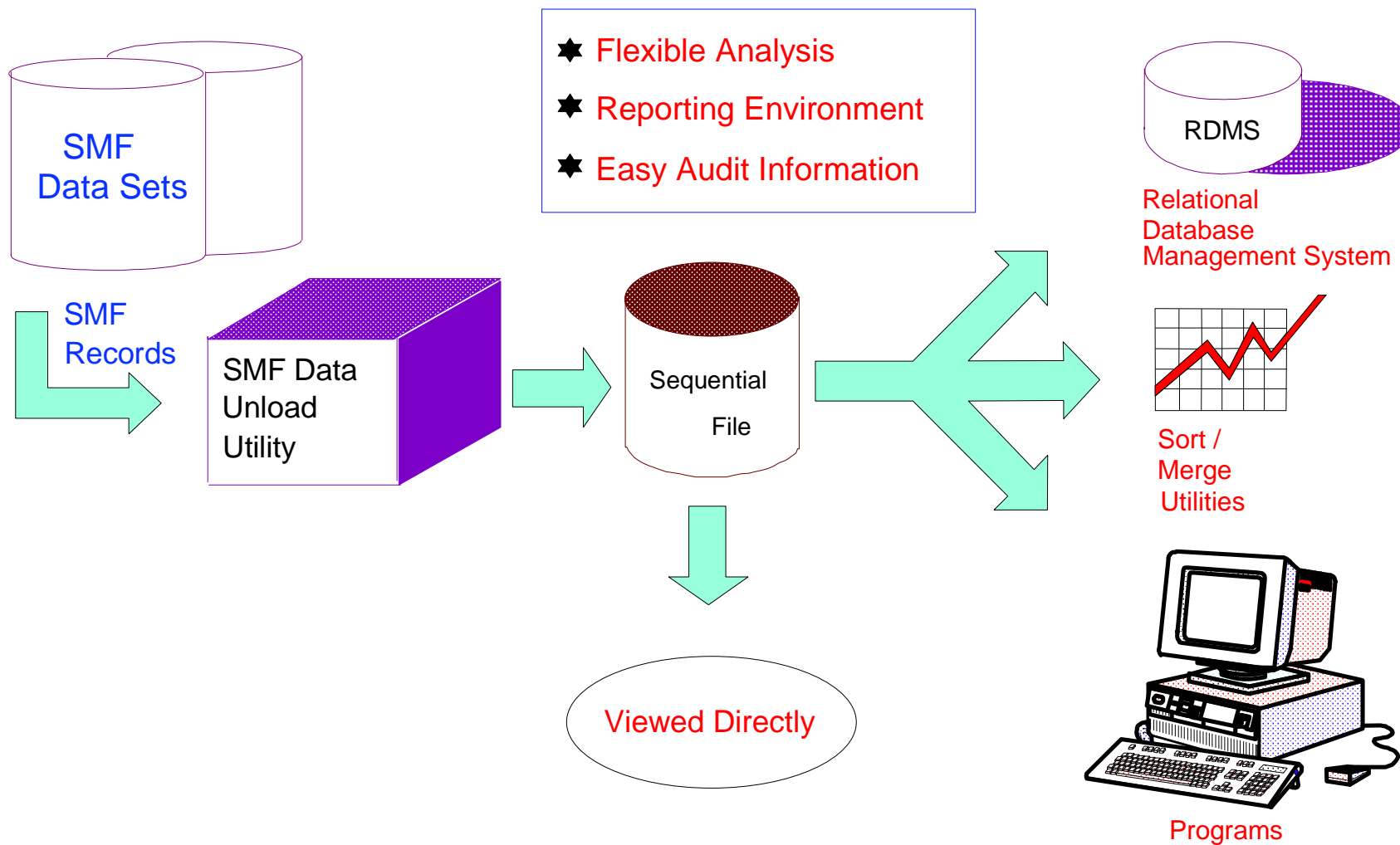
```
RDEFINE STARTED JES2.* STDATA(USER(JES2)
    GROUP(STCGRP) TRUSTED(YES))
RDEFINE STARTED ** STDATA(USER(=MEMBER)
    GROUP(STCGRP) TRACE(YES))
SETROPTS CLASSACT(STARTED) RACLIST(STARTED)
```

JES2.*	User ID	Group ID	Flags
CICS.PROD*		

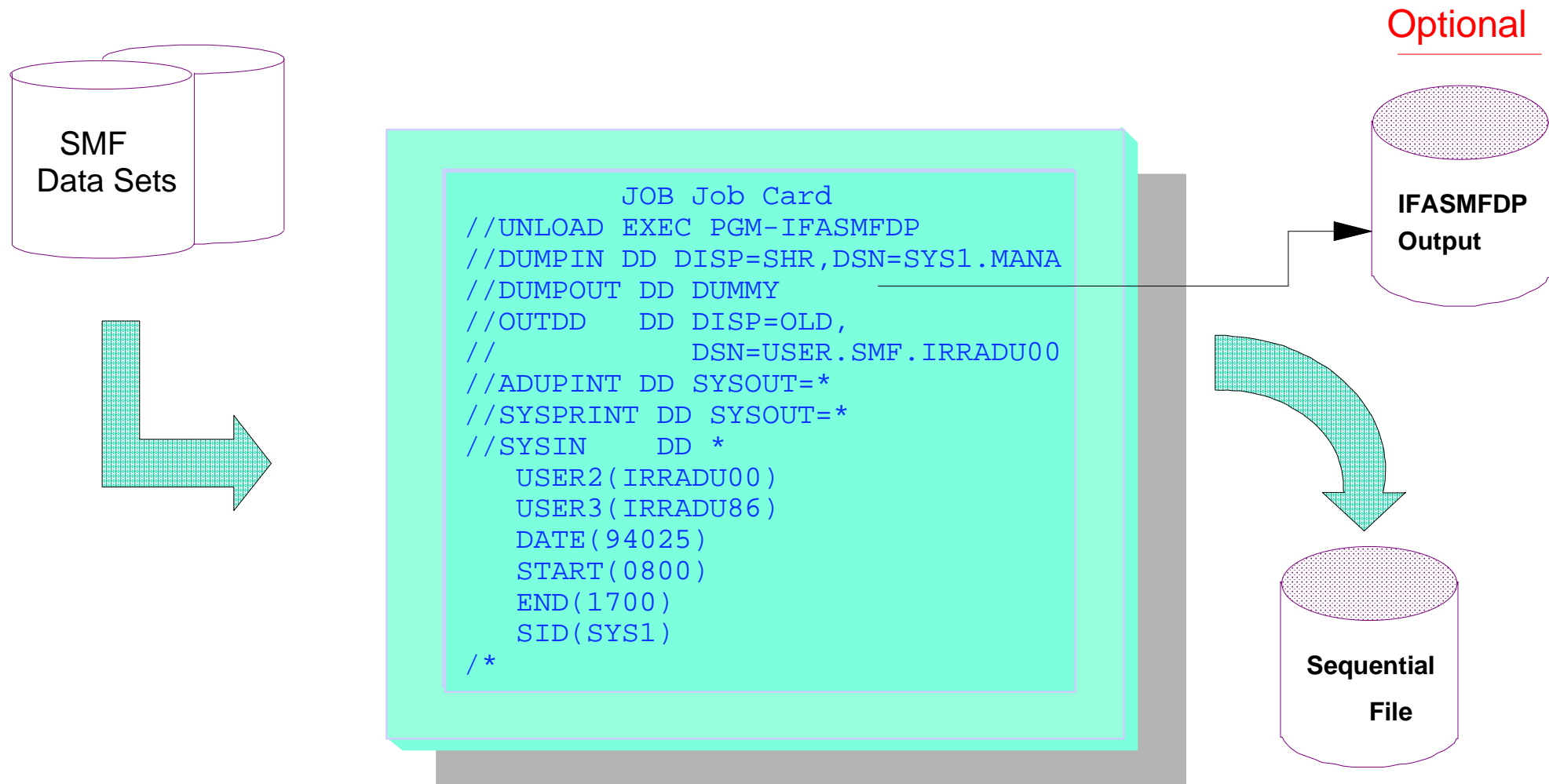
Dynamic Started Procedures Table - Migration

- **SYS1.SAMPLIB Support:**
 - ▶ New member ICHSPTCV - REXX exec to convert ICHRIN03 entries
- **New Messages:**
 - ▶ IRR812I - issued when STARTED class profile used (TRACE=YES)
 - ▶ IRR813I - issued when STARTED class profile not found
 - ▶ IRR814I - issued when STARTED class profile incomplete
- **Works on any MVS release supported by RACF 2.1**
- **Must keep ICHRIN03!**

RACF SMF Data Unload Utility

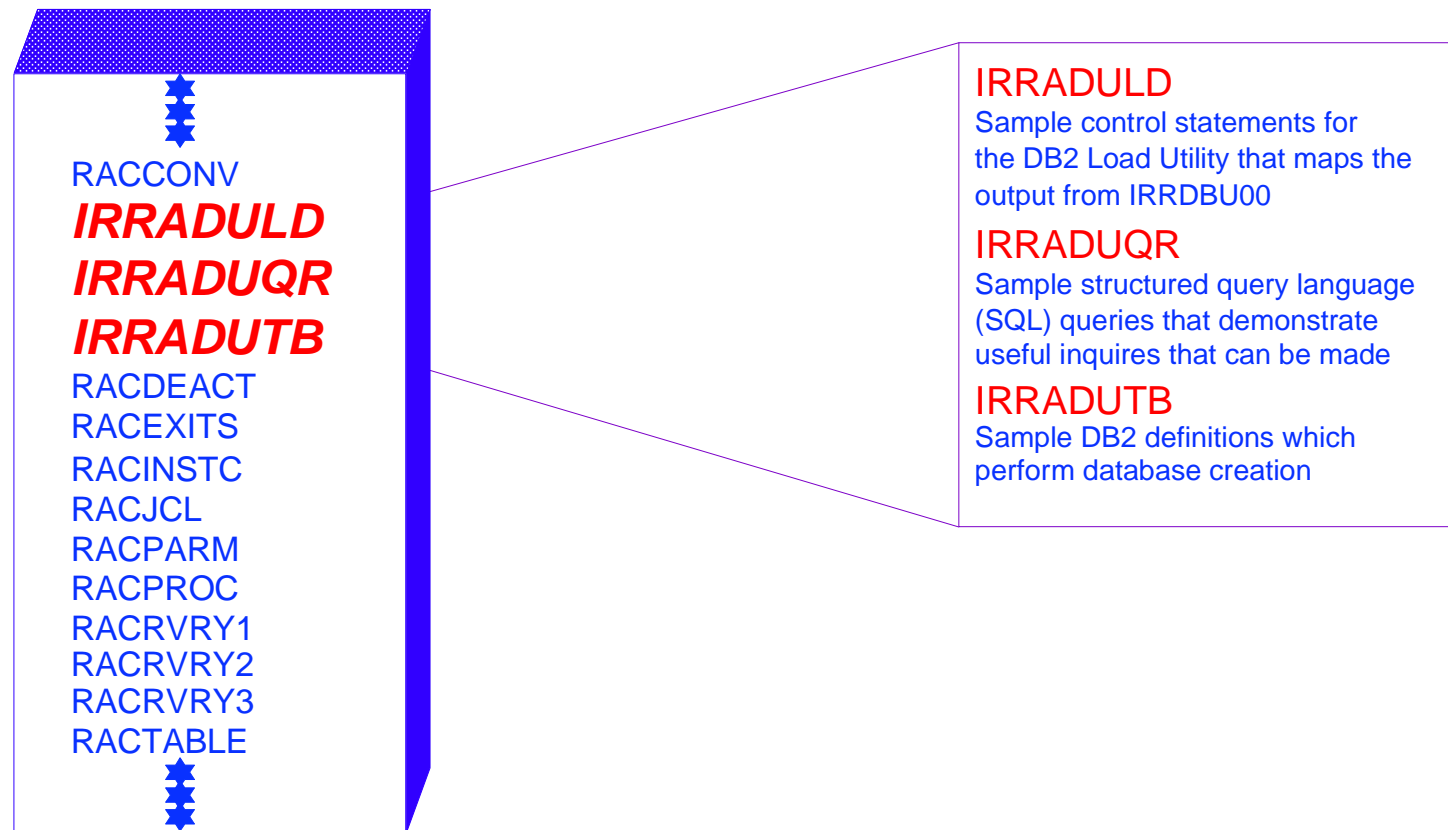


How is the Utility invoked ?

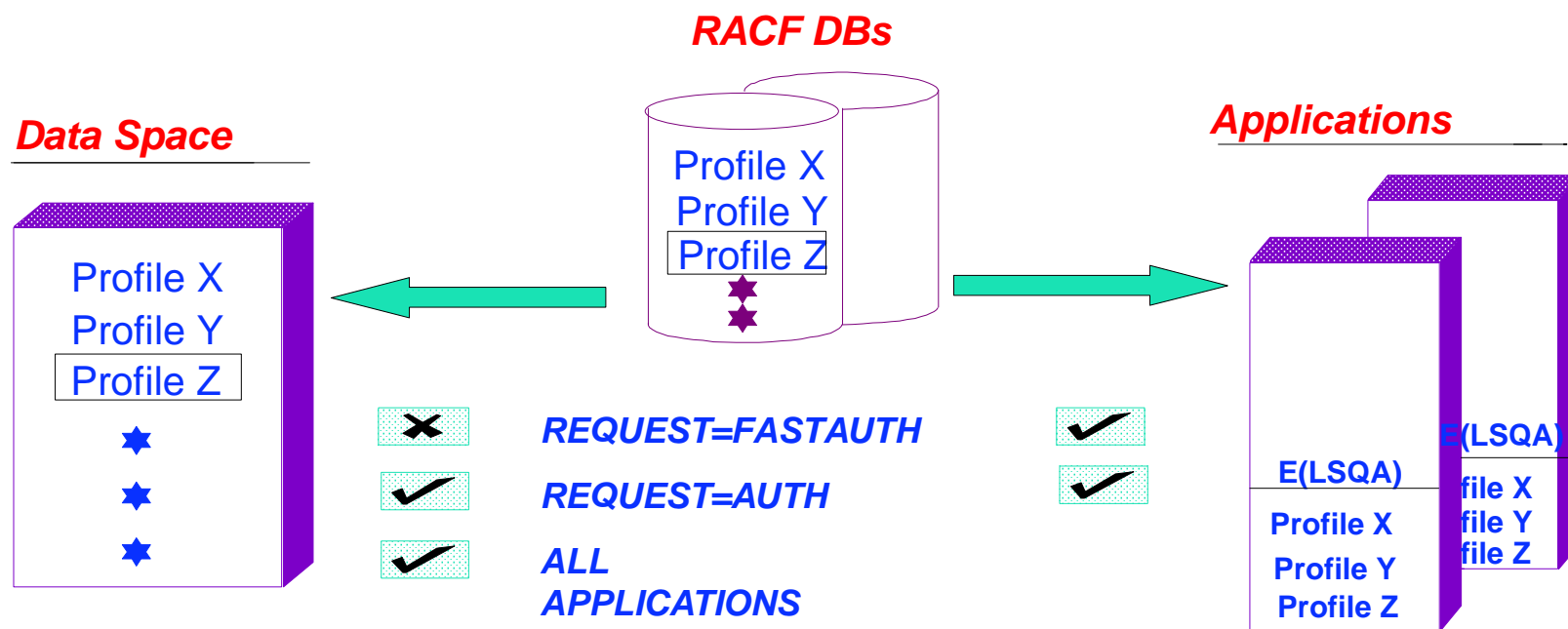


Sample DB2 Mappings

SYS1.SAMPLIB



RACLIST PROCESSING (PRE 2.1)



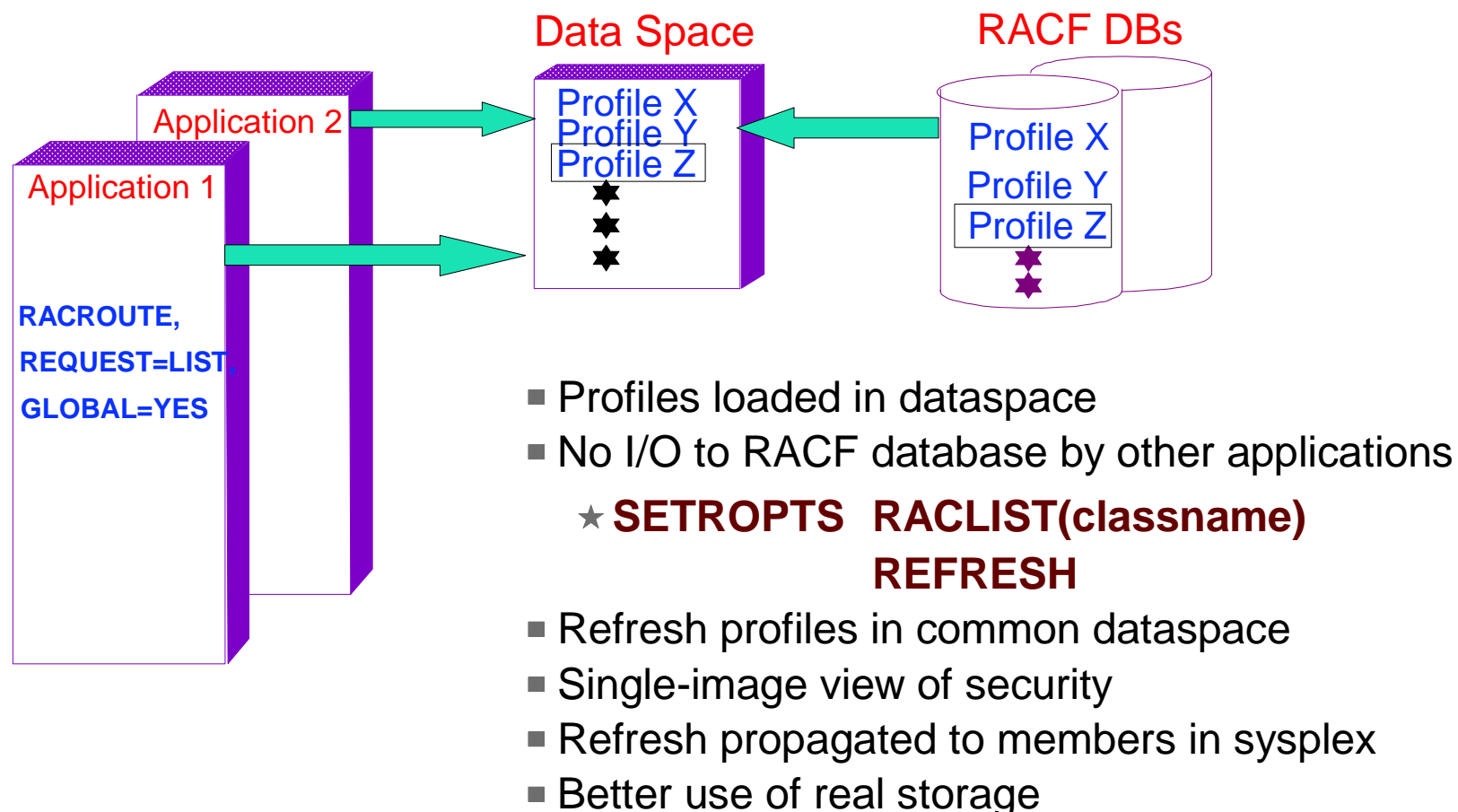
SETROPTS RACLIST(classname)

- ★ Read from database into dataspace
- ★ Access information in CDT
- ★ Profile change, refresh with SETROPTS

RACROUTE REQUEST=LIST

- ★ Read from database into E(LSQA)
- ★ Profiles chained off of ACEE
- ★ Refresh each application

RACROUTE REQUEST=LIST,GLOBAL=YES



RACF 2.2

Program Class Enhancement

- **Volume specification for program definitions is now optional!**

OLD: RDEFINE PROGRAM xxx ADDMEM('library'/volser)

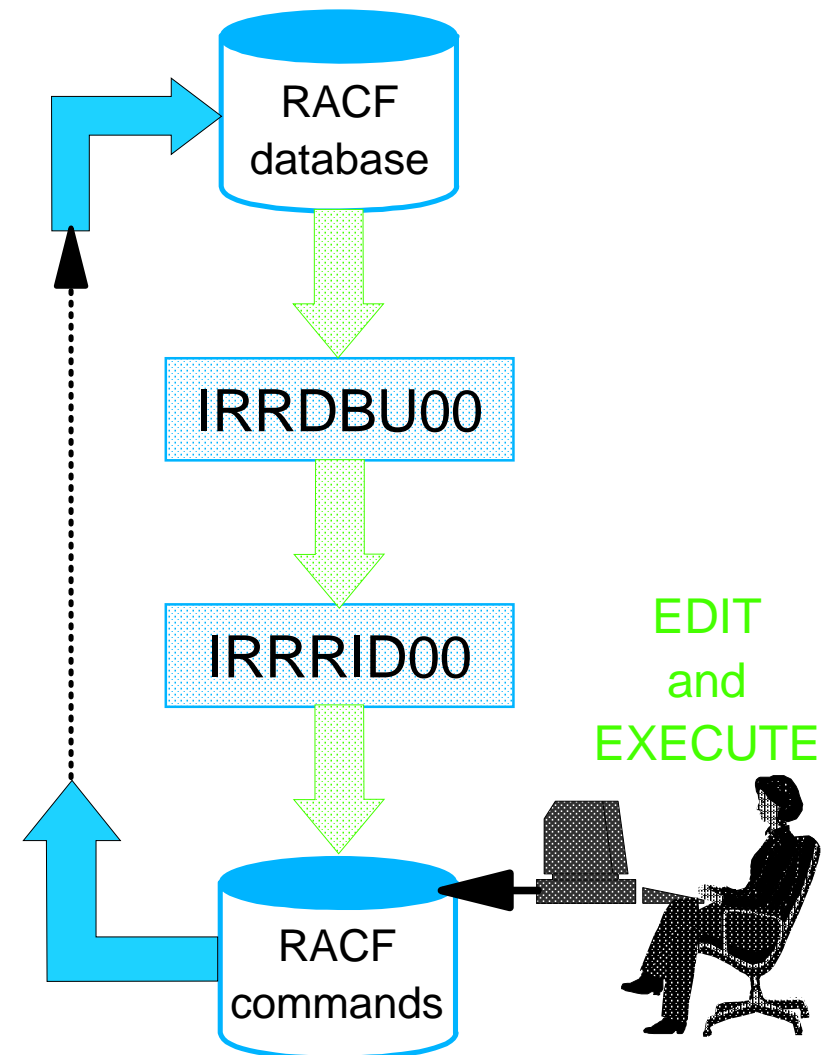
NEW: RDEFINE PROGRAM xxx ADDMEM('library')

- **Shipped with APAR OW24881**

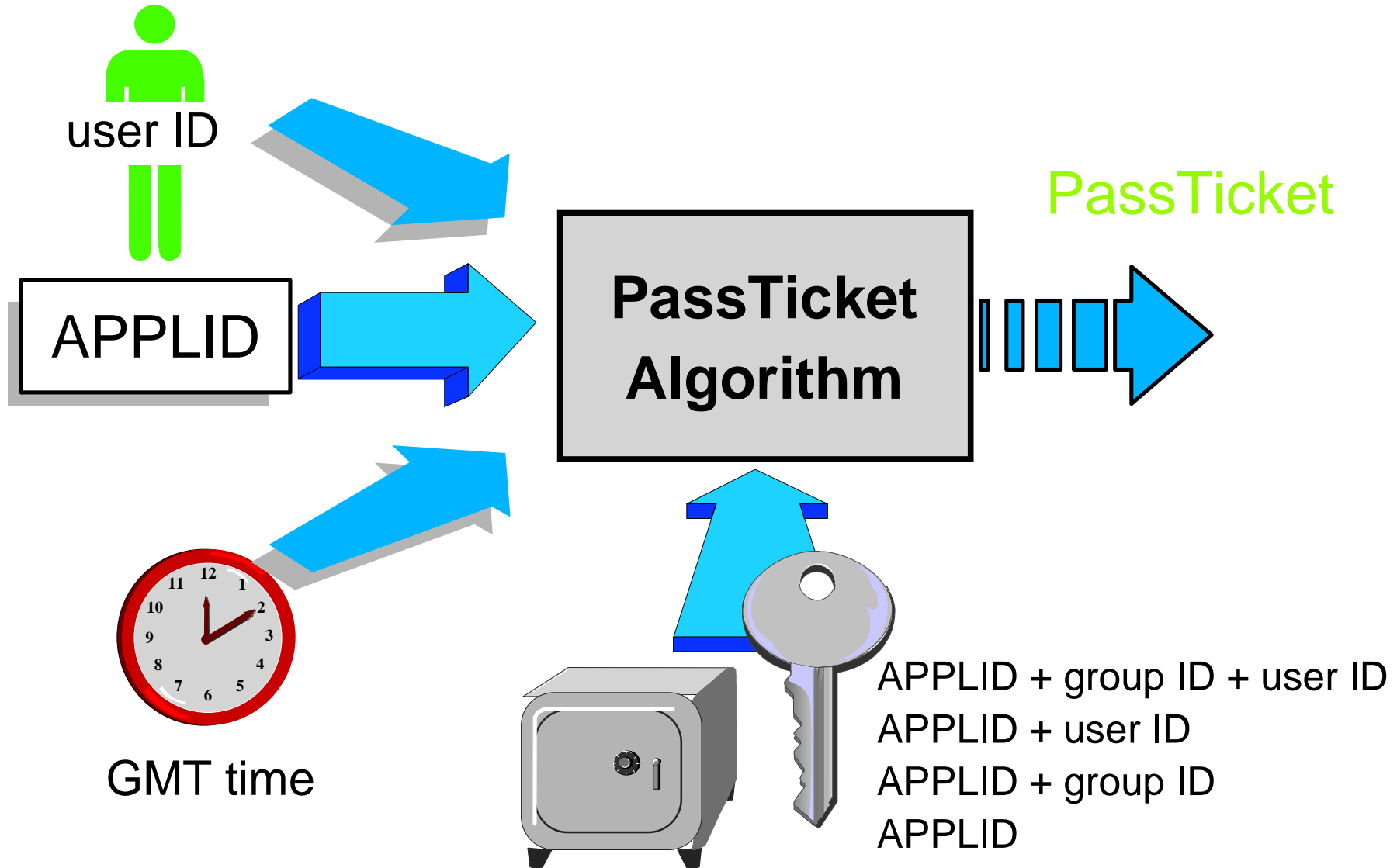
- ▶ PTF UW36135 for RACF 2.2, OS/390 Security Server Release 1 and OS/390 Security Server Release 2
- ▶ PTF UW36136 for OS/390 Security Server Release 3

RACF Remove ID Utility

- **Creates RACF commands that assist in housekeeping**
- **Output must be reviewed and edited**
- **Can be used to remove any reference to residual IDs**
- **Removes deleted user IDs and group IDs from access lists**
- **Replaces user IDs and group IDs in owner fields**



Qualified PassTicket Profile



Unloading SETROPTS and RVARY

- **IRRADU00 now unloads the keywords that were specified on SETROPTS and RVARY**
- **When more than 10 classes are specified on a keyword, such as "CLASSACT(class1, class2...)", the first 10 classes are unloaded, along with a count of the classes not unloaded**
- **Specifying "*" for a class list yields a "*" in IRRADU00 output**
- **New field in SETROPTS SMF type 6 relocate section to indicate that "*" was specified .**
- **Support delivered via APAR OW30252, for RACF 2.2 and all OS/390 releases**

RACF Remote Sharing Facility

- **Links multiple RACF DBs, providing:**
 - ▶ Command direction
 - ▶ Password synchronization
 - ▶ Automatic command direction
 - ▶ Automatic password direction
- **Benefits of using with one RACF DB:**
 - ▶ Execute commands under different ID
 - ▶ Password sync on single system
 - ▶ RACF commands from the operator's console

Year 2000

- **RACF is Year 2000 compliant with APAR OW19521**
- **RACF has many dates in the RACF database that are three character packed decimal values, of the form yydddf, where "yy" represents the year.**
- **Dates with a "yy" value of "70" or earlier are considered to be in the year 20yy. Dates with a "yy" greater than 70 are considered to be in the year 19yy.**
- **APAR OW19251**

OS/390 Security Server Release 3

RACF Command Exit

- **New exit point IRREVX01 invoked for each end-user RACF command (operator commands, RVARY, and BLKUPD excluded)**
- **Uses MVS Dynamic Exit Services**
 - ▶ Exit can be replaced without an IPL
 - ▶ Exit can have an installation-chosen name
 - ▶ Multiple modules can be associated with a single exit point
- **Exit may fail the command with or without a message**

Prevent Automatic Addition of User ID to Access List

- **New SETROPTS option to control the placement of the profile creator on the access list**
- **ADDCREATOR - Adds the creator (business as usual)**
- **NOADDCREATOR - Do not add the creator**
 - ▶ Any profile created by ADDSD or RDEFINE
 - ▶ Any generic profile created by RACROUTE REQUEST=DEFINE
 - ▶ Discrete profiles excluding DATASET and TAPEVOL

Controlling Program Access by SYSID

- Access to programs (load modules) can now be controlled based on SMF system ID

- New WHEN option:

```
PERMIT progname CLASS (PROGRAM) ID (MARKN)  
      WHEN (SYSID (smf_system_id))
```

- WHEN(SYSID(....)) valid only for PROGRAM profiles
- No class associated with the SYSID
- value not verified
- Support delivered via APAR OW25727, PTFs UW91104 for R3, and UW91105 for R4

Password Reset Only

- **Users may now be authorized to reset passwords, resume user IDs, and list profiles for others without being given SPECIAL or group-SPECIAL authority.**
- **Controlled by FACILITY Class Profiles :**
 - ▶ **IRR.PASSWORD.RESET**
 - **READ** Access - Reset password to expired value and ability to resume a user.
 - **UPDATE** Access - May reset password to a non-expired value and resume a user
 - ▶ **IRR.LISTUSER**
 - **READ** Access - May list other user's profiles via LISTUSER, subject to field-level access checks
- **Available on R3 in support of TIVOLI Roles Based Administration Enhancements.**

User Administration Enhancements

- **Prior to release 6, a user's password was set to an expired temporary password value when the password was changed by an administrator.**
- **Now, there is a new option (NOEXPIRED) on ALTUSER which allows the setting of a password which does not have to be changed on first use.**
- **Available with APAR OW26060 on R3 and R4.**

OS/390 Security Server Release 4

RACF Control of DB2 Objects

■ **DB2 - Access Control Authorization Exit Point**

- ▶ A new exit point documented by DB2
- ▶ Exit point is driven:
 - Once at subsystem startup
 - For each DB2 authorization request
 - Once at subsystem Termination
- ▶ DB2 Provides dummy DSNX@XAC routine

■ **RACF - The RACF/DB2 External Security Module**

- ▶ Fully supported exit module designed to receive control from the DB2 Access Control Authorization Exit Point
- ▶ Translates DB2 authorization checks into checks in RACF general resource classes

Password History Enhancement

- **Pre-release 4, a user's current password was not placed in the password history when the password was changed by an administrator.**
- **With release 4, the user's current password is placed in the password history when the password is changed by an administrator.**
- **Helps prevent users from circumventing password change frequency rules by calling up the help desk and having the administrator reset their password to a temp value, which they can change back to their favorite value that they had been using.**

Default UID/GID

- **Pre-release 4, all UNIX System Services users must:**
 - ▶ Have a valid UID
 - ▶ Be connected to at least one group with a valid GID
- **With release 4, installations can:**
 - ▶ Assign users without a UID/GID an installation defined UID/GID
 - ▶ Assigned through a FACILITY class profile:
 - BPX.DEFAULT.USER APPLDATA('userid/groupid'), where *userid* and *groupid* are the RACF user ID and group ID that are to be assigned.
 - Access list and UACC are not used
- **Benefits:**
 - ▶ Ease of administration without loss of audit trail

RACF Support for Digital Certificates

- **With OS/390 Security Server R4, RACF can be used to map certificates to a RACF user ID.**
 - ▶ New general resource class (DIGTCERT)
 - New segment (CERTDATA) contains the certificate
 - APPLDATA contains the user associated with the certificate
 - UACC contains the TRUST status of the certificate
 - New user profile repeat group points to the certificate
 - ▶ New RACF command (RACDCERT) to manage the certificates

RACDCERT Command Syntax

RACDCERT

[ID(UserID)]

[LIST

| ADD('Dataset-Name')

[TRUST | NOTRUST]

| ALTER [(SERIALNUMBER(Serial-Number)

[ISSUERSDN('Issuer's Distinguished
Name')])]

TRUST | NOTRUST

| DELETE [(SERIALNUMBER(Serial-Number)

[ISSUERSDN('Issuer's Distinguished
Name')])]

}

How are Certificates Used?

- **initACEE callable service is enhanced to allow the specification of a certificate**
- **RACF verifies that the certificate is:**
 - ▶ Registered with RACF
 - ▶ Trusted
 - ▶ Maps to a valid user ID
- **initACEE returns the security environment for the user to which the certificate is associated**
- **Used by the Lotus Go Domino Webserver for OS/390 (formerly the Internet Connection Secure Server)**

OS/390 Security Server Release 5

How are Certificates Used?

- **Certificate Autoregistration**
- **RACLISTing DIGTCERT optional**
- **New Base64 certificate format**
- **CICS certificate to user ID translation**
- **Additional functions/keywords on RACDCERT to associate a label with a certificate**
- **OS/390 V2R5 APARs**
 - ▶ **RACF (R4) - OW31933**
 - ▶ **SAF OW31934**
 - ▶ **OpenEdition - OW33091**
 - ▶ **LE (C-RTL) - PQ15716**

New Certificate Support in V2R5

RACDCERT

```
[ ID(UserID) ]
[ LIST [(LABEL('label-name') | [
        SERIALNUMBER(Serial-Number)
        [ ISSUERSDN('Issuer's Distinguished Name') ] ] ) ]
| ADD('Dataset-Name')
  [ TRUST | NOTRUST ]
  [WITHLABEL('label-name')]
| CHECKCERT('data-set-name')
| ALTER [(LABEL('label-name') | [
        SERIALNUMBER(Serial-Number)
        [ ISSUERSDN('Issuer's Distinguished Name') ] ] ) ]
  [TRUST | NOTRUST]
| DELETE [(LABEL('label-name') |
  [ (SERIALNUMBER(Serial-Number)
  [ ISSUERSDN('Issuer's Distinguished Name') ] ] ) ] ]
```

OS/390 Security Server Release 6

NQN - Network Qualified Names

- **Ability to specify an additional qualifier in APPC information passed to RACF to identify the remote network in existing APPCLU, APPCPORT classes.**
- **Allows customers with interconnected networks containing like named LU's to differentiate them.**
- **Changes you'll see :**
 - ▶ New Keyword POENET on RACROUTE
 - ▶ APPCPORT class expanded from 8 - 17 chars using new MAXLENX parameter on ICHERCDE macro
 - ▶ DISPLAY, PERMIT and TARGET commands accept 17 char partner-LU name
 - ▶ Panels, SMF Unload and DB Unload will support new extended name length.

OS/390 Security Server Release 8

Certificate Name Filtering

- **Maps many certificates to a single user ID based on**
 - ▶ Name in certificate
 - Subject's distinguished name
 - Issuer's distinguished name
 - ▶ System information (optional)
 - SMF ID or application specific
- **DIGTCRIT and DIGTNMAP general resource classes**
- **Keywords on RACDCERT command to add, modify, list, or delete mappings**
- **"Anchor" user ID: irrmulti**
- **Delivered via APARs OW40129, OW41030**
 - ▶ available on R8 or later

Restricted User IDs

- **Makes use of shared or PUBLIC user IDs safer**
 - ▶ PUBLIC
 - ▶ ANONYMOS
 - ▶ Certificate Name Filtering mappings
- **Ignore UACC, ID(*), and GLOBAL when performing access checks for the user ID**
- **Enhancements to ADDUSER, ALTUSER, LISTUSER commands**
 - `ADDUSER user1 RESTRICTED`
 - `ALTUSER user1 RESTRICTED | NORESTRICTED`
- **Delivered via APARs OW40129, OW41030**
 - ▶ available on R8 or later

Mixed Case Profiles

- **Classes can be defined to accept mixed case profile names**
 - ▶ CDT option CASE= UPPER | ASIS
 - ▶ Existing IBM classes are unchanged
 - Maintain compatability and avoid admin surprises
- **Enterprise Java Beans in WebSphere classes EJBROLE and GEJBROLE**

```
RDEFINE EJBROLE ( xyz XYZ xYz ) /*3 classes!*/
```
- **Available on OS/390 V2R8 and V2R10 via SPE**
 - ▶ OW46859

Protected User ID

- **User ID which has no password and may not be logged on**
 - ▶ TSO, CICS sign-on, or rlogin from a workstation
- **Protects user IDs assigned to**
 - ▶ Started tasks
 - ▶ UNIX daemons
 - ▶ Subsystem resource managers
- **Protected from**
 - ▶ Use for unintended purposes
 - ▶ From being revoked for invalid password attempts
 - ▶ Avoids risk when password is not changed from default value
- **ADDUSER and ALTUSER commands**

```
ADDUSER server1 NOPASSWORD NOOIDCARD
```

```
ALTUSER server1 NOPASSWORD NOOIDCARD
```

SuperUser Granularity

- **Authorize selected users to do selected SuperUser functions without giving UID 0 or access to BPX.SUPERUSER profile**
- **New UNIXPRIV class to define resources**
- **Example: give user LAURIE the authority to mount and unmount any file system:**

```
RDEFINE UNIXPRIV SUPERUSER.FILESYS.MOUNT UACC(NONE)
PERMIT SUPERUSER.FILESYS.MOUNT CLASS(UNIXPRIV)
        ID(LAURIE) ACCESS(UPDATE)
SETROPTS CLASSACT(UNIXPRIV) RACLIST(UNIXPRIV)
```

- **Some other things you can use this for:**
 - ▶ Allow a user to read or write to any HFS file
 - ▶ Allow a user to send signals to any process
 - ▶ Allow a user to view all processes
 - ▶ Allow all users to issue chown for their own files

User Limits

- **Allow selected users to exceed resource limits in the BPXPRMxx member of PARMLIB without giving UID 0**
- **New fields in the OMVS segment of the user profile to define resource limits**
- **Example: Give user UNIXUSR the ability to use more CPU time than the maximum specified by the MAXCPU TIME parameter of BPXPRMxx**

```
ALTUSER UNIXUSR OMVS(CPUTIMEMAX(5000))
```

- **Some other things you can use this for:**
 - ▶ Set maximum address space size
 - ▶ Set maximum number of files per process
 - ▶ Set maximum number of processes per UID
 - ▶ Set maximum number of threads per process
 - ▶ Set maximum memory map size

OS/390 Security Server Release 10

Program Control Usability

- **Reduce the need for GTF traces to resolve program control and PADS problems**
- **Diagnostic messages when functions requiring "clean" environment fail**
 - ▶ PADS, execute-control, UNIX servers/daemons
- **Messages**
 - Failure occurred because of "dirty" environment
 - Reason environment became dirty: module name, library name, etc.
`ICH420I PROGRAM PAYROL5 FROM LIBRARY SYS2.PAYLIB
CAUSED THE ENVIRONMENT TO BECOME UNCONTROLLED.`
- **RACROUTE REQUEST=AUTH and ICHRCX02 Exit**
 - Reason code indicating the request would have succeeded if environment were clean

Application Identity Mapping

- **Eliminates need for some kinds of "mapping" profiles**
 - ▶ UNIXMAP - UNIX UID / GID to user ID or group name
 - ▶ NDSLINK - Novell Directory Services UNAME to user ID
 - ▶ NOTELINK - Lotus Notes (Domino) SNAME to user ID
- **Benefits**
 - ▶ Fewer profiles in the RACF database
 - ▶ Better data integrity in the database
 - ▶ Consistent mappings for shared UIDs or GIDs
 - ▶ Better performance than UNIXMAP profiles
- **Uses new "alias" index structure in the RACF database**
- **Staged migration path for existing databases**

Security Server Network Authentication Service

- **OS/390 and z/OS implementation of MIT's Kerberos Version 5**
- **Provides services for**
 - ▶ USER AUTHENTICATION
 - ▶ DELEGATION
 - ▶ DATA CONFIDENTIALITY
- **Interoperates with other industry Kerberos Version 5 implementations**
- **Can provide consistent user authentication for Kerberos-aware applications spanning a network including OS/390, z/OS, Windows 2000, UNIX, OS/400**

Security Server Network Authentication Service...

- **RACF support for the server includes:**
 - ▶ Definition of local Kerberos principals (users) with KERB segment
 - ▶ Definition of the local Kerberos realm & foreign realms with the REALM class
 - ▶ Definition of foreign Kerberos principals with a local identity with KERBLINK profiles
 - ▶ Basically, the RACF database ***IS*** the kerberos registry
 - ▶ RACF password ***IS*** the user's Kerberos password
- **Server uses SAF callable services to interact with RACF: parse Kerberos tickets to obtain principal names; map from principal to RACF user and the reverse**
 - ▶ R_usermap, R_kerbinfo, R_ticketserv

Automatic UID/GID Assignment

- **Derived values are guaranteed to be unique**

```
RDEFINE FACILITY BPX.NEXT.USER
```

```
    APPLDATA( starting uid / starting gid)
```

```
RDEFINE FACILITY BPX.NEXT.USER APPLDATA(uid range / gid range)
```

```
RDEFINE FACILITY BPX.NEXT.USER APPLDATA(uid range / NOAUTO)
```

```
RDEFINE FACILITY BPX.NEXT.USER APPLDATA(NOAUTO / starting gid)
```

- **Commands**

```
ADDUSER user1 OMVS( AUTOUID )
```

```
IRR52177I User user1 was assigned an OMVS UID value of 4646.
```

```
ADDGROUP group1 OMVS( AUTOGID )
```

```
IRR52177I Group group1 was assigned an OMVS GID value of 10.
```

- **Available on OS/390 V2R10 through z/OS V1R3 via SPE APAR OW52135**

- ▶ PTF UW89970 (OS/390 V2R10, z/OS V1R1)
- ▶ PTF UW89971 (z/OS V1R2)
- ▶ PTF UW89972 (z/OS V1R3)

z/OS Security Server Release 2

Universal Groups

- Goal: You want to connect many (say, 10K) users to a group
- Problem: RACF limits you to 5957 users per group
- Solution: Universal groups

ADDGROUP xyz UNIVERSAL

- Can have an unlimited number of regular users (USE authority)
- Limit to 5957 still applies to users with more privilege
 - ▶ Users with CREATE, CONNECT, or JOIN in the group
 - ▶ Users with group-SPECIAL, group-OPERATIONS, or group-AUDITOR
- Available only for ADDGROUP, not ALTGROUP

Universal Groups...

CONNECT user1 GROUP(xyz) AUTH(use)

- Updates user1 USER profile to show a connection to xyz
- Does not update xyz GROUP profile

LISTGRP xyz

- Regular users not shown; they are not in the GROUP profile
- Listing would be difficult to use given its size, anyway
- For reporting, use IRRDBU00 output

LISTUSER user1

- Shows xyz as one of the user's groups

RACROUTE REQUEST=VERIFY

- Includes xyz in the ACEE
- Access lists with xyz in them will work as you expect

SAF TRACE

- **Problem diagnosis tool**
 - ▶ Traces RACROUTE's, SAF callable services, and ICHEINTY's
- **Specify requests and address spaces to trace**
 - Trace all RACROUTE REQUEST=AUTH from job xyz

```
SET TRACE( RACROUTE( TYPE(1)) JOBNAME(xyz) )
```

- Trace all ICHEINTY ALTER, ADD, DELETE, RENAME from address space 25

```
SET TRACE( DATABASE(ALTER) ASID(25) )
```

- Trace stored in GTF
- Use IPCS to read the trace
 - GTF USR command

z/OS Security Server Release 3

UNIX File Security Enhancements - RESTRICTED attribute support

- **A restricted user ID must be on a resource's access list before it can have access to the resource.**
- **RESTRICTED attribute is optionally recognized by UNIX**
 - ▶ 'OTHER' bits analogous to RACF profile UACC
- **Default: 'OTHER' bits are checked for all user IDs**
- **Enable file system to recognize the RESTRICTED attribute and bypass 'OTHER' bits**

```
RDEFINE UNIXPRIV RESTRICTED.FILESYS.ACCESS UACC(NONE)
```
- **Permit RESTRICTED user IDs access**

```
PERMIT RESTRICTED.FILESYS.ACCESS CLASS(UNIXPRIV)  
ACCESS(READ) ID(user1)
```

 - ▶ Note: This does not grant access to the file. The ACL (and 'OTHER' bits) are used.

Access Control Lists (ACLs)

- **Defines specific owner/group permission bits for a specific user / group**
- **Enabled**
`SETROPTS CLASSACT(FSSEC)`
- **Created/modified/deleted with UNIX command**
`setfacl`
- **Displayed with UNIX command**
`getfacl`
- **UNIX user must have UID(0), be file owner, or READ access to SUPERUSER.FILESYS.CHANGEPERMS in UNIXPRIV class**
- **Maximum 1024 entries**
 - ▶ type (user or group) and identifier (UID or GID) and permissions(read, write, and execute)
- **Supports inheritance from parent directory**

z/OS Security Server Release 4

Prevention of Shared UID/GID

- **Acts as a system-wide switch to prevent assignment of a UID or GID that is already in use**
- **Only applies to new IDs**
 - ▶ Can use IRRICE to find shared UIDs and GIDs
- **Requires**
 - ▶ Application Identity Mapping (AIM) stage 2 or 3
 - ▶ Requires SPECIAL or READ authority to SHARED.IDS profile in UNIXPRIV class

■ **Commands**

```
RDEFINE UNIXPRIV SHARED.IDS UACC(NONE)
SETROPTS RACLIST(UNIXPRIV) REFRESH
ADDUSER MARCY OMVS(UID(12))
IRR52174I Incorrect UID 12. This value is already in use by BRADY.
ADDGROUP ADK OMVS(GID(46))
IRR52174I Incorrect GID 46. This value is already in use by PATS.
```

- **Non-unique UID/GID can be useful, ex. UID(0) for started task user IDS.**

```
/* special or */
PERMIT SHARED.IDS CLASS(UNIXPRIV) ACCESS(READ) ID(admin1)
ADDUSER server1 OMVS(UID(0) SHARED)
ADDGROUP servgrp OMVS(GID(0) SHARED)
```

Search enhancement for mapped UID/GUIDs

```
SEARCH CLASS(USER) UID(0)
```

```
OMVSKERN
```

```
BPXOINIT
```

```
SUPERGUY
```

```
SEARCH CLASS(GROUP) GID(99)
```

```
RACFDEV
```

```
SEARCH CLASS(USER) UID(1234567)
```

```
ICH31005I NO ENTRIES MEET SEARCH CRITERIA
```

UNIX File Group-Ownership

- UNIX files have an owner (UID) and an owning group (GID)
- Assign from owning group of directory, as before
- Assign from effective GID of user creating the file
- **RDEFINE UNIXPRIV FILE.GROUPOWNER.SETGID**
 - ▶ Directory set-gid on: assign from directory
 - ▶ Directory set-gid off: assign from user

Basic PADS Usability

■ Suppose

- ▶ User runs program ABC
- ▶ You want to allow READ to ABC.DATA from program ABC
- ▶ However, ABC invokes ABC2, and ABC2 does the OPEN

■ Previously

```
RDEFINE PROGRAM ABC* ADDMEM('ABC.LINKLIB'//NOPADCHK)
PERMIT ABC.DATA ID(*) ACCESS(READ) WHEN(PROGRAM(ABC2))
```

■ New alternative

```
RDEFINE PROGRAM ABC* ADDMEM('ABC.LINKLIB'//NOPADCHK)
PERMIT 'ABC.DATA' ID(*) ACCESS(READ) WHEN (PROGRAM(ABC))
```

■ Benefits

- ▶ Administrator needs less knowledge about application structure
- ▶ Less chance for error

■ Better security

```
PERMIT 'SYS1.LINKLIB' ID(SYSPROG) ACCESS(UPDATE)
WHEN (PROGRAM(GIMSMP))
```

Program Security Modes

■ Two modes of operation

- ▶ Basic mode (original/default)

```
RDEFINE FACILITY IRR.PGMSECURITY APPLDATA('BASIC')
```

- ▶ Enhanced mode (better security - PADS and EXECUTE work only from programs defined as MAIN)

```
RDEFINE FACILITY IRR.PGMSECURITY APPLDATA('ENHANCED')
```

- ▶ Enhanced warning mode

```
RDEFINE FACILITY IRR.PGMSECURITY
```

■ Three types of programs

- ▶ MAIN

```
RDEFINE PROGRAM xyz ... APPLDATA('MAIN')
```

- ▶ BASIC

```
RDEFINE PROGRAM XYZ ... APPLDATA('BASIC')
```

- ▶ normal

```
RDEFINE PROGRAM XYZ ...
```

■ You still need to keep environment clean!

Program Security Modes...

■ Example

```
// EXEC PGM=AAA  
TSOEXEC AAA
```

▶ where

- AAA OPENS AAA.DATA and you want to use PADS to allow this access; or
- AAA calls AAA2, and AAA2 OPENS AAA.DATA and you want to use PADS

■ Setup from ENHANCED MODE and AAA is MAIN

```
RDEFINE FACILITY IRR.PGMSECURITY APPLDATA('ENHANCED')  
RDEFINE PROGRAM AAA ADDMEM('library.name'//NOPADCHK)  
APPLDATA('MAIN')
```

■ Setup from ENHANCED MODE and AAA or AAA2 is BASIC

```
RDEFINE FACILITY IRR.PGMSECURITY APPLDATA('ENHANCED')  
RDEFINE PROGRAM AAA ADDMEM('library.name'//NOPADCHK)  
APPLDATA('BASIC')
```

■ Note: Setup slightly different when AAA invoked from TSO READY, ISPF, or via TSO/E CALL command

Reminder: Service End Dates

- **Out of service**
 - ▶ All OS/390 Releases V2R9 and below

RACF Home Page

- **<http://www.ibm.com/servers/eserver/zseries/zos/racf/>**
 - ▶ Latest release information on RACF
 - ▶ Links to announcement letters
 - ▶ Sample code
 - ▶ Frequently asked questions
 - ▶ RACF user group information
 - ▶ RACF-L information
 - ▶ Presentations on RACF-related topics