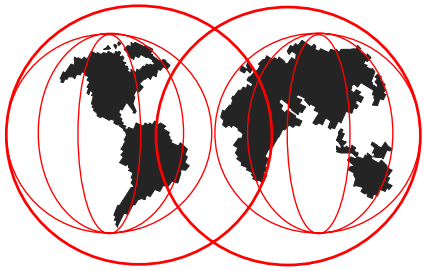
OS/390 Security Server
General Enhancements

Paul de Graaff IBM ITSO Poughkeepsie S/390 Security

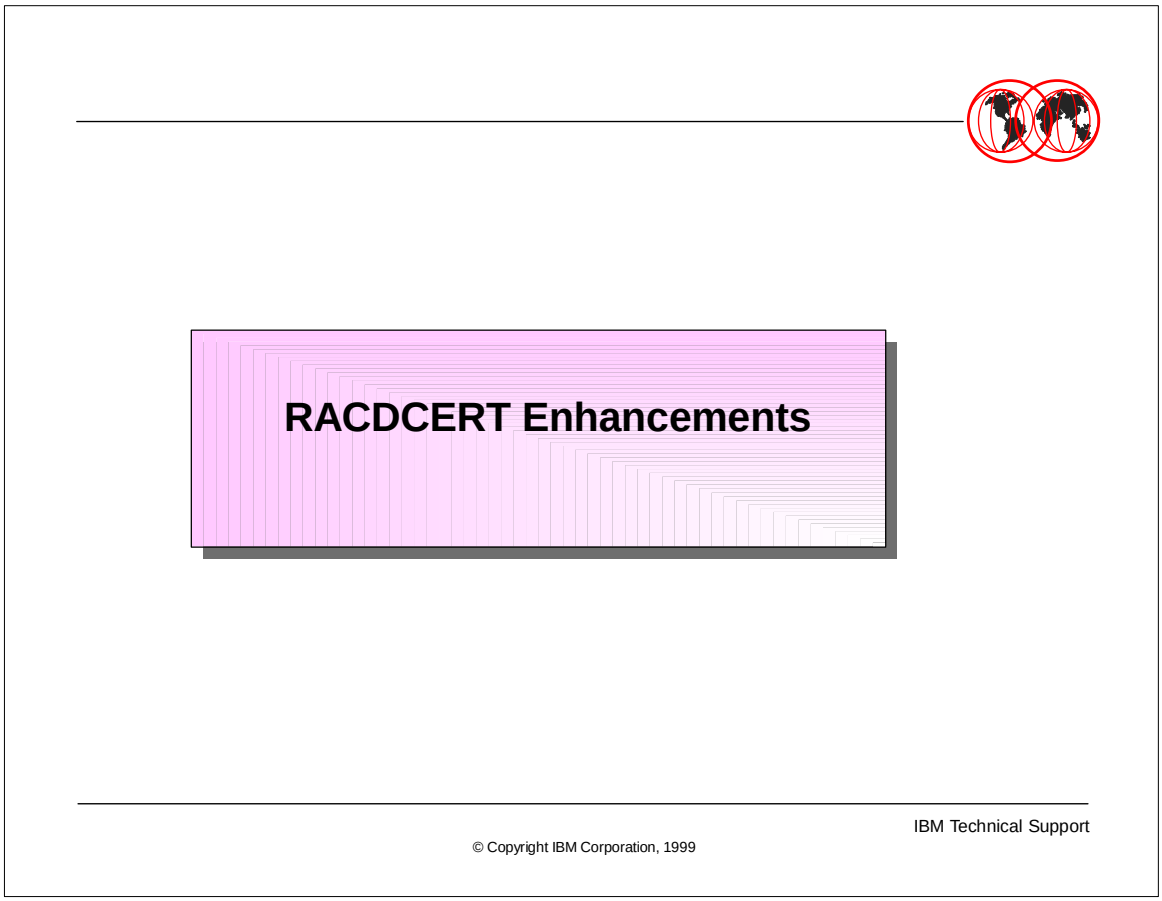


IBM Technical Support

- The digital certificate is the basis for security in any e-business application. In this session we explore cryptography, the core technology of the digital certificate and its applications. We focus on how the RACF component of OS/390 Security Server can be used to map digital certificates to OS/390 user IDs and how with release 8 RACF can be used to create, store, and manage digital certificates and their associated private keys for OS/390-based servers,
-
- Paul M. de Graaff is a Certified I/T Specialist at the International Technical Support Organization, Poughkeepse Center. He writes extensively and teaches IBM classes worlwide on all areas of S/390 Security. Before joining the ITSO, Paul worked with IBM Global Services in The Netherlands as a senior I/T Specialist

Agenda

- Enhancements covered in this presentation
  - RACDCERT Enhancements
  - RACF Enhancements in support of DB2
  - Generic Identity Mapping Support



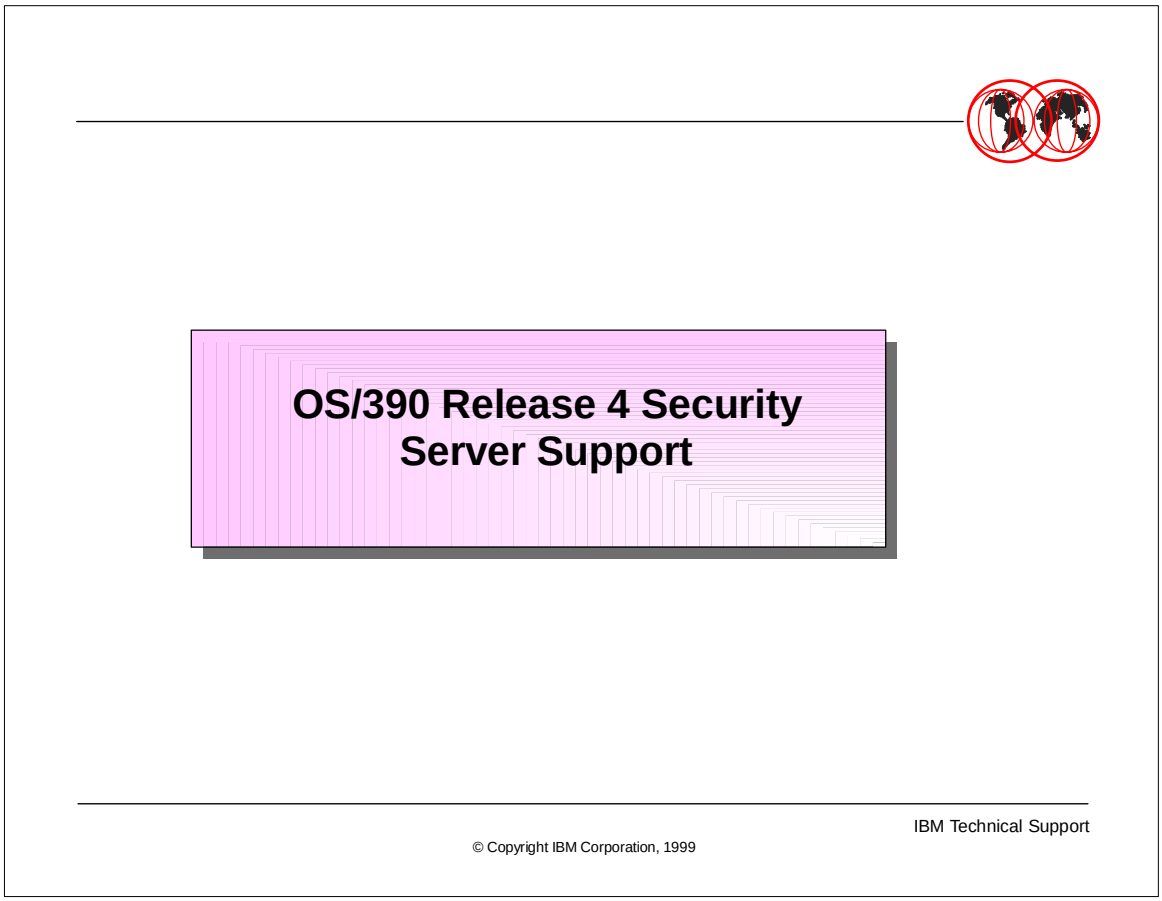
- This sectio will cover the RACDCERT Enhancements

Agenda Digital Certifcates in RACF

- Release 4 Support
- Release 6 Support
- Release 8 Support
  - New RACDCERT functions
    - Creating certificates (GENCERT)
    - Creating certificate requests (GENREQ)
    - Exporting certificates (EXPORT)
    - Key Rings: Listing (LISTRING), creating (ADDRING), deleting (DELREING) and modifying contents (CONNECT and REMOVE)
  - How is all of this funciton used?
  - Callable services
  - Changes to Database Unload (IRRDBU00)
  - Changes to SMF Data Unload (IRRADU00)
  - Changes to the Remove ID Utility (IRRRID00)
  - Changes to BLKUPD (IRRUT300)

IBM Technical Support

- After a quick review of RACF's release 4 and release 6 support we'll have a good foundation to explore the new support introduced in OS/390 Release 8.
-
- RACF's release 8 support continues the evolution of RACF in the age of the digital certificate. With release 8, RACF extends the function of the RACDCERT command to create certificates and certificate requests. In addition, RACDCERT has been extended to support the creation and management of key rings.
-
- Certificate data is now available through a new callable service (IRRSDL00), which is in turn used by the OS/390 Release 8 Open Cryptographic Support Facility (OCSF) support.



- Now that we have a good understanding of the core technologies, we can take a quick look at RACF's current support for digital certificates.

How does RACF Support Public Key?

- 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
- **Certificates are uniquely identified by the issuer's distinguished name and serial number**
  - RACDCERT requires only sufficient information to uniquely identify the certificate

IBM Technical Support

- RACF's support for digital certificates began with release 4 when we supplied RACF commands and modifications to our callable services to store digital certificate information in the RACF database and associate those certificates with OS/390 user IDs.
-

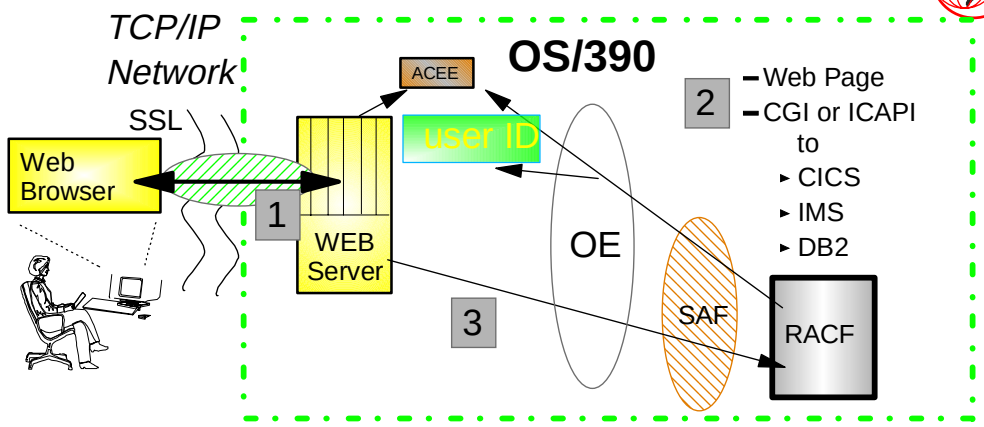
R4: RACDCERT Command Syntax

```
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') ] ) ]
```

IBM Technical Support

- RACF's original certificate introduced the RACDCERT command to associate a digital certificate with an OS/390 user ID. The digital certificate was defined to RACF by placing it in a data set and using the RACDCERT ID(user-ID) ADD(data-set-name) command to associate it with an OS/390 user ID and store it in the RACF database. The RACDCERT ALTER command could be used to change the TRUST status of the certificate. RACDCERT DELETE could be used to delete the certificate and disassociate it from any user ID.

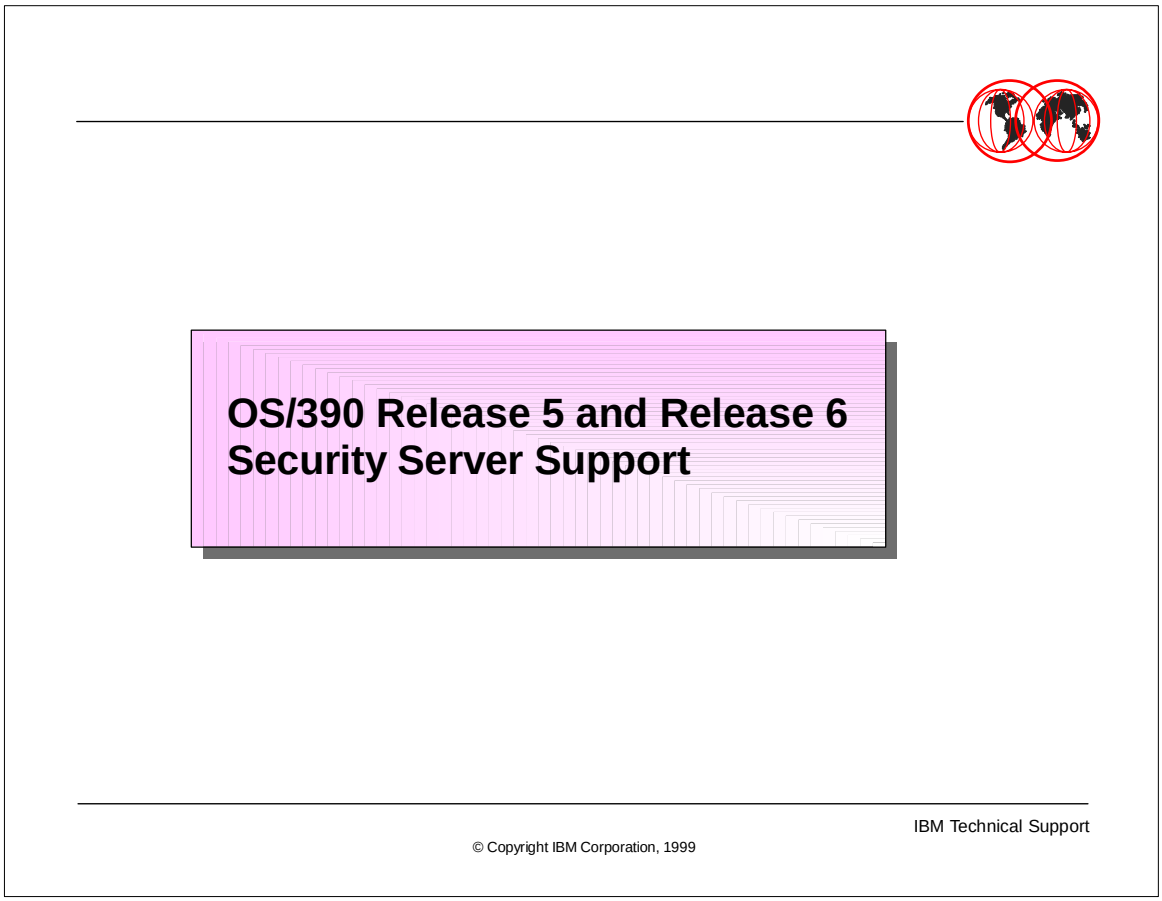
Digital Certificates and RACF



1- User authenticates to Secured Sockets Layer (SSL)
2- User requests OS/390 secured resource via browser
3- Web Server invokes RACF via OpenEdition to build local security context (ACEE),
passing SSL validated certificate instead of prompting for user ID & password

IBM Technical Support

- How does this all fit together? It all starts when a user at a client browser requests a secure session by specifying a URL that starts with https:. The web server establishes an SSL session using the SSL protocol. Once this is done, when the client requests access to an OS/390-secured resource, the web server passes the user's certificate to UNIX system services, which in turn passes the certificate to RACF to establish a security environment for the client. This environment establishes the identity of the client for the resource accesses which are performed on OS/390.
-
- Note that the client does not pass in their OS/390 user ID or OS/390 password. Note also that this process relies on the proper protection of the client's private key.



- RACF made several improvements to our original support in following releases. Many of these improvements were rolled back to release 4 due to customer demand..

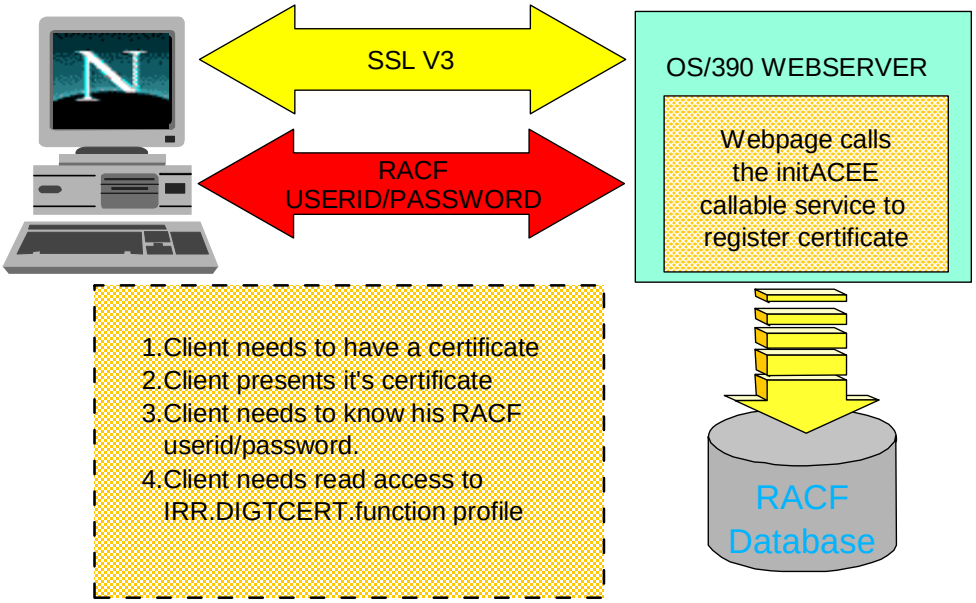
New Certificate Support in V2R5

- Certificate Autoregistration
- RACLISTing DIGTCERT optional
- New Base64 certificate format
- CICS certificate to user ID translation

IBM Technical Support

- With the OS/390 Release 5, RACF introduced several new items, the most important of which is a facility to automate the registration of client certificates with RACF. This allows an installation to allow users to register their own certificates with RACF as long as they know the password of the user ID with which the association is being made.
-
-

Overview of the Self registration process



IBM Technical Support

- To enhance the registration process no OS/390 dataset is needed, but the certficate is pulled from environment variable from the webserver and inserted through a callable service into RACF and associated with the right userid.

Enhancements to RACDCERT

- **New RACDCERT keywords to support:**
  - Associating a 1-32 character user -specified LABEL with a certificate
  - Added CHECKCERT function to display the contents of a certificate and its user association
  - Allow LABEL to be used on ADD, ALTER, DELETE, a CHECKCERT
- **Support shipped back to OS/390 V2R4 with APARs:**
  - RACF (R4) - OW31933
  - SAF OW31934
  - OpenEdition - OW33091
  - LE (C-RTL) - PQ15716

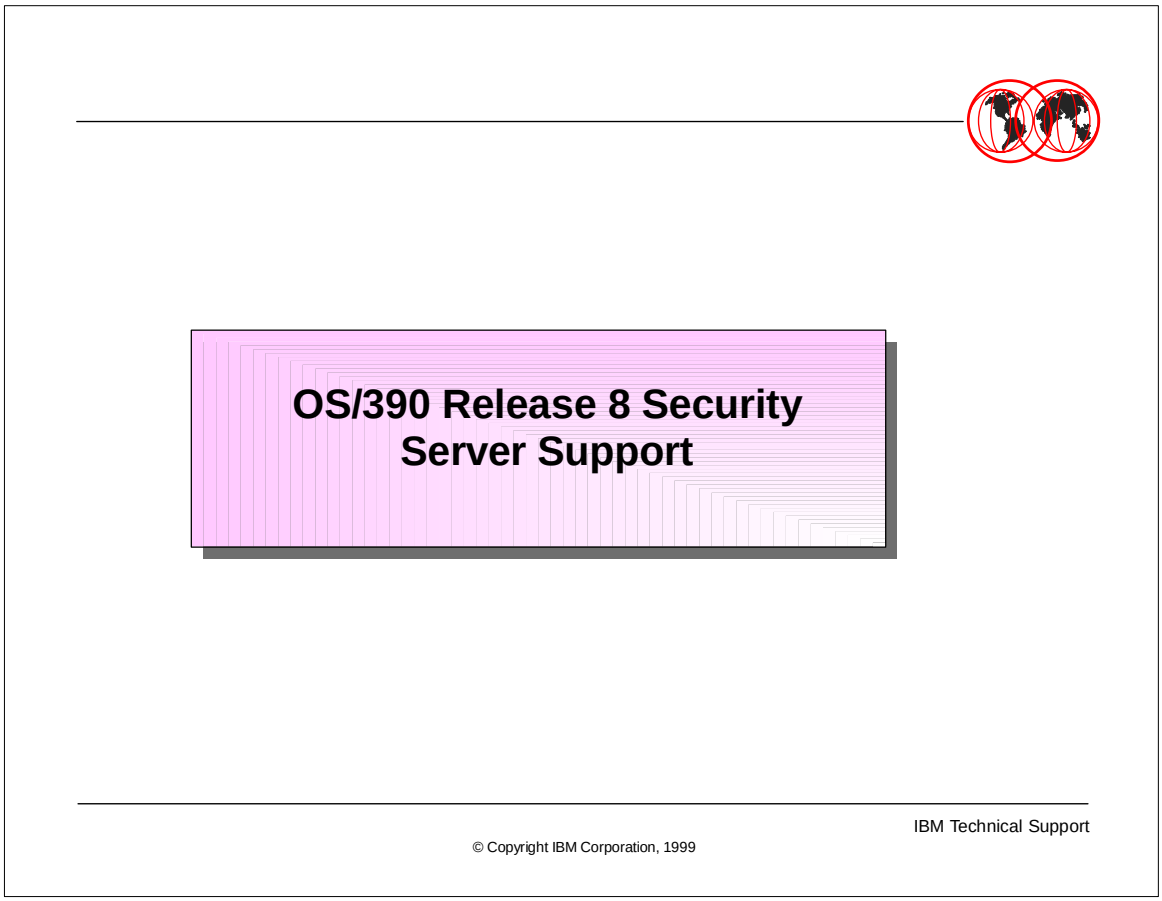
- By allowing customers to assign a LABEL to certificates, RACF eliminated the requirement that customer's enter the issuer's distinguished name and/or certificate serial number when manipulating certificates.

New RACDCERT Command Syntax

```
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') ] ] ) ]
```

IBM Technical Support

- The extensions to the RACDCERT command allowed the use of LABEL wherever SERIALNUMBER and ISSUERSDN were allowed.



- Now, on to release 8!

Problem Statement

- **RACF's existing digital certificate support focused on mapping client certificates to OS/390 user IDs**
- **Servers implemented on OS/390 relied on:**
  - Private keys stored in the local file system
  - Each server establishing its own security policy
- **The opportunity for RACF was to utilize existing OS/390 facilities (e.g. ICSF, the RACF data base) to allow the implementation of a secure and consolidated security policy**

IBM Technical Support

- Up to release 8, RACF focused on mapping client certificates to OS/390 user IDs. While this was an important first step, it was just a first step toward enabling OS/390 for e-business servers. Existing servers on OS/390 stored private keys in the local file system. This meant that they could be read by anyone who had read privileges to the files in which the keys were stored. Client certificates were encrypted using a password supplied by the owner of the key ring at the time that the key ring was opened. For servers, there was no "password provider" to enable the opening of key rings. A new technology was required to securely store information such as the private key associated with a certificate.

OS/390 Release 8 Support

- **New RACDCERT functions that 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 info**
- **New RACF database unload (IRRDBU00) and modified RACF SMF unload (IRRADU00) records**
- **BLKUPD allows mixed case ENTRY**

IBM Technical Support

- With release 8, RACF moves from being just a repository of certificates to being able to create and sign certificates. To do this, RACF now supports certificate authority certificates, site certificates, and key rings, and can receive PKCS-12 format certificates.
-
- A new callable service (IRRSDL00) allows applications (including OCEP) to retrieve certificate information.
-
- OCEP (Open Cryptographic Enhanced Plug-ins) is a new element of the OS/390 Security Server that enables applications that work with the OCSF Framework to retrieve certificate data from RACF.
-
- BLKUPD allows the specification of mixed case ENTRY

GENCERT: Creating A Certificate

- **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 353-1024; Default: 512
  - Signature: Default: Self-signed

- Let's look at each of the new and modified RACDCERT functions, starting with GENCERT.

RACDCERT Example 1

- RACDCERT Example #1- Create a certificate for the user ID (SRVR01) which is the user ID associated with the inventory server:

```
RACDCERT ID(SRVR01)
        GENCERT
        SUBJECTSDN(CN('co-name.com')
                OU('Inventory')
                 C('US'))
        WITHLABEL('Inventory Server')
```

  - Notes: SSL convention is that the "common name" (CN) is the same as the domain name

IBM Technical Support

- Note that this creates a self-signed certificate.

RACDCERT Example 2 - Part 1

- RACDCERT Example #2 (Part 1)- Creating the CERTAUTH certificate

```
RACDCERT CERTAUTH
        GENCERT
        SUBJECTSDN(CN('Local CertAuth')
                OU('My Company')
                C('US'))
        WITHLABEL('XYZZY CertAuth')
```

  - Note: This certificate is a certificate authority certificate (CERTAUTH), which can be used to sign other certificates.

IBM Technical Support

- Let's expand on the previous example by having create the certificate as a non-self signed certificate. Before we can create a certificate signed by a certificate authority, we need to create the certificate authority certificate.
-
- RACDCERT GENCERT is used to create the certificate authority certificate. These certificates are created by specifying "CERTAUTH" prior to the GENCERT keyword.

RACDCERT Example 2 - Part 2

- RACDCERT Example #2 (Part 2)- Create a certificate for the user ID (SRVR01) which is the user ID associated with the inventory server, this time signed by a certificate authority certificate managed by RACF:

```
RACDCERT ID(SRVR01)
      GENCERT
      SUBJECTSDN(CN('co-name.com')
            OU('Inventory')
            C('US'))
      WITHLABEL('Inventory Server')
      SIGNWITH(CERTAUTH
         LABEL('XYZZY CertAuth'))
```

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. "Lamont Cranston"
  - Title (T), e.g. "RACF Developer"
  - 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
  - Lamont Cranston\RACF Developer\RACF Development\S390 Development\Server Group\IBM Corporation\Poughkeepsie\New York\US

IBM Technical Support

- Distinguished names are an important concept in understanding digital certificates. Note the hierarchical nature of these names.

GENREQ: Creating a Certificate

- RACDCERT GENREQ can be used to create a certificate request which can be submitted to an off-platform certificate authority to sign the certificate.

RACDCERT ID(SRVR01)
GENREQ(LABEL('Inventory Server'))
DSN('GRAAFF.EQUIFAX.GENREQ')

IBM Technical Support

- In addition to creating certificates, RACDCERT can be used to create certificate requests. Certificate requests can be sent to a certificate authority, which then creates a certificate with the contents of the certificate request and signs it with the certificate authority's private key.

EXPORT: Writing a Certificate to a Data Set

- RACDCERT EXPORT can be used to extract a certificate from the RACF data base and place it into a data set

  RACDCERT ID(SRVR01)
  EXPORT(LABEL('Inventory Server'))
  DSN('GRAAFF.EQUIFAX.GENREQ')

- One in a data set, the certificate can be moved to the OS/390 HFS, where it can be loaded by a web browser for use on a client system.

IBM Technical Support

- RACDCERT EXPORT can be used to take a certificate in the RACF database and place it in a data set. Once there, it can be moved elsewhere, such as to the OS/390 hierarchical file system (HFS), where it can then be accessed by an OS/390 web server.
-
- Certificates can be exported as a DER encoded X.509 certificate or as a BER encoded X.509 certificate, encoded using base64.

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 "irrcitec"
  - 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.

IBM Technical Support

- Key rings are an essential component of RACF's release 8 support. Key rings contain all of the certificates, site certificates, and certificate authority certificates which can be used by a user ID.
-
- Key rings information is stored in the new DIGTRING class.

Advantages of RACF Key Rings

- Why are RACF key rings superior to other platforms key ring implementations?
  - Application/server owners may implement a trust hierarchy that is a subset of the installation policy. That is, they may not allow non-approved certificate authorities.

IBM Technical Support

- In a traditional server environment, each server has its own key ring. The contents of the server's key ring are usually left up to the server's administrators. This means that each server administrator sets up their own security or trust policy by virtue of the certificate authority certificates that they choose to place in the server's key ring.
- With OS/390, key ring content is determined by the RACF security administrator. Server administrators can only define a trust policy that is a subset of the installation security policy. That is, they may place into the server's key ring only those certificate authority certificates which have been approved by the RACF security administrator,

ADDRING: Creating a Key Ring

- RACDCERT ADDRING is used to create a key ring. To create a key ring called "INCB" for the user ID SRVR01, the command is:

  RACDCERT ID(SRVR01)
  ADDRING(INCB)

IBM Technical Support

- RACDCERT has five commands to manipulate key rings: ADDRING to create a ring, DELRING to delete a ring, LISTRING to show the contents of a ring, CONNECT to place a certificate into a key ring, and REMOVE to take a certificate out of a key ring.

CONNECT: Adding a Certificate to a Key Ring

- RACDCERT CONNECT is used to add a certificate to a key ring. To connect the certificate labeled "Inventory Server" which is associated with the user ID SRV01 to a key ring called RING01 that is associated with the user ID SRVR01, the command is:

```
RACDCERT ID(SRVR01)
        CONNECT(
           LABEL('Inventory Server')
           RING(RING01)
           DEFAULT)
```

IBM Technical Support

- The usage of the "Inventory Server" certificate is as a PERSONAL certificate.
-
- RACF supports the concept of the "DEFAULT" certificate. This is the first certificate that is returned when using the IRRSEQ00 or Open Cryptographic Enhanced Plug-in (OCEP) callable service to return the certificates within a key ring.

CONNECT: Example

- To connect a certificate authority certificate to a key ring, the CERTAUTH keyword is added to the RACDCERT CONNECT command:

```
RACDCERT ID(SRVR01)
        CONNECT(CERTAUTH
           LABEL('CertAuth 1')
           RING(RING01)
           DEFAULT)
```

IBM Technical Support

- The keyword CERTAUTH indicate that 'CertAuth 1' is a certificate authority certificate.

REMOVE: Taking a Cert out of a Key Ring

- RACDCERT REMOVE is used to take a certificate out of a key ring. To remote the certificate labeled "Inventory Server" from key ring RING01 for the user ID SRVR01, the command is:

```
RACDCERT ID(SRVR01)
        REMOVE(
           LABEL('Inventory Server')
           RING(RING01))
```

DELRING: Deleting a Key Ring

- RACDCERT DELRING is used to delete a key ring. To delete the key ring called "INCB" for the user ID SRVR01, the command is:

  RACDCERT ID(SRVR01)
  DELRING(INCB)

- DELRING does not delete the certificates themselves. It merely deletes the relationship between the certificate and the key ring.

LISTRING: Listing a Key Ring

- RACDCERT LISTRING is used to lis the contents of a key ring. If a listing of all rings associated with a user ID is desired, then LISTRING(*) is specified.
- LISTRING displays:
  - The ring name
  - The label of the certificate
  - The DEFAULT status of the certificate within the ring
  - The usage within the ring

LISTRING: Sample Output

```
Digital ring information for user GEORGEM:

  Ring:
       >GEORGEMsNewRing01<
  Certificate Label Name              Cert Owner     USAGE      DEFAULT
  --------------------------------    ------------   --------   -------
  New Cert Type - Ser # 00            ID(GEORGEM)    PERSONAL     YES
  New Type Cert - VsignC1             ID(GEORGEM)    CERTAUTH     NO
  New Type Cert - VsignC2             ID(GEORGEM)    SITE         NO
  65                                  ID(JOHNP)      PERSONAL     NO

  Ring:
       >GEORGEMsRing<
  Certificate Label Name              Cert Owner     USAGE      DEFAULT
  --------------------------------    ------------   --------   -------
  GEORGEM's Cert # 48                 ID(GEORGEM)    PERSONAL     NO
  GEORGEM's Cert # 84                 ID(GEORGEM)    PERSONAL     NO
  New Cert Type - Ser # 00            ID(GEORGEM)    PERSONAL     YES

  Ring:
       >GEORGEMsRing#2<
  Certificate Label Name              Cert Owner     USAGE      DEFAULT
  --------------------------------    ------------   --------   -------
  GEORGEM's Cert # 84                 ID(GEORGEM)    PERSONAL     NO
  GEORGEM's Cert # 48                 ID(GEORGEM)    PERSONAL     NO

  Ring:
       >GEORGEMsRing#3<
*** No certificates connected ***
```

IBM Technical Support

A Word About "irrcerta" and "irrsitec"

- The two special user IDs "irrcerta" and "irrcitec" are anchor points for certificate authority certificates and site certificates respectively. 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. Note that a "LISTUSER *" will list the information about these 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

IBM Technical Support

- The net of this is that "irrsitec" and "irrcerta" can not be logged on or SURROGATed to.
-
- Applications which used ICHEINTY, RACROUTE REQUEST=EXTRACT or RACXTRT to find all users must be sensitive to these two new user IDs which can be returned.

Changes to RACDCERT Processing

- Changes to RACDCERT ADD
  - SITE and CERTAUTH certificates may now be added.
  - Replacement certificates may be added. This allows
    - Replacement certificates to be added
    - Certificates returned from certificate requests:
  - PKCS#12 "certificate packages" (which contain a private key) may be RACDCERT ADDed

IBM Technical Support

- In addition to the new RACDCERT GENCERT, EXPORT, GENREQ, ADDRING, DELRING, LISTRING, CONNECT, and REMOVE functions, the existing RACDCERT ADD, CHECKCERT, ALTER, DELETE, and LIST have been modified.

Changes to RACDCERT Processing...

- 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

IBM Technical Support

- CHECKCERT reads the specified data set and reports on the certificate within the data set. The only access check that is performed for this part of CHECKCERT's function is DFP's check to ensure that you have READ authority to the specified data set.
-
- CHECKCERT reports on the RACF registration status of the certificate only after checking that the user is authorized.
- This is done by checking the resource name IRR.DIGTCERT.LIST. Note that this is the resource name, not IRR.DIGTCERT.CHECKCERT.
-

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

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<
```

Remote Sharing Considerations

- RRSF does not propagate private key information
  - CERTPRVK (private key)
  - CERTPRVS (private key size)
  - CERTPRVT (private key type)
- Customers must ensure that RRSF has identical propagation rules for the DIGTCERT and DIGTRING class
  - Recommendation: Define the propagation with the profile AUTODIRECT.node.DIGT*.APPL to have a single set of rules for both classes.

IBM Technical Support

- Customers who are using RACF's remote sharing facility (RRSF) should be aware that RRSF does not propagate private key information. The intent of all this new support is to have private key information stored in ICSF, in which case, the private key information in the RACF data base would not be useful on a remote system
-

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)
  - If ICSF is not being used, BSafe (software encryption) is used

IBM Technical Support

- ICSF is a key component of S/390's security advantage. S/390 cryptographic hardware is shipped with our latest processors. Use of ICSF keeps the private key under ICSF's control.
-

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.

- The reason that we cannot move an ICSF private key to a non-ICSF environment is that once the private key is in ICSF the private key may not be retrieved. Only the ICSF handle on the key may be retrieved. It is the responsibility of the application extracting the ICSF private-key-handle to use the appropriate ICSF services with that handle to perform operations using the private key.

Authority Checking

- Users with SPECIAL authority can do practically anything to anybody.
- For everyone else, authority checks are performed against the resource 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.

IBM Technical Support

- <function> represents any of the RACDCERT functions (e.g. GENCERT, ADDRING, EXPORT, LIST) with the exception of CHECKCERT. Recall that CHECKCERT performs access checks against the resource IRR.DIGTCERT.LIST.

Authority Checking Summary

Function	READ	UPDATE	**CONTROL**
ADD	Add a cert to one's own user ID	Add a cert to someone else's ID	**Add a SITE or CERTAUTH cert**
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**
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 8

IBM Technical Support

- This is a summary of the authority checking that is performed by RACDCERT. Note that release 8 introduced the use of CONTROL authority.

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

IBM Technical Support

- Since key rings, generating certificates, and exporting certificates are new functions, all of these authority checks are new. All of these checks are performed against the resource IRR.DIGTCERT.<function>.

Authority Checking...

Special processing for SIGNWITH based on signing certificate and CONNECTing with USAGE is shown in the "Reference Material" section.

IBM Technical Support

- The GENCERT function allows a certificate to be generated and signed. Effective controls on what certificate is being used to sign the generated certificate are essential. These are shown in the "Reference Materials" section.
-

Changes to IRRDBU00 Output

- Changes to database unload utility (IRRDBU00)
  - 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

Changes to SMF Records

- Changes RACF's Type 80 Record:
  - For event code 66, relocate section 6 contains the 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")

Changes to IRRADU00 Output

- IRRADU00 unloads the new RACDCERT keywords
- No new IRRADU00 record types
- No existing IRRADU00 record formats are altered

IBM Technical Support

- Since no new IRRADU00 records are created and no existing IRRADU00 record formats are altered, the sample SQL data definition language statements for IRRADU00 data (IRRADUTB) and the sample DB2 Load Utility statements (IRRADULD) are not changed.

Changes to 'SYS1.SAMPLIB'

- Member RACDBUTB
  - Updated DB2 CREATE TABLE, and CREATE INDEX statements to process the new IRRDBU00 output
- Member RACDBULD
  - Updated DB2 Load Utility statements to process the new IRRDBU00 output

Changes to the Block Update Utility

- BLKUPD is updated to:
  - Support mixed case values on the ENTRY statement. This allows using BLKUPD on the "irrcerta" and "irrsitec" user IDs
  - RACF automatically folds non-quoted ENTRY values to upper case
    - LOCATE ENTRY(IRRCERTA) CLASS USER finds the user IRRCERTA in the user class
    - LOCATE ENTRY('irrcerta') CLASS USER finds the user irrcerta in the user class
  - The FIND and REP subcommands also support mixed case values by specifying them as quoted strings

New Callable Service: IRRSDL00

- RACF is providing a new callable service, IRRSDL00, for use in implementing the Common Data Security Architecture (CDSA) Data Library (DL) functions
- IRRSDL00 is a key-8, non-APF, problem state programming interface
- Access to IRRSDL00 functions are controlled by checks against the IRR.DIGTCERT.<function> resources in the FACILITY class
  - READ to IRR.DIGTCERT.LISTRING to retrieve one's own
  - UPDATE to IRR.DIGTCERT.LISTRING to retrieve someone else's
- 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.

IRRSDL00 Parameters

```
CALL IRRSDL00 (Work_area,
               ALET, SAF_return_code,
               ALET, RACF_return_code,
               ALET, RACF_reason_code,
                     Function_code,
                     Attributes,
                     RACF_user_ID,
                     Ring_name,
                     Parm_list_version,
                     Parm_list
              )
```

IBM Technical Support

- Work_area is the name of a 1024 byte SAF/RACF work area.
- SAF_return_code, RACF_return_code, and RACF_reason code are self explanatory.
- Function_code is the function that is being requested.
- RACF_user_ID is the user ID for which this request is being performed. If not specified, it defaults to the ring owner.
- Ring_name is the name of the ring that is being manipulated.
- Parm_list_version is the version of the parameter list and must be set to zero.
- Parm_list is the set of parameters specific to each function.

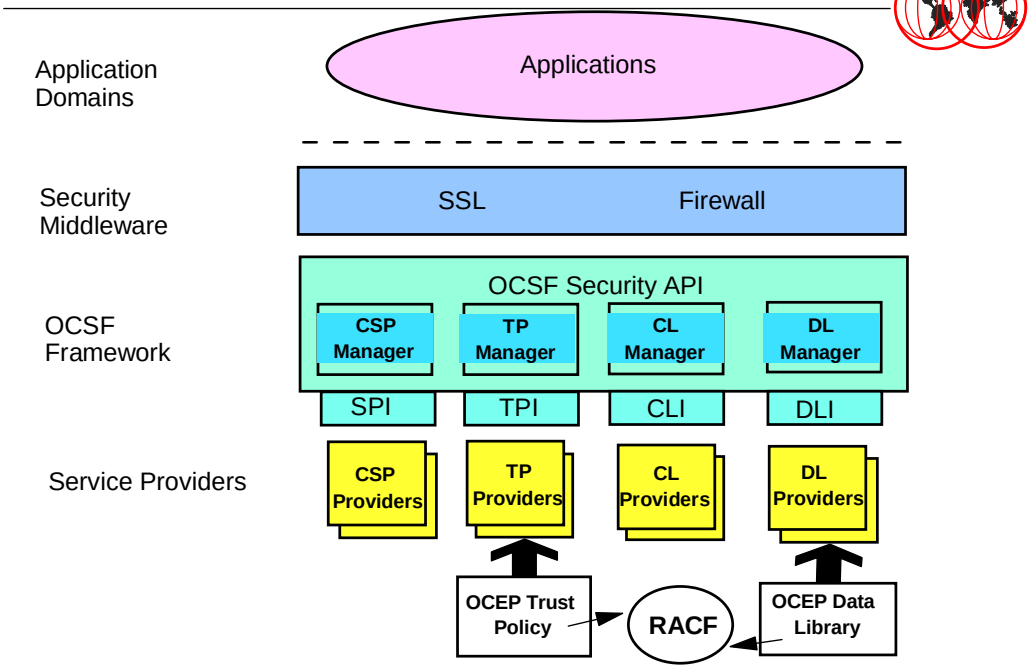
IRRSDL00 Functions

- X'01' - DataGetFirst
  - Locate and return the first trusted certificate in the ring which matches the selection criteria
- X'02' - DataGetNext
  - Locate and return the next trusted certificate in the ring which matches the selection criteria
- X'03' - DataAbortQuery
  - Free resources from previous DataGetFirst and DataGetNext request
- X'04' - CheckStatus
  - Return the TRUST/NOTRUST status for the specified certificate
- X''05' GetUpdateCode
  - Return the change count for the specified key ring

IBM Technical Support

- These are the values which can be specified as the Function_code in the IRRSDL00 parameter list.

OCSF/OCEP Infrastructure



IBM Technical Support

- The Open Cryptographic Support Facility(OCSF) Framework provides the standard APIs which are typically called by security middleware, but can be called directly by applications.
- The provider plug-ins actually provide the function.
- The Open Cryptographic Enahnced Plug-ins (OCEP) Trust Policy and Data Library plug in to the framework as additional providers. They do not replace the existing providers.

Reference Material

R8: RACDCERT Command Syntax

```
RACDCERT
 [ID(UserID) | SITE | CERTAUTH ]
 [LIST   [(LABEL('label-name') | [
                SERIALNUMBER(Serial-Number)
                [ ISSUERSDN('Issuer's Distinguished Name')]])]
  | ADD('Dataset-Name')
        [ TRUST | NOTRUST ]
        [WITHLABEL('label-name')]
        [PASSWORD('pkcs12-password')]
        [ICSF]
  | CHECKCERT('data-set-name')
         [PASSWORD('pkcs12-password')]
  | ALTER [(LABEL('label-name') | [
                SERIALNUMBER(Serial-Number)
      [ ISSUERSDN('Issuer's Distinguished Name')]])]
                 [TRUST | NOTRUST]
                 [NEWLABEL('label-name'')]
```

IBM Technical Support

- This is the complete RACDCERT command syntax. Keywords that are new with release 8 are shown in bold.
-
- Note the addition of the "SITE" and "CERTAUTH" keywords. If required, these are specified before the name of function being requested (e.g. "LIST", "GENCERT"). ID(user-ID), SITE, and CERTAUTH identify the target of the function. That is, for:
-
- - LIST, it is the type (or User ID) of the certificate being listed,
- - ADD, it is the type of the certificate being added (SITE or CERTAUTH) or the user ID with which the certificate is associated
- - CHECKCERT, it is ignored
- - ALTER, it is the type of the certificate that is being changed or the user ID that is associated with the certificate,
- - GENCERT, it is the type of the certificate being created (SITE or CERTAUTH) or the user ID with which the certificate is associated
- - EXPORT, it is the type of the certificate that is being exported or the user ID that is associated with the certificate,
- - ADDRING/DELRING/LISTRING/CONNECT/REMOVE, it is the user ID that owns the key ring (SITE and CERTAUTH are not valid)
-
- Do not confuse this SITE and CERTAUTH with the SITE and CERTAUTH that may

R8: RACDCERT Command Syntax...

```
GENCERT('request-data-set-name')
        [SUBJECTSDN([CN('common-name')]
                    [T('title')]
                    [OU('organizational-unit-name1',
                        'organizational-unit-name2', ...)]
                    [O('organization')]
                    [L('locality')]
                    [SP('state-or-province')]
                    [C('country')]
                    )]
        [SIZE(key-size)]
        [NOTBEFORE([DATE(yyyy-dd-dd)] [TIME(hh:mm:ss)])]
        [NOTAFTER([DATE(yyyy-dd-dd)] [TIME(hh:mm:ss)])]
        [WITHLABEL('label-name')]
        [SIGNWITH([CERTAUTH SITE] LABEL('label-name')]
        [ICSF]
```

IBM Technical Support

- Date ranges from 1950-01-01 to 2040-12-31 are supported.
-
- The TIME values that are specified are converted to UTC time using the CVTLDTO value. Note that this value may differ from the CVTLDTO value in effect on the specific date specified due to moving to and from daylight savings time.
-
- To assist customers who are more familiar with the standard RACF delineation character in date values, date may be specified as "yyyy/mm/dd".

R8: RACDCERT Command Syntax...

```
EXPORT(LABEL('label-name'))
        DSN('output-data-set-name')
        [FORMAT(CERTDER CERTB64)

GENREQ(LABEL('label-name'))
       DSN('output-data-set-name')
```

R8: RACDCERT Command Syntax...

```
ADDRING(ring-name)

DELRING(ring-name)

LISTRING(ring-name)

CONNECT(ID(user-ID)  | SITE | CERTAUTH)
          LABEL('label-name')
          RING(ring-name)
          [DEFAULT]
          [USAGE(PERSONAL) | SITE | CERTAUTH)])

REMOVE(ID(user-ID)  | SITE | CERTAUTH)
          LABEL('label-name')
          RING(ring-name)
```

IBM Technical Support

- The USAGE keyword allows a properly authorized user to connect a certificate to a key ring and change its use. USAGE is not specified, then the default usage is the same as the type of certificate which is being connected.

SIGNWITH Authority Checking

SIGNWITH	Own Certificate	Someone else's Certificate	SITE or CERTAUTH Certificate
SIGNWITH one's one certificate	READ to IRR.DIGTCERT.ADD plus READ to IRR.DIGTCERT.GENCERT	UPDATE to IRR.DIGTCERT.ADD plus READ to IRR.DIGTCERT. GENCERT	CONTROL to IRR.DIGTCERT.ADD plus READ to IRR.DIGTCERT.GENCERT
SIGNWITH a SITE or CERTAUTH certificate	READ to IRR.DIGTCERT.ADD plus CONTROL to IRR.DIGTCERT.GENCERT	UPDATE to IRR.DIGTCERT.ADD plus CONTROL to IRR.DIGTCERT.GENCERT	CONTROL to IRR.DIGTCERT.ADD plus CONTROL to IRR.DIGTCERT.GENCERT
SIGNWITH not specified	READ to IRR.DIGTCERT.ADD plus READ to IRR.DIGTCERT.GENCERT	UPDATE to IRR.DIGTCERT.ADD plus UPDATE to IRR.DIGTCERT.GENCERT	CONTROL to IRR.DIGTCERT.ADD plus CONTROL to IRR.DIGTCERT.GENCERT

- The GENCERT function allows a certificate to be generated and signed. Effective controls on what certificate is being used to sign the generated certificate are essential.
-
- Creating a certificate requires two distinct authority checks:
-
- - Is the user allowed to add this certificate?
-
- - Is the user allowed to sign this certificate?
-
- This means that there are checks performed against the IRR.DIGTCERT.ADD and IRR.DIGTCERT.GENCERT resources.
-
- This table shows the resource checks that are performed for the various SIGNWITH possibilities.

CONNECTing to One's Own Key Ring

Usage	Own Certificate	Someone Else's Certificate	SITE or CERTAUTH Certificate
PERSONAL	READ to IRR.DIGTCERT.CONNECT	UPDATE to IRR.DIGTCERT.CONNECT	UPDATE to IRR.DIGTCERT.CONNECT
SITE or CERTAUTH	CONTROL to IRR.DIGTCERT.ADD plus READ to IRR.DIGTCERT.CONNECT	CONTROL to IRR.DIGTCERT.ADD plus UPDATE to IRR.DIGTCERT.CONNECT	UPDATE to IRR.DIGTCERT.CONNECT

IBM Technical Support

- The USAGE keyword on RACDCERT CONNECT is powerful and must be controlled. This table shows the access checks that are performed when a certificate is being connected to one's own ring.
-
- Note that these checks are only performed if the user does not have the SPECIAL authority.

CONNECTing to Another's Key Ring

Usage	Own Certificate	Someone Else's Certificate	SITE or CERTAUTH Certificate
PERSONAL	CONTROL to IRR.DIGTCERT.CONNECT	CONTROL to IRR.DIGTCERT.CONNECT	CONTROL to IRR.DIGTCERT.CONNECT
SITE or CERTAUTH	CONTROL to IRR.DIGTCERT.ADD plus CONTROL to IRR.DIGTCERT.CONNECT	CONTROL to IRR.DIGTCERT.ADD plus CONTROL to IRR.DIGTCERT.CONNECT	CONTROL to IRR.DIGTCERT.CONNECT

- This table shows the access checks that are performed when a certificate is being connected to the ring of another user.
-
- Note that these checks are only performed if the user does not have the SPECIAL authority.

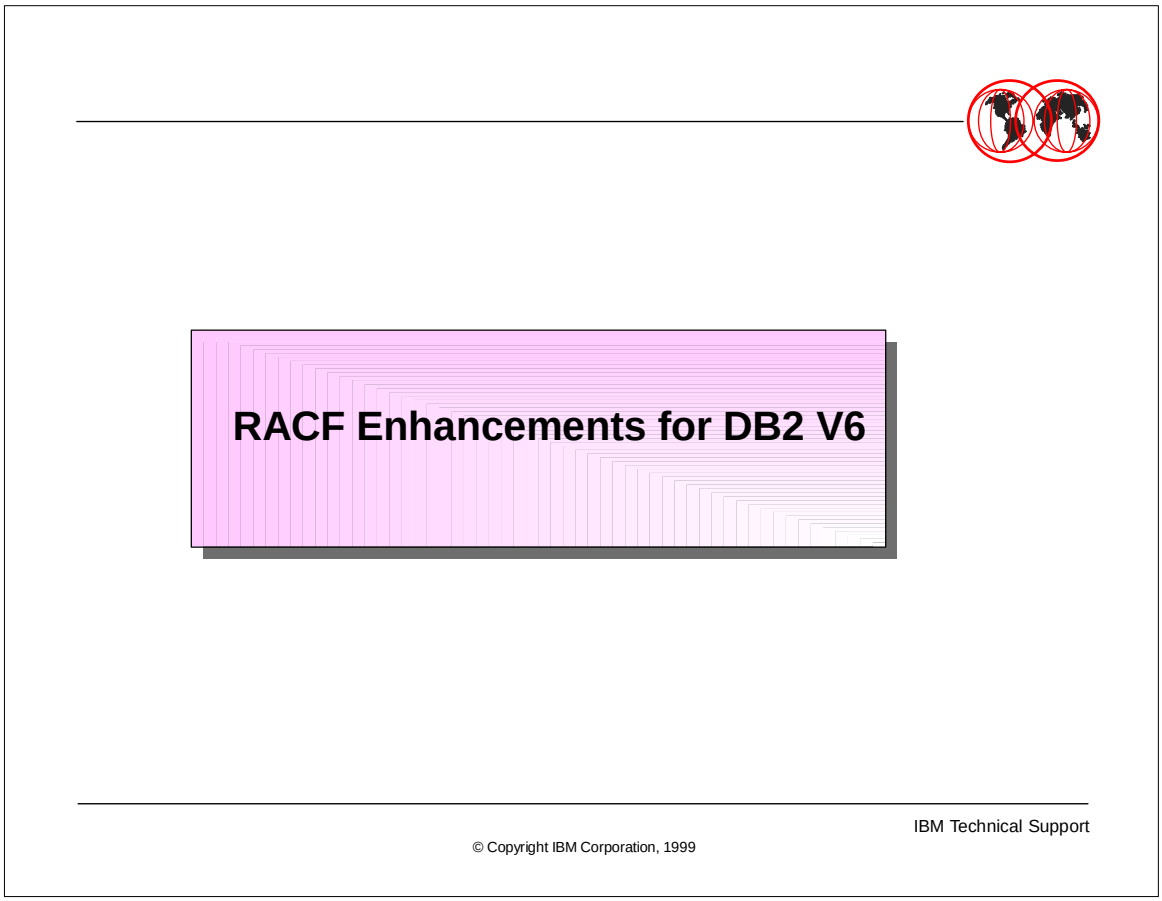
References...

- 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 (SA22-7249)
- OS/390 OCEP Module Developer's Guide and Reference (SC24-5876)
- OS/390 OCEP Application Developer's Guide and Reference (SC24-5875)

- These are the RACF manuals with additional information on digital certificates are RACF.

References...

- **RACF Web Page: http://www.ibm.com/s390/racf**
  - Latest release information on RACF
  - Links to announcement letters
  - Sample code
    - DBSYNC to compare two RACF data bases
    - RACFDB2 to migrate DB2 access control to RACF
    - RACFICE to create reports
    - OS390ART for a web-based reporting tool
    - RACTRACE tracing facility
  - Frequently asked questions (FAQ)
  - RACF user group information



- Now, on to release 8!

RACF Enhancements for DB2 V6

- Identify enhancements to the RACF/DB2 Security Module in support of DB2 V6
- Understand how the support is provided
  - CDT (class descriptor table) changes for R8
  - CDT and code changes provided via APAR OW38710
- Compatablilty with previous releases of security server (RACF) and DB2

Overview

- Problem
  - Need to provide and administer security from a single point
    - DB2 has its own security mechanisms and security administrators
- Solution
  - RACF/DB2 External Security Module (IRR@XACS)
    - Satisfies customer requirements for additional security function
- Customer Value
  - Allows consolidation of security administration
  - Integrates DB2 processing with RACF security

IBM Technical Support

- New function was provided in the following releases as the result of numerous customer requirements to allow RACF to serve as the single point of security administration.
- OS/390 Security Server R4 (GA: September, 1997)
- DB2 Version 5 (GA: June 1997)
- This presentation will provide some background on the original support but will focus on recent changes.

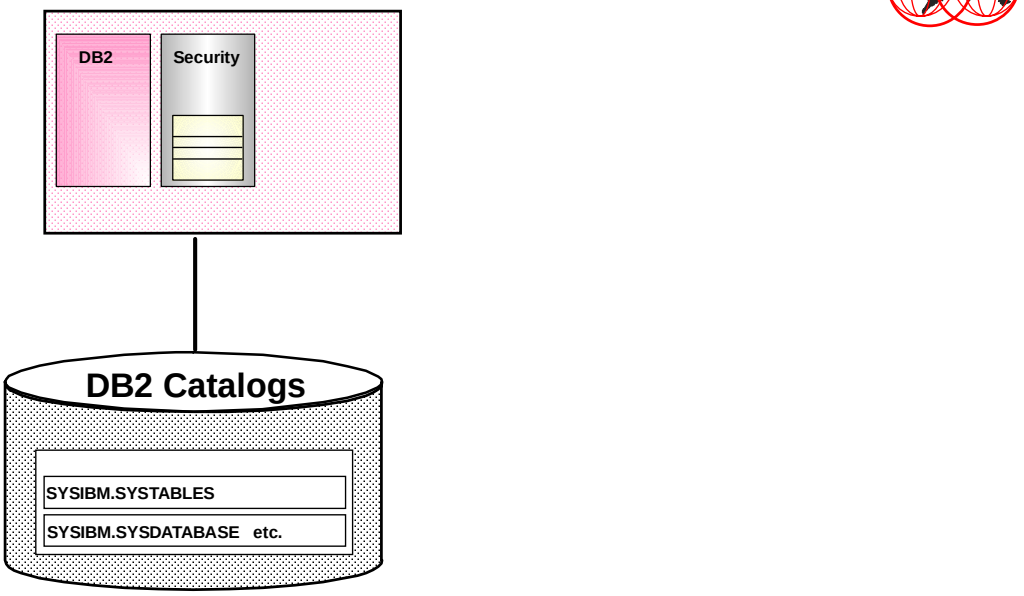
Overview ...

- 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
- Customer Value
  - Updates to IRR@XACS to allow installations to control access to these DB2 V6 functions using RACF

IBM Technical Support

- Schema - A logical grouping for UDFs, UDTs, SPROCs and TRIGGERS. A schema name is a short SQL identifier, used as a qualifier of the name of an object and is often an authorization ID.
- UDF - Extends existing built in functions of SQL language
- UDT - Provides capability to define a data type that shares its internal representation with an existing type.
- Triggers - Provides automatic execution of a set of SQL statements whenever a specified event occurs.
- SPROCs - Can now CREATE, ALTER and DROP. Prior to V6, users defined stored procedures by inserting rows into a DB2 catalog table (SYSIBM.SYSPROCEDURES); they were not created and thus had no owner.

Native DB2 Security



IBM Technical Support

- DB2 is a relational database made up of objects such as databases and tables. A table in turn is made up of rows and columns. Actions (e.g. create, delete or manipulate) can be performed on objects. Actions require authorization.
- DB2 has existing security which is implemented by storing security information in tables prefixed with SYSIBM.
- Authorization is managed by GRANT and REVOKE commands; ownership or Admistrative authorities.
- For example, to create a table, a user would need authorization to a database. So when the action (CREATE) was taken, DB2 would look in SYSIBM.DATABASE to see if the user was authorized.
- As the creator (owner) the user would be authorized to all privileges on that table. The user could give (GRANT) a priviliege (e.g. UPDATE) to some other user and could later take it away (REVOKE)..

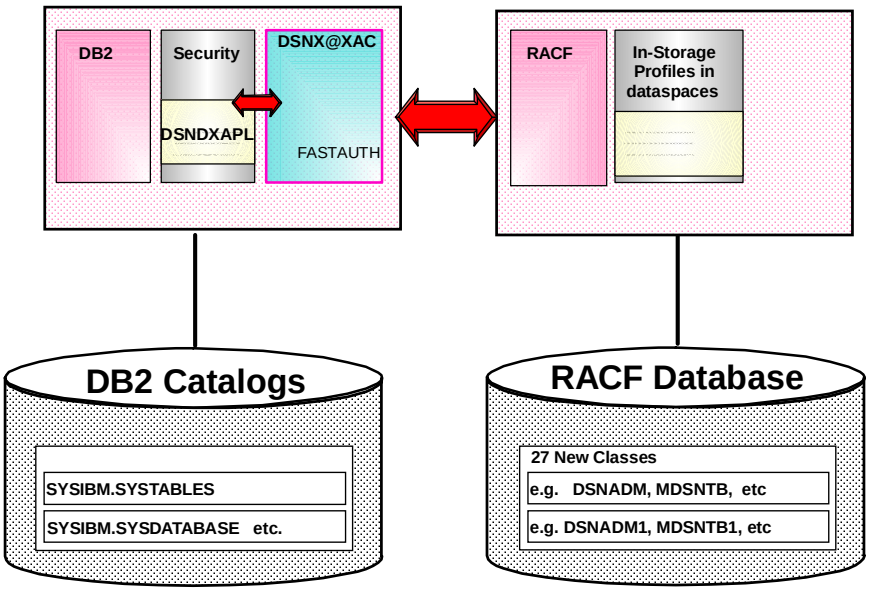
Requirements

- 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

IBM Technical Support

- Customers submitted requirements asking for changes in the way security was implemented in native DB2. Some examples are:
- Cascading revoke - e.g. userA GRANTS a privilege to userb and userc. userA then has that privilege revoked... the REVOKE cascades to userb and userc.
- With RACF security rules can be defined ahead of time (e.g. a generic profile).
- When a DB2 object (e.g. a table) is dropped, the security rules go away too.
- DB2 Administrative authorities are hierarchical (e.g. SYSADM includes SYSCTRL).

DB2 with RACF



IBM Technical Support

- When an action occurs that needs authorization, DB2 builds a control block (XAPL) that contains security information and passes it to a common security module (DSNX@XAC).
- When the security module was initialized, a RACLIST GLOBAL=YES was done for each active class so the RACF profiles would be placed in storage (a dataspace) to improve performance.
- The security module uses the information in the XAPL and in rules tables (defined in the module) to construct a series of RACROUTE FASTAUTH requests.
- The security module will pass a return code to DB2 (rc=0 if allowed; rc=8 if failed; rc =4 if deferred).
- If RACF defers to DB2 (e.g. no profile found for resource), DB2 will make the final decision by looking in it's catalogs.

RACF External Security Module Functions

- Initialization Function
  - Loads profiles for RACF/DB2 authorization checking function
    - Profiles loaded into data spaces
    - Classes targeted for use must be active
  - If unsuccessful or if no classes are active, exit point will not be driven again
- Authorization Checking Function
  - Check user's authority to specified DB2 resource
    - *Details provided in later foils*
- Termination Function
  - Clean-up profiles loaded into data spaces

IBM Technical Support

- -START DB2 causes security module to be initialized. If unsuccessful, RC=12 passed to DB2 and the module will not be called again.
- -STOP DB2 causes security module to be terminated.

New Objects & Classes for DB2 V6

DB2 Object Type	RACF Class Name
User Defined Distinct Type	MDSNUT
User Defined Function	MDSNUF
Stored Procedure	MDSNSP
Schema	MDSNSC

Note:

The above classes are defined in the IBM supplied Class Descriptor Table. In addition, for each member class, there is also a grouping class profile defined.

IBM Technical Support

- DB2 V6 introduced four new objects types.
- Note that SCHEMA is not really an object but RACF maps it to a class as if it were an object.
- The CDT is updated with eight new classes (one member and grouping class for each of the four new objects).

New Privileges for DB2 V6

Schema Privileges
ALTER
COMMENT ON &&
CREATEIN
DROP
QUALIFIER CHANGE &&

Started Procedures Privileges
EXECUTE
DISPLAY **
START **
STOP **

User Defined Function Privileges
EXECUTE
DISPLAY **
START **
STOP **

User Defined Distinct Type Privileges
USAGE

Table Privileges
TRIGGER

- A *privilege* allows a specific function to be performed, often on a specific object.
- Not all DB2 privileges are explicitly GRANTable
- Privileges marked with && are not GRANTable
- Privileges marked with ** are DB2 Operator commands, will always defer to DB2, and START & STOP are not GRANTable.

IBM Technical Support

- Privileges are actions that can be taken on DB2 objects.
- DB2 operator commands (those which are prefixed by the DB2 subsystem prefix... e.g. '-') do not provide an ACEE address in the XAPL so they will always be deferred to DB2. This was also true of the SYSTEM object class in the original support (for DB2 V5).
- This page shows other actions (which are not GRANTable privileges) that can be taken on objects.
- Note that to Create, Alter, Drop, etc. a UDF, UDT or SPROC authority is required in the SCHEMA class.

Profiles for Schemas

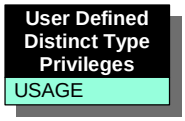
Class Name **Profile Name**

MDSNSC *subsystem.schema.object.privilege-name*

IBM Technical Support

- schema = schema-name
- object = object name (e.g name of a UDT, UDF, SPROC)
- Reminder: a schema is a logical grouping for UDFs, UDTs, SPROCs and TRIGGERs. A schema is a short SQL identifier, used as a qualifier of the name of an object and is often an authorization ID.

Profiles for User Defined Distinct Type



Class Name	Profile Name
MDSNUT	*subsystem.schema.UDT.USAGE*

IBM Technical Support

- schema = schema-name
- UDT = type-name.
- Note that there is only one privilige for this type of profile.
- Reminder: A UDT provides capability to define a data type that shares its internal representation with an existing type.

Profiles for User Defined Functions

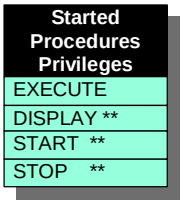
User Defined Function Privileges
EXECUTE
DISPLAY **
START **
STOP **

Class Name	Profile Name
MDSNUT	*subsystem.schema.UDF.privilege-name*

IBM Technical Support

- schema = schema-name
- UDF = function-name
- Reminder: A UDF extends existing built in functions of SQL language.

Profiles for Stored Procedures



Class Name **Profile Name**

MDSNSP
subsystem.schema.SPROC.privilege-name

IBM Technical Support

- schema = schema-name
- SPROC = procedure-name
- Reminder: Can now CREATE, ALTER and DROP SPROCS. Prior to DB2 V6, users defined stored procedures by inserting rows into a DB2 catalog table (SYSIBM.SYSPROCEDURES); they were not created and this had no owner.

Notes on Access Control

- Each DB2 SQL statement, Command, Utility, etc. requires a set of sufficient privileges and/or authorities
- The RACF/DB2 External Security Module will check the RACF profiles corresponding to that set of privileges and/or authorities
- Prior to DB2 V6, implicit privileges of ownership will only be checked for tables.

  RACF will document the profiles required to access DB2 resources

IBM Technical Support

- The processing described in the first two bullets is unchanged for DB2 V6.
- Access checking is done in the order in which they were defined in the rules table in the RACF/DB2 External Security Module (same order as DB2 checking whenever possible. There were a few exceptions which are documented in the RACF Security Administrators Guide. The rules are also in the appendix of that book).
- There are changes to implicit privileges for DB2 V6 and they are described on the next page.

Changes to Ownership in DB2 V6

- Ownership is checked for User Defined Functions, User Defined Types and Stored Procedures.
- A check for MATCH is also done for the above objects.
- Ownership check for BIND privilege (for PLANS and PACKAGES).
- Ownership check for COPY privilege (PACKAGES)

  RACF will document the profiles required to access DB2 resources

IBM Technical Support

- New Objects (UDTs, UDFs, SPROCs, and TRIGGERS) have an owner and a qualifier (for TABLES, the qualifier is always the owner).
- The qualifier is referred to as the SCHEMA to which the object is associated. The SCHEMA and OWNER need not be the same.
- So if USERA created a UDF called USERB.FUNC1 USERA would pass the ownership check, USERB would pass the MATCH check.
- The addition of ownership checks to certain PLAN and PACKAGE privileges was done to satisfy a customer request, not for DB2 V6 function.

Migration/Compatibility

- This support must work with all OS/390 releases which support DB2 V6
  - New CDT entries are in base OS/390 R8
  - APAR OW38710 will provide new version of DSNX@XAC & CDT changes
    - CDT entries for OS/390 R4 thru R7; IPL required to pick up changes
  - When additional classes have been setup and activated, stop and then restart DB2

IBM Technical Support

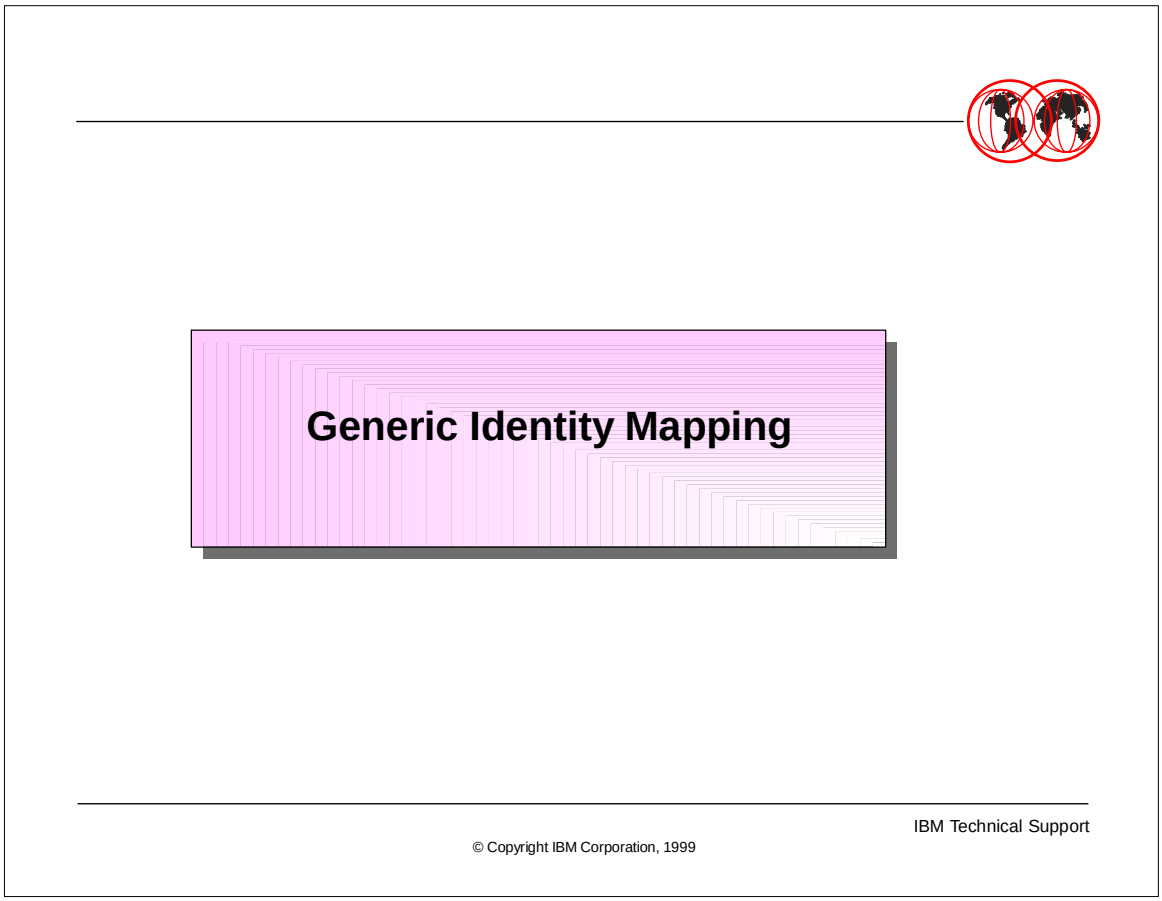
- OS/390 R4 thru R8 support DB2 V5 & V6.
- An IPL is needed to pick up changes to the CDT
- RACF profiles for the new classes must exist in virtual storage (dataspaces) for FASTAUTH to find them. Stopping and then starting DB2 causes initialization of the security module and during this time the RACF profiles are RACLISTED to dataspaces (one dataspace per class).

Documentation

- OS/390 Security Server (RACF) Security Administrator's Guide
  - SC28-1915
- OS/390 Security Server (RACF) System Programmer's Guide
  - SC28-1913
- ITSO Red book - OS/390 Security Server Enhancements
  - SG24-5158
  - http://www.redbooks.ibm.com
- RACF home page
  - http://www.ibm.com/s390/racf/
- DB2 for OS/390 Administration Guide
  - SC26-8957

Availability

- OS/390 Security Server (RACF) R8 GA: September, 1999
- OS/390 Security Server (RACF) APAR OW38710 June, 1999
- DB2 Version 6 GA: June, 1999



- Now, on to release 8!

Rationale

- **Creates a flexible interface for mapping application identities to RACF user IDs**
  - **Past mappings were application-specific**
- **Customer Value**
  - **Allows applications to interoperate with RACF for user identification through RACF ID associated with application identity or digital certificate**
  - **Allows applications to access OS/390 resources through the RACF ID**

IBM Technical Support

- This function was implemented at the request of Lotus and
- NDS.

Functional Overview *(continued)*

- **New RACF mapping classes**
  - **Lotus: NOTELINK. RACF class profile name is the Lotus "short name"**
  - **NDS: NDSLINK. RACF class profile name is the NDS "user name"**
- **APPLDATA field of the class profiles contain the RACF ID associated with the application ID**

Functional Overview *(continued)*

- **New USER profile segments**
  - **LNOTES**
    - **one keyword, SNAME, which contains the Lotus application identity "short name"**
  - **NDS**
    - **one keyword, UNAME, which contains the NDS application identity "user name"**
  - **Application identities must be unique**
  - **Mapping profiles maintained through RACF "user" commands**

Functional Overview *(continued)*

- **New FACILITY class profile IRR.RUSERMAP**
  - **READ access required to use R_usermap service if caller is not in supervisor state or in system key state**

Use of Function

- Database template change requires running IRRMIN00 to update database templates followed by IPL
- Dynamic parse data set IRRDPSDS is updated to include new USER profile segments
- Existing USER profiles must be updated using ALTUSER
- Problem state or non-system key users must be given read access to FACILITY class profile IRR.RUSERMAP to use R_usermap

ADDUSER Enhancements

ADDUSER *userid*
[LNOTES(
[SNAME(*short-name*) | NOSNAME]
)

| NOLNOTES]
[NDS(
[UNAME(*short-name*) | NOUNAME]
)
| NONDS]

ALTUSER Enhancements

ALTUSER *userid*
[**LNOTES**(
[**SNAME**(*short-name*) | **NOSNAME**]
)
| **NOLNOTES**]
[**NDS**(
[**UNAME**(*short-name*) | **NOUNAME**]
)
| **NONDS**]

ADDUSER/ALTUSER Considerations

SNAME

1-64 characters ([A-Z] [a-z][0-9] &-._ , blank)

UNAME

1-246 characters (anything except *+|=,"`/:;[])

Trailing/leading blanks ignored

"Cent" sign excluded (used to replace blanks in profile names)

IBM Technical Support

- Imbedded blanks are allowed.
- If imbedded blanks are present, the name must be in single quotes. Imbedded single quotes are allowed in NDS UNAME. These must be doubled in the parameter.

ADDUSER/ALTUSER Considerations ..

- **SNAME/UNAME must be unique for each user defined or else new message IRR52161I will be invoked:**
- **The application user identity must be unique for each RACF User ID. The mapping profile for User ID will not be updated**

IBM Technical Support

- Example: AU (U1 U2) SNAME('Joe User') is not allowed.

LISTUSER Enhancements

- **Allows listing of LNOTES and NDS segments**
- **If no LNOTES SNAME or NDS UNAME is specified the word NONE appears in the listing**

RACF Utility Updates

- **IRRRID00 -- Remove ID utility. Delete NDSLINK and NOTELINK classes.**

- **Database Unload**
  - **RACDBUTB -- Database Unload DB/2 table definition. New segments and keywords added.**
  - **RACDBULD -- DB/2 Database Unload sample. New segments and keywords added.**

IBM Technical Support

- These are enhancements to existing RACF facilities.
-
- Residual User IDs should not normally exist. They could exist if NOTELINK or NDSLINK profiles were deleted using RDELETE or altered using RALTER. This is only possible if the profiles are upper case. Another cause is the failure to create/delete the NOTELINK/NDSLINK classes properly during ADDUSER or ALTUSER or the failure to delete the classes properly during DELUSER. This should not happen.