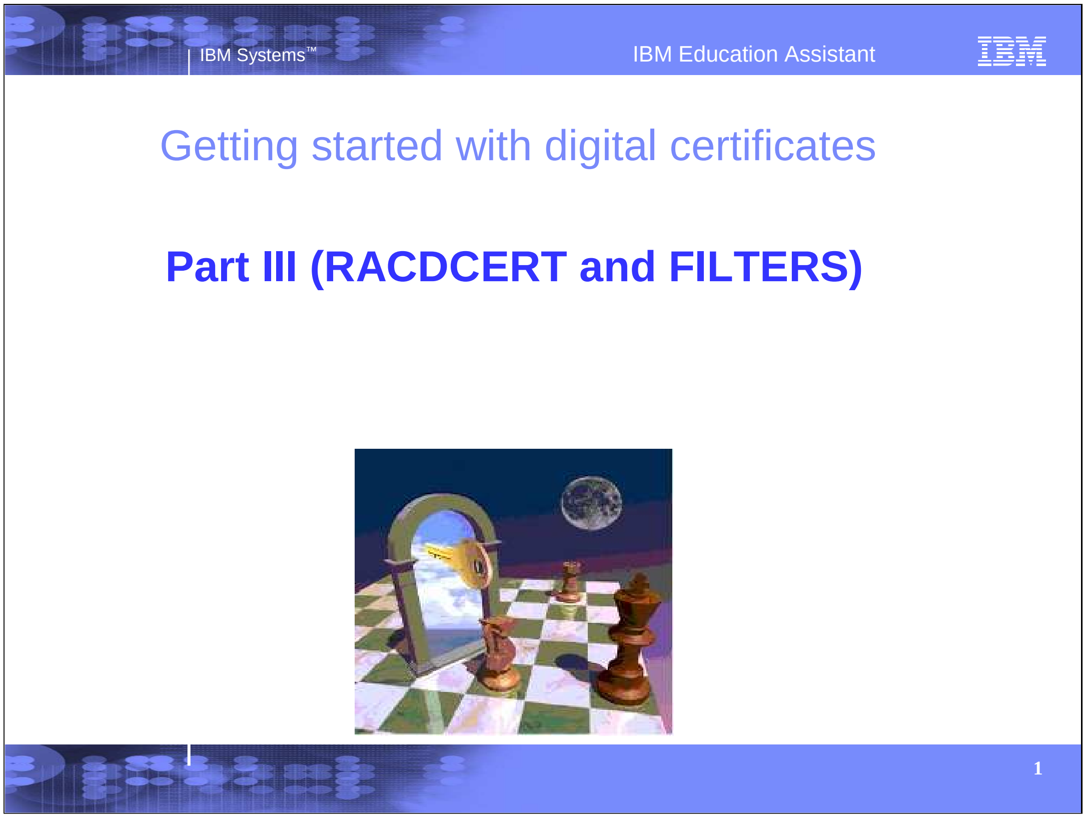
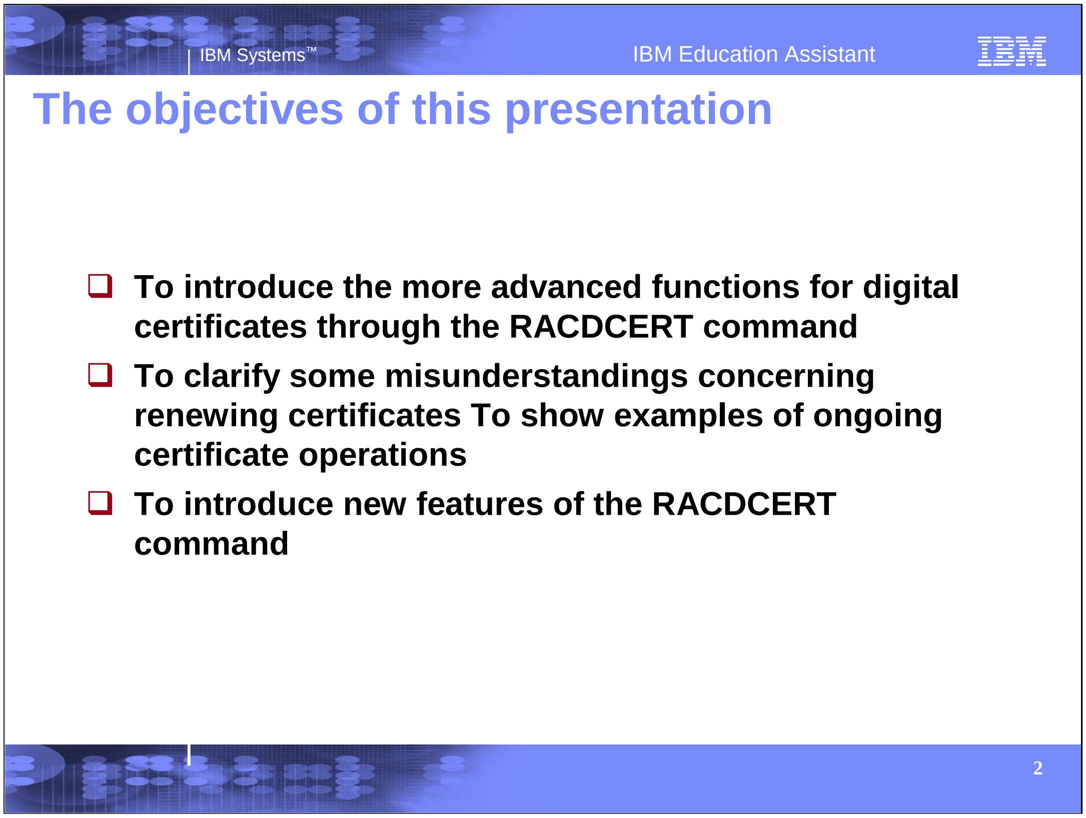


Getting started with digital certificates

Part III (RACDCERT and FILTERS)

This presentation is a continuation of RACF® and its world of digital certificates, “Getting Started with Digital Certificates Part II”. Previously, we talked about certificate and ring management. What if this management becomes too cumbersome for your business? What other areas of opportunities can be found using RACF and the RACDCERT command? We will attempt to explain some advanced functions available to you. We will go through some examples and explanations of these functions. For an explanation of Symmetric keys, Asymmetric keys and the foundations of digital certificates, please refer to Part I of this series, ‘Getting Started with Digital Certificates, Part I’.



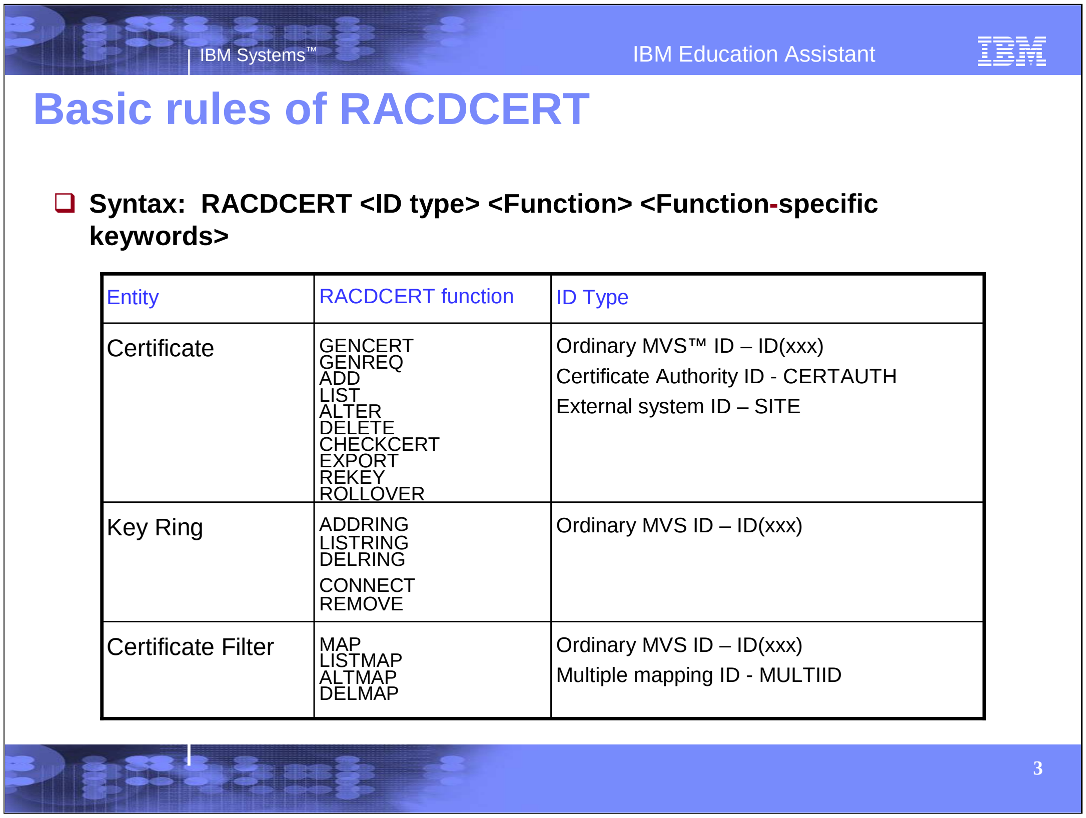
IBM Systems™ IBM Education Assistant

The objectives of this presentation

- □ **To introduce the more advanced functions for digital certificates through the RACDCERT command**
- □ **To clarify some misunderstandings concerning renewing certificates To show examples of ongoing certificate operations**
- □ **To introduce new features of the RACDCERT command**

2

- The objectives of this presentation is to look at the more advanced functions in RACF’s support through the RACDCERT command.
- If our business has a large certificate base, is it necessarily a good idea for us to store these certificates in the RACF database?
- Digital certificates do expire. How can we renew these certificates and continue seamless usage through Ring support? What are some of the common mistakes in renewing certificates?
- What happens to a certificate if the private key gets compromised?
- We will look at some examples of how to use these more advanced functions.
- And lastly, we will look at some of the new functions that are available with the RACDCERT command up to z/OS Release 8.



IBM Systems™

IBM Education Assistant

Basic rules of RACDCERT

- Syntax: **RACDCERT <ID type> <Function> <Function-specific keywords>**

Entity	RACDCERT function	ID Type
Certificate	GENCERT GENREQ ADD LIST ALTER DELETE CHECKCERT EXPORT REKEY ROLLOVER	Ordinary MVS™ ID – ID(xxx) Certificate Authority ID - CERTAUTH External system ID – SITE
Key Ring	ADDRING LISTRING DELRING CONNECT REMOVE	Ordinary MVS ID – ID(xxx)
Certificate Filter	MAP LISTMAP ALTMAP DELMAP	Ordinary MVS ID – ID(xxx) Multiple mapping ID - MULTIID

3

•First, let’s do a quick review of what functions are available in the RACDCERT command.

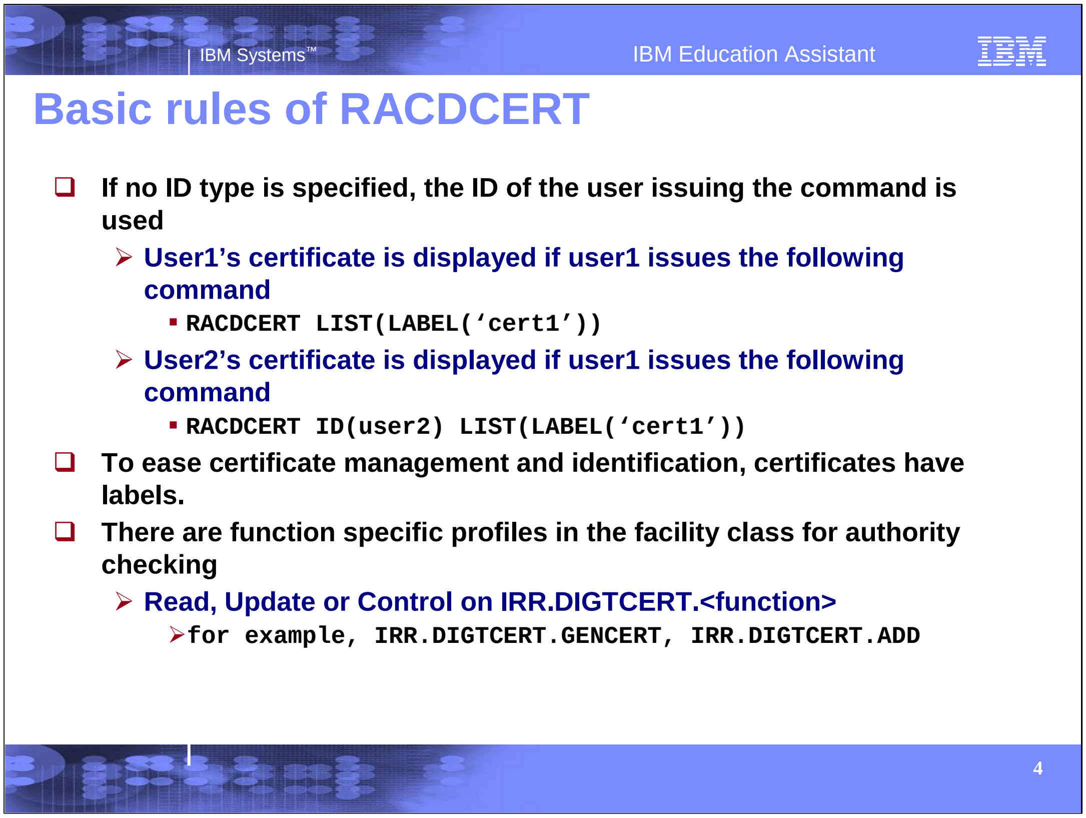
•The RACDCERT command has many functions with function specific keywords for the management of certificates, certificate key rings and certificate mappings.

For certificates, ID Type is who or what the certificate is to be associated with.   The valid ID types would be an ordinary MVS userID (ID), a Certificate Authority (CERTAUTH) or an external system entity or something shared between multiple user IDs (SITE).

•For certificate key rings, the ID type would be an ordinary MVS userID for the ownership of a key ring.

•For certificate filters, the ID type would again be an ordinary MVS userID or a system defined ID (MULTIID) and there is also the ability to map multiple certificates with specific criteria to one userID. Mappings will be discussed in Part III.

•This presentation just indicates the overall syntax in a high level format to illustrate the basic concepts involved. For detailed syntax, refer to the RACF Command Language Reference publication.


IBM Systems™
IBM Education Assistant
4

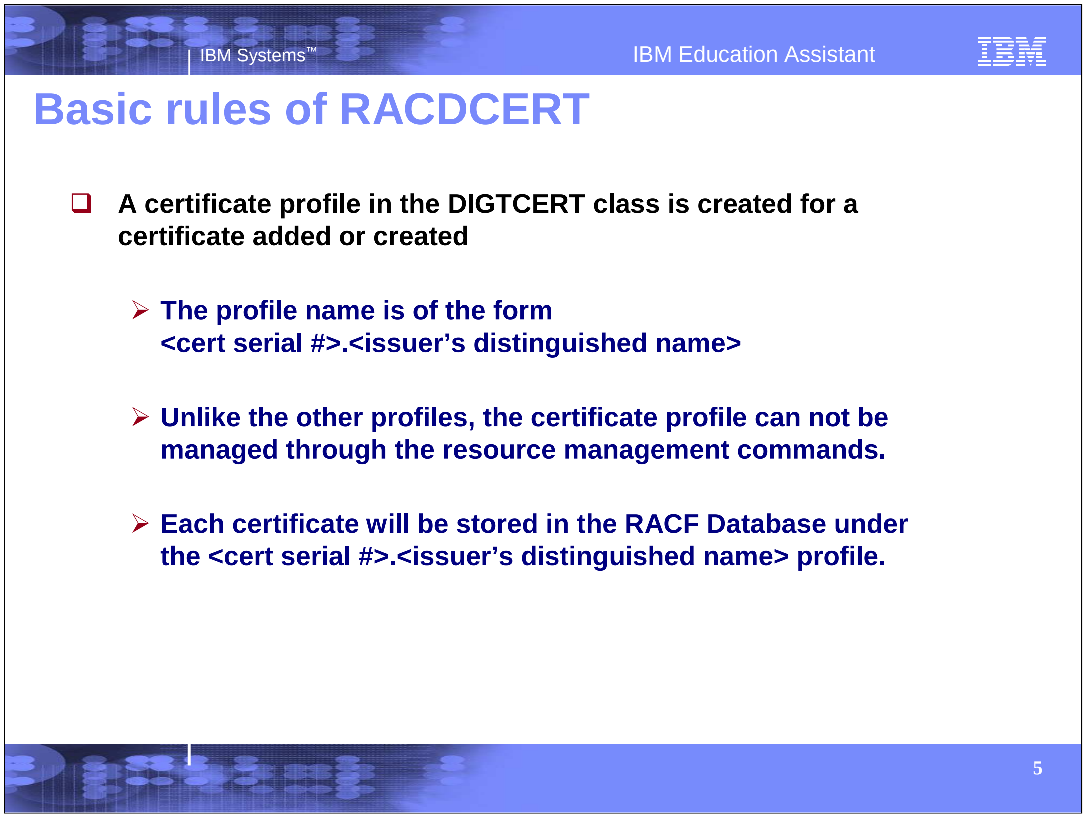
Basic rules of RACDCERT

- If no ID type is specified, the ID of the user issuing the command is used
  - User1's certificate is displayed if user1 issues the following command
    - `RACDCERT LIST(LABEL('cert1'))`
  - User2's certificate is displayed if user1 issues the following command
    - `RACDCERT ID(user2) LIST(LABEL('cert1'))`
- To ease certificate management and identification, certificates have labels.
- There are function specific profiles in the facility class for authority checking
  - Read, Update or Control on IRR.DIGTCERT.<function>
    - `for example, IRR.DIGTCERT.GENCERT, IRR.DIGTCERT.ADD`

•There are three categories of certificates; Personal (ID), Certificate Authority (CERTAUTH) and SITE. For most certificate operations, one of these three can be used. If none are used, the default would be a Personal certificate (ID) and the user ID of the command issuer would be the one used. [enter]

•To be able to manage certificates and mappings, certificates and mappings have labels. Labels are case sensitive, quoted strings with a maximum length of 32 characters. [enter]

•For users to have the RACF authority to issue the RACDCERT command, profiles in the FACILITY class as IRR.DIGTCERT.<function> must be created for the specific functions. For example, if USER1 has the need to LIST certificates for other userIDs, they would need at least UPDATE authority in the profile IRR.DIGTCERT.LIST in the FACILITY class.



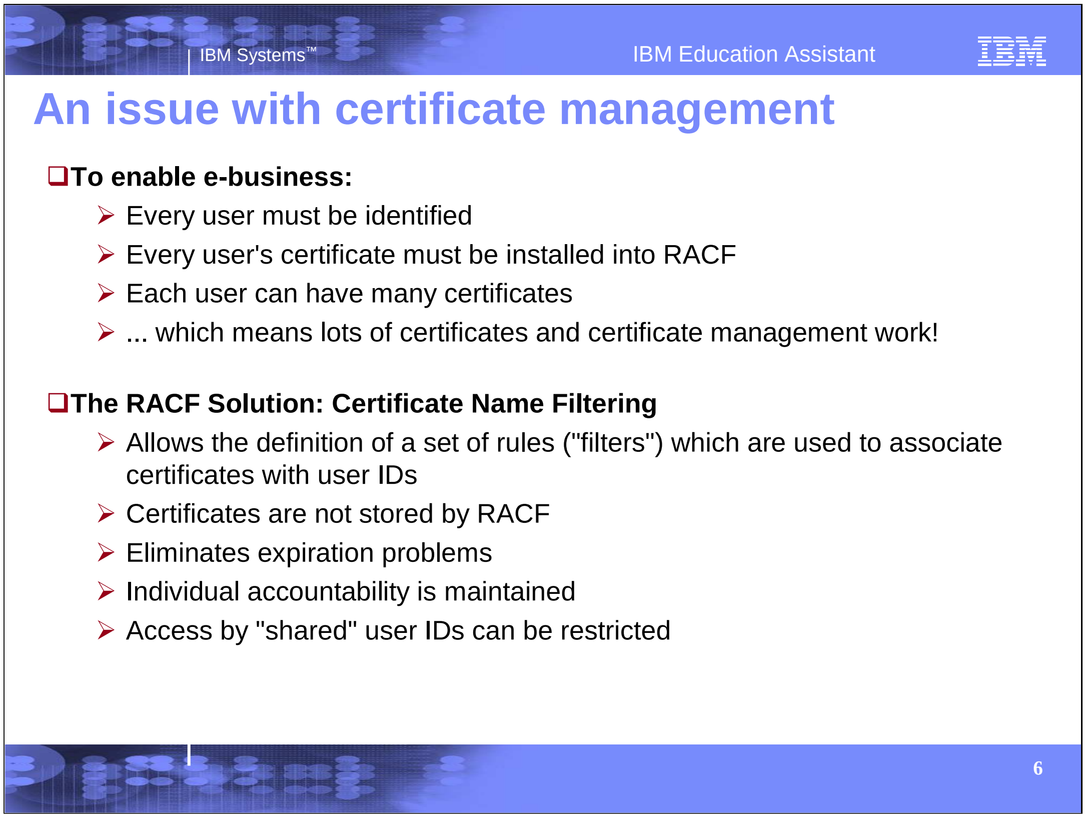
Basic rules of RACDCERT

- **A certificate profile in the DIGTCERT class is created for a certificate added or created**
  - **The profile name is of the form <cert serial #>.<issuer’s distinguished name>**
  - **Unlike the other profiles, the certificate profile can not be managed through the resource management commands.**
  - **Each certificate will be stored in the RACF Database under the <cert serial #>.<issuer’s distinguished name> profile.**

•For RACF to manage the certificate that is created or added in the RACF database, a profile is created in the DIGTCERT class. This profile is in the form of certificate serial number dot issuer’s distinguished name. As we mentioned previously, each certificate needs to be uniquely identified. That is done with the guarantee that no two certificates will have the combination of the same serial number and the same issuer’s distinguished name.

•Since these certificate profiles need to be managed differently, the resources management commands such as RDEFINE, RALTER and RDELETE cannot be used. Additionally, the owner field in these profiles indicates the issuer of the original RACDCERT command that created the profile, not the owner of the certificate.

•Since each certificate is stored in the RACF Database, if your business deals with a large number of certificates to associate to a specific user ID, this may become difficult to manage.



IBM Systems™ IBM Education Assistant

An issue with certificate management

❑ **To enable e-business:**

- ➢ Every user must be identified
- ➢ Every user's certificate must be installed into RACF
- ➢ Each user can have many certificates
- ➢ ... which means lots of certificates and certificate management work!

❑ **The RACF Solution: Certificate Name Filtering**

- ➢ Allows the definition of a set of rules ("filters") which are used to associate certificates with user IDs
- ➢ Certificates are not stored by RACF
- ➢ Eliminates expiration problems
- ➢ Individual accountability is maintained
- ➢ Access by "shared" user IDs can be restricted

6

•As more and more users access your system from the Web, you face an increasing administrative burden to securely manage their digital certificates. Every user must be identified through a digital certificate. Using the RACDCERT ADD/GENCERT functions with RACF, every user’s certificate will be installed in the RACF database. To add to the complexity, some users may have many certificates that identify them.

•Large numbers of certificates will cause a large amount of certificate management work.

•RACF does have a solution – Mapping certificates through Certificate Name Filtering. *Certificate name* filtering is a method for administering large numbers of user certificates, without storing each certificate in the RACF database**.**

•Certificates managed using certificate name filtering:

Require no individual administration to be registered or to be replaced when they expire. If the certificate is not installed in RACF, there is no need to update the renewed certificate. The filter stays the same but the certificate itself can be renewed.

Occupy very little space in the RACF database. The set of rules or filters can be defined to associate to specific user IDs. The filters are stored in the RACF database, not the actual certificates. One filter can map to many certificates.

Can be used to allow several users to share the same user ID in a secure manner.

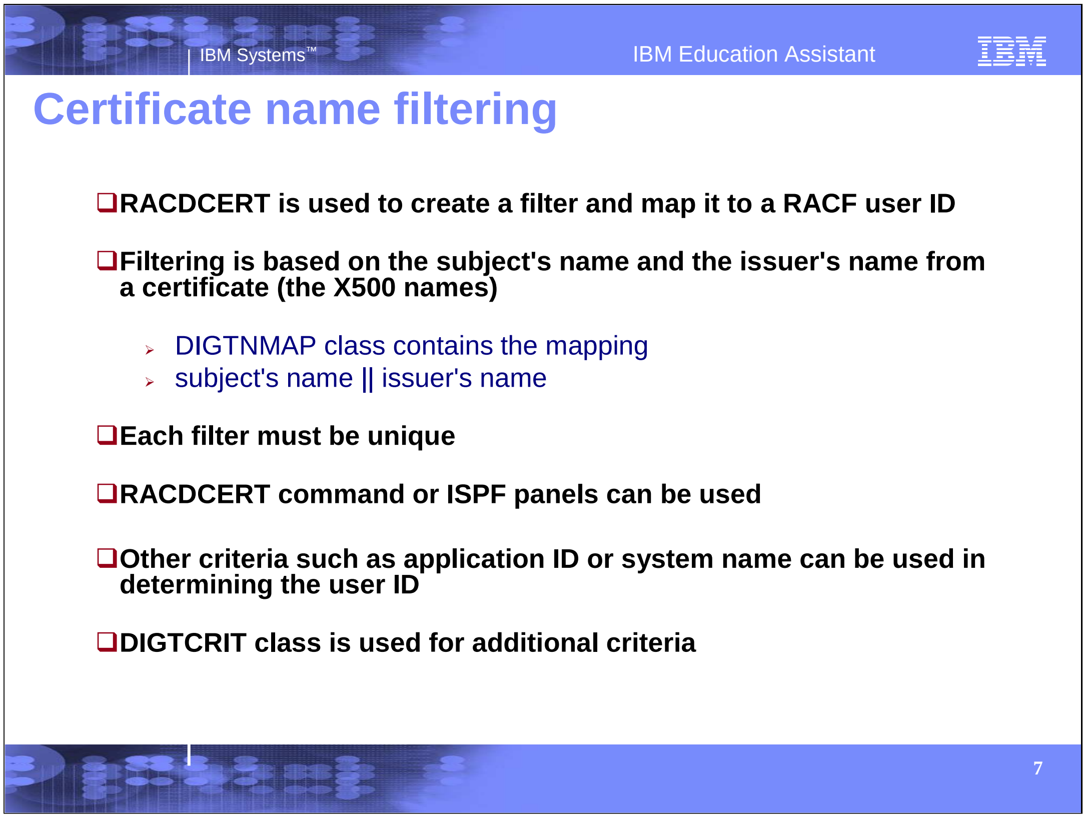
Can be selectively mapped to different user IDs based on system and application criteria.

Are logged on use with audit records that include the associated user ID and the certificate's full subject's and issuer's name. Through SMF recording, the individual accountability is maintained. The Subject’s DN and Issuer’s DN is recorded in the SMF record.

•CNF is only for creating security contexts (ACEEs) when clients are authenticating to z/OS using a certificate. CNF cannot be used as a replacement for a real certificate (and key ring) for, say, an SSL server application.

•As we will see a little later, shared user IDs can also be restricted.

•So let us explore how to set up these filters or mappings.



IBM Systems™

IBM Education Assistant

Certificate name filtering

- RACDCERT is used to create a filter and map it to a RACF user ID
- Filtering is based on the subject's name and the issuer's name from a certificate (the X500 names)
  - DIGTNMAP class contains the mapping
  - subject's name || issuer's name
- Each filter must be unique
- RACDCERT command or ISPF panels can be used
- Other criteria such as application ID or system name can be used in determining the user ID
- DIGTCRIT class is used for additional criteria

7

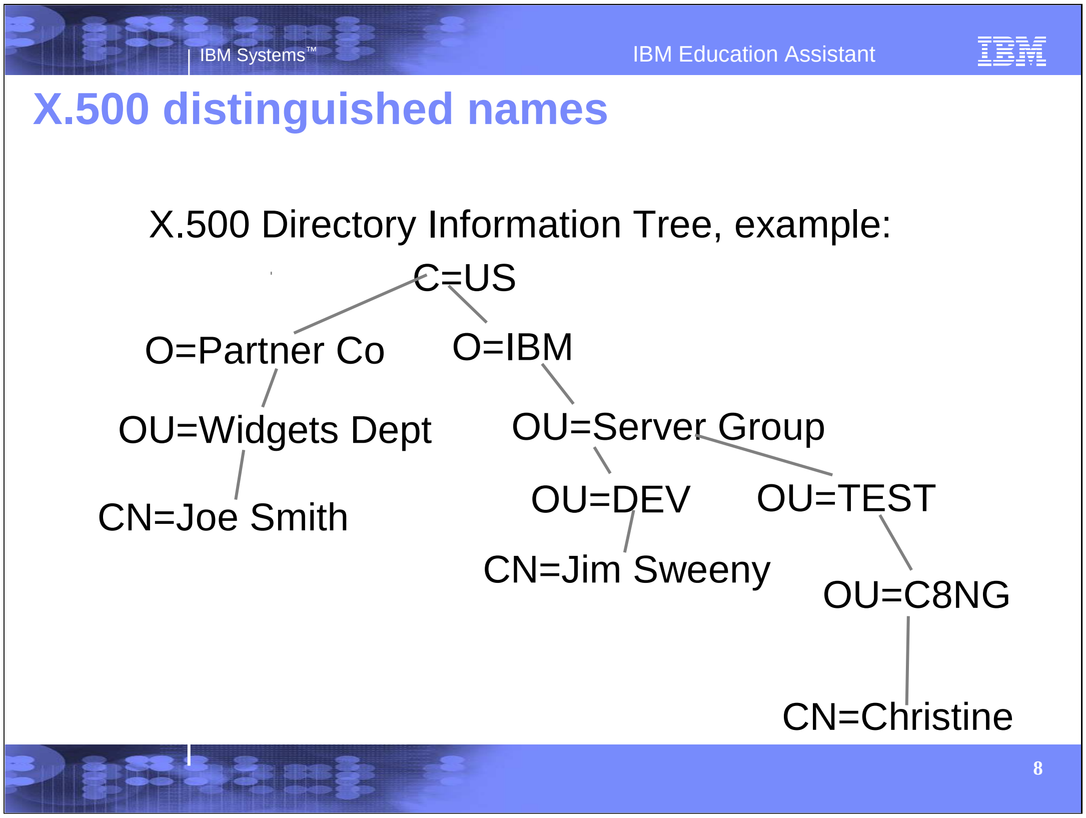
•So, how can we create these filters? Using RACF's digital certificate management command, RACDCERT, filters can be added to the RACF database that will allow users to be mapped to certificates.

•These filters or mappings are based on the subject's distinguished name and the issuer's distinguished name (the x500 names) located in a certificate. The actual filters are stored in a RACF profile. The profiles for these filters are created in the format of a hash of the subject's name concatenated with a hash of the issuer's name. These profiles are in the DIGTNMAP class. When you create a certificate name filter, RACDCERT MAP processing automatically creates a mapping profile in the DIGTNMAP class to represent the new filter. The DIGTNMAP class must be active and SETROPTS RACLIST processing must be active for the DIGTNMAP class.

•In order to find the proper mapping, each filter must be unique.

•Filters can be created using TSO with the RACDCERT command or ISPF panels.

•Besides the filtering with the subject's name and issuer's name, additional criteria can be utilized in associating the certificate with a user ID. We will examine the additional criteria in a moment.



IBM Systems™ IBM Education Assistant

X.500 distinguished names

X.500 Directory Information Tree, example:

C=US

O=Partner Co

O=IBM

OU=Widgets Dept

OU=Server Group

CN=Joe Smith

OU=DEV

OU=TEST

CN=Jim Sweeny

OU=C8NG

CN=Christine

To better understand how the filters are created and examined, let’s first look at an X.500 Directory Information Tree. Looking at the above example, there are three different paths.

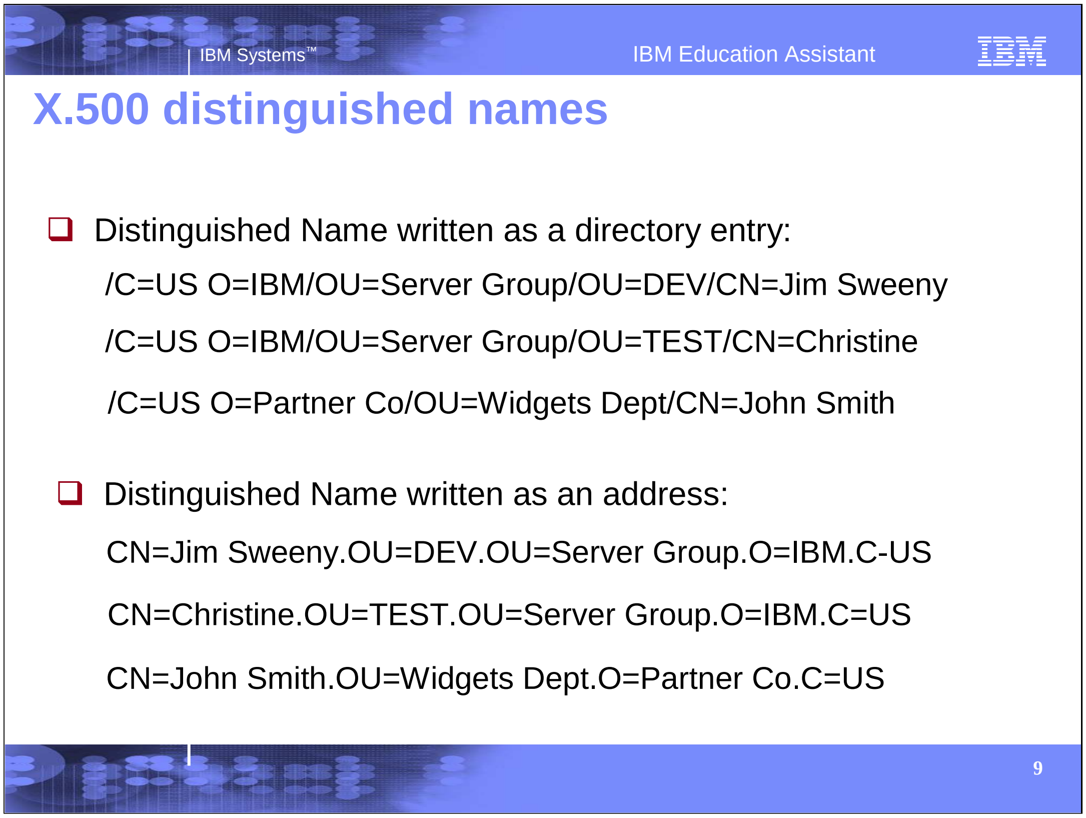
•We start at the top of the tree where Country(C)=US

•There are two unique Organizational RDNs (Relative Distinguished Name); O=Partner Co and O=IBM.

•Following down the tree from O=IBM, the next least significant RDN is OU=Server Group.

•From this point, the tree diverges again, one branch to OU=DEV and the other branch to OU=TEST.

•This is a way to uniquely identify a subject.



IBM Systems™

IBM Education Assistant

X.500 distinguished names

- ❑ Distinguished Name written as a directory entry:

  /C=US O=IBM/OU=Server Group/OU=DEV/CN=Jim Sweeny

  /C=US O=IBM/OU=Server Group/OU=TEST/CN=Christine

  /C=US O=Partner Co/OU=Widgets Dept/CN=John Smith

- ❑ Distinguished Name written as an address:

  CN=Jim Sweeny.OU=DEV.OU=Server Group.O=IBM.C-US

  CN=Christine.OU=TEST.OU=Server Group.O=IBM.C=US

  CN=John Smith.OU=Widgets Dept.O=Partner Co.C=US

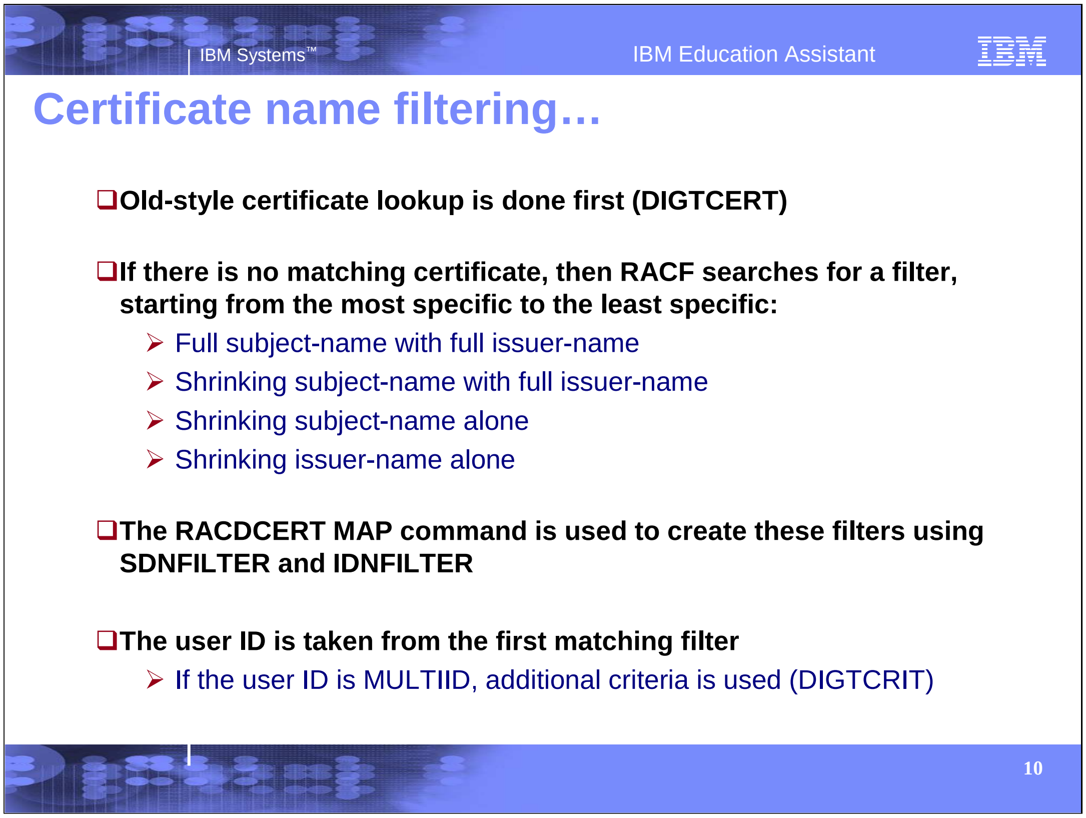
9

•So, looking at how the X.500 Distinguished names are written in a directory, the RDNs start at the top of the tree and work down to the least significant.

•In the first example, Country (C)=US is the top of the tree. The next RDN is Organization (O) = IBM. Followed by Organizational Unit (OU) = Server Group; another Organization Unit = DEV and, lastly, Common Name (CN)=Jim Sweeny is the least significant RDN.

•If you were to write the Distinguished Name as an address, however, the order would be reversed. CN=Jim Sweeny would be the leftmost RDN. A subject’s distinguished name, for example, would be CN=Jim Sweeny.OU=DEV.OU=Server Group.O=IBM.C=US.

•This is how it appears in RACF and how the filters for Certificate Name Filtering will be stored.



IBM Systems™

IBM Education Assistant

Certificate name filtering…

- ❑ **Old-style certificate lookup is done first (DIGTCERT)**
- ❑ **If there is no matching certificate, then RACF searches for a filter, starting from the most specific to the least specific:**
  - ➢ Full subject-name with full issuer-name
  - ➢ Shrinking subject-name with full issuer-name
  - ➢ Shrinking subject-name alone
  - ➢ Shrinking issuer-name alone
- ❑ **The RACDCERT MAP command is used to create these filters using SDNFILTER and IDNFILTER**
- ❑ **The user ID is taken from the first matching filter**
  - ➢ If the user ID is MULTIID, additional criteria is used (DIGTCRIT)

10

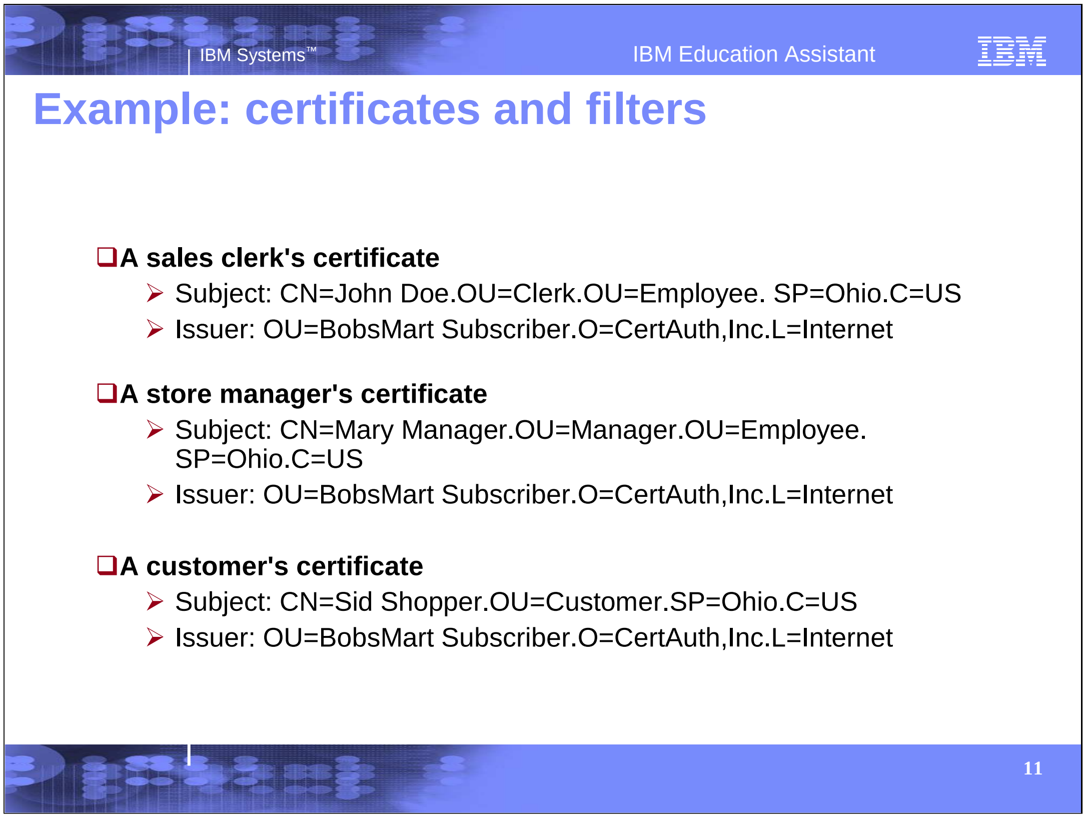
•When determining if the incoming certificate is associated with a RACF user ID, the original design to do a certificate lookup in the RACF database is done (checking the profiles in the DIGTCERT class).

•If there is no match, RACF will search for a filter, starting from the most specific to the least specific. As in the above description, first the profiles in the DIGTNMAP class will be a searched using the full subject's distinguished name concatenated with the full issuer's distinguished name. If no mapping profile is found, the next search will be on a continual shortening of the subject's distinguished name concatenated with a full issuer's distinguished name. If, again, no mapping profile is found for that, the next search will be based on the continual shortening of the subject's distinguished name only. Finally, if there is still no profile found, the last search will be on the continual shortening of the issuer's distinguished name. To make this a little more clear, we will go through some examples of this shortly.

•The MAP function of the RACDCERT command is used to set up the filters. SDNFILTER for the subject's distinguished name filter and IDNFILTER for the issuer's distinguished name filter. These subfunctions specify the significant portion of the subject's distinguished name and possibly the issuer's distinguished name. This is the part of the name that will be used as a filter when associating a user ID with a certificate. The IDNFILTER is optional if the SDNFILTER is specified. More information to follow after some examples.

•As soon as a match occurs, the user ID associated with that filter is taken from that profile.

•With the MULTIID keyword as the user ID, additional criteria is used.



Example: certificates and filters

❑ **A sales clerk's certificate**
- ➢ Subject: CN=John Doe.OU=Clerk.OU=Employee. SP=Ohio.C=US
- ➢ Issuer: OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet

❑ **A store manager's certificate**
- ➢ Subject: CN=Mary Manager.OU=Manager.OU=Employee. SP=Ohio.C=US
- ➢ Issuer: OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet

❑ **A customer's certificate**
- ➢ Subject: CN=Sid Shopper.OU=Customer.SP=Ohio.C=US
- ➢ Issuer: OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet

•Let’s look at three different certificates all stated in the x500 format.

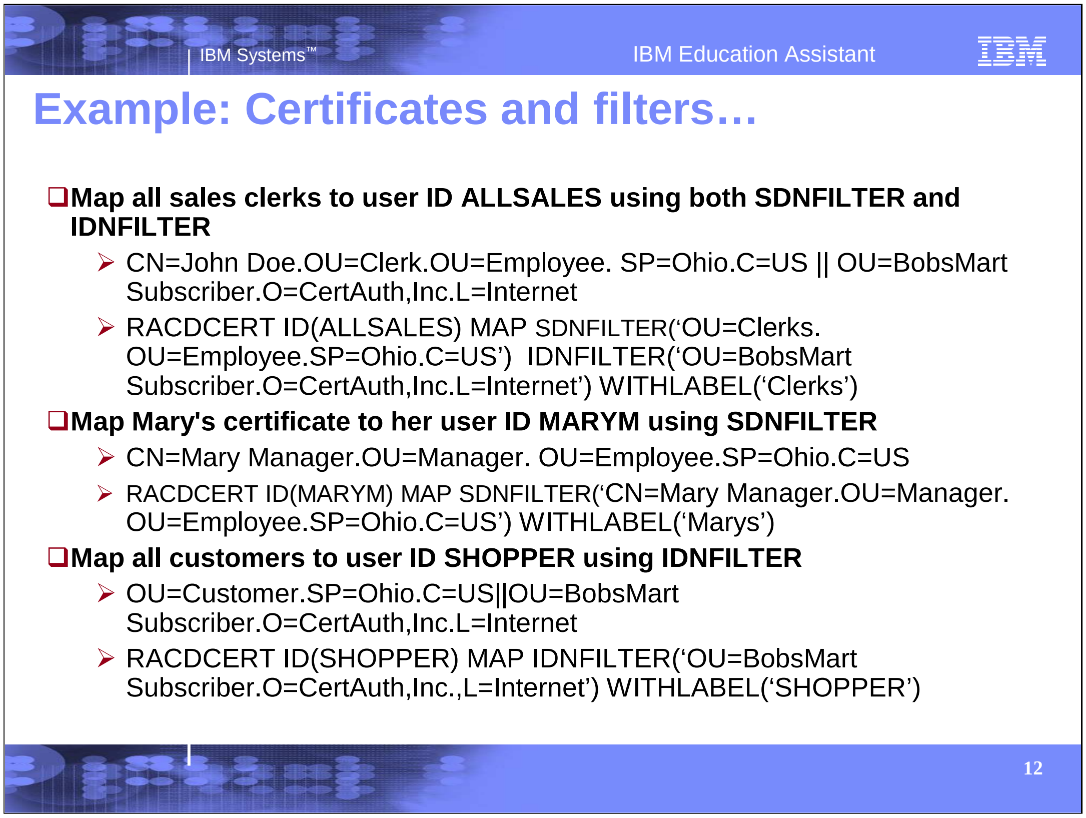
•All three certificates have the same Issuer’s distinguished name. That issuer’s name is the Organizational unit of BobsMart Subscriber, with the Organization of CertAuth, Inc and the Locality of Internet. All certificates for shoppers and store clerks will have this issuer.

•The sales clerk’s certificate has the Common name as John Doe, organizational units of Clerk and Employee, the state or province of Ohio, and country is United States.

•Mary, the store manager has the common name of Mary Manager with the organizational units of manager and employee, with the state or province being Ohio and the country is United States.

•The last certificate is issued to a customer, Sid Shopper. Sid’s certificate has the common name of Sid Shopper with the Organizational unit of Customer, the State as Ohio and the country is United States.

•Now that we have the certificates issued, let’s see how we can use these as filters.


IBM Systems™
IBM Education Assistant
12

Example: Certificates and filters…

❑ **Map all sales clerks to user ID ALLSALES using both SDNFILTER and IDNFILTER**

- ➢ CN=John Doe.OU=Clerk.OU=Employee. SP=Ohio.C=US || OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet
- ➢ RACDCERT ID(ALLSALES) MAP SDNFILTER(‘OU=Clerks. OU=Employee.SP=Ohio.C=US’) IDNFILTER(‘OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet’) WITHLABEL(‘Clerks’)

❑ **Map Mary's certificate to her user ID MARYM using SDNFILTER**

- ➢ CN=Mary Manager.OU=Manager. OU=Employee.SP=Ohio.C=US
- ➢ RACDCERT ID(MARYM) MAP SDNFILTER(‘CN=Mary Manager.OU=Manager. OU=Employee.SP=Ohio.C=US’) WITHLABEL(‘Marys’)

❑ **Map all customers to user ID SHOPPER using IDNFILTER**

- ➢ OU=Customer.SP=Ohio.C=US||OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet
- ➢ RACDCERT ID(SHOPPER) MAP IDNFILTER(‘OU=BobsMart Subscriber.O=CertAuth,Inc.,L=Internet’) WITHLABEL(‘SHOPPER’)

•All the sales clerks are issued certificates signed by the same Issuer’s Distinguished Name plus in the Subject’s Distinguished name the Organization Unit of ‘Clerks’ should identify the certificates for use by the sales clerks. [enter] The first example creates the mapping to ALLSALES using this rule. This filter uses the issuer’s distinguished name in it’s entirety with a partial subject’s distinguished name in the filter. To do this, issue the following:

RACDCERT ID(ALLSALES) MAP SDNFILTER(‘OU=Clerks.OU=Employee.SP=Ohio.C=US’) IDNFILTER(‘OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet’) WITHLABEL(‘Clerks’)

•Next, we want to set up the manager’s user ID. Mary Manager’s user ID is MARYM. We want to set up her filter on just the subject’s name. All certificates issued to Mary Manager with the same subject’s distinguished name should be associated with the user ID MARYM regardless of the issuer of the certificate. [enter] To do this, issue the following:

RACDCERT ID(MARYM) MAP SDNFILTER(‘CN=Mary Manager.OU=Manager. OU=Employee.SP=Ohio.C=US’)

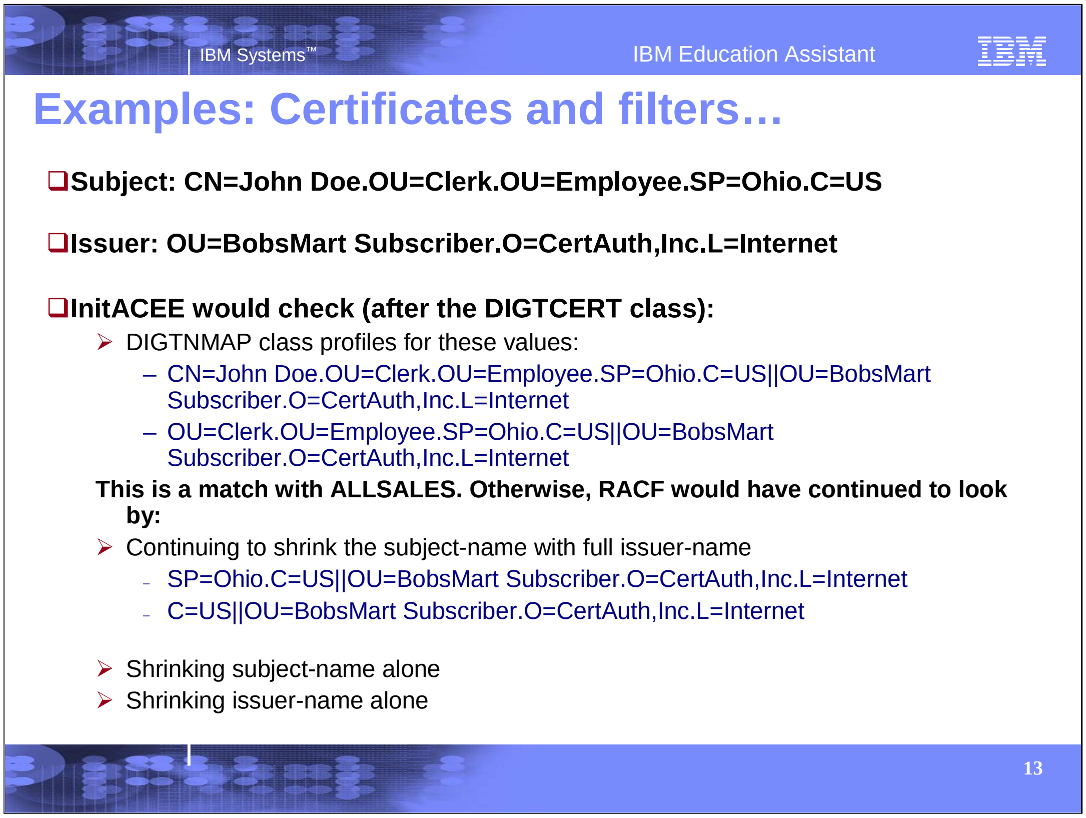
WITHLABEL(‘Marys’)

This filter uses the subject’s distinguished name in it’s entirety with no issuer’s distinguished name in the filter.

•Customer’s may only need to be associated with one user ID. However, only certificates issued by Bob’sMart will be accepted. Therefore, using only the Issuer’s Distinguished Name in the mapping will suffice. [enter] Looking at the third example, the filter of IDNFILTER(‘OU=BobsMart Subscriber, O=CertAuth, Inc.,L=Internet will map to the user ID of SHOPPER. This filter uses the issuer’s distinguished name in it’s entirety. To do this, issue the following:

RACDCERT ID(SHOPPER) MAP IDNFILTER(‘OU=BobsMart Subscriber.O=CertAuth,Inc.,L=Internet’) WITHLABEL(‘SHOPPER’)

It is important to note that this filter would give the user ID of SHOPPER and in all the above examples, the same Issuer’s distinguished name is used. If, for example, Mary Manager’s subject’s distinguished name changes slightly in a renewed certificate to CN= Mary I Manager and the issuer’s name is OU=BobsMart Subscriber.O=CertAuth,Inc..L=Internet, the user ID of SHOPPER would be the match. That might not be the intended outcome. It is important to understand the certificates and the rules that will be used when setting up filters.



IBM Systems™ IBM Education Assistant

Examples: Certificates and filters…

- ❑**Subject: CN=John Doe.OU=Clerk.OU=Employee.SP=Ohio.C=US**
- ❑**Issuer: OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet**
- ❑**InitACEE would check (after the DIGTCERT class):**
  - ➢ DIGTNMAP class profiles for these values:
    - – CN=John Doe.OU=Clerk.OU=Employee.SP=Ohio.C=US||OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet
    - – OU=Clerk.OU=Employee.SP=Ohio.C=US||OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet

  This is a match with ALLSALES. Otherwise, RACF would have continued to look by:
  - ➢ Continuing to shrink the subject-name with full issuer-name
    - – SP=Ohio.C=US||OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet
    - – C=US||OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet
  - ➢ Shrinking subject-name alone
  - ➢ Shrinking issuer-name alone

•Now let us look at the process that RACF will go through to associate the certificate with the above subject's distinguished name and issuer's distinguished name.

•First, the callable service InitACEE would check if the certificate is installed in the RACF database and associated with what user ID. If that is not found, then the DIGTNMAP profiles will be searched starting with a full subject's distinguished name concatenated with a full issuer's distinguished name. So for the example above, a search for the profile that has :

> CN=John Doe.OU=Clerk.OU=Employee.SP=Ohio.C=US||OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet will be done. If that is not found, and for this example, it is not, the leftmost RDN (relative distinguished name) would be removed. CN=John Doe would be taken out of the search. The profile that has the filter of OU=Clerk.OU=Employee.SP=Ohio.C=US||OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet would be searched next. For our example, that is a match with the user ID ALLSALES.

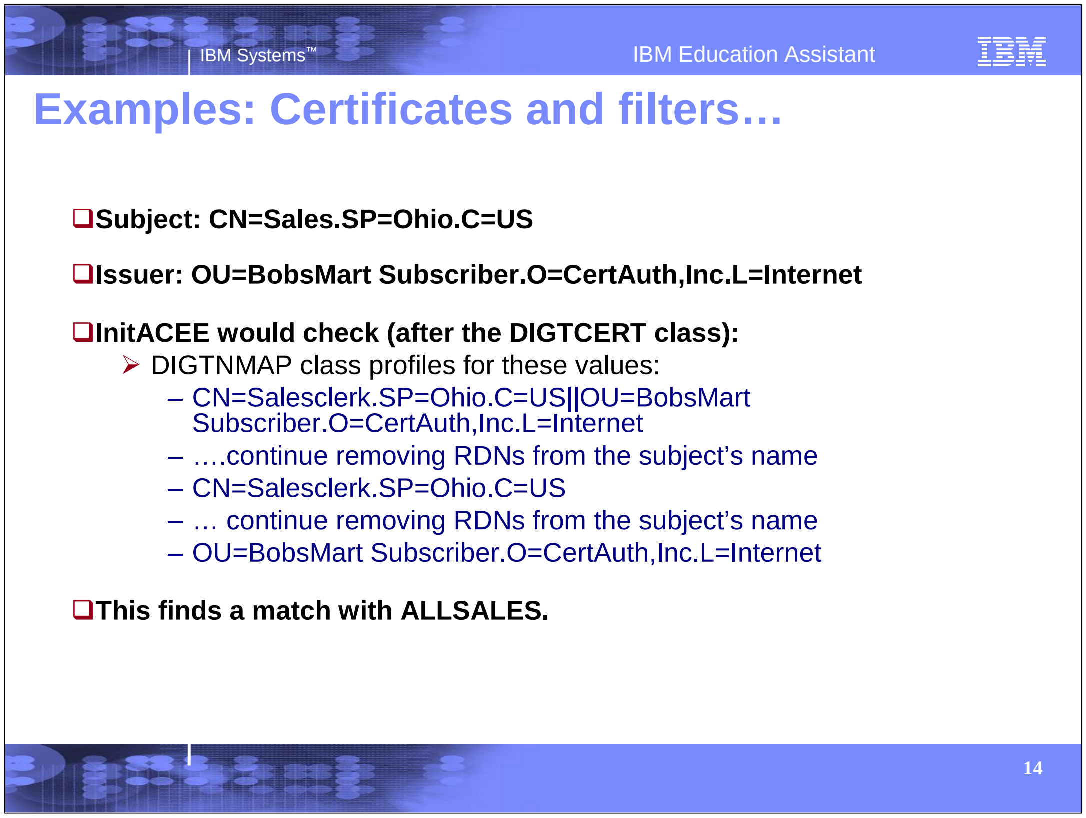
•ALLSALES would be the RACF user ID used for the transaction.

•If there was still no profile match, RACF would continue removing the leftmost RDN from the subject's distinguished name and continue searching until there were no more RDNs in the subject's name.

•At that point, a new search would begin with only using the subject's distinguished name and removing the leftmost for each level of search. For example: first search would be CN=John Doe.OU=Clerk.OU=Employee.SP=Ohio.C=US, if that does not find a match, the next search would be OU=Clerk.OU=Employee.SP=Ohio.C=US and so on and so forth.

•If there was still no filter found, a search on issuer's distinguished name only will be done the same way as the subject's distinguished name.

•As mentioned above, for our example, a match was found and the user ID was ALLSALES.



Examples: Certificates and filters…

❑**Subject: CN=Sales.SP=Ohio.C=US**

❑**Issuer: OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet**

❑**InitACEE would check (after the DIGTCERT class):**

- ➢ DIGTNMAP class profiles for these values:
  - – CN=Salesclerk.SP=Ohio.C=US||OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet
  - – ….continue removing RDNs from the subject's name
  - – CN=Salesclerk.SP=Ohio.C=US
  - – … continue removing RDNs from the subject's name
  - – OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet

❑**This finds a match with ALLSALES.**

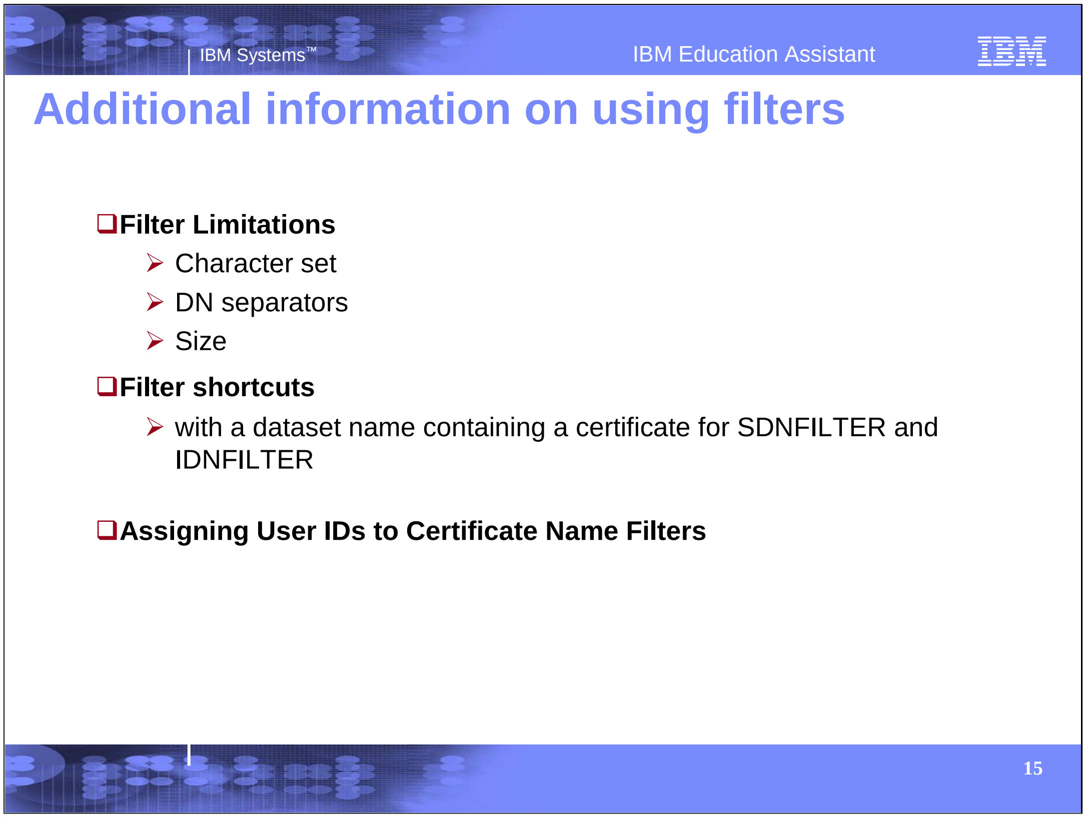
•For the example we created with the second certificate, the same lookup would be done. First, starting with the certificate located in the RACF database (a search in the DIGTCERT class) and then the searching through the RDNs for the filter that would match in the DIGTNMAP class.

•In this case, the subject's distinguished name was not a part of the filter. The search still started with the full subject's name and full issuer's name down to the search of issuer's name only.

•That filter matched the mapping we set up on a previous slide with the command RACDCERT ID(ALLSALES) MAP IDNFILTER('OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet') WITHLABEL('Clerks').

•As you see, the more full the filter, the faster the search will be satisfied.

•Also note that the RDNs are removed with the leftmost being removed. If the filter needs to be for the above certificate, a filter with one of the RDNs removed from the middle would not match. For example, if there was a filter CN=Salesclerk.C=US for user ID JOHNDOE there would not be a match on the above certificate. The match would be on ALLSALES.



Additional information on using filters

- ❑**Filter Limitations**
  - ➢ Character set
  - ➢ DN separators
  - ➢ Size
- ❑**Filter shortcuts**
  - ➢ with a dataset name containing a certificate for SDNFILTER and IDNFILTER
- ❑**Assigning User IDs to Certificate Name Filters**

•The value specified for SDNFILTER and IDNFILTER must begin with a prefix found in the following list, followed by an equal sign (X'7E'). Each component should be separated by a period (X'4B'). The case, blanks, and punctuation displayed when the digital certificate information is listed must be maintained in the SDNFILTER and IDNFILTER. Since digital certificates only contain characters available in the ASCII character set, the same characters should be used for the SDNFILTER and IDNFILTER value. Valid prefixes are:

Common Name Specified as CN= .**Title** Specified as T= .**Organizational Unit** Specified as OU=

Organization Specified as O= .**Locality** Specified as L= .**State/Province** Specified as SP= . **Country** Specified as C=

IDNFILTER is optional if SDNFILTER is specified. If IDNFILTER is not specified, only the subject's name is used as a filter. If IDNFILTER is specified and only a portion of the issuer's name is to be used as the filter, SDNFILTER must not be specified.

If both IDNFILTER and SDNFILTER are specified, the IDNFILTER value does not need to begin with a valid prefix from the list above. This allows the use of certificates from a certificate authority that chooses to include nonstandard data in the issuer's distinguished name.

•There is a limit of 255 characters for the subject's distinguished name and 255 characters for the issuer's distinguished name.

•A data set name can be specified with the MAP keyword. The *data-set-name* value is the name of the data set that contains a certificate. The certificate provides a model for the filter names specified with SDNFILTER and IDNFILTER. The subject's distinguished name is used beginning with the value specified by SDNFILTER. The issuer's distinguished name is used beginning with the value specified by IDNFILTER. For example, using our certificates created previously, if there was a certificate in a dataset that had the Issuer's distinguished name of OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet, the IDNFILTER('OU=') would create the filter 'OU=BobsMart Subscriber.O=CertAuth,Inc.L=Internet'.

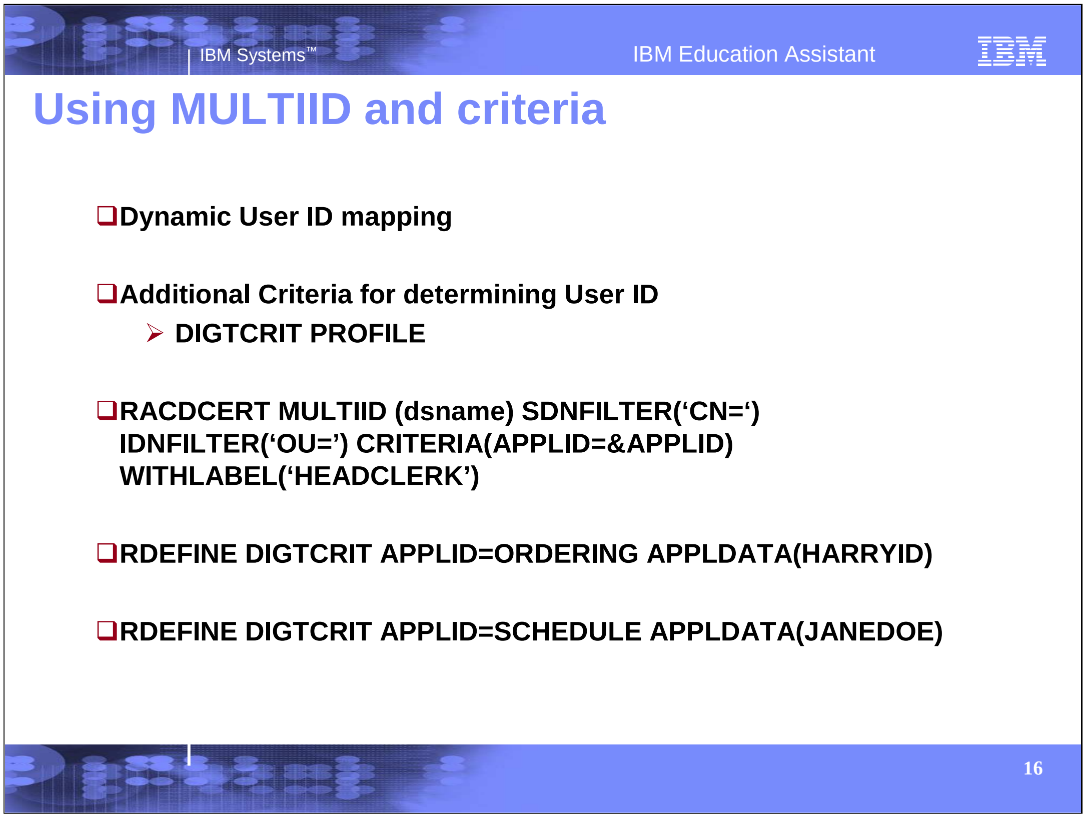
•Using a model certificate is optional but can reduce the chance of typographical errors when entering long filters for SDNFILTER or IDNFILTER.

•The model certificate used with the MAP keyword can have an issuer's distinguished name or subject's distinguished name that exceeds 255 characters. However, the portion of each used in the filter to associate a user ID with the certificate cannot exceed 255 characters.

•You must define a RACF user ID for each user ID you associate with a certificate name filter. Since these user IDs may be shared, you should consider assigning the PROTECTED and RESTRICTED attributes to each one. For example:

```
ALTUSER OHIOUSER NOPASSWORD RESTRICTED
```

The PROTECTED attribute protects the user ID from being used to logon directly to the system and from being revoked through incorrect password and pass phrase attempts.



IBM Systems™ IBM Education Assistant

Using MULTIID and criteria

❑ **Dynamic User ID mapping**

❑ **Additional Criteria for determining User ID**

  ➢ **DIGTCRIT PROFILE**

❑ **RACDCERT MULTIID (dsname) SDNFILTER(‘CN=‘) IDNFILTER(‘OU=’) CRITERIA(APPLID=&APPLID) WITHLABEL(‘HEADCLERK’)**

❑ **RDEFINE DIGTCRIT APPLID=ORDERING APPLDATA(HARRYID)**

❑ **RDEFINE DIGTCRIT APPLID=SCHEDULE APPLDATA(JANEDOE)**

16

•We mentioned earlier that with using MULTIID additional criteria can be added in determining the user ID associated with the certificate. Let’s look at how this can be done.

•When the RACDCERT MAP command is specified with MULTIID, it indicates a dynamic user ID mapping. The user ID associated with this mapping profile is based not only on the issuer's distinguished name and the subject's distinguished name found in the certificate, but also on additional criteria. The *criteria-profile-name-template* specifies the additional criteria in the form of a profile name containing one or more variable names, separated by free-form text. These variable names begin with an ampersand (&) and end with a period.

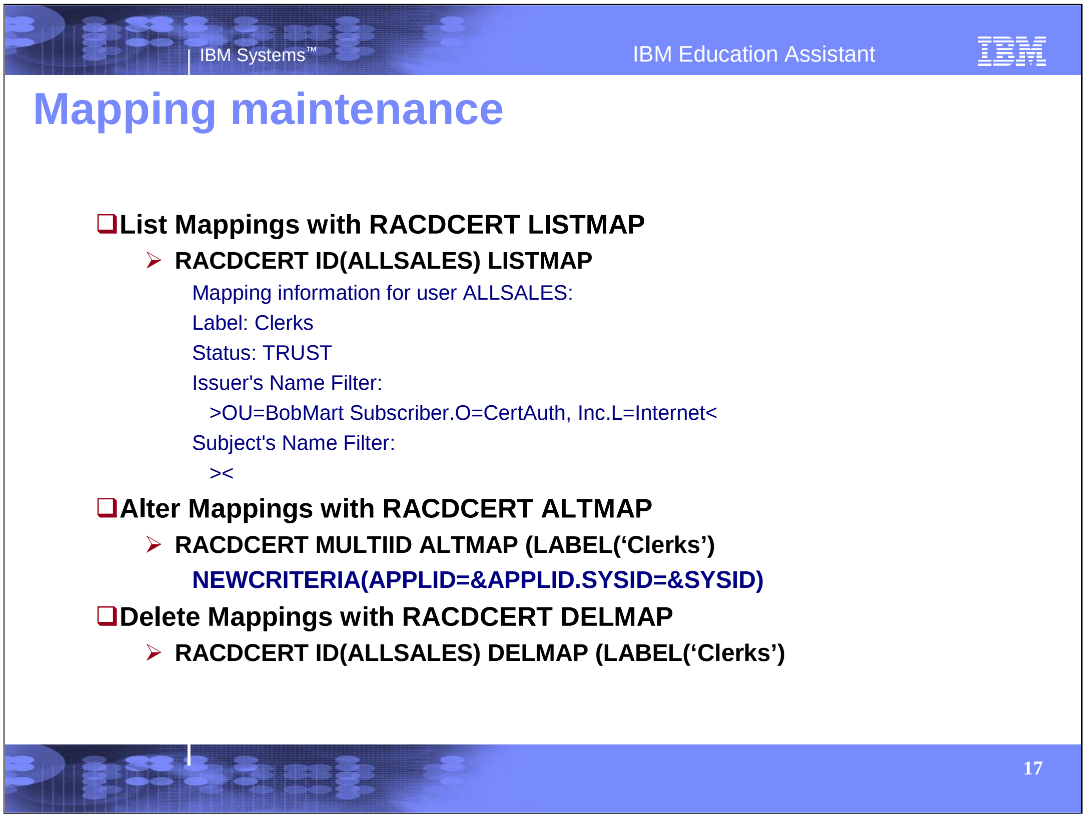
•For example, if the application identity is to be considered in determining the user ID associated with this mapping, the CRITERIA keyword should be specified as follows:

CRITERIA(APPLID=&APPLID)

•When a user presents a certificate to the system for identification, the identity of the application being accessed becomes part of the criteria. The application passes its identity to RACF. The value Is substituted for &APPLID in the criteria. Once the substitution is made, the fully expanded criteria template is used as a resource name to find a matching profile defined in the DIGTCRIT class using the RDEFINE command. For example, if the application being accessed is ODERING, the template is:

APPLID=ODERING

•You define a profile in the DIGTCRIT class using the RDEFINE command for this name. The user ID to be associated with these certificates must be specified as the APPLDATA. In the above example, if the application is SCHEDULE, the user ID would be JANEDOE, if the application is ORDERING, the user ID would be HARRYID.



IBM Systems™ IBM Education Assistant IBM

Mapping maintenance

❑ **List Mappings with RACDCERT LISTMAP**

➢ **RACDCERT ID(ALLSALES) LISTMAP**

```
Mapping information for user ALLSALES:
Label: Clerks
Status: TRUST
Issuer's Name Filter:
  >OU=BobMart Subscriber.O=CertAuth, Inc.L=Internet<
Subject's Name Filter:
  ><
```

❑ **Alter Mappings with RACDCERT ALTMAP**

➢ **RACDCERT MULTIID ALTMAP (LABEL('Clerks')**

NEWCRITERIA(APPLID=&APPLID.SYSID=&SYSID)

❑ **Delete Mappings with RACDCERT DELMAP**

➢ **RACDCERT ID(ALLSALES) DELMAP (LABEL('Clerks')**

17

•We will need to maintain the mappings we created. Let's look at the additional functions available to us through the RACDCERT command.

•RACDCERT MAP processing automatically creates mapping profiles in the DIGTNMAP class for each certificate name filter you create. When you map a certificate name filter to a RACF user ID, both the filter and the user ID are stored in the mapping profile. DIGTNMAP profiles should not be administered using the RDEFINE, RALTER or RDELETE commands. These commands do not operate with the DIGTNMAP class.

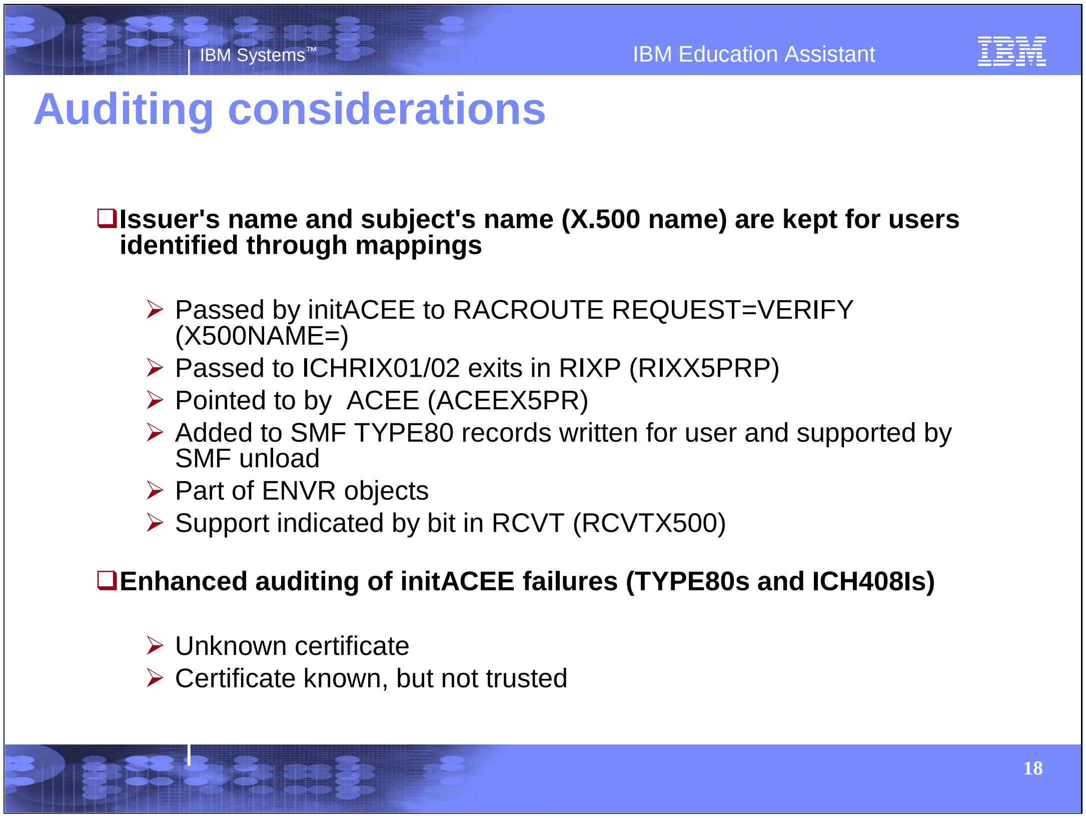
•The SEARCH FILTER and RLIST commands are not intended for use with profiles in the DIGTNMAP class and will deliver unpredictable results. These profiles can only be displayed using the RACDCERT LISTMAP command: For example:

RACDCERT ID(ALLSALES) LISTMAP

Based on the output of the RACDCERT LISTMAP command shown above, there is one certificate name filter associated with the ALLSALES user ID.

•To change the label, trust status, or criteria associated with the mapping identified by label-name, the ALTMAP function is used . Specifying label name is required if more than one mapping is associated with the user ID. TRUST indicates whether this mapping can be used to associate a user ID to a certificate presented by a user accessing the system. If the criteria changes, the subkeyword used is NEWCRITERIA. In the above example, we are adding the criteria of SYSID (the system identifier (SYSID). The SYSID is the 4-character SID value specified in the SMFPRMxx member of SYS1.PARMLIB on each system.

•As expected, to discard a current mapping, the RACDCERT DELMAP function is used. Specifying label-name is required if more than one mapping is associated with the user ID. Note that mappings might also be deleted as part of DELUSER processing.



IBM Systems™ IBM Education Assistant

Auditing considerations

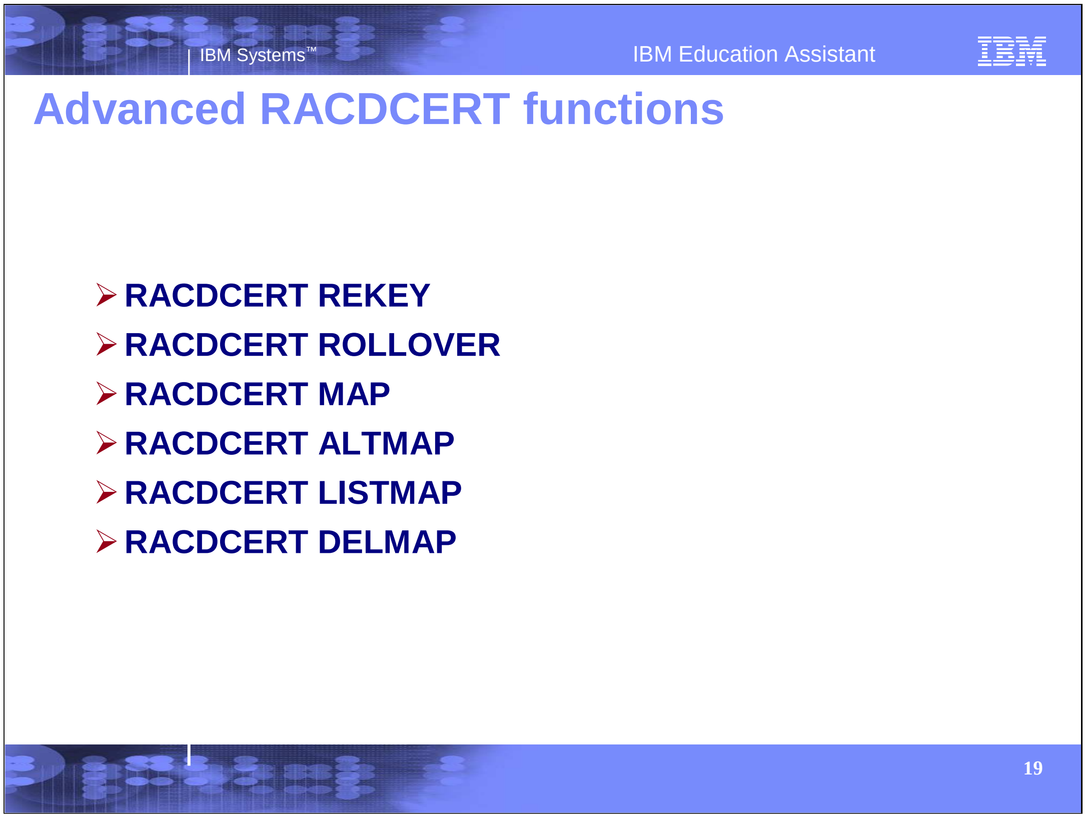
- ❑ **Issuer's name and subject's name (X.500 name) are kept for users identified through mappings**
  - ➢ Passed by initACEE to RACROUTE REQUEST=VERIFY (X500NAME=)
  - ➢ Passed to ICHRIX01/02 exits in RIXP (RIXX5PRP)
  - ➢ Pointed to by ACEE (ACEEX5PR)
  - ➢ Added to SMF TYPE80 records written for user and supported by SMF unload
  - ➢ Part of ENVR objects
  - ➢ Support indicated by bit in RCVT (RCVTX500)
- ❑ **Enhanced auditing of initACEE failures (TYPE80s and ICH408Is)**
  - ➢ Unknown certificate
  - ➢ Certificate known, but not trusted

18

•An auditor is responsible for checking that RACF is meeting the installation's needs for access control and accountability. Access control means that you can control user accesses to resources and verify that the accesses allowed are appropriate to the particular resource.

•As you can imagine, understanding and knowing the certificates that created user IDs on your system would be an important part of your security. We have created a way to audit these certificates by using the x500 name (issuer’s distinguished name concatenated with the subject’s distinguished name). This x500 name is passed by initACEE to RACROUTE, also to the VERIFY exits and is stored in the ACEE. When the user ID associated with that certificate uses a resource, SMF will record the x500 name in the Type 80 record and it is also supported by SMF Unload. Since the x500 name is part of the ACEE (ACEEX5PR), this is also a part of ENVR objects.

•Additionally, for auditing and notification of certificate failures such as the certificate is not known (no user ID association has been created) or the certificate is not trusted either by the actual certificate status or the status of the mapping, additional TYPE 80 records will be created and ICH408I messages will be given.

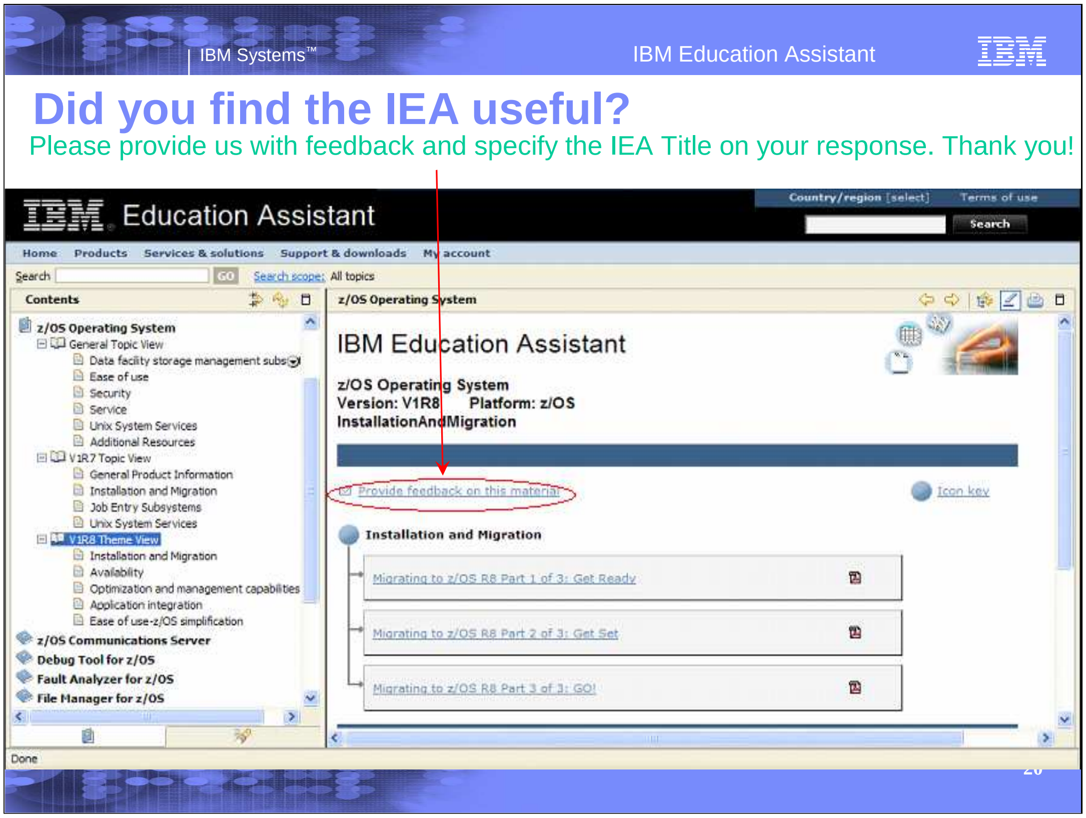


Advanced RACDCERT functions

- ➢ RACDCERT REKEY
- ➢ RACDCERT ROLLOVER
- ➢ RACDCERT MAP
- ➢ RACDCERT ALTMAP
- ➢ RACDCERT LISTMAP
- ➢ RACDCERT DELMAP

•There are other more advanced functions available with the RACDCERT command. REKEY and ROLLOVER functions are used for renewing certificate and keys and the MAP, ALTMAP, LISTMAP and DELMAP functions are used for certificate mapping, associating user IDs to special criteria.

•This brings us to the end of this presentation. See Digital Certificates and RACF Part III, for more information and examples. Part III will also go through some actual examples and ideas on how to renew certificates, log in a system without a user ID and password, how to share a certificate's associated private key in a key ring and how to use the mapping functions of RACDCERT.



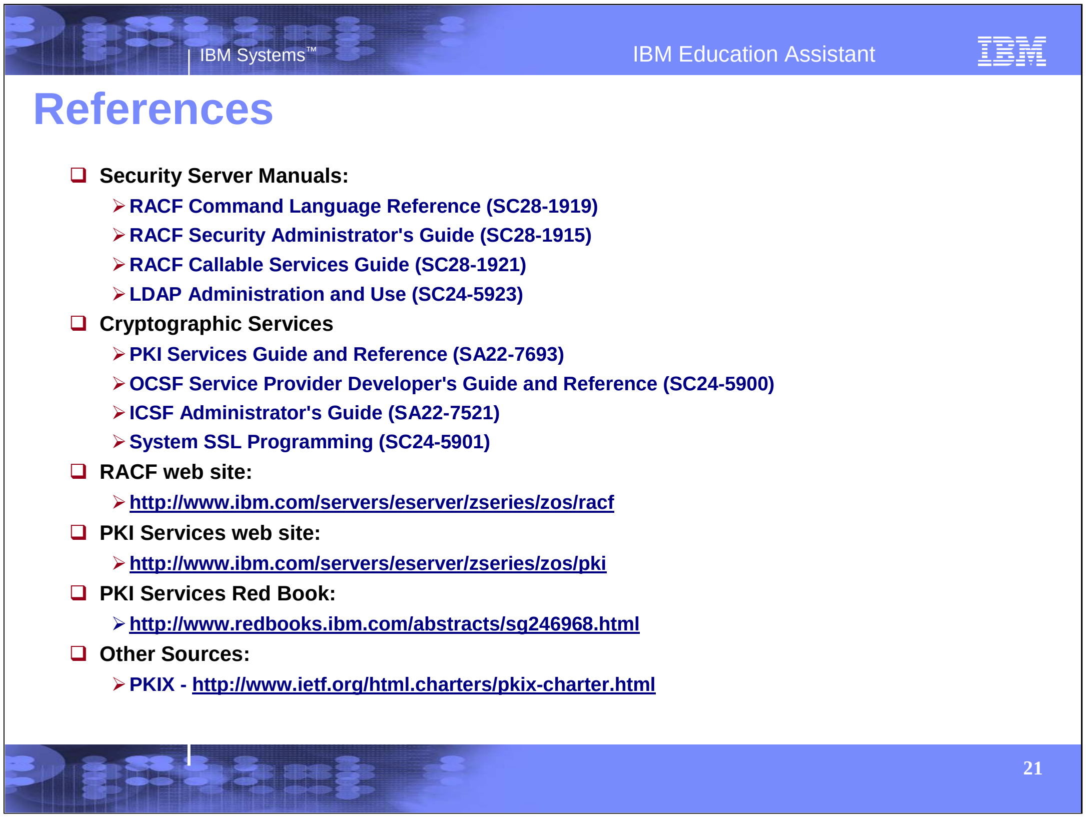
Did you find the IEA useful?

Please provide us with feedback and specify the IEA Title on your response. Thank you!

We would appreciate getting your opinions on this IBM Education Assistant module. Please take the time to help us out. In your feedback to IBM please answer the following three questions:

1. **How helpful was this IEA presentation? Please give it a rating from 1 to 5 where 1 = very helpful and 5 = not at all helpful**
2. **Did this presentation save you a service call to IBM? Yes or No**
3. **If there are any other topics would you like see covered in IEA, what are they?**

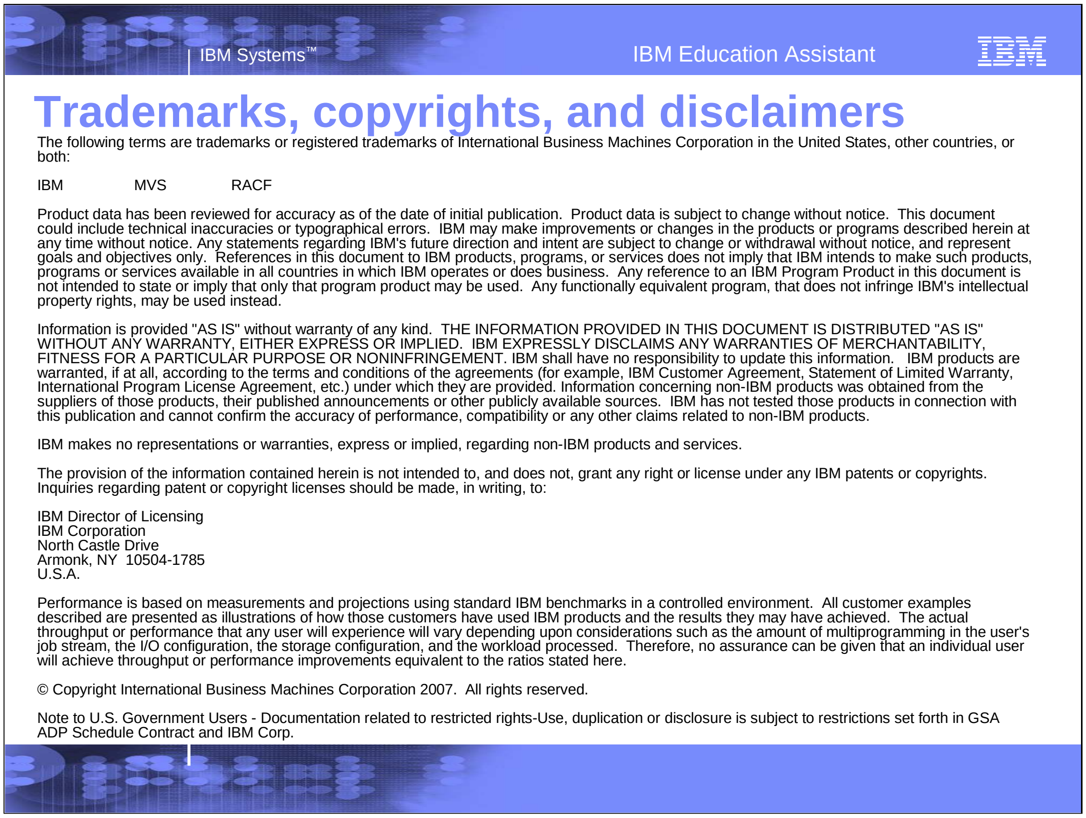
____



References

- ❑ Security Server Manuals:
  - ➢ RACF Command Language Reference (SC28-1919)
  - ➢ RACF Security Administrator's Guide (SC28-1915)
  - ➢ RACF Callable Services Guide (SC28-1921)
  - ➢ LDAP Administration and Use (SC24-5923)
- ❑ Cryptographic Services
  - ➢ PKI Services Guide and Reference (SA22-7693)
  - ➢ OCSF Service Provider Developer's Guide and Reference (SC24-5900)
  - ➢ ICSF Administrator's Guide (SA22-7521)
  - ➢ System SSL Programming (SC24-5901)
- ❑ RACF web site:
  - ➢ http://www.ibm.com/servers/eserver/zseries/zos/racf
- ❑ PKI Services web site:
  - ➢ http://www.ibm.com/servers/eserver/zseries/zos/pki
- ❑ PKI Services Red Book:
  - ➢ http://www.redbooks.ibm.com/abstracts/sg246968.html
- ❑ Other Sources:
  - ➢ PKIX - http://www.ietf.org/html.charters/pkix-charter.html

Here is a list of references to learn more about Digital Certificates, Security products such as RACF, and other Cryptographic services available with z/OS.



IBM Systems™ IBM Education Assistant

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM MVS RACF

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.