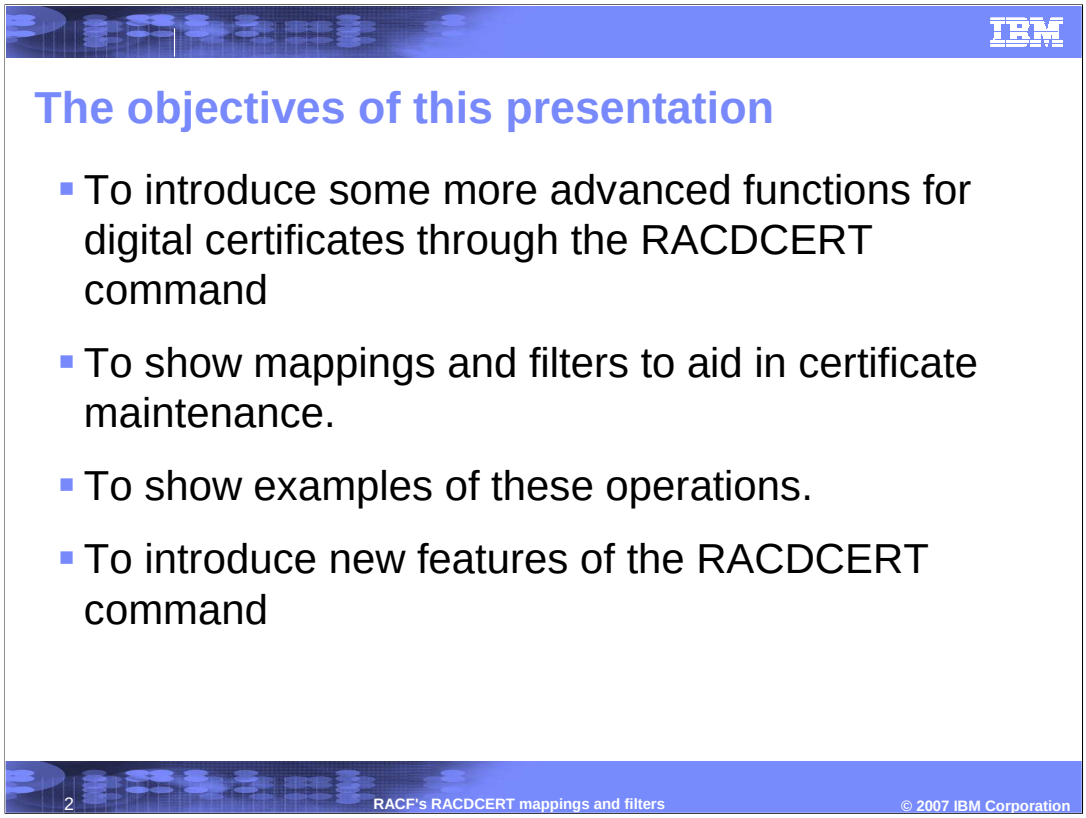
RACF's RACDCERT Mappings and filters

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



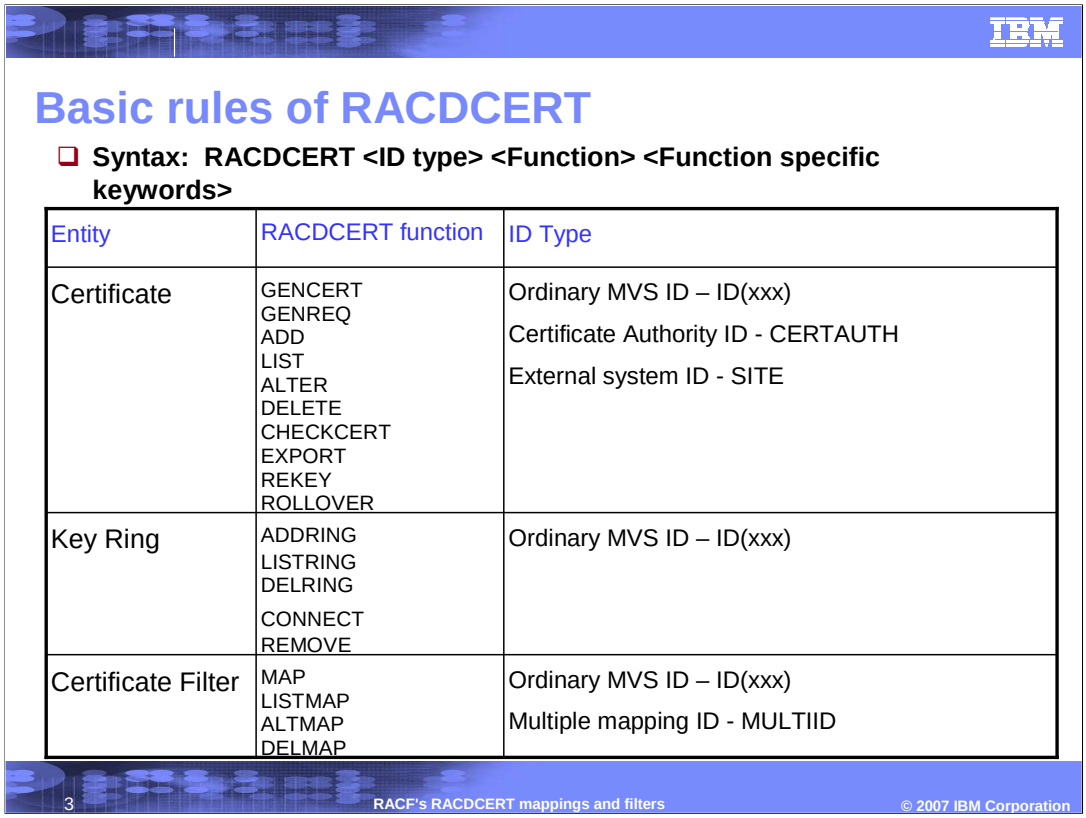
The objectives of this presentation is to look at some more advanced functions in RACF's support through the RACDCERT command.

If your business has a large certificate base, is it necessarily a good idea for you to store these certificates in the RACF database?

Can mappings and filters help with the maintenance of digital certificates?

This presentation will look at some examples of how to use these more advanced functions for mapping and filtering.

And lastly, this presentation will introduce some of the new functions that are available with the RACDCERT command and the renewal of certificates and keys..



First, a quick review of what functions are available in the RACDCERT command.

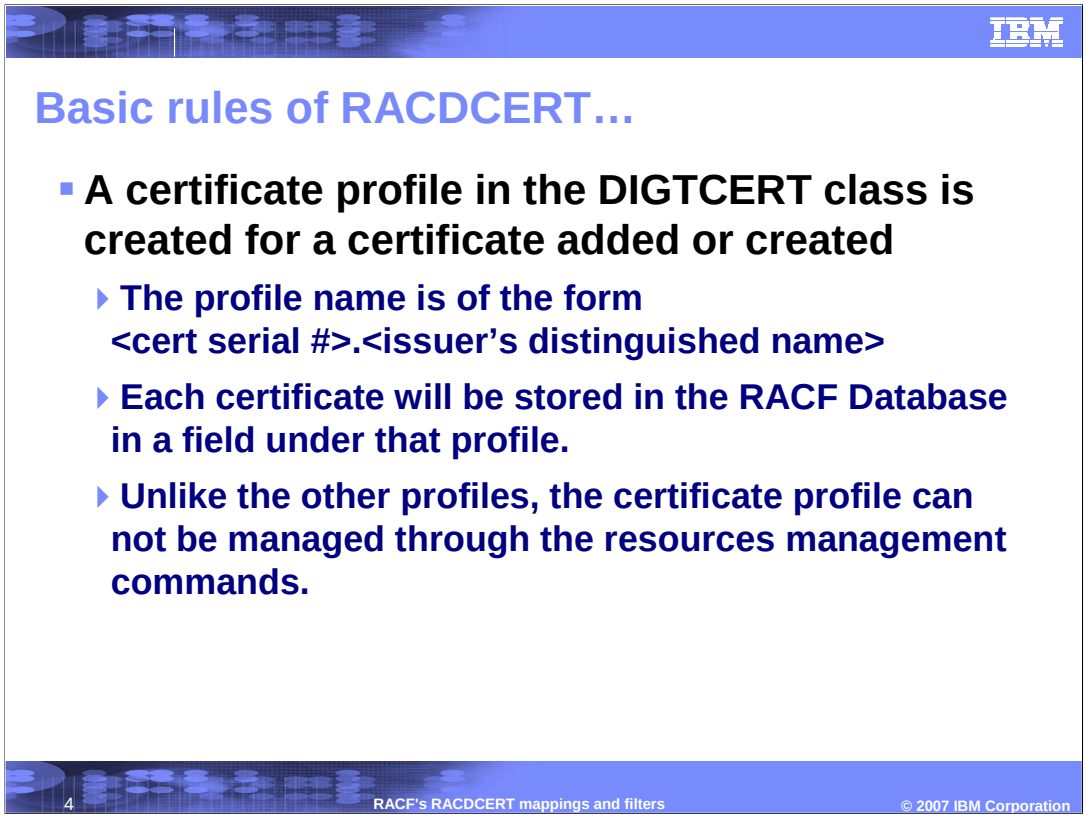
The RACDCERT command has many functions with function specific keywords for the management of certificates, certificate key rings and certificate mappings.

For certificate management, a specific user ID's certificate, a certificate authority certificate or a site certificate can be specified through ID(userid), CERTAUTH or SITE respectively. CERTAUTH and SITE are system defined IDs. SITE is used when you want to trust another site's certificate without going through the complete validation chain.

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

For certificate filters, the ID type would again be an ordinary MVS user ID or a system defined ID (MULTIID). MULTIID indicates a dynamic mapping which is based on additional criteria.

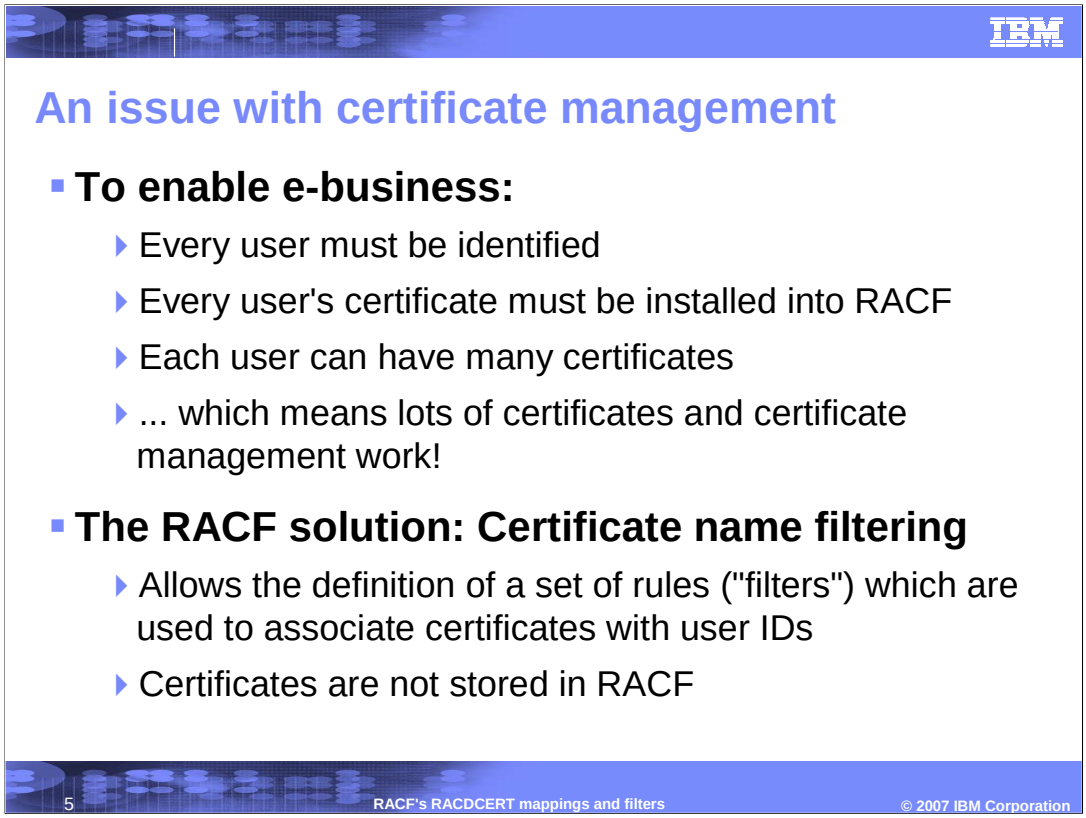
This indicates the overall syntax in a high level format to illustrate the basic concepts involved. For detailed syntax, refer to the RACF Command Language Reference publication.



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 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.

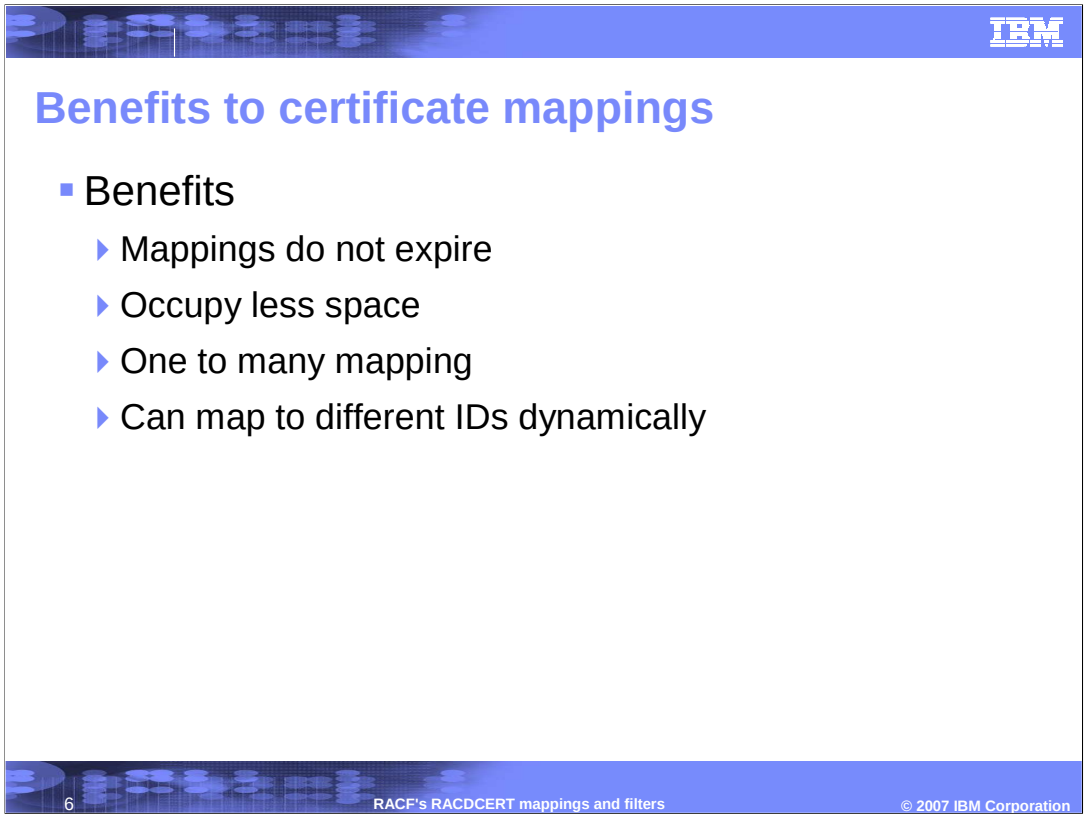
Since these certificate profiles need to be managed differently, the resources management commands such as RDEFINE, RALTER and RDELETE cannot be used. Additionally, the owner field in these profiles indicates the issuer of the original RACDCERT command that created the profile, not the owner of the certificate.

To enable authentication of a user through a certificate basically requires that certificate to be in the RACF database. For a large number of users, the effort to install and manage a large number of certificates is significant.



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 or 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. With many certificates, certificate management may become burdensome.

RACF does have a solution. Mapping certificates through Certificate Name Filtering to associate certificates with user IDs. Certificate name filtering provides a method for authenticating a user using a certificate, without storing that certificate in the RACF database.



There are benefits to using managed certificate mappings verses stored certificates.

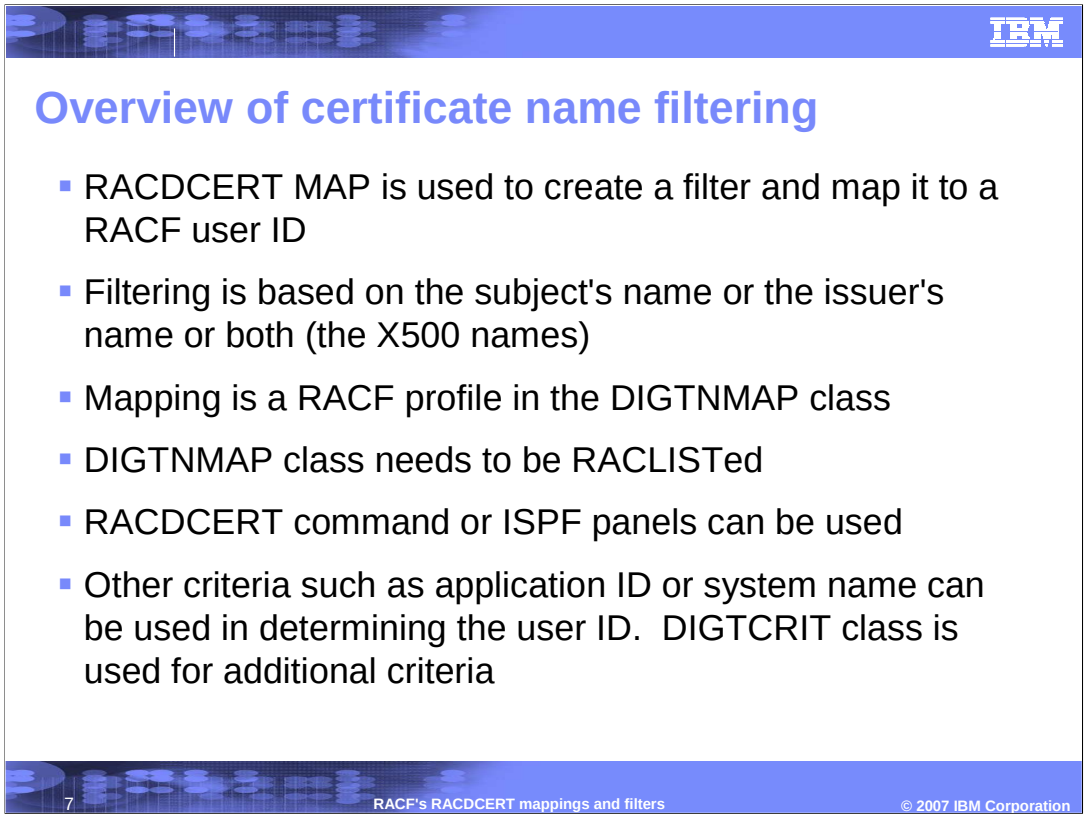
One benefit is that the certificate mapping requires no update even after the certificate that the mapping is based on has been renewed.

Another benefit is that the mapping occupies less space than a certificate in the RACF database. Additionally, one single mapping can map to many certificates coming from different user IDs in a secure manner.

Finally, the mapping can also be created dynamically using additional criteria based on your need, for example user ID or system ID. This kind of mapping can maintain individual accountability.

Certificate Name Filtering (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.

So now to explore how to set up these filters or mappings.

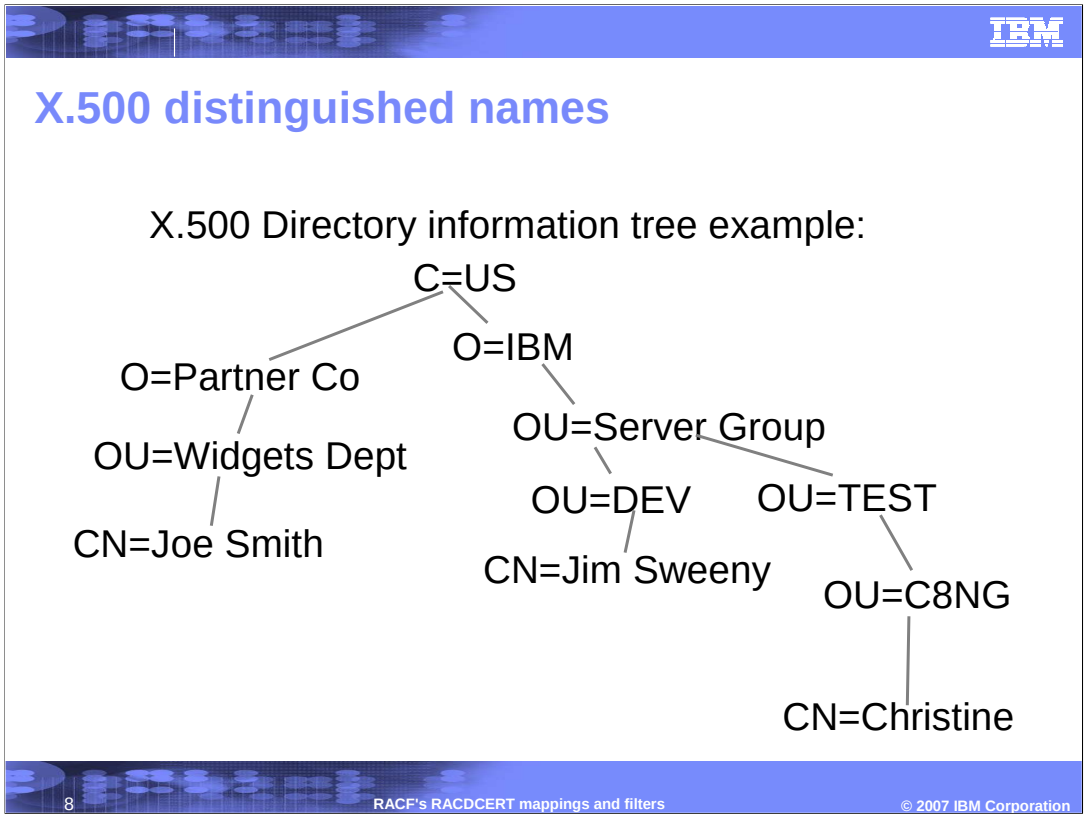


So, how can you create these filters? Using RACF's digital certificate management command, RACDCERT MAP function, filters can be added to the RACF database that will allow users to be mapped to certificates.

RACDCERT MAP processing creates a mapping profile in the DIGTNMAP class to represent the mapping. The filters in the mapping are based on the subject's distinguished name or the issuer's distinguished name or both (the x500 names). The mapping is stored as a RACF profile in the DIGTNAMP class. The profile is created in the format of a hash of the subject's name or a hash of the issuer's name, or a hash of the subject's name concatenated with a hash of the issuer's name. The DIGTNMAP class must be active and SETROPTS RACLISTed.

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. Additional criteria will be examined in a moment.



To better understand how the filters are created and examined, first look at an X.500 Directory information tree. Looking at the above example, there are three different paths.

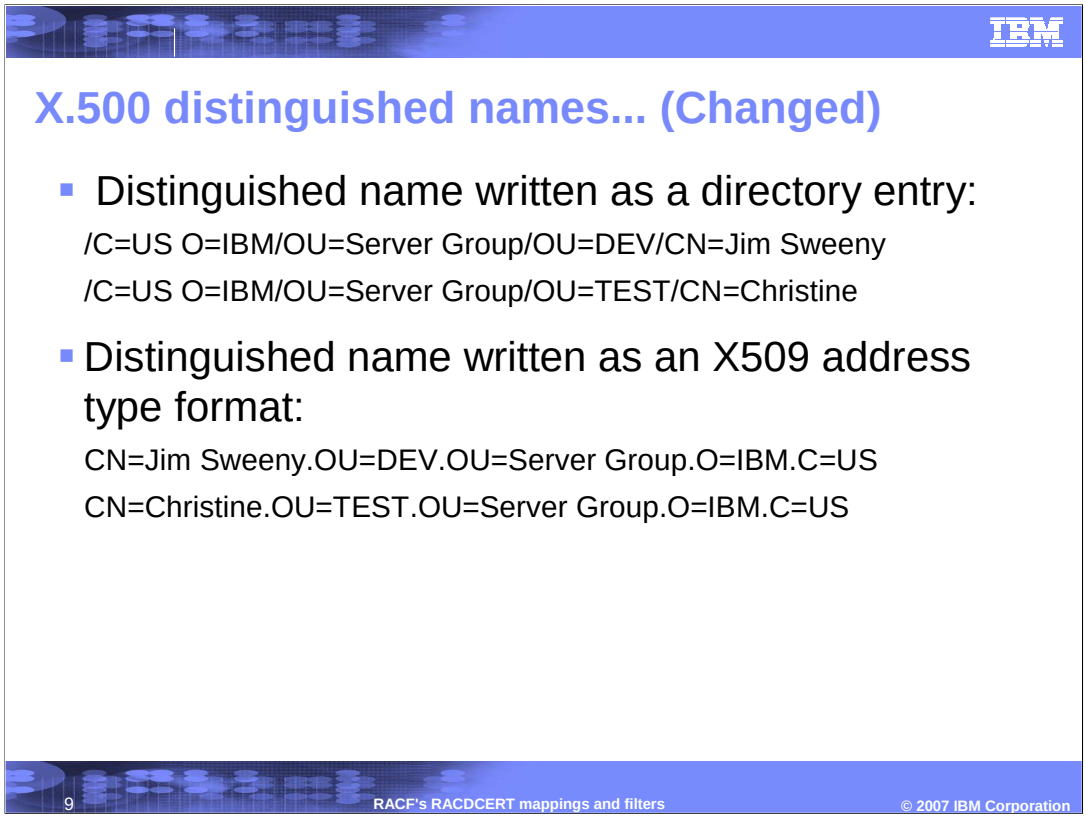
Start at the top of the tree where Country(C)=US

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.

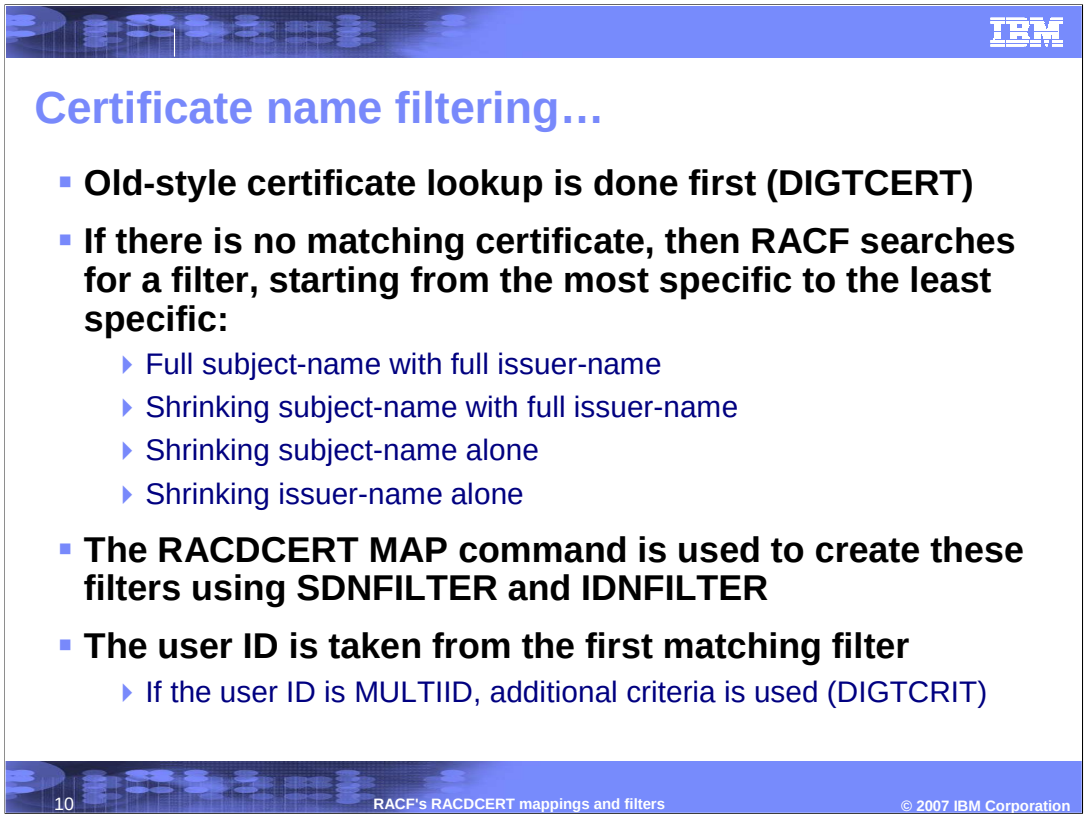


So, looking at how the X.500 Distinguished names are written in a directory, the RDNs start at the top of the tree and work down to the least significant.

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 X509 address type format, however, the order would be reversed. The least significant RDN would be the leftmost one. 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.

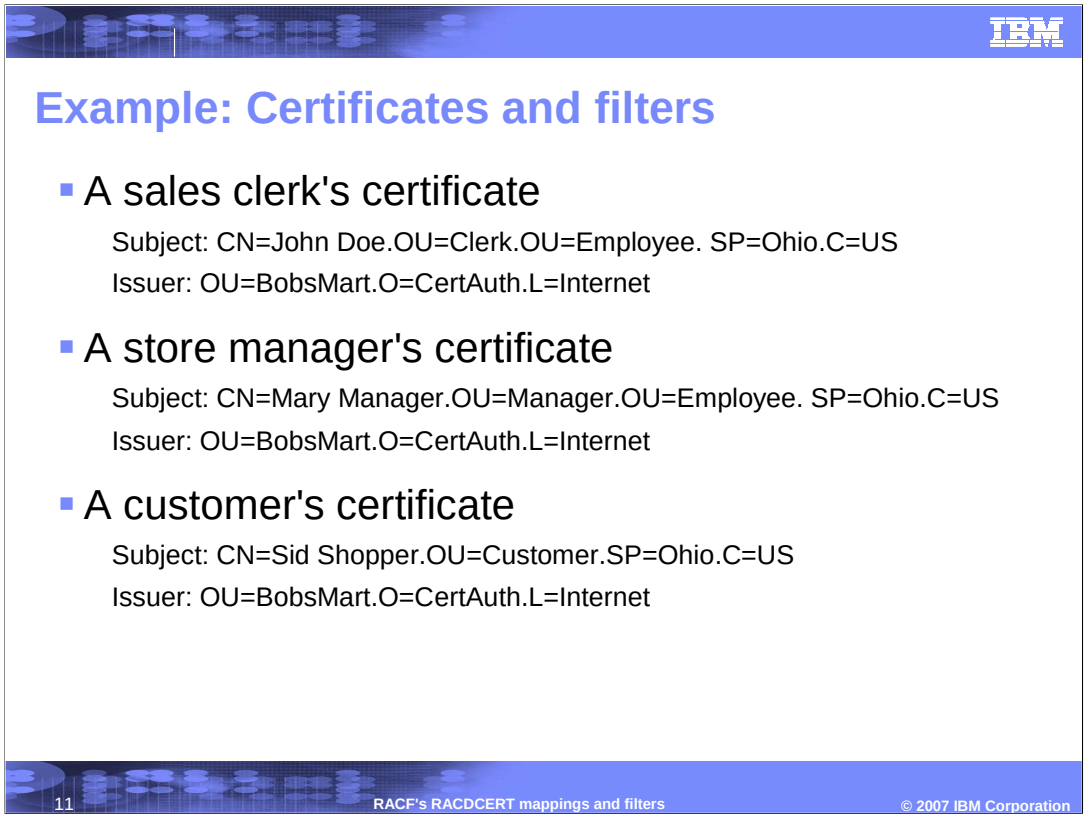


When determining if the incoming certificate is associated with a RACF user ID, a certificate lookup in the RACF database is done (checking the profiles in the DIGTCERT class).

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 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, 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. Examples will be following to help make this a little more clear.

The MAP function of the RACDCERT command is used to set up the filters with keywords SDNFILTER and IDNFILTER: SDNFILTER for the subject's distinguished name filter and IDNFILTER for the issuer's distinguished name filter. These keywords 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. You can specify either SDNFILTER or IDNFILTER or both. More information to follow after some examples.

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



Now look at three different certificates all stated in the x500 format.

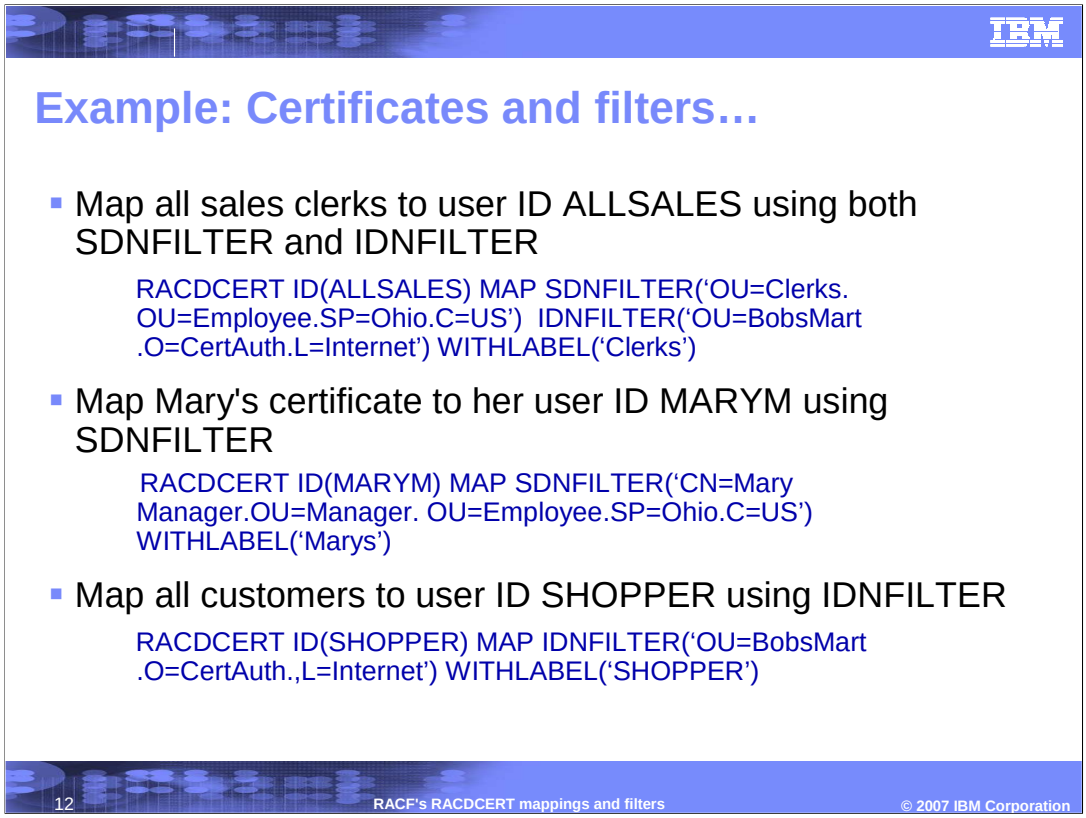
All three certificates have the same Issuer's distinguished name. That issuer's name is composed of the Organizational unit (OU) of BobsMart, with the Organization(O) of CertAuth and the Locality(L) of Internet. All certificates for shoppers and store clerks will have this issuer.

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 the certificates are issued, you will see how these certificates map to the filters based on the distinguished name.



Looking at how this is done - In the first example, you want to set up an ID for all the sales clerks. If all the sales clerks' certificates have issuer's subject name:OU=BobsMart.O=CertAuth.L=Internet, and have: OU=Clerks.OU=Employee.SP=Ohio.C=US as part of the subject name, in order to map all the sales clerks to ID ALLSALES, a map is created using SDNFILTER: OU=Clerks.OU=Employee.SP=Ohio.C=US and IDNFILTER: OU=BobsMart.O=CertAuth.L=Internet. To do this, issue the RACDCERT command in the first example using the SDNFILTER and the IDNFILTER subkeyword. [enter]

The second example shows the set up of the mapping under the manager's ID MARYM. If you want to map all certificates issued to Mary Manager with the same subject's distinguished name: CN=Mary Manager.OU=Manager. OU=Employee.SP=Ohio.C=US to ID MARYM regardless of the issuer of the certificate, a filter is created based on just the subject's name. To create the mappings, issue the next example of the RACDCERT MAP command with the SDNFILTER subkeyword only. This filter specifies the subject's distinguished name in it's entirety with no issuer's distinguished name. [enter]

The third example is to show that you want to map all the customers to one user ID SHOPPER as long as their certificates have the issuer's distinguished name: OU=BobsMart.O=CertAuth.,L=Internet. Therefore, using only the Issuer's Distinguished Name in the filter will suffice. This filter specifies the issuer's distinguished name in it's entirety. To do this, issue the third example of the RACDCERT command.

It is important to note that the less restrictive mapping in the third example will be used if the more restrictive ones can not be found. If, for example, Mary Manager's subject's distinguished name changes slightly in a renewed certificate to CN= Mary I Manager and

Examples: Certificates and filters…

- Certificate with distinguished names of
  Subject: CN=John Doe.OU=Clerk.OU=Employee.SP=Ohio.C=US
  Issuer: OU=BobsMart.O=CertAuth.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 .O=CertAuth.L=Internet
    OU=Clerk.OU=Employee.SP=Ohio.C=US||OU=BobsMart .O=CertAuth.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.O=CertAuth.L=Internet
    C=US||OU=BobsMart.O=CertAuth.L=Internet
  - Shrinking subject-name alone
  - Shrinking issuer-name alone

This is 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 a 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.O=CertAuth.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.O=CertAuth.L=Internet would be searched next. For this example, that is a match with the user ID ALLSALES.

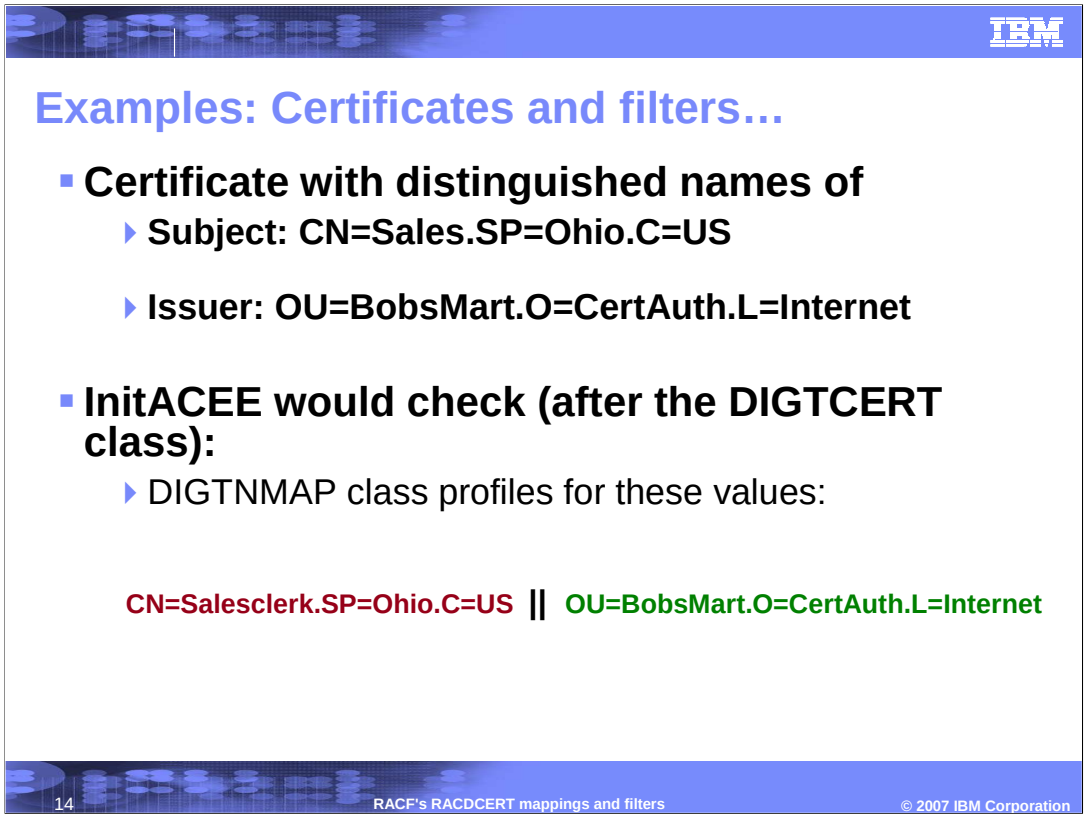
ALLSALES would be the RACF user ID used for the transaction.

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, the 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 in the same manner as the subject's distinguished name.

For the above example, a match was found and the user ID was ALLSALES.



For the example 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.

The search through the mappings start with the full subject's name and full issuer's name.

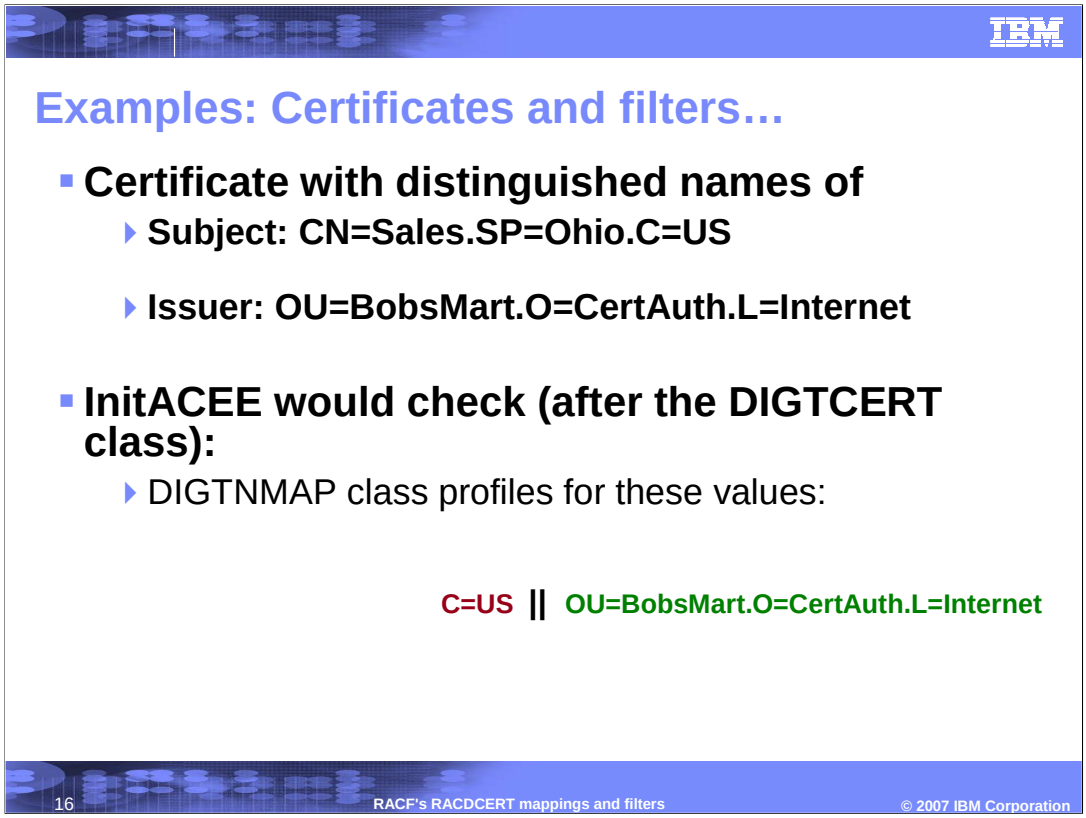
The first search for mapping will be on the profile that has CN=Salesclerk.SP=Ohio.C=US||OU=BobsMart .O=CertAuth.L=Internet**.**

Examples: Certificates and filters…

- **Certificate with distinguished names of**
  - **Subject: CN=Sales.SP=Ohio.C=US**
  - **Issuer: OU=BobsMart.O=CertAuth.L=Internet**
- **InitACEE would check (after the DIGTCERT class):**
  - DIGTNMAP class profiles for these values:

SP=Ohio.C=US || OU=BobsMart.O=CertAuth.L=Internet

The second search would remove CN=Salesclerk for the search.



The third search would remove SP=Ohio next leaving C=US of the subject's name and the full issuer's name.

Examples: Certificates and filters…

- **Certificate with distinguished names of**
  - **Subject: CN=Sales.SP=Ohio.C=US**
  - **Issuer: OU=BobsMart.O=CertAuth.L=Internet**
- **InitACEE would check (after the DIGTCERT class):**
  - DIGTNMAP class profiles for these values:

CN=Salesclerk.SP=Ohio.C=US

The fourth search will be on the profile that only has the subject filter CN=Saleclerk.SP=Ohio.C=US

Examples: Certificates and filters…

- **Certificate with distinguished names of**
  - **Subject: CN=Sales.SP=Ohio.C=US**
  - **Issuer: OU=BobsMart.O=CertAuth.L=Internet**
- **InitACEE would check (after the DIGTCERT class):**
  - DIGTNMAP class profiles for these values:

SP=Ohio.C=US

The fifth search will be on SP=Ohio.C=US

Examples: Certificates and filters…

- **Certificate with distinguished names of**
  - **Subject: CN=Sales.SP=Ohio.C=US**
  - **Issuer: OU=BobsMart.O=CertAuth.L=Internet**
- **InitACEE would check (after the DIGTCERT class):**
  - DIGTNMAP class profiles for these values:

C=US

The sixth search will be on C=US

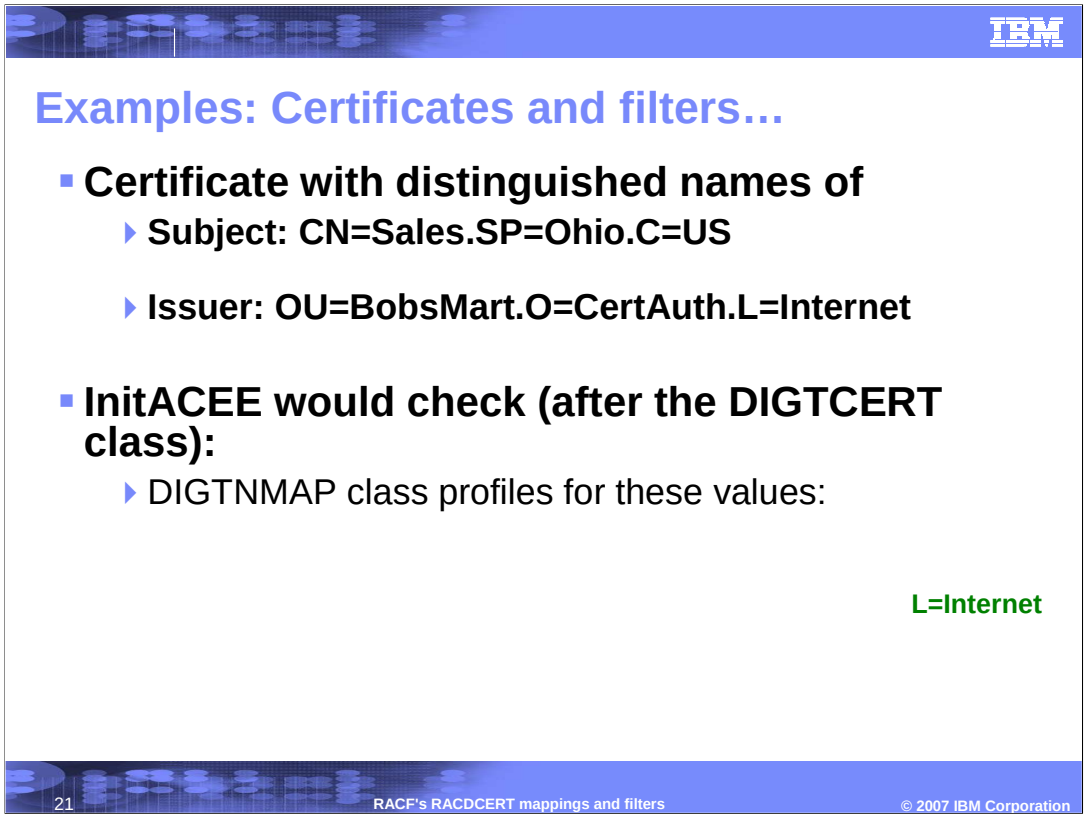
Examples: Certificates and filters…

- **Certificate with distinguished names of**
  - **Subject: CN=Sales.SP=Ohio.C=US**
  - **Issuer: OU=BobsMart.O=CertAuth.L=Internet**
- **InitACEE would check (after the DIGTCERT class):**
  - DIGTNMAP class profiles for these values:

OU=BobsMart.O=CertAuth.L=Internet

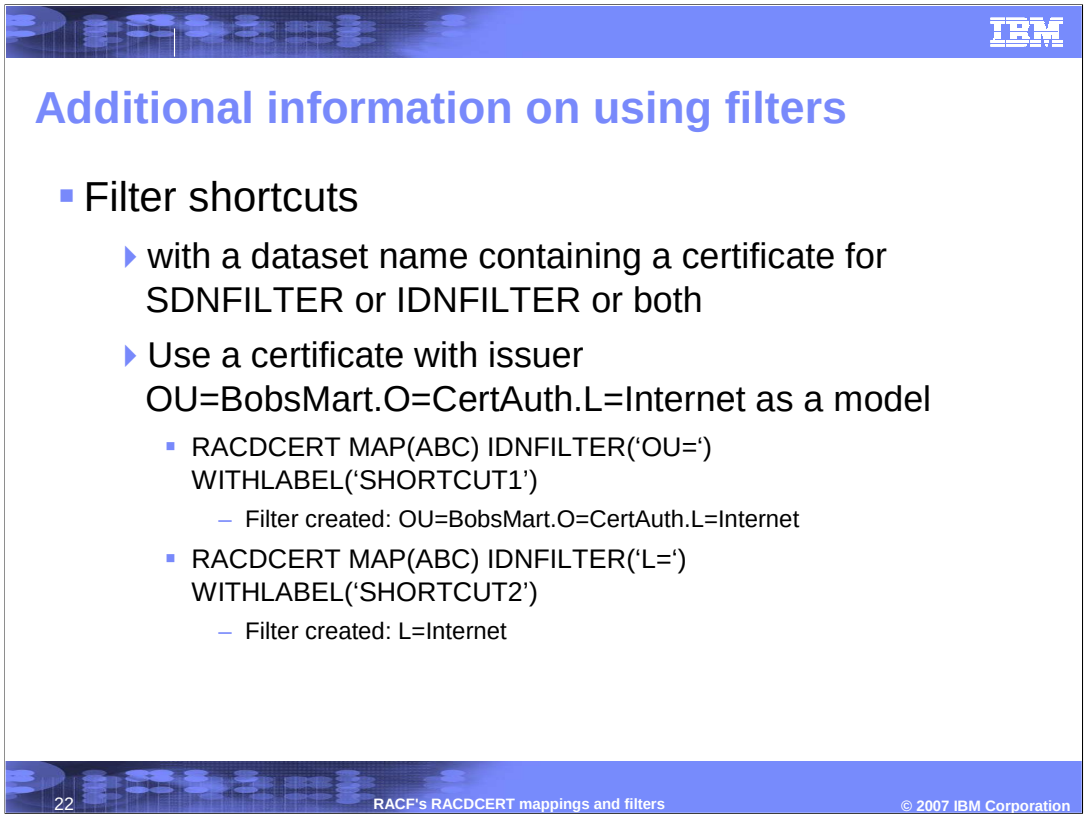
The seventh search will be on the profile that only has the issuer filter OU=BobsMart.O=CertAuth.L=Internet.

So according to the mappings that have been created in the previous foil, the seventh search will find a match on the mapping profile under ID SHOPPER, although the certificate contains 'Salesclerk' in its subject's name. If this did not find a mapping, the RDNs from the IDN filter would continue to be removed down to L=Internet.



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.



To reduce the chance of typographical errors when entering long filters for SDNFILTER or IDNFILTER, a model certificate can be used.

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 constructing the filter names specified with SDNFILTER and IDNFILTER. The portion of subject's distinguished name beginning with the value specified by SDNFILTER is used. The portion of issuer's distinguished name beginning with the value specified by IDNFILTER is used.

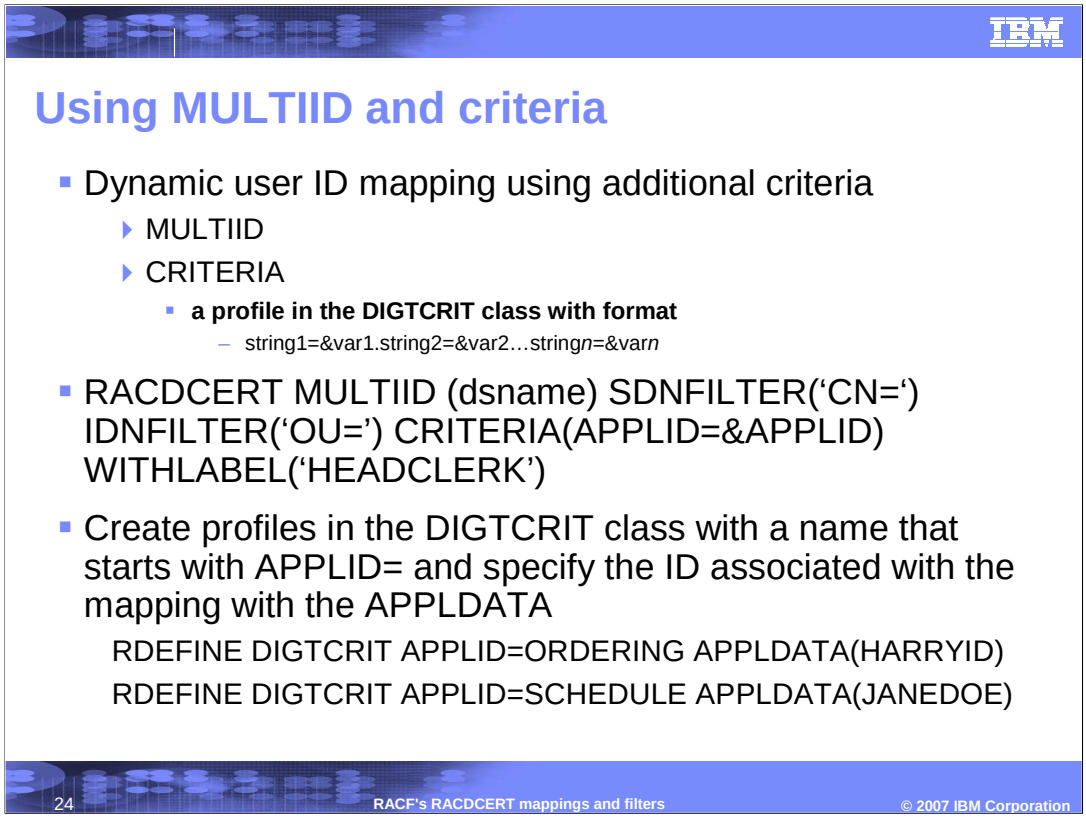
For example, if dataset ABC contains a certificate with Issuer's distinguished name OU=BobsMart .O=CertAuth.L=Internet is specified with the command RACDCERT MAP(ABC) IDNFILTER('OU=') WITHLABEL('SHORTCUT1'), the issuer's filter will be created with the entire issuer's name 'OU=BobsMart .O=CertAuth.L=Internet'. If IDNFILTER is 'L=' is specified in the above MAP command, then the filter created will be 'L=Internet'.

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.

Additional information on using filters

- **Some consideration for the user IDs associated with certificate name filters**
  - Protected and restricted
  - Use the ALTUSER command
  - ALTUSER OHIOUSER NOPASSWORD RESTRICTED

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. Use the ALTUSER command as shown in the slide. 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.



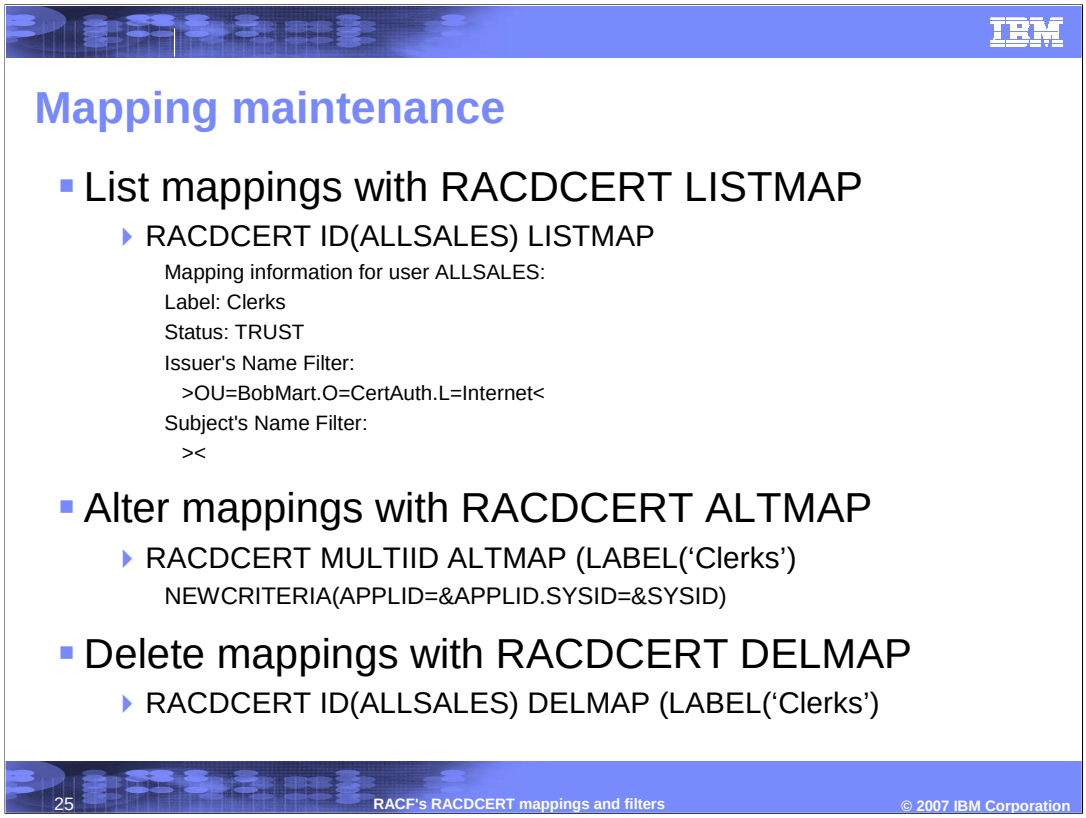
As mentioned earlier, with MULTIID, additional criteria can be added in determining the user ID associated with the certificate. Now look at how this can be done.

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 is specified 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 if it is not the last string.

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 CRITERIA(APPLID=&APPLID).

In order to make use of the criteria created above, create profiles in the DIGTCRIT class with names that start with APPLID= and specify the ID associated with the mapping with the APPLDATA parameter. For example create the profiles using the RDEFINE command: RDEFINE DIGTCRIT APPLID=ORDERING APPLDATA(HARRYID) and RDEFINE DIGTCRIT APPLID=SCHEDULE APPLDATA(JANEDOE)

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 it's 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. For example, if the application being accessed is ORDERING, the profile in the DIGTCRIT class being used for searching is APPLID=ORDERING, the ID associated will be HARRYID. If the application



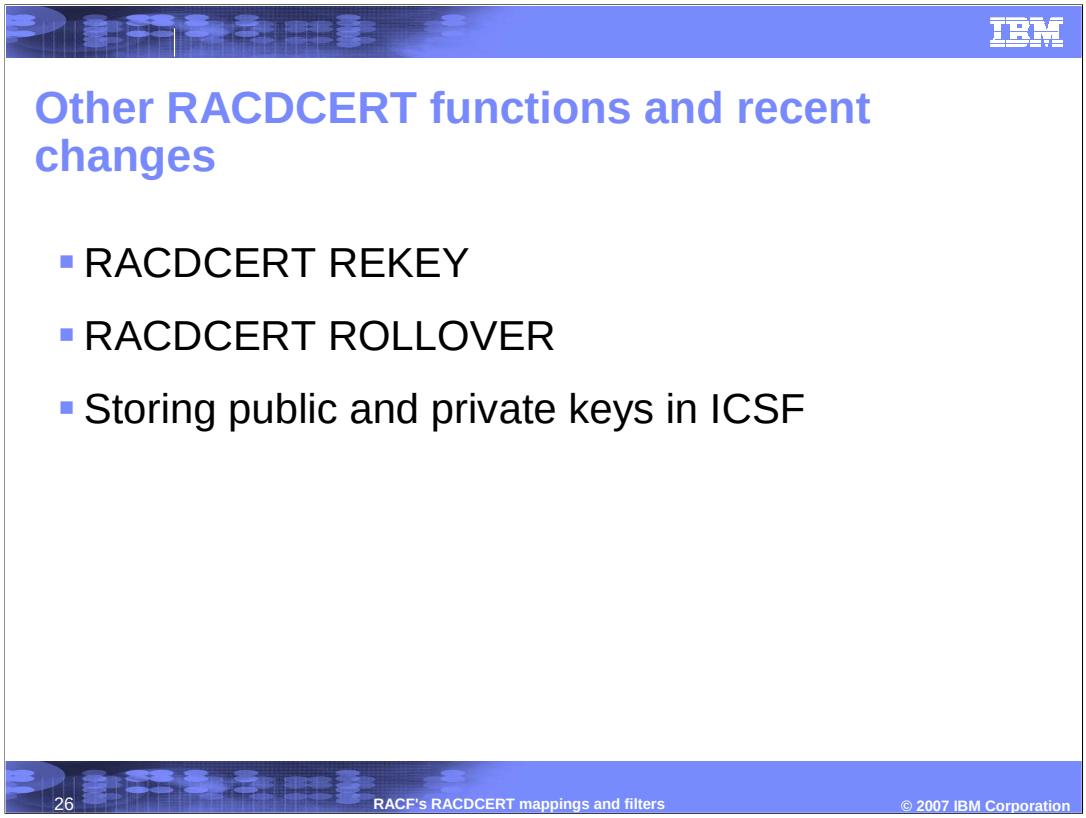
The mappings created will need to maintained. Now you will look at the additional functions available through the RACDCERT command.

RACDCERT MAP processing creates mapping profile associates with a RACF user ID in the DIGTNMAP class for each certificate name filter you create. DIGTNMAP profiles can 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. 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. This example shows adding the criteria of SYSID (the system identifier). 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. Mappings will be deleted as part of DELUSER processing.



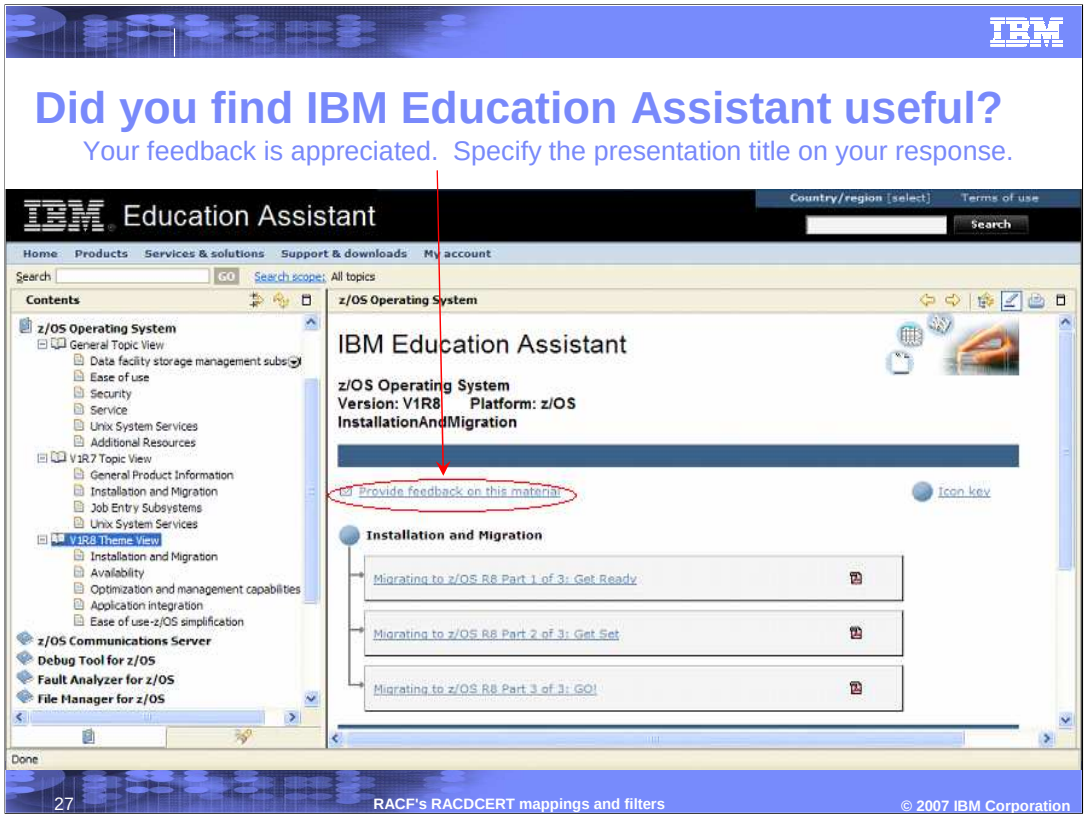
Other areas of interest to explore with the RACDCERT command are the REKEY and ROLLOVER functions.

You can choose to renew the certificate using the same private key, thereby extending the life of the private key. Or you can retire the private key and replace it with a new private key (also called *certificate rekeying* or *key rollover*). There are other more advanced functions available with the RACDCERT command to help with this rekeying or key rollover. The RACDCERT functions of REKEY and ROLLOVER functions are used for renewing certificate and keys.

Originally, when using the ICSF or PCICC keyword with RACDCERT ADD or RACDCERT GENCERT the private key in the certificate would be stored in ICSF's PKDS. You can now store the private or public key associated with the certificate in ICSF's PKDS and give it a friendly label. This support will help with encryption of data at rest.

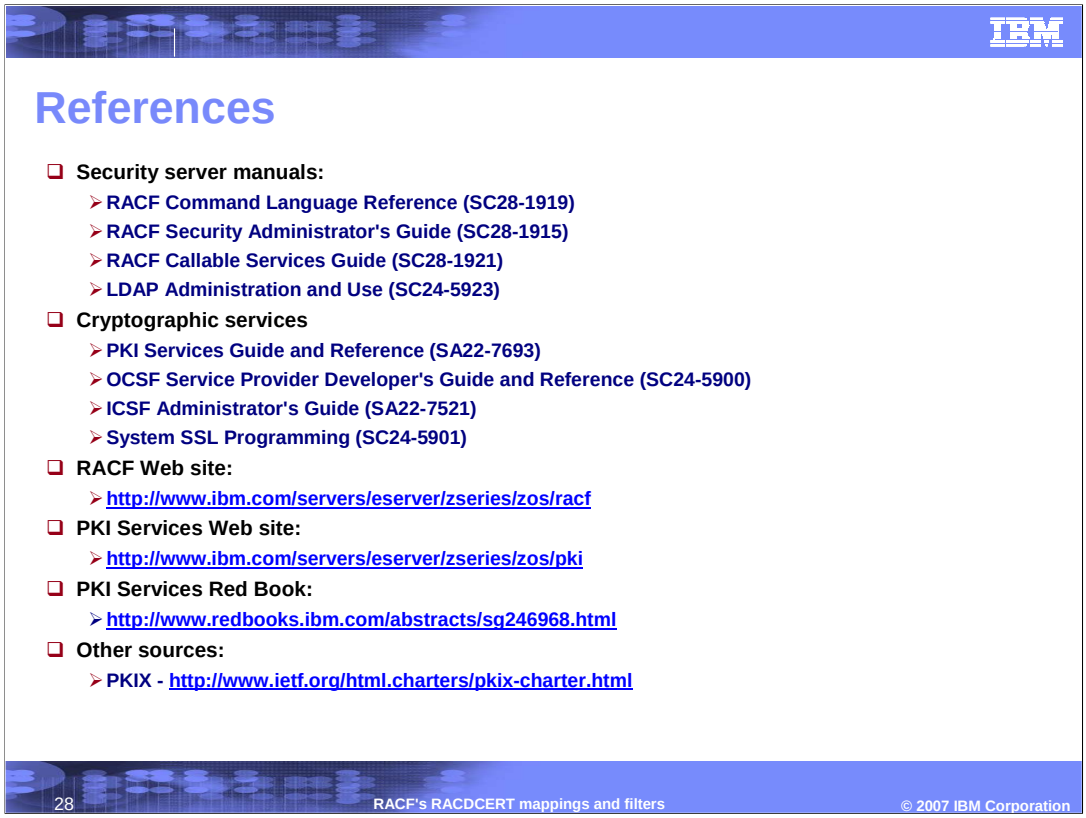
These functions will be explored in more detail in the next installment of RACDCERT.

This is the end of this presentation. The next installment of RACDCERT will go through some examples and ideas on how to renew certificates and why you might need a new private key through RACDCERT REKEY and RACDCERT ROLLOVER and how and why private or public keys are stored in ICSF.



In order to supply you with pertinent and timely information in IBM Education modules, your opinions are important. To help IBM in creating these modules, take the time to help us out. In your feedback to IBM please answer these three questions:

1. **How helpful was this presentation? Give 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 you would like to see covered in IBM Education Assistant, what are they? _____**



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.

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 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.