SecureWay Security Server for OS/390 Update 9/13/2000

Walter B. Farrell
SecureWay Security Server for OS/390 Design
(845) 435-7750
wfarrell@us.ibm.com

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 environmenst.

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:
  - IBM, CICS, DB2, OS/390, RACF, SecureWay, S/390
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Other company, product, and service names may be trademarks or service marks of others.

What's New in Release 6?

- User Administration Enhancements
- SETROPTS and RVARY Support in SMF
- Web Browser Enhancements
- GTF Trace Facility
- UNIX System Services Multi User/ Multi Proc
- and a bit more .....

User Administration Enhancements

- **Ability for authorized users to reset passwords, resume userids and list profiles for others without being given "special" authority**
- **Allows greater granularity of control. Does NOT override current authorization mechanisms such as system-special, owner, group-special.**
- **Allows authorized administrator to set a new non-expired password for a user using ALTUSER ... NOEXPIRED**

User Administration Enhancements ..... continued

- **Controlled by FACILITY Class Profiles :**
  - IRR.PASSWORD.RESET
    - READ Access - Reset password to expired value and ability to resume a user.
    - UPDATE Acess - May reset password to a non-expired value and resume a user
  - IRR.LISTUSER
    - READ Access - May list other's user profiles via LISTUSER, base segment subject to FLAC
- **This support is rolled back to OS/390 Rel. 3 along with other callable services changes in support of TIVOLI Roles Based Administration Enhancements by APAR OW26060. See SYS1.SAMPLIB(IRR26060)**

IRRADU00 Processing of 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

UNIX System Services Multi-User/Multi-Proc

- Provides security for multiple users in an address space containing multiple UNIX processes.
- Allows customers to more easily port applications to the OS/390 environment.
- Provides an option on the initACEE callable service to prevent cached ACEEs from timing out.
- Provides a new audit function code via SMF Type80 record to allow auditors a full audit trail to determine when a user is a superuser and who that user is.

Misc. Improvements

- **GTF Trace Facility (R3 and R4) :**
  - Provide a mechanism to capture and format trace information for some RACF Callable Services.
  - Simplify and speed up diagnostic work with L2 Service Support using trace records and IPCS formatting support to save customer and L2 debugging time.
- **Web Browser Enhancements:**
  - Transportable ACEEs - Easier retrieval, construction and transportation of security environments across Address Spaces and members of a sysplex.
  - Optimized CDT Search Algorithm

Misc. Improvements, continued

- **Exploitation of DB2 Enhancements for IRRDBU00 and IRRADU00 --> DB2 - load statements and for IRRDBU00 - indices for USER_GROUPS and USER_CONNECT_DATA shipped in SAMPLIB .**

What's New in Release 8 ?

- **Protected Userids**
- **OS/390 UNIX SS Superuser Granularity**
- **OS/390 UNIX SS User Limits**
- **Extensions to DB2 Support**
- **Digital Certificate Enhancements**

PROTECTED USERIDs

- **Allows a user to be defined to RACF that :**
  - may NOT be used to logon to TSO
  - may NOT sign on to CICS
  - may NOT rlogin from a workstation etc.
- **Protects userids assigned to OS/390 UNIX, UNIX daemons and other important started tasks and subsystems :**
  - from being used for other unintended purposes
  - from being REVOKED for invalid password attempts
  - helps prevent these IDs from being misused if administrator forgets to change password from a default group value

PROTECTED USERIDs .....

- **implemented through the use of NOPASSWORD on ADDUSER and ALTUSER**
- **LISTUSER ouput now displays "PROTECTED" for these users**
- **new field in the ACEE indicates that the protected userid may NOT enter the system with a password , nor by any means that normally requires a password**
- **changes to RACF panels, utilities such as database unload etc. were made**

UNIX System Services 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. Issue the commands:
    - RDEFINE UNIXPRIV SUPERUSER.FILESIZE.MOUNT UACC(NONE)
    - PERMIT SUPERUSER.FILESYS.MOUNT CLASS(UNIXPRIV) ID(LAURIE) ACCESS(UPDATE)
    - SETR CLASSACT(UNIXPRIV) RACLIST(UNIXPRIV)
  - Other uses : allow a user to read or write to any HFS file, send signals to any process, view all processes, issue chown for their own files

UNIX System Services User Limits

- **Allow selected users to exceed resource limits in the BPXPRMxx member of PARMLIB without UID 0.**
  - Useful for server and daemon user IDs
- **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 MAXCPUTIME parameter of BPXPRMxx.**
  - ALTUSER UNIXUSR OMVS(CPUTIMEMAX(5000))
  - Other uses : override maximum address space size, number of files per process,number of processes per UID, number of threads per process, memory map size

Extensions to existing DB2 Support

- **New Function SPE for the RACF component of the Security Server to support DB2 Version 6**
- **Four new DB2 resources**
  - User Defined Distinct Type
  - User Defined Function
  - Stored Procedure
  - Schemas
- **TRIGGER privilege added to existing TABLE resource**
- **New RACF member & grouping classes for each new resource**
- **Updates to IRR@XACS to allow installations to control access to these DB2 V6 functions through RACF**

Digital Certificate Background

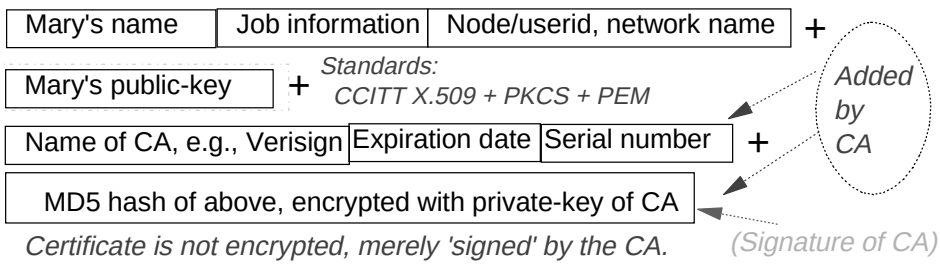
- **What is a digital certificate?**
  - **Data token which contains a public key, user information, and an endorsement of the validity of the certificate**
  - **Basis for the distribution of public keys**
  - **Certificate endorsement is done by Certificate Authorities**
  - **Certificate validation is done using public key technology**
  - **Certificates are managed by users**

Digital Certificate Background...

Mary

Certifying Authority (CA)

Mary's Digital Certificate looks about like this.



Digital Certificate Background...

- In OS/390 V2R4 RACF could map a user certificate to the appropriate user ID
  - ►Administrator used RACDCERT command to create the association
  - ►Used DIGTCERT class to contain user's certificate data
- Enhancements in V2R4 allowed users to register their own certificates via a web browser in a controlled way
- IBM HTTP server could accept a certificate via SSL, map it to a user ID using initACEE, and run work using that user ID.

Digital Certificate Enhancements...

- In OS/390 V2R8, new RACDCERT functions allow :
- The generation of certificates and certificate requests
- The definition of certificate authority (CERTAUTH) and site (SITE) certificates.
- The aggregation of certificates into key rings
- The importation of PKCS-12 certificates
- The renaming of the LABEL that is associated with a certificate
- New RACF callable service to retrieve certificate information
- New RACF database unload (IRRDBU00) and modified RACF SMF unload (IRRADU00) records
- BLKUPD allows the specification of mixed case ENTRY

Creating Certificates

- The RACDCERT GENCERT function creates a public/private key pair and a digital certificate.
- X.509-style keywords are used to specify certificate information, such as:
  - ►Subject's distinguished name
    - –Default: User's name
  - ►Certificate validity dates (start date/time & end date/time)
    - –Default: Current date as start, one year from start date as the end date
  - ►Size of key
    - –Range: 512-1024; Default: 1024
  - ►Signature
    - –Default: Self Signed

Key Rings

- Certificates are collected into sets called key rings. Key facts about key rings:
  - ►Each key ring is associated with an OS/390 user ID.
  - ►User IDs may have more than key ring.
  - ►CertAuth and Site certificates are associated with the "reserved" user IDs "irrcerta" and "irrsitec"
  - ►Key rings are identified by a 1 to 237 character ring name
- Authority to manage key rings may be distributed. However, the system security administrator has the ability to define the superset of key ring contents.

Key Rings, continued

- Without RACF key ring support:
  - Key rings contained in application data files
    - private keys may be exposed
  - Application installer determines which certificate authorities to trust
- However, with RACF key ring support:
  - Key rings stored more-securely in RACF database
    - private keys may be secured using ICSF and hardware crypto
  - Security Administrator determines which certificate authorities to trust

A word about irrcerta, irrsitec, and irrmulti

- The two special user IDs "irrcerta" and "irrsitec" are anchor points for certificate authority certificates and site certificates respectively. Also, "irrmulti" provides an anchor for name-filtering rules. Key points about these IDs:
- They are marked as REVOKED in the RACF data base
- RACROUTE REQUEST=VERIFY requests fail for these user IDs as they have no default group
- ADDUSER, DELUSER, and LISTUSER may not be used against these specific IDs.
- The SEARCH command for CLASS(USER) will return these user IDs if they fall within the SEARCH criteria
- ICHEINTY NEXT and RACROUTE EXTRACTN processing will return these IDs if they match the selection criteria

More about irrcerta, irrsitec, and irrmulti

- RACF initialization creates these IDs during first IPL
- If in a sysplex with RACF DATASHARING active, either:
  - switch DATASHARING off via RVARY NODATASHARE before IPLing first R8 system into an active sysplex, and then use RVARY DATASHARE after that IPL completes; or
  - ensure you have the fix for APAR OW43284 installed

Changes to RACDCERT Processing

- Changes to RACDCERT ADD
  - SITE and CERTAUTH certificates may now be added.
  - Replacement certificates may be added
  - PKCS#12 "certificate packages" (which contain a private key) are now supported and may be RACDCERT ADDed
- Changes to RACDCERT CHECKCERT
  - SITE and CERTAUTH certificates may now be CHECKCERTed
  - CHECKCERT now reports if a certificate is defined as a certificate authority certificate or a site certificate; This is done only after checking IRR.DIGTCERT.LIST in the FACILITY class
  - CHECKCERT may now be used to check a PKCS#12 certificate package

Changes to RACDCERT Processing...

- **Changes to RACDCERT ALTER:**
  - **SITE and CERTAUTH certificates may now be ALTERed**
  - **ALTER now supports the altering of the label of a certificate through the use of the LABEL and NEWLABEL keyword**
- **Changes to RACDCERT DELETE:**
  - **SITE and CERTAUTH certificates may now be DELETEd**
- **Changes to RACDCERT LIST:**
  - **SITE and CERTAUTH certificates may now be LISTed**
  - **LIST now displays information about the private key (type and size**

RACDCERT List

- **Sample Output**

```
Digital certificate information for user GEORGEM:

  Label: New Cert Type - Ser # 00
  Status: TRUST
  Start Date: 1996/04/18 03:01:13
  End Date:   1998/02/13 03:01:13
  Serial Number:
       >00<
  Issuer's Name:
       >OU=Internet Demo CA.O=Xcert Software Inc.<
  Subject's Name:
       >OU=Internet Demo CA.O=Xcert Software Inc.<
  Private Key Type: ICSF
  Private Key Size: 1024

Ring Associations:
  Ring Owner: GEORGEM
  Ring:
     >GEORGEMsNewRing01<
  Ring Owner: GEORGEM
  Ring:
     >GEORGEMsRing<
```

ICSF Considerations

- IBM recommends the use of the S/390 Integrated Cryptographic Support Facility (ICSF) for the storage of private keys.
- ICSF ensures that the user's private key is stored within ICSF, encrypted under the ICSF master key for the installation
- If the RACF database is shared among systems, then all of the ICSFs must have the same master key
- Master keys may be managed using the Trusted Key Entry (TKE) workstation
- ICSF is not required; it is used if available (and configured) and explicitly requested on RACDCERT
- If ICSF is not being used, BSafe (software encryption) is used

ICSF Considerations...

- ICSF-stored private keys are requested by using the "ICSF" keyword on RACDCERT GENCERT and RACDCERT ADD.
- Non-ICSF-managed private keys may be moved into ICSF storage by:
  - ►RACDCERT EXPORTing the certificate to a data set and then
  - ► Re-ADDing the certificate specifying the "ICSF" keyword.
    - – Since the subject's distinguished name, public key, and issuer's distinguished name are the same, RACF replaces the certificate, and migrates the private key to ICSF
- Note that the reverse process is not possible.

RACDCERT Authority Checking

- **Users with SPECIAL authority can perform all functions.**
- **For everyone else, authority checks are performed using FACILITY resources IRR.DIGTCERT.<function>. The authority required to this resource is:**
  - **READ to perform the function on their own certificate or key ring,**
  - **UPDATE to perform the function on the certificate or key ring of another, and**
  - **CONTROL to perform the function on a certificate authority or site certificate.**

Authority Checking Summary

Function	READ	UPDATE	**CONTROL**
ADD	Add a cert to one's own user ID **(also to GENCERT for self)**	Add a cert to someone else's ID **(also to GENCERT for someone else)**	**Add or GENCERT a SITE or CERTAUTH certificate**
ALTER	Change the trust status or label of one's own cert	Change the trust status or label of someone else's cert	**Change the trust status or label of a SITE or CERTAUTH cert**
DELETE	Delete one's own cert	Delete someone else's cert	**Delete a SITE or CERTAUTH cert**
EXPORT	**Export one's own cert**	**Export someone else's cert**	**Export a SITE or CERTAUTH cert**
GENCERT	**Generate any cert, signed with own cert; or for self if SIGNWITH not used**	**Generate cert for another user, if SIGNWITH not used**	**Generate cert for any user, SIGNWITH SITE or CERTAUTH cert; or generate cert for SITE or CERTAUTH, if SIGNWITH not used**
GENREQ	**Generate a request based on one's own cert**	**Generate a request based on someone else's cert**	**Generate a request based on a SITE or CERTAUTH cert**
LIST	List one's own cert	List the someone else's cert	**List a SITE or CERTAUTH cert**

BOLD indicates new with Release

Authority Checking Summary...

Function	READ	UPDATE	CONTROL
ADDRING	Create a key ring for one's own ID	Create a key ring for someone else's ID	N/A
CONNECT	Place ones own certificate in one's own ring	Place a CERTAUTH or SITE cert in one's own ring	Place a certificate into someone else's ring
DELRING	Delete one's own key ring	Delete someone else's key ring	N/A
LISTRING	List one's own key ring	List someone else's key ring	N/A
REMOVE	Remove a certificate from one's own key ring	Remove a SITE or CERTAUTH certificate from one's own key ring	Delete a certificate from the ring of another

BOLD indicates new with Release 8

Changes to IRRDBU00 Output

- **Record type 0560 ("Certificate Data Record") is now unloaded. This record contains:**
  - **Start and end dates and times for the certificate**
  - **The type of private key associated with the certificate. Valid values are PKCSDER, ICSFTOKN, NONE, and UNKNOWN**
  - **The size of the private key, expressed in bits**
  - **The hexadecimal representation of the 8 byte serial number of the last certificate signed with this key**
  - **The ring sequence number**
- **RACDBUTB and RACDBULD have been updated in 'SYS1.SAMPLIB'**

Changes to SMF Records

- Type 80, Event code 66, Relocate section 6:
  - new RACDCERT keywords and values
- Eight new relocate sections have been created:
  - 320: Ring name
  - 321: SUBJECTSDN country value ("C")
  - 322: SUBJECTSDN state or province value ("SP")
  - 323: SUBJECTSDN locality value ("L")
  - 324: SUBJECTSDN organization value ("O")
  - 325: SUBJECTSDN organizational unit value ("OU")
  - 326: SUBJECTSDN title value ("T")
  - 327: SUBJECTSDN common name ("CN")

Cryptography Enhancements

- Open Cryptographic Services Facility:
  - OS/390 base component
  - Implements IBM Keyworks (CDSA standard) for OS/390
  - Provides framework for base set of cryptographic functions
    - encrypt, decrypt, generate keys, etc.
  - Allows Service Provider Modules to "plug-in" to perform functions
- Open Cryptographic Enhanced Plug-ins:
  - New component of SecureWay Security Server for OS/390
  - Provides plug-ins to implement Data Library and Trust Policy functions for OS/390
  - Uses certificates and key rings stored in RACF

New RACF Callable Service: IRRSDL00

- For use in implementing the Data Library (DL) functions in Open Cryptographic Enhanced Plug-ins
- IRRSDL00 is a key-8, non-APF, problem state programming interface allowing retrieval of certificates and keys
- Access to IRRSDL00 functions are controlled by checks against the IRR.DIGTCERT.<function> resources in the FACILITY class
  - ►READ to IRR.DIGTCERT.LISTRING to read one's own keyring
  - ►UPDATE to IRR.DIGTCERT.LISTRING to read someone else's keyring
- The private key or private key label that is associated with the certificate may not be retrieved unless the execution user ID is equal to the user ID that is associated with the certificate.

Exploiters of RACF Certificates

- Client support only:
  - ►IBM HTTP Server
  - ►CICS
- Client support and server support through System SSL:
  - ►LDAP
  - ►Host on Demand
- Server support using Open Cryptographic Enhanced Plug-ins:
  - ►Firewall Technologies

What's New with OS/390 V2R9 ?

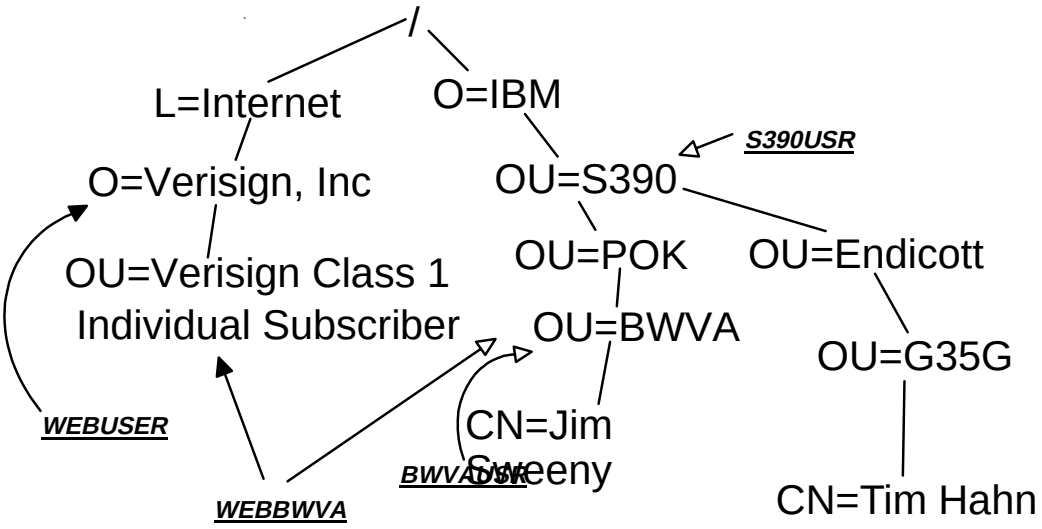
- Certificate Name Filtering
- Restricted User IDs

Certificate Name Filtering (CNF)

- IBM investment in Public Key, Digital Certificate Technology in RACF continues .....
- Usability and Functional Enhancement to RACF Digital Certificate Support
  - ►Certificate used to have to be installed in RACF for each user, can now use profiles based on issuer's and subject's distinguished names to choose the userid to assign for a particular certificate
  - ►With CNF - Greater accountability/audit capabilities
  - ►Greater granularity of access control
  - ►Easier maintenance of expired certificate processing
- OW40129 - Shipped in R9 timeframe on R8 and R9 along with accompanying SAF apar

Examples

X.500 Directory Information Tree (DIT) , example:



X.500 Distinguished Names. . .

- **Hypothetical certificates containing:**
  - **Subject Name - CN=Jim Sweeny.OU=BWVA.OU=POK.OU=S390.O=IBM**
  - **Issuer Name - OU=Verisign Class 1 Individual Subscriber.O=Verisign, Inc.L=Internet**
  - **Subject Name - CN=Tim Hahn.OU=G35G.OU=Endicott.OU=S390.O=IBM**
  - **Issuer Name - OU=Verisign Class 1 Individual Subscriber.O=Verisign, Inc.L=Internet**

Solution (Part A)

- **Subject and Issuer Name Filtering**
  - **Create DIGTNMAP class and profiles to...**
    - **Assign UserID based on Subject's placement in DIT**
    - **Assign UserID based on Issuer's Name**
    - **Assign UserID based on both the Subject's placement in DIT and full Issuer's Name**
  - **Profile form: subject-filter<delimiter>issuer-filter**
    - **New field FLTRUSER contains UserID**

Solution (Part B)

- **Additional Criteria For UserID Determination**
  - **Allow a given name filter to map to multiple UserIDs**
  - **Actual UserID determined by system and/or user variables (APPLID, SYSID, and new InitACEE variable list parameter)**
    - **FLTRUSER contains profile template containing variable names**
    - **Variable values substituted to form real profile name**
    - **Get UserID from APPLDATA field of new DIGTCRIT Class profile**

InitACEE Processing

- Do old style certificate lookup first
- If not found search for Map profiles more specific to least specific:
  1. Iteratively-shrinking-subject-name with full-issuer-name
  2. Iteratively-shrinking-subject-name alone
  3. Iteratively-shrinking-issuer-name alone
- Get UserID from FLTRUSER of first match

Access Control / Auditing

- InitACEE CREATE would save full Subject's and Issuer's name off ACEE
  - ►New RACROUTE VERIFY parameter, X500NAME
- InitACEE QUERY may return X500NAME in addition to UserID
  - ►CICS does their own RACROUTE VERIFY
- RACHECK Exit can retrieve X500NAME
- Subject's and Issuer's names recorded on every audit record (max 255 bytes each)

RACDCERT Command Syntax

```
RACDCERT [ID(user-id) | MULTIID]
  MAP [('cert-dsn')]
    [SDNFILTER('subject-dist-name-filter')]
    [IDNFILTER('issuer-dist-name-filter')]
    [CRITERIA('criteria-profile-name-template')]
    [WITHLABEL('label-name')]) [TRUST | NOTRUST]

  LISTMAP (LABEL('label-name'))

  ALTMAP (LABEL('label-name'))
    [NEWCRITERIA('criteria-profile-name-template')]
    [NEWLABEL('label-name')] [TRUST | NOTRUST]

  DELMAP (LABEL('label-name'))
```

RACDCERT Authority Checking (R9)

Function	READ	UPDATE
MAP	Create a mapping associated with one's own ID	Create a mapping associated with another ID or MULTIID
ALTMAP	Alter a mapping associated with one's own ID	Alter a mapping associated with another ID or MULTIID
DELMAP	Delete a mapping associated with one's own ID	Delete a mapping associated with another ID or MULTIID
LISTMAP	List mapping info associated with one's own ID	List mapping info associated with another ID or MULTIID

Restricted User IDs

- **Makes use of shared or PUBLIC user IDs safer**
- **Enhancements to ADDUSER, ALTUSER, LISTUSER**
  - **ADDUSER xxx RESTRICTED**
  - **ALTUSER xxx RESTRICTED | NORESTRICTED**
- **RESTRICTED: Ignore UACC, ID(*), and GLOBAL when performing access checks**
- **Available on OS/390 V2R8 or V2R9 via APAR OW40129**

But Wait, there's still more... What's New in Release 10?

- **SecureWay Security Server for OS/390 RACF:**
  - PROGRAM Control Usability Enhancements
  - Application Identity Mapping
  - Digital Certificate Enhancements
- **SecureWay Security Server for OS/390:**
  - Network Authentication and Privacy Service (New)
  - LDAP Server Enhancements
- **IBM Communications Server:**
  - Network Security and Usability Enhancements

Program Control Usability

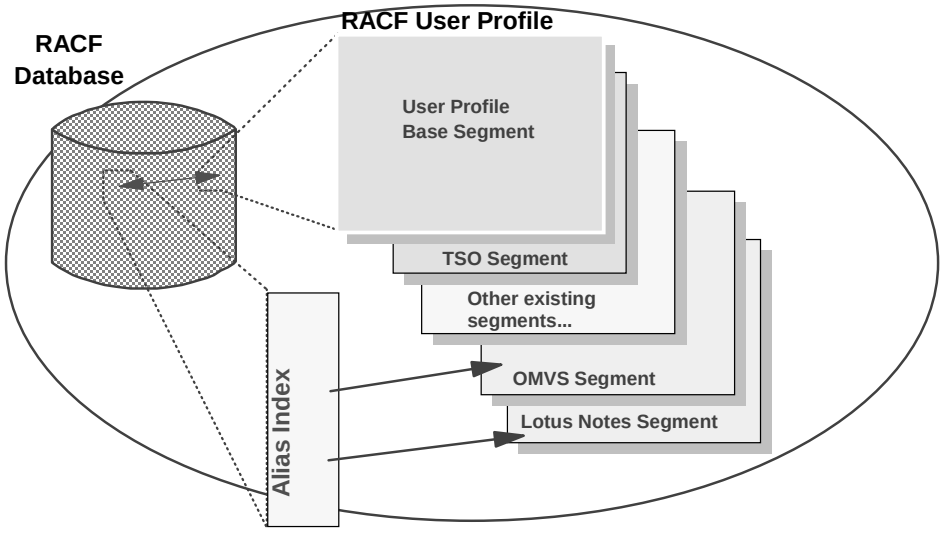
- New diagnostic messages when functions requiring "clean" environment (PADS, execute-control, UNIX server / daemon) fail
  - ►Messages will state that failure occurred because of "dirty" environment
  - ►Messages will give the reason environment became dirty
    - –module name, library name, etc.
  - ►Example: ICH420I PROGRAM PAYROL5 FROM LIBRARY SYS2.PAYLIB CAUSED THE ENVIRONMENT TO BECOME UNCONTROLLED.
- New RACROUTE REQUEST=AUTH reason code to inform ICHRCX02 that the request would have worked except for dirty environment
- Should greatly reduce the need for GTF tracing for Program Control and PADS problems.

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
- Should
  - ►reduce size of RACF database by eliminating the profiles
  - ►provide better data integrity in the database
  - ►provide consistent mapping for shared UIDs or GIDs
  - ►provide better performance than UNIXMAP profiles
- Uses new "alias" index structure in RACF data base

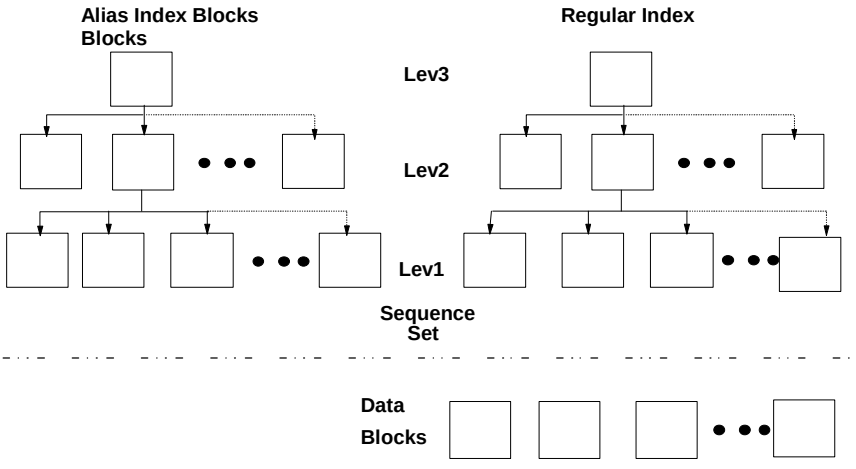
Alias Index Structure...

Conceptual View



Alias Index Structure...

- Alias IX blocks, are similar to regular IX blocks at upper levels. In the Sequence Set, instead of pointers to data profiles, Alias IX entries contain base profile info.



Digital Certificate Enhancements

- RACF enhancements to RACDCERT and initACEE
- RACDCERT certificate generation
  - Support for KeyUsage extension: handshake, dataencrypt, docsign, certsign
  - Support for subjectAltName extension: IP address, Domain name, EMAIL address, URI
  - New certificate export format, PKCS12. Packages certificate chain and user's private key to allow generation of client certificates and standard usage by web browsers.
  - Ability to mark Certifying Authority (CA) certificate as "highly trusted"
- initACEE enhancement:
  - Can accept an optional Host-ID-Mapping extension in a certificate and assign a user ID based on that extension
    - Only from highly trusted Certifying Authorities
  - Provides 3rd mechanism for assigning user ID given a certificate

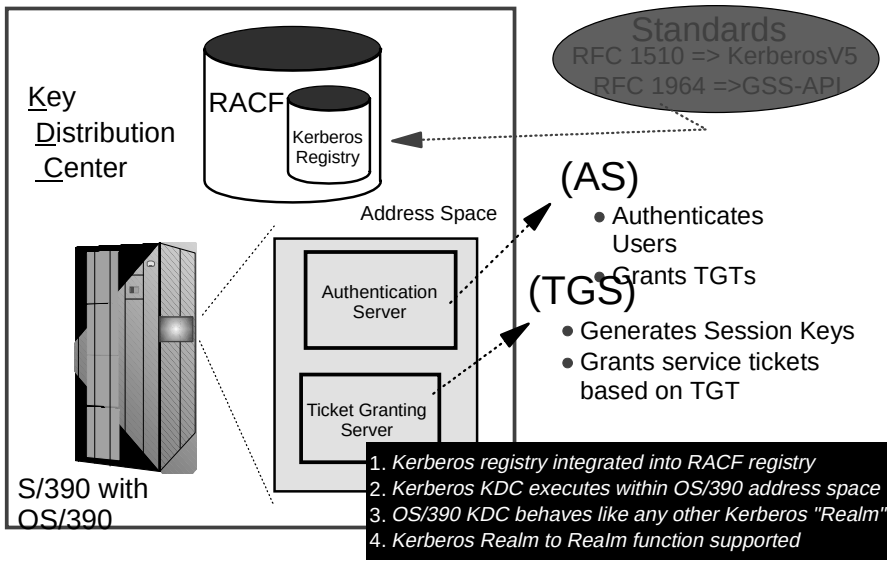
Network Authentication & Privacy Service

- New Security Server component
  - licensed with OS/390 base, for all OS/390 customers, like the LDAP server
  - requires RACF support or compatible other security product
- OS/390 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, e.g. OS/390, Windows 2000, UNIX, AS/400

Network Authentication & Privacy Service...

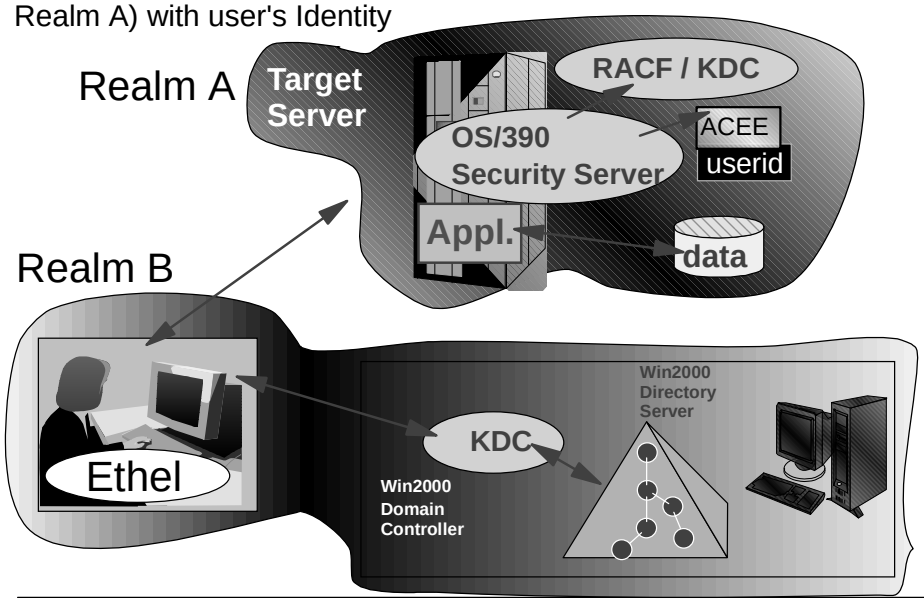
- **RACF provides support for the server:**
  - **definition of local Kerberos principals (users)**
    - **KERB segment**
  - **definition of the local Kerberos realm& foreign realms**
    - **REALM class**
  - **definition of foreign Kerberos principals with a local identity**
    - **KERBLINK profiles**
  - **Basically, the RACF database *IS* the Kerberos registry for OS/390**
  - **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 vice versa**
  - **Enhanced R_usermap service**
  - **new R_kerbinfo service**
  - **new R_ticketserv service**

Network Authentication & Privacy Service...



Network Authentication & Privacy Service Example

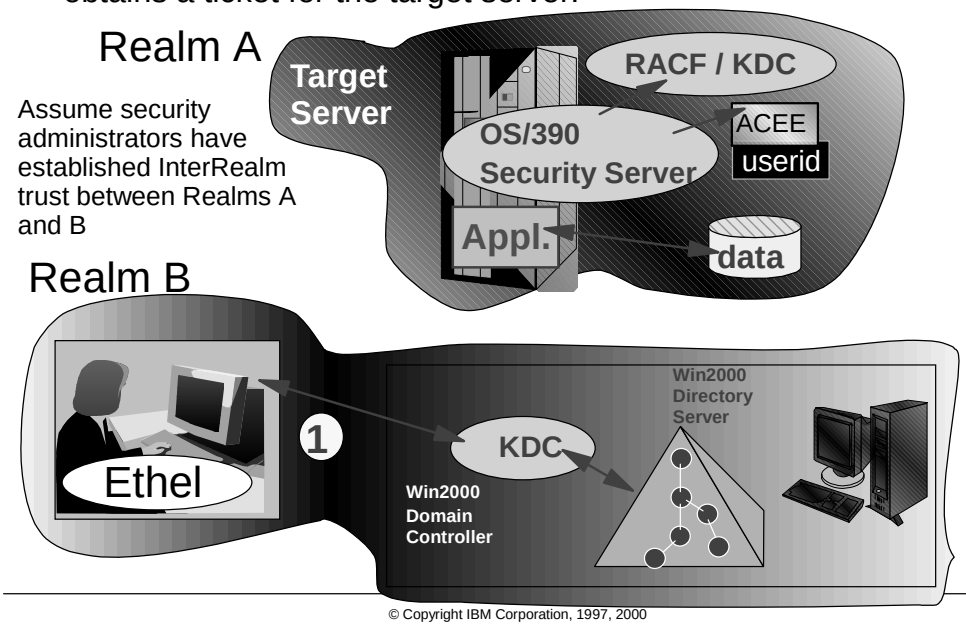
Scenario: User defined to Win2000 Active Directory (Kerberos Realm B) wishes to access application on OS/390 (kerberos Realm A) with user's Identity



Network Authentication & Privacy Service Example...

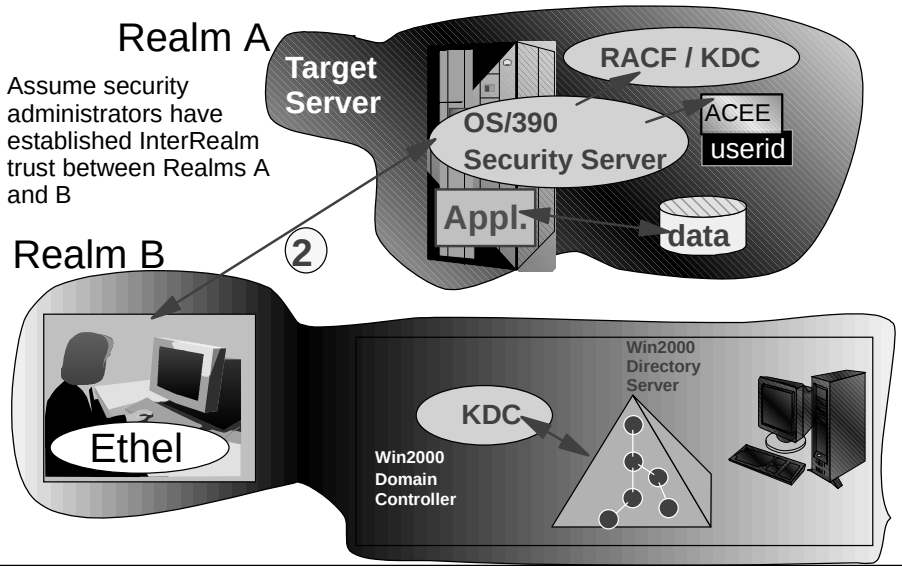
1- The client authenticates to the Win2000 KDC, and obtains a ticket for the target server.

Assume security administrators have established InterRealm trust between Realms A and B



Network Authentication & Privacy Service Example...

2- On OS/390, target application using SAF services, validates the ticket, and if necessary, via SAF / RACF maps the Kerberos principal contained in the ticket to an OS/390 User ID.



LDAP Server Enhancements

- **Enhancements for customer (not RACF) data in LDAP**
- **LDAP V3 Schema Publication and Update**
  - **Better interoperation with other LDAP V3 servers on other platforms**
  - **Allows administrators to dynamically add and modify LDAP schema describing their information**
  - **Eliminates server restart after changing schema**
  - **Allows LDAP clients to query the schema definition using LDAP**
- **Bulk load utility**
  - **Allows loading of large numbers of directory entries into the server**
  - **Eases migration of data from other platforms to OS/390**
  - **Eases migration of data from test into production**
- **Greatly increased storage capacity**
  - **Single server can manage millions of directory entries across multiple DB2 databases**

Network Security and Usability

- Functions provided by IBM Communications Server for OS/390
- TN3270E Server SSL enhancements
  - Implements SSL negotiation based on enterprise security policy
  - Can force use of SSL basede on IP address, hostname, or link
  - Allows use of same port for SSL and non-SSL, simplifying server and client configuration
- TCP/IP protection of network resources
  - Controls OS/390 users' access to
    - TCP/IP stack
    - TCP or UDP port
    - Network
  - Uses profiles in the SERVAUTH class
  - Allows grouping of network IP addresses into a "security zone" that you can protect as a RACF resource.

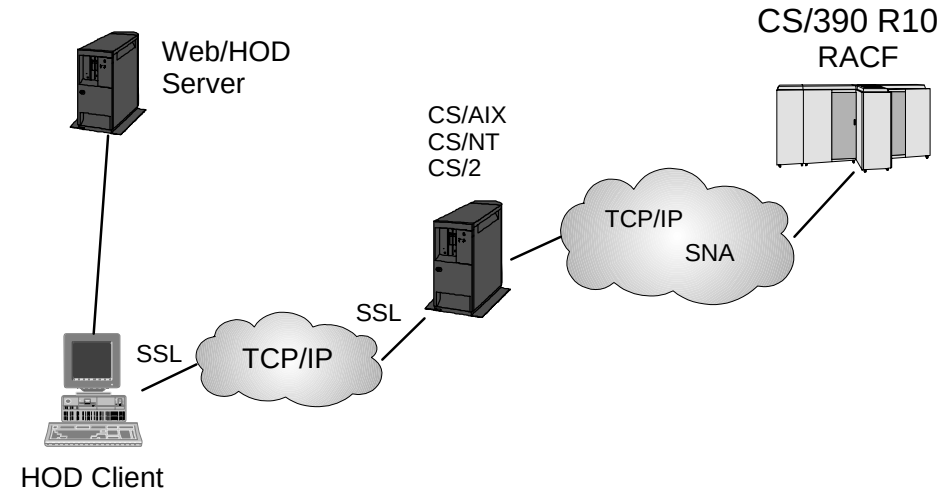
Network Security and Usability ...

- Virtual Private Network "On-Demand" Tunnels
  - Tunnel: An encrypted data pipe from one system to another
  - Before OS/390 V2R8: configured manually by the administrator
  - With OS/390 V2R8: dynamic configuration (key exchange) possible
    - clients could request creation of tunnel for data sent to OS/390
    - or administrator could manually create one for data sent from OS/390
  - New support: Policy can cause automatic creation of tunnels for data sent from OS/390, too.

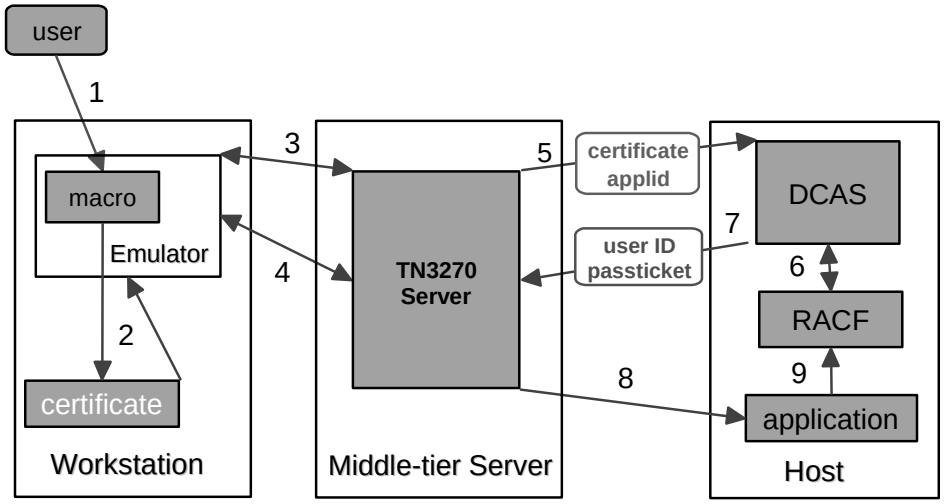
Network Security and Usability ...

- **Digital Certificate Access Server (DCAS)**
  - **Part of Express Logon solution**
  - **Allows TN3270 client with X509 V3 Certificate to logon to SNA application without specifying user ID or password**
  - **Currently requires:**
    - **Host on Demand V5.0 TN3270 Client**
    - **Middle tier TN3270 Server CS/2, CS/NT, CS/AIX**
  - **Exploits RACF certificate technology including key rings, system SSL, and PassTickets**

Network Security and Usability ...



Network Security and Usability ...



Summary

- **Digital certificates are the backbone of the security for e-business arena applications**
- **RACF's support for server-side digital certificates is a natural evolution of the existing RACDCERT support for client certificates, providing:**
  - ►Confidentiality of private keys
  - ►An implementation of key rings that allows central control and easier management of the security policy
  - ►Callable service support which enables CDSA-support (OCSF) for the RACF-managed certificate data by applications
- Continued investment in functionality and ease of use is essential

Reminder!

Service End Dates

Reminder: Service End Dates

- **March 31, 2001:**
  - RACF V2 and MVS/ESA V5
  - OS/390 V1 (including Security Server components)
  - OS/390 V2R4 (including Security Server components)
  - OS/390 V2R5 (including Security Server components)
- **Announcement Letter 900-040 (March 7, 2000) contains the details**

References

- RACF Command Language Reference (SC28-1919)
- RACF Macros and Interfaces (SC28-1914)
- RACF Security Administrator's Guide (SC28-1915)
- RACF Auditor's Guide (SC28-1916)
- RACF Callable Services Guide (SC28-1921)
- OS/390 Security Server Open Cryptographic Enhanced Plug-ins (OCEP) Guide and Reference (SA22-7429)
- OS/390 OCEP Module Developer's Guide and Reference (SC24-5876)
- OS/390 OCEP Application Developer's Guide and Reference (SC24-5875)
- OS/390 Security Server LDAP Server Administration and Usage Guide (SC24-5861)
- OS/390 Security Server LDAP Client Application Development Guide and Reference (SC24-5878)

References...

- Or on the web, in either PDF or Book Manager formats:
  - ►http://www.ibm.com/s390/os390/bkserv/

RACF Home Page

- **http://www.ibm.com/s390/racf/**
  - Latest release information on RACF
  - Links to announcement letters
  - Sample code
    - ►DBSYNC to compare/sync. two RACF data bases
    - ►RACFICE to create audit/analysis reports
    - ►OS390ART for a web-based reporting tool
    - ►RACTRACE tracing facility
    - ►RACFDB2 Conversion Utility
  - Frequently Asked Questions
  - RACF user group information
  - RACF-L information
  - Presentations on RACF-related topics

OS/390 Security Home Page

- http://www.ibm.com/s390/security/
  - Overview of security concepts, including animations
  - Overview of S/390 & OS/390 security functions
  - Links to related web sites for OS/390 components

Background Information

Honorable mentions prior to Rel. 4

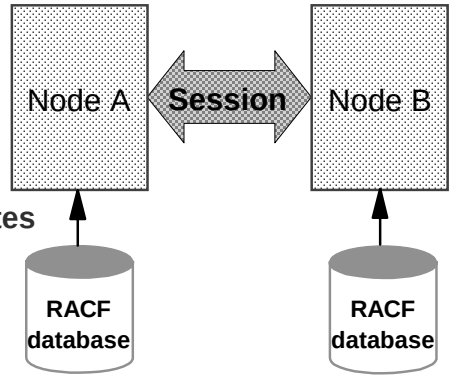
- **RACF RemoteSharing Facility (RACF 2.2)**
- **RACF Command Exit (OS/390 V1R3)**

which are all included in OS/390 Security Server

RACF Remote Sharing Facility

Initial support in RACF 2.2
- **Password synchronization**
- **Command direction**
- **Automatic command direction**
- **Automatic password direction**

New Support in OS/390 V1R3
- **Autodirection of Application updates**
  - ✓**ICHEINTY**
  - ✓**RACROUTE**



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**
- **Code samples provided in 'SYS1.SAMPLIB':**
  - ✓**IRREVX1A: Sample exit showing entry and exit linkages**
  - ✓**IRREVX1B: Sample exit to allow helpdesk users to list user IDs, resume user IDs, and reset passwords ("obsolete")**

What's New in Release 4?

- Password History Enhancement
- Default UID and GID for UNIX System Services
- RACF Control of DB2 Objects
- Support for Digital Certificates
- .... and a few other goodies we've rolled back ....

Generally available 29 September, 1997

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 and GID

- **Pre-release 4, all UNIX System Services users must:**
  - Have a valid UID
  - Have at least a default 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 provide the UID and GID.
    - Access list and UACC are not used

Default UID and GID, Continued

- **Benefits:**
  - Ease of administration without loss of audit trail
- **Usage Note:**
  - Intended for users who really aren't using UNIX services and features.
  - For "real" UNIX users (users of shell, rlogin, etc.) assign individual UIDs and GIDs via OMVS segments

DB2 Security Requirements

- **Provide the ability to control DB2 resources from RACF, specifically the ability to:**
  - Validate auth IDs before granting DB2 authorities
  - Define security rules before object is created
  - Eliminate the ability to define duplicate security rules
  - Preserve security rules for dropped objects
  - Control and audit resources for multiple DB2 subsystems from single point
  - Separate Control rights from Access rights
  - Administer DB2 security with a minimum of DB2 skill
  - Eliminate DB2 cascading revoke
- **Provide an exit point which can control access to DB2 resources**

RACF and DB2 Solution

- **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
  - Exit CSECT Name - DSNX@XAC
  - Exit parameter list - DSNDXAPL
  - DB2 Provides dummy DSNX@XAC routine
  - Available with DB2 5.1
- **RACF - The RACF/DB2 External Security Module**
  - Fully supported exit module designed to receive control from the DB2 Access Control Authorization Exit Point

RACFDB2 Conversion Utility

- **Utility to automate conversion of existing DB2 security authorities to equivalent RACF profiles.**
- **Must have :**
  - SELECT authority to SYSIBM.SYSxxxAUTH table
  - To run utility generated CLIST --> RACF-special or CLAUTH and either OWNER of new profiles or within scope of group to which you have Group-Special
  - Add-on for REXX/TSO from IBM called RXSQL, or DB2 V6 or refreshed DB2 V5, or BatchPipes or MVS Pipes.
- **Utility doesn't execute commands, just generates them to a CLIST for your review/modification.**
- **One set of JCL and two execs (RXSADM + RXSRES).**

RACFDB2 Conversion Utility

- **What the RACFDB2 utility does :**
  - Finds all privileges or resources which must be protected and generates RDEF commands for them.
  - Determines whether the privileges or resources were granted to PUBLIC and changes UACC to READ.
  - Determines all authorization IDs without GRANT and generates a PERMIT with ACCESS(READ).
  - Determines all authorization IDs with GRANT and generates a PERMIT with ACCESS(ALTER).
  - Builds a CLIST that you can review, modify, execute etc.
- **Downloadable from the RACF Home Page where more details are also available.**
- **This is provided on an "as-is" basis by IBM.**

RACF Support for Digital Certificates

How does RACF Support Public Key?

- **With OS/390 Security Server R4 (OW26930), RACF can be used to map certificates to a RACF user ID**
  - General resource class **DIGTCERT**
    - Segment **CERTDATA** contains the certificate
    - APPLDATA contains the user associated with the certificate
    - UACC contains the TRUST status of the certificate
    - User profile repeat group points to the certificate
  - RACF command **RACDCERT** to manage the certificates
- **Certificates are uniquely identified by the issuer's distinguished name and serial number**

A Word About Distinguished Names...

- **X.509 certificates are identified by distinguished names, which are multi-part hierarchical names**
- **Distinguished names consist of these parts:**
  - **Common name (CN), e.g. "Bob Hanson"**
  - **Title (T), e.g. "RACF Development Team Leader"**
  - **One or more organizational units (OU), e.g. "RACF Development", "S390 Development", "Server Group"**
  - **Organization (O), e.g. "IBM Corporation"**
  - **Locality (L),e.g. "Poughkeepsie"**
  - **State or Province (SP), e.g. "New York"**
  - **Country (C), e.g. "US"**
- **Think of the distinguished name as a hierarchical name**
  - **Walter Farrell\RACF Development\S390 Development\Server Group\IBM Corporation\Poughkeepsie\New York\US**

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 IBM HTTP Server for OS/390 (formerly the Internet Connection Secure Server or Lotus Domino Go Webserver)**

RACDCERT Command Processor R4 ...

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') ] ) ]
```


RACDCERT Command Processor ...

- ADD - Adds a certificate for a user
  - ►Reads certificate from dataset
  - ►Possible certificate formats:
    - –BER encoded X.509 - Standard binary
    - –BER encoded PKCS#7 - Also binary. Downloadable from Verisign in this format
    - –Privacy Enhanced Mail (PEM) - Most certificate generating tools use this format
- ALTER - changes TRUST status
- DELETE - Deletes certificate from user
- LIST - Lists all certificates for the user

RACDCERT Command Processor ...

Authority Checking

To issue the RACDCERT command the user MUST have one of the following authorities:

- RACF Special
- READ authority to FACILITY Class profile IRR.DIGTCERT.*function* to perform the *function(s)* for him/her self.
- UPDATE authority to FACILITY Class profile IRR.DIGTCERT.*function* to perform the *function(s)* for others.

Where: function ===> LIST, ADD, ALTER, or DELETE

RACDCERT LIST Example - R4

```
Digital certificate information for user IBMUSER:

  Serial Number:
       >41D87A2B05DE6FBD466C2069661E3872<
  Issuer's Name:
       >OU=VeriSign Class 1 CA - Individual
Subscriber.O=VeriSign, Inc..L=Int<
       >ernet<
  Status: NOTRUST
  Subject's Name:
       >sweeny@mhv.net.CN=James Sweeny.OU=Digital ID
Class 1 - Netscape.OU=ww<
       >w.verisign.com/repository/CPS Incorp. by
Ref.,LIAB.LTD(c)96.OU=VeriSi<
       >gn Class 1 CA - Individual
Subscriber.O=VeriSign, Inc..L=Internet<
```

New Self Registration support for Digital Certificates

- APAR OW31933 introduces a new function to register and deregister a digital certificate via the initACEE callable service
- APAR OW33091 introduces a new syscall BPX1SEC to allow for register/deregister a certificate. It also provides a REXX interface CERT into the callable service.
- SYS1.SAMPLIB members contain more information:
  - ✓ RACINSTL - REXX procedure and Webpages for self registration.
  - ✓ IRR31933 - Additional information
- Self Registration Process:
  - ✓ Configure SSL, Sample Webpage, and REXX on OS/390 DGW
  - ✓ Request and Install Client certificate, (in browser)
  - ✓ User initiates an SSL session with OS/390 DGW
  - ✓ Registration steps authenticate user via RACF userid/password

And a few more R4 improvements .....

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

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**
- **SYSID value not verified during PERMIT command**
- **Support delivered via APAR OW25727, PTFs UW91104 for R3, and UW91105 for R4**