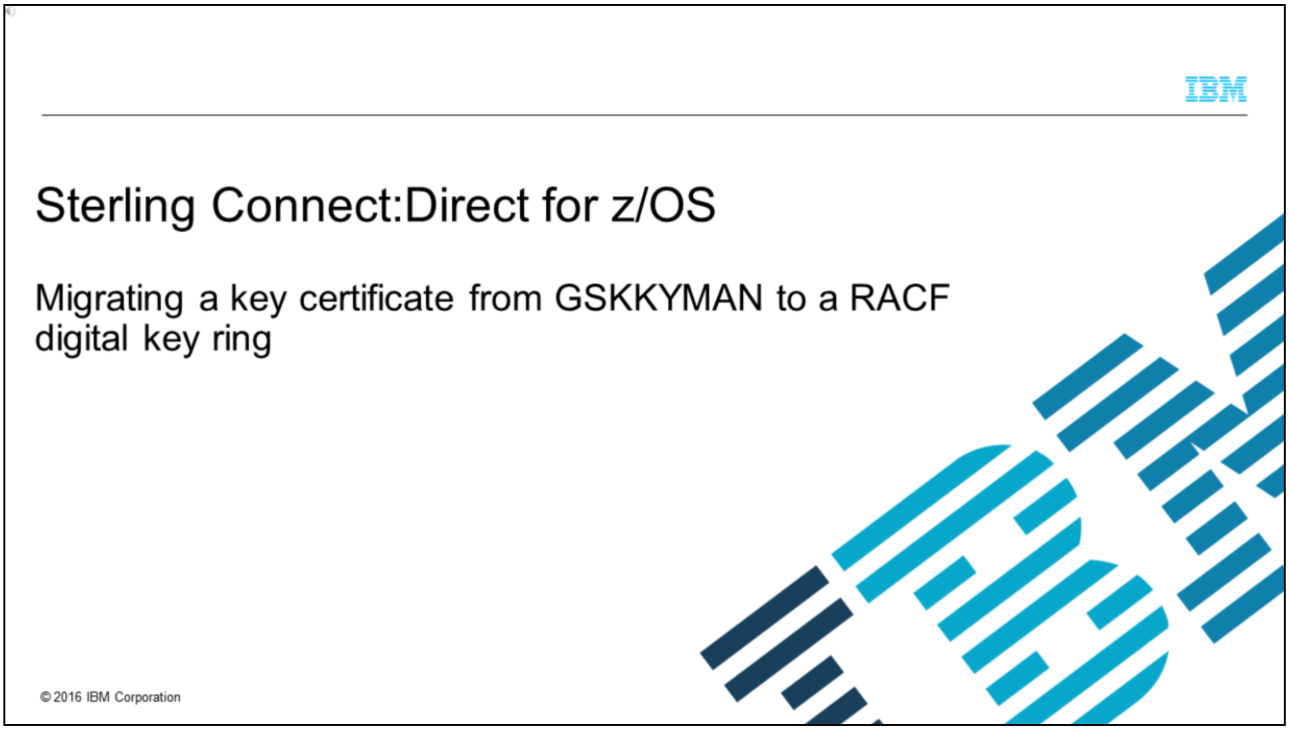


Sterling Connect:Direct for z/OS

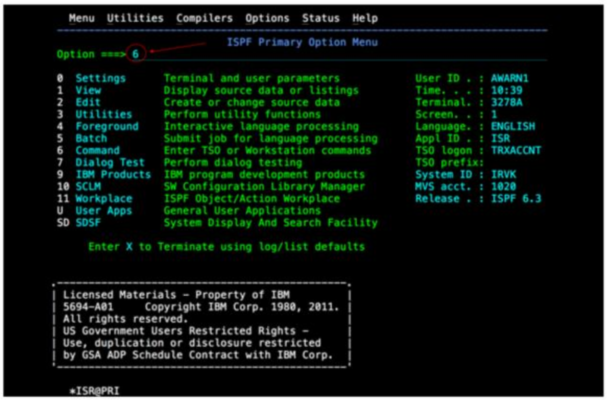
Migrating a key certificate from GSKKYMAN to a RACF digital key ring

This presentation shows you how to migrate a key certificate from GSKKYMAN to a RACF® digital key ring. You will export and create a PKCS12 key certificate by using IBM GSKKYMAN, which is a component of z/OS®. You will add it to a newly created RACF key ring for use with Sterling Connect:Direct® for z/OS.

IBM

Start UNIX System Services (USS)

- Enter 6 from the ISPF Primary Option menu



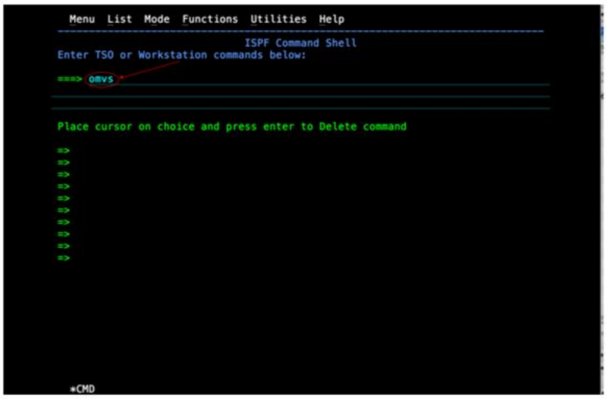
```
  Menu  Utilities  Compilers  Options  Status  Help
 ------------------------------------------------------------------------------
                            ISPF Primary Option Menu
 Option ===> 6

 0  Settings      Terminal and user parameters            User ID . : AWARN1
 1  View          Display source data or listings         Time. . . : 10:39
 2  Edit          Create or change source data            Terminal. : 3278A
 3  Utilities     Perform utility functions               Screen. . : 1
 4  Foreground    Interactive language processing         Language. : ENGLISH
 5  Batch         Submit job for language processing      Appl ID . : ISR
 6  Command       Enter TSO or Workstation commands       TSO logon : TRXACCNT
 7  Dialog Test   Perform dialog testing                  TSO prefix:
 9  IBM Products  IBM program development products        System ID : IRVK
 10 SCLM          SW Configuration Library Manager        MVS acct. : 1020
 11 Workplace     ISPF Object/Action Workplace            Release . : ISPF 6.3
 U  User Apps     General User Applications
 SD SDSF          System Display And Search Facility

      Enter X to Terminate using log/list defaults


 .-----------------------------------------------.
 | Licensed Materials - Property of IBM          |
 | 5694-A01     Copyright IBM Corp. 1980, 2011.  |
 | All rights reserved.                          |
 | US Government Users Restricted Rights -       |
 | Use, duplication or disclosure restricted     |
 | by GSA ADP Schedule Contract with IBM Corp.   |
 '-----------------------------------------------'

   *ISR@PRI
```

2 Migrating a key certificate from GSKKYMAN to a RACF digital key ring © 2016 IBM Corporation

To migrate a key certificate from a key database to a RACF key ring, you must first access the GSKKYMAN application, which is a component of z/OS. If you are not already signed on to GSKKYMAN, key in 6 on the command line to enter TSO or workstation commands and press enter. If you are already in GSKKYMAN, you will begin at slide 5.

Start UNIX System Services

- Key in OMVS on the command line
- ENTER

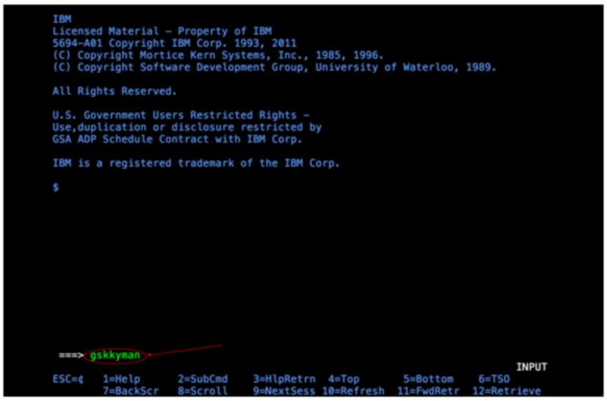


```
                         ISPF Command Shell
Enter TSO or Workstation commands below:

===> omvs


Place cursor on choice and press enter to Delete command

=>
=>
=>
=>
=>
=>
=>
=>
=>
=>



  *CMD
```

On the ISPF Command Shell panel, key in OMVS to access UNIX® System Services and press enter to continue.

Start the Key Database Menu

- Key in gskkyman
- ENTER

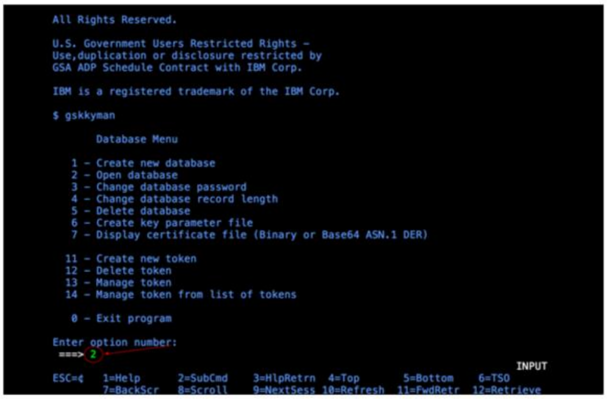


```
IBM
Licensed Material - Property of IBM
5694-A01 Copyright IBM Corp. 1993, 2011
(C) Copyright Mortice Kern Systems, Inc., 1985, 1996.
(C) Copyright Software Development Group, University of Waterloo, 1989.

All Rights Reserved.

U.S. Government Users Restricted Rights -
Use,duplication or disclosure restricted by
GSA ADP Schedule Contract with IBM Corp.

IBM is a registered trademark of the IBM Corp.

$




 ===> gskkyman
                                                              INPUT
ESC=¢   1=Help     2=SubCmd    3=HlpRetrn  4=Top      5=Bottom   6=TSO
        7=BackScr  8=Scroll    9=NextSess 10=Refresh 11=FwdRetr 12=Retrieve
```

On the UNIX System Services panel, enter gskkyman to display the GSKKYMAN application menu options. Press enter to continue.

Create a database

- Select option 2 – Open database
- ENTER

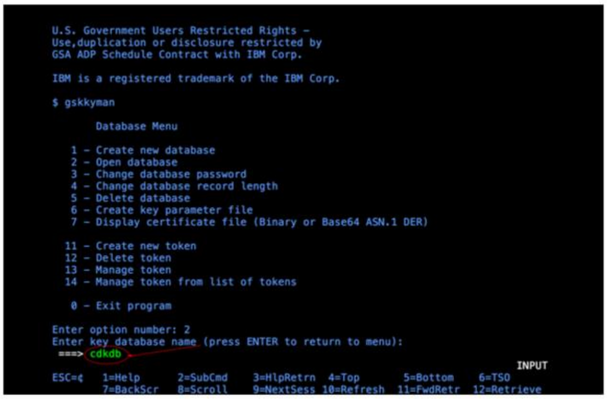


```
All Rights Reserved.

U.S. Government Users Restricted Rights -
Use,duplication or disclosure restricted by
GSA ADP Schedule Contract with IBM Corp.

IBM is a registered trademark of the IBM Corp.

$ gskkyman

       Database Menu

   1 - Create new database
   2 - Open database
   3 - Change database password
   4 - Change database record length
   5 - Delete database
   6 - Create key parameter file
   7 - Display certificate file (Binary or Base64 ASN.1 DER)

  11 - Create new token
  12 - Delete token
  13 - Manage token
  14 - Manage token from list of tokens

   0 - Exit program

Enter option number:
 ===> 2
                                                                INPUT
ESC=¢    1=Help      2=SubCmd    3=HlpRetrn  4=Top      5=Bottom    6=TSO
         7=BackScr   8=Scroll    9=NextSess 10=Refresh 11=FwdRetr  12=Retrieve
```

From the GSKKYMAN Database Menu panel, select option 2 to open an existing database. Press enter to continue.

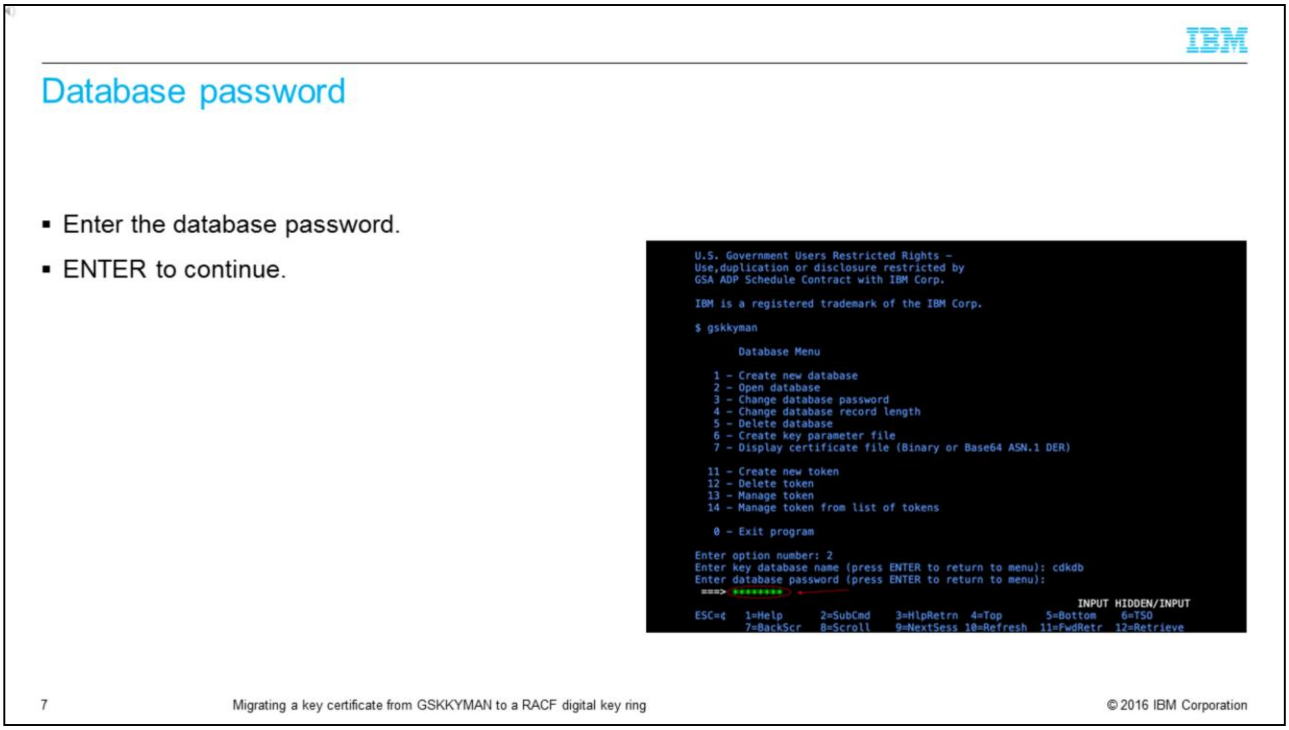
Database name

- Key in your key database name.
- ENTER to continue.



```
U.S. Government Users Restricted Rights -
Use,duplication or disclosure restricted by
GSA ADP Schedule Contract with IBM Corp.

IBM is a registered trademark of the IBM Corp.

$ gskkyman

       Database Menu

   1 - Create new database
   2 - Open database
   3 - Change database password
   4 - Change database record length
   5 - Delete database
   6 - Create key parameter file
   7 - Display certificate file (Binary or Base64 ASN.1 DER)

  11 - Create new token
  12 - Delete token
  13 - Manage token
  14 - Manage token from list of tokens

   0 - Exit program

Enter option number: 2
Enter key database name (press ENTER to return to menu):
 ===> cdkdb
                                                                      INPUT
ESC=¢   1=Help     2=SubCmd    3=HlpRetrn  4=Top      5=Bottom    6=TSO
        7=BackScr  8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will see a request to enter a key database name. Key in the name for your existing GSKKYMAN key database and enter to continue. You can return to the Database Menu by leaving the field blank and pressing ENTER if you want to continue later.



Database password

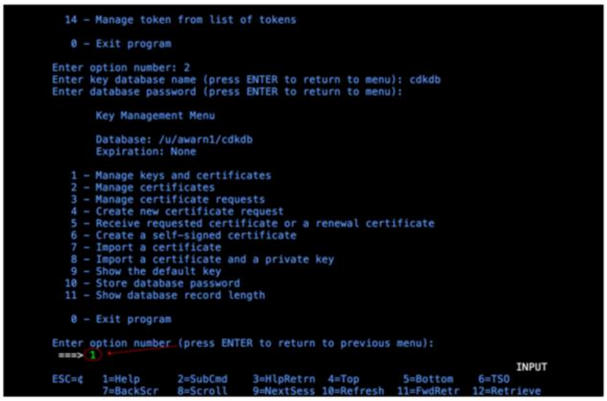
- Enter the database password.
- ENTER to continue.

```
U.S. Government Users Restricted Rights -
Use,duplication or disclosure restricted by
GSA ADP Schedule Contract with IBM Corp.

IBM is a registered trademark of the IBM Corp.

$ gskkyman

       Database Menu

   1 - Create new database
   2 - Open database
   3 - Change database password
   4 - Change database record length
   5 - Delete database
   6 - Create key parameter file
   7 - Display certificate file (Binary or Base64 ASN.1 DER)

  11 - Create new token
  12 - Delete token
  13 - Manage token
  14 - Manage token from list of tokens

   0 - Exit program

Enter option number: 2
Enter key database name (press ENTER to return to menu): cdkdb
Enter database password (press ENTER to return to menu):
 ===> ********
                                                              INPUT HIDDEN/INPUT
ESC=¢    1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
         7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will now see a request to enter a database password. Key in the database password and press enter to continue.

Self-signed certificate

- Key in 1 to manage keys and certificates
- ENTER

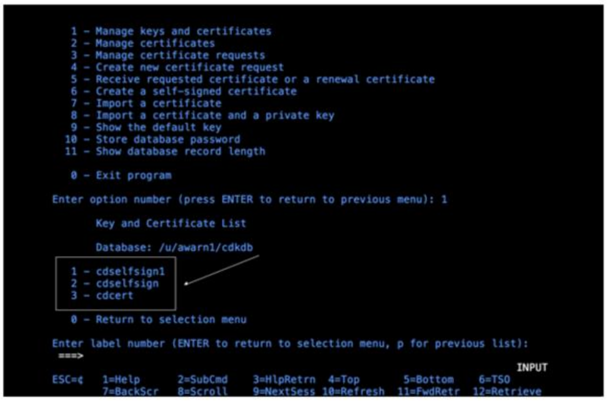


```
  14 - Manage token from list of tokens

   0 - Exit program

Enter option number: 2
Enter key database name (press ENTER to return to menu): cdkdb
Enter database password (press ENTER to return to menu):

       Key Management Menu

       Database: /u/awarn1/cdkdb
       Expiration: None

   1 - Manage keys and certificates
   2 - Manage certificates
   3 - Manage certificate requests
   4 - Create new certificate request
   5 - Receive requested certificate or a renewal certificate
   6 - Create a self-signed certificate
   7 - Import a certificate
   8 - Import a certificate and a private key
   9 - Show the default key
  10 - Store database password
  11 - Show database record length

   0 - Exit program

Enter option number (press ENTER to return to previous menu):
 ===> 1
                                                                INPUT
ESC=¢   1=Help     2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
        7=BackScr  8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will see a menu titled Key Management menu, you will type in 1 on the command line to manage keys and certificates. Press enter to continue.

Database display

- Certificate labels displayed for your database

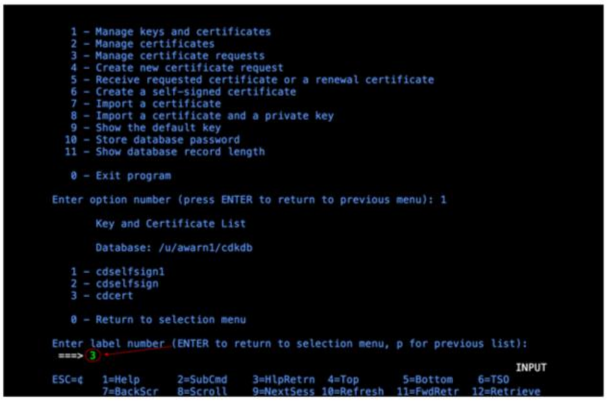


```
    1 - Manage keys and certificates
    2 - Manage certificates
    3 - Manage certificate requests
    4 - Create new certificate request
    5 - Receive requested certificate or a renewal certificate
    6 - Create a self-signed certificate
    7 - Import a certificate
    8 - Import a certificate and a private key
    9 - Show the default key
   10 - Store database password
   11 - Show database record length

    0 - Exit program

 Enter option number (press ENTER to return to previous menu): 1

        Key and Certificate List

        Database: /u/awarn1/cdkdb

    1 - cdselfsign1
    2 - cdselfsign
    3 - cdcert

    0 - Return to selection menu

 Enter label number (ENTER to return to selection menu, p for previous list):
  ===>
                                                                         INPUT
 ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
         7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

In the output, you will see the contents of your key database displayed. You will select one of the certificate labels to export.

Select certificate

- Key in label number
- Enter



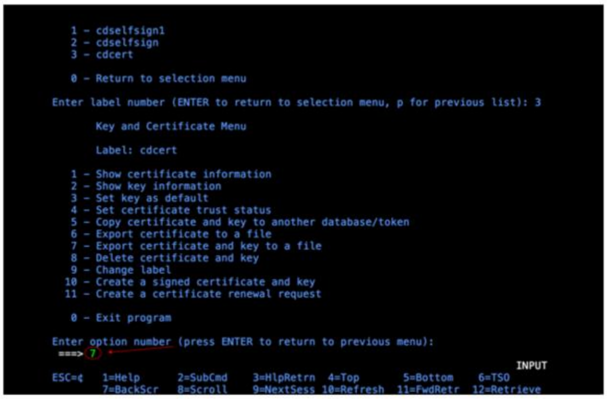
```
    1 - Manage keys and certificates
    2 - Manage certificates
    3 - Manage certificate requests
    4 - Create new certificate request
    5 - Receive requested certificate or a renewal certificate
    6 - Create a self-signed certificate
    7 - Import a certificate
    8 - Import a certificate and a private key
    9 - Show the default key
   10 - Store database password
   11 - Show database record length

    0 - Exit program

Enter option number (press ENTER to return to previous menu): 1

       Key and Certificate List

       Database: /u/awarn1/cdkdb

    1 - cdselfsign1
    2 - cdselfsign
    3 - cdcert

    0 - Return to selection menu

Enter label number (ENTER to return to selection menu, p for previous list):
 ===> 3
                                                                        INPUT
ESC=¢    1=Help      2=SubCmd     3=HlpRetrn  4=Top       5=Bottom    6=TSO
         7=BackScr   8=Scroll     9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

Under enter label number, key in the number alongside the key certificate you want to export. Press enter to continue.

IBM

Export the certificate and key

- Key in number 7
- Enter

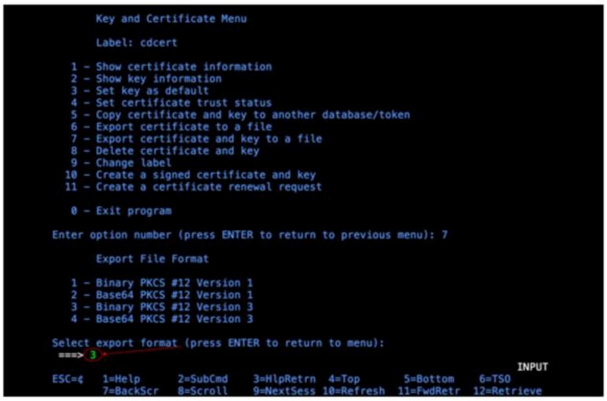


```
     1 - cdselfsign1
     2 - cdselfsign
     3 - cdcert

     0 - Return to selection menu

 Enter label number (ENTER to return to selection menu, p for previous list): 3

       Key and Certificate Menu

       Label: cdcert

     1 - Show certificate information
     2 - Show key information
     3 - Set key as default
     4 - Set certificate trust status
     5 - Copy certificate and key to another database/token
     6 - Export certificate to a file
     7 - Export certificate and key to a file
     8 - Delete certificate and key
     9 - Change label
    10 - Create a signed certificate and key
    11 - Create a certificate renewal request

     0 - Exit program

 Enter option number (press ENTER to return to previous menu):
  ===> 7
                                                                        INPUT
 ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
         7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will key in 7 on the command line to export your key certificate to a UNIX System Services file. Press enter.

Export file Format

- Key in 3 – Binary PKCS #12 version 3
- Enter

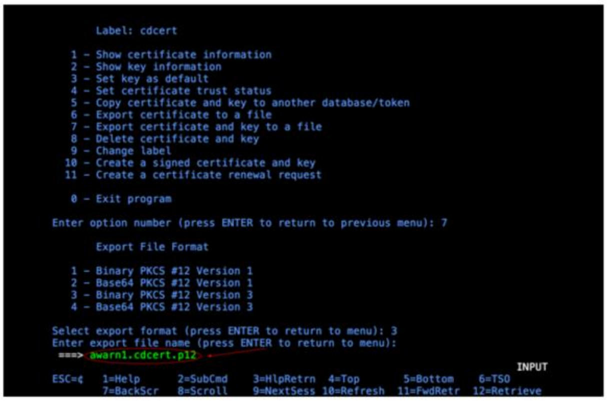


```
        Key and Certificate Menu

        Label: cdcert

    1 - Show certificate information
    2 - Show key information
    3 - Set key as default
    4 - Set certificate trust status
    5 - Copy certificate and key to another database/token
    6 - Export certificate to a file
    7 - Export certificate and key to a file
    8 - Delete certificate and key
    9 - Change label
   10 - Create a signed certificate and key
   11 - Create a certificate renewal request

    0 - Exit program

Enter option number (press ENTER to return to previous menu): 7

        Export File Format

    1 - Binary PKCS #12 Version 1
    2 - Base64 PKCS #12 Version 1
    3 - Binary PKCS #12 Version 3
    4 - Base64 PKCS #12 Version 3

Select export format (press ENTER to return to menu):
 ===> 3
                                                              INPUT
ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top      5=Bottom    6=TSO
        7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will see a choice of file formats that you can use to export your key certificate, you will select 3 to export your certificate as binary PKCS12 Version 3 file. Press enter to continue.

Export file name

- Key in an export file name
- Enter



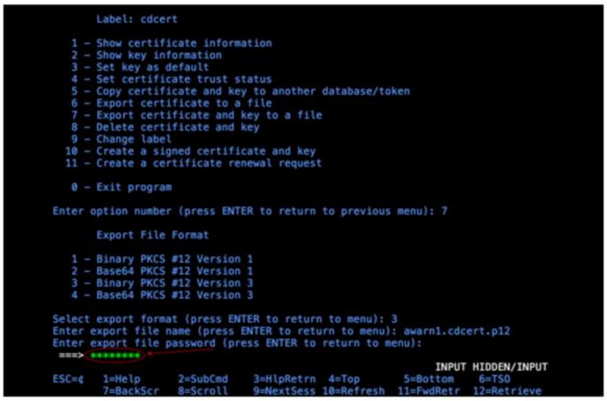
```
       Label: cdcert

   1 - Show certificate information
   2 - Show key information
   3 - Set key as default
   4 - Set certificate trust status
   5 - Copy certificate and key to another database/token
   6 - Export certificate to a file
   7 - Export certificate and key to a file
   8 - Delete certificate and key
   9 - Change label
  10 - Create a signed certificate and key
  11 - Create a certificate renewal request

   0 - Exit program

Enter option number (press ENTER to return to previous menu): 7

       Export File Format

   1 - Binary PKCS #12 Version 1
   2 - Base64 PKCS #12 Version 1
   3 - Binary PKCS #12 Version 3
   4 - Base64 PKCS #12 Version 3

Select export format (press ENTER to return to menu): 3
Enter export file name (press ENTER to return to menu):
 ===> awarn1.cdcert.p12
                                                                  INPUT
ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
        7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will enter an export file name on the command line. Press enter to continue.

IBM

Export file password

- Key in export file password
- Enter



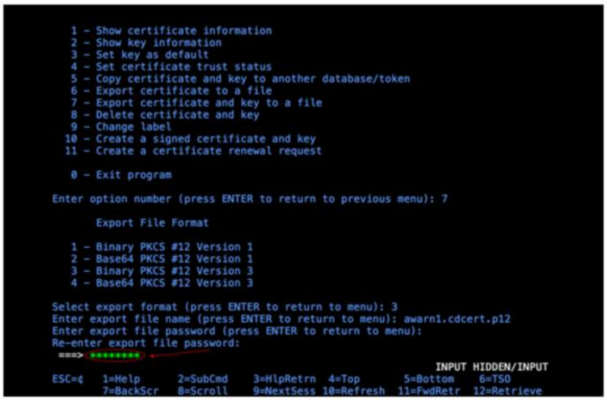
```
        Label: cdcert

    1 - Show certificate information
    2 - Show key information
    3 - Set key as default
    4 - Set certificate trust status
    5 - Copy certificate and key to another database/token
    6 - Export certificate to a file
    7 - Export certificate and key to a file
    8 - Delete certificate and key
    9 - Change label
   10 - Create a signed certificate and key
   11 - Create a certificate renewal request

    0 - Exit program

Enter option number (press ENTER to return to previous menu): 7

        Export File Format

    1 - Binary PKCS #12 Version 1
    2 - Base64 PKCS #12 Version 1
    3 - Binary PKCS #12 Version 3
    4 - Base64 PKCS #12 Version 3

Select export format (press ENTER to return to menu): 3
Enter export file name (press ENTER to return to menu): awarn1.cdcert.p12
Enter export file password (press ENTER to return to menu):
 ===> ********
                                                      INPUT HIDDEN/INPUT
ESC=¢    1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
         7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

14 Migrating a key certificate from GSKKYMAN to a RACF digital key ring

Next, you will enter an export file password on the command line. Press enter to continue.

Confirm export file password

- Key in export file password again
- Enter

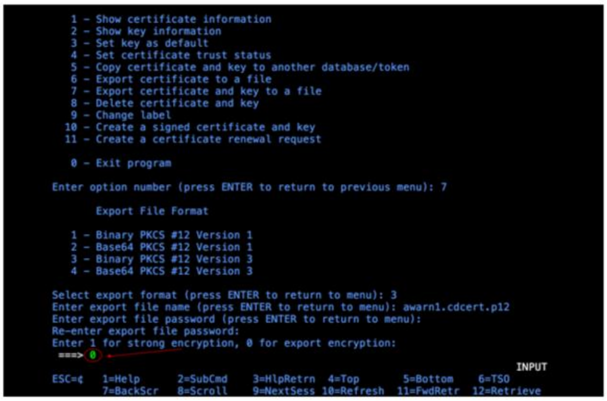


```
    1 - Show certificate information
    2 - Show key information
    3 - Set key as default
    4 - Set certificate trust status
    5 - Copy certificate and key to another database/token
    6 - Export certificate to a file
    7 - Export certificate and key to a file
    8 - Delete certificate and key
    9 - Change label
   10 - Create a signed certificate and key
   11 - Create a certificate renewal request

    0 - Exit program

Enter option number (press ENTER to return to previous menu): 7

       Export File Format

    1 - Binary PKCS #12 Version 1
    2 - Base64 PKCS #12 Version 1
    3 - Binary PKCS #12 Version 3
    4 - Base64 PKCS #12 Version 3

Select export format (press ENTER to return to menu): 3
Enter export file name (press ENTER to return to menu): awarn1.cdcert.p12
Enter export file password (press ENTER to return to menu):
Re-enter export file password:
 ===> ********
                                                         INPUT HIDDEN/INPUT
ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
        7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will key in your export file password a second time on the command line to confirm it. You must make a note of this password as you will need it to add the key certificate to RACF. Press enter to continue.

Encryption type

- Key in encryption type
- Enter

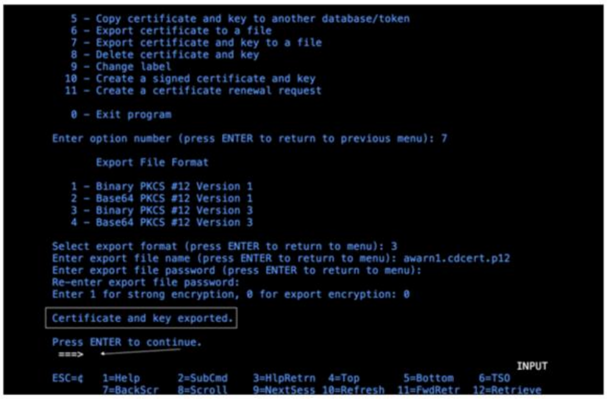


```
      1 - Show certificate information
      2 - Show key information
      3 - Set key as default
      4 - Set certificate trust status
      5 - Copy certificate and key to another database/token
      6 - Export certificate to a file
      7 - Export certificate and key to a file
      8 - Delete certificate and key
      9 - Change label
     10 - Create a signed certificate and key
     11 - Create a certificate renewal request

      0 - Exit program

  Enter option number (press ENTER to return to previous menu): 7

         Export File Format

      1 - Binary PKCS #12 Version 1
      2 - Base64 PKCS #12 Version 1
      3 - Binary PKCS #12 Version 3
      4 - Base64 PKCS #12 Version 3

  Select export format (press ENTER to return to menu): 3
  Enter export file name (press ENTER to return to menu): awarn1.cdcert.p12
  Enter export file password (press ENTER to return to menu):
  Re-enter export file password:
  Enter 1 for strong encryption, 0 for export encryption:
   ===> 0
                                                                      INPUT
  ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
          7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will key in the encryption type you require on the command line. You will key in 1 for strong encryption or 0 for export encryption. In this example, 0 is selected. Press enter to continue.

Certificate and key exported

- Certificate and key exported message displayed
- Enter

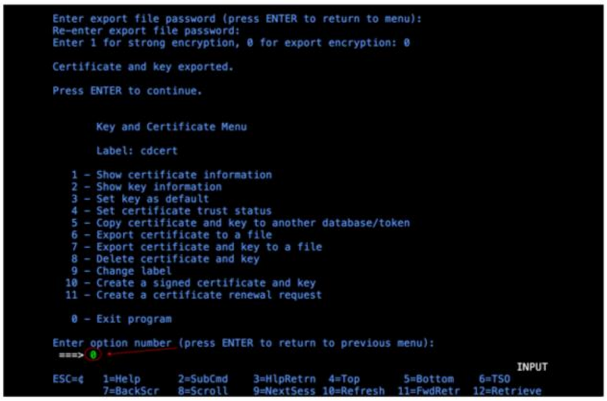


```
     5 - Copy certificate and key to another database/token
     6 - Export certificate to a file
     7 - Export certificate and key to a file
     8 - Delete certificate and key
     9 - Change label
    10 - Create a signed certificate and key
    11 - Create a certificate renewal request

     0 - Exit program

  Enter option number (press ENTER to return to previous menu): 7

         Export File Format

     1 - Binary PKCS #12 Version 1
     2 - Base64 PKCS #12 Version 1
     3 - Binary PKCS #12 Version 3
     4 - Base64 PKCS #12 Version 3

  Select export format (press ENTER to return to menu): 3
  Enter export file name (press ENTER to return to menu): awarn1.cdcert.p12
  Enter export file password (press ENTER to return to menu):
  Re-enter export file password:
  Enter 1 for strong encryption, 0 for export encryption: 0

  Certificate and key exported.

  Press ENTER to continue.
   ===>
                                                                    INPUT
  ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
          7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will see a certificate and key exported confirmation message. Press enter to continue.

Exit GSKKYMAN

- Key in 0
- Enter

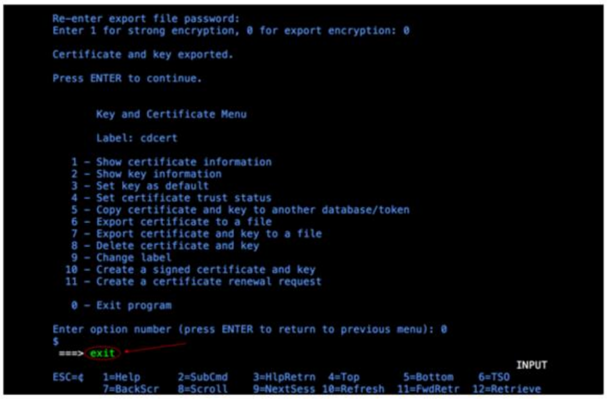


```
Enter export file password (press ENTER to return to menu):
Re-enter export file password:
Enter 1 for strong encryption, 0 for export encryption: 0

Certificate and key exported.

Press ENTER to continue.


       Key and Certificate Menu

       Label: cdcert

   1 - Show certificate information
   2 - Show key information
   3 - Set key as default
   4 - Set certificate trust status
   5 - Copy certificate and key to another database/token
   6 - Export certificate to a file
   7 - Export certificate and key to a file
   8 - Delete certificate and key
   9 - Change label
  10 - Create a signed certificate and key
  11 - Create a certificate renewal request

   0 - Exit program

Enter option number (press ENTER to return to previous menu):
 ===> 0
                                                                      INPUT
ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
        7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will now exit GSKKYMAN. Key in 0 and press enter to continue.

Exit OMVS

- Key in EXIT
- Enter

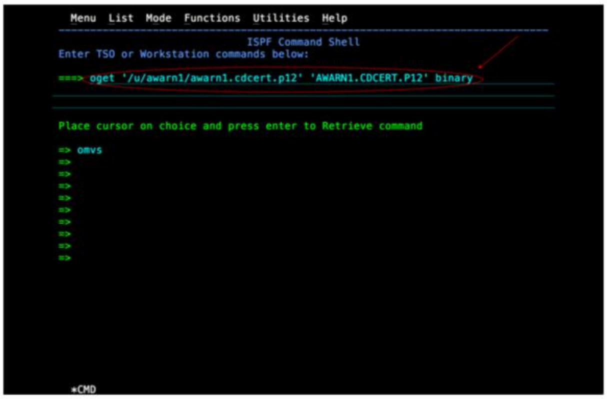


```
Re-enter export file password:
Enter 1 for strong encryption, 0 for export encryption: 0

Certificate and key exported.

Press ENTER to continue.


      Key and Certificate Menu

      Label: cdcert

   1 - Show certificate information
   2 - Show key information
   3 - Set key as default
   4 - Set certificate trust status
   5 - Copy certificate and key to another database/token
   6 - Export certificate to a file
   7 - Export certificate and key to a file
   8 - Delete certificate and key
   9 - Change label
  10 - Create a signed certificate and key
  11 - Create a certificate renewal request

   0 - Exit program

Enter option number (press ENTER to return to previous menu): 0
$
 ===> exit
                                                                    INPUT
ESC=¢   1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
        7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

You will key in exit on the command line to return to ISPF and press enter. Press enter again to exit OMVS. You will now move your exported PKCS12 file from the UNIX System Services file system to a z/OS data set.

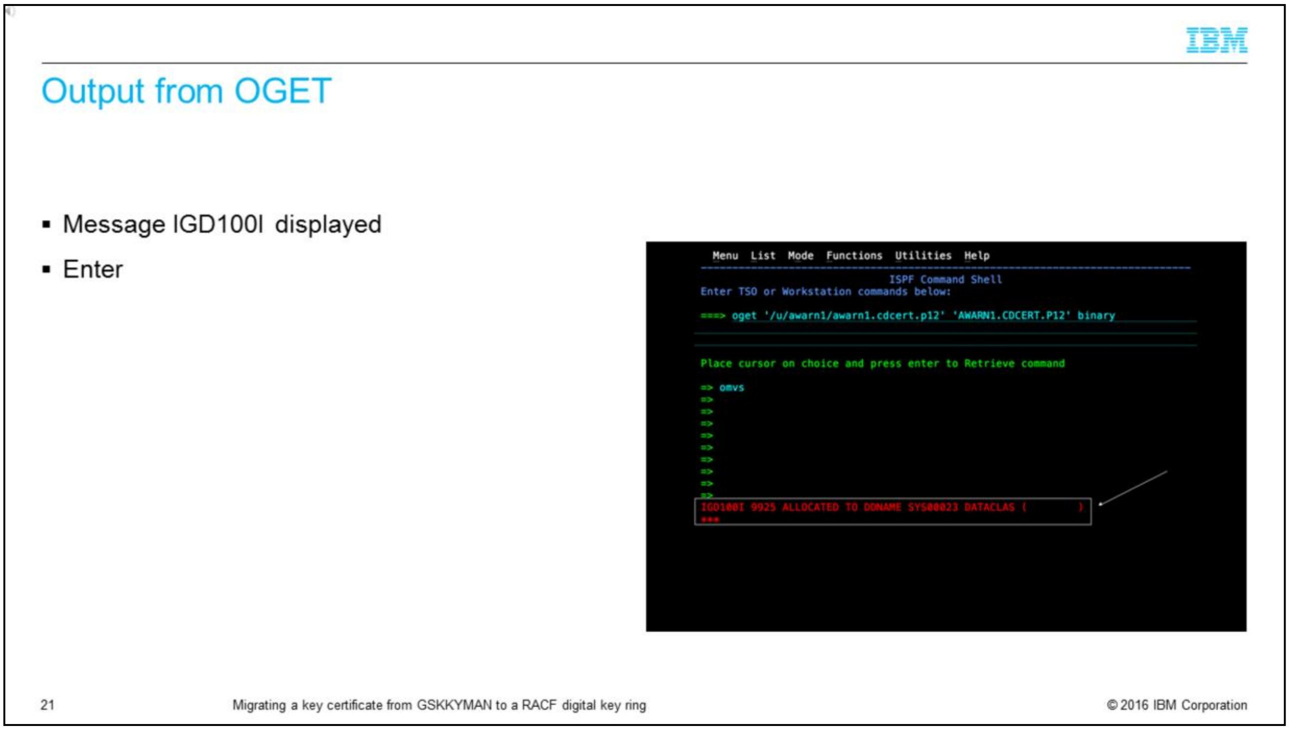
Move exported PKCS12 file to data set

- ISPF option 6
- Key in OGET ‘/u/userid/pkcs12filename’ ‘userid.pkcs12.dsname’ BINARY
- Enter



```
                           ISPF Command Shell
Enter TSO or Workstation commands below:

===> oget '/u/awarn1/awarn1.cdcert.p12' 'AWARN1.CDCERT.P12' binary


Place cursor on choice and press enter to Retrieve command

=> omvs
=>
=>
=>
=>
=>
=>
=>
=>
=>



  *CMD
```

You will enter a command in ISPF option 6 to move your exported PKCS12 file from UNIX System Services to a z/OS data set. Enter the oget command displayed on this slide on the command line. Use your PKCS12 file name and give it a z/OS data set name. You must move the file as a binary file. Press enter to continue.



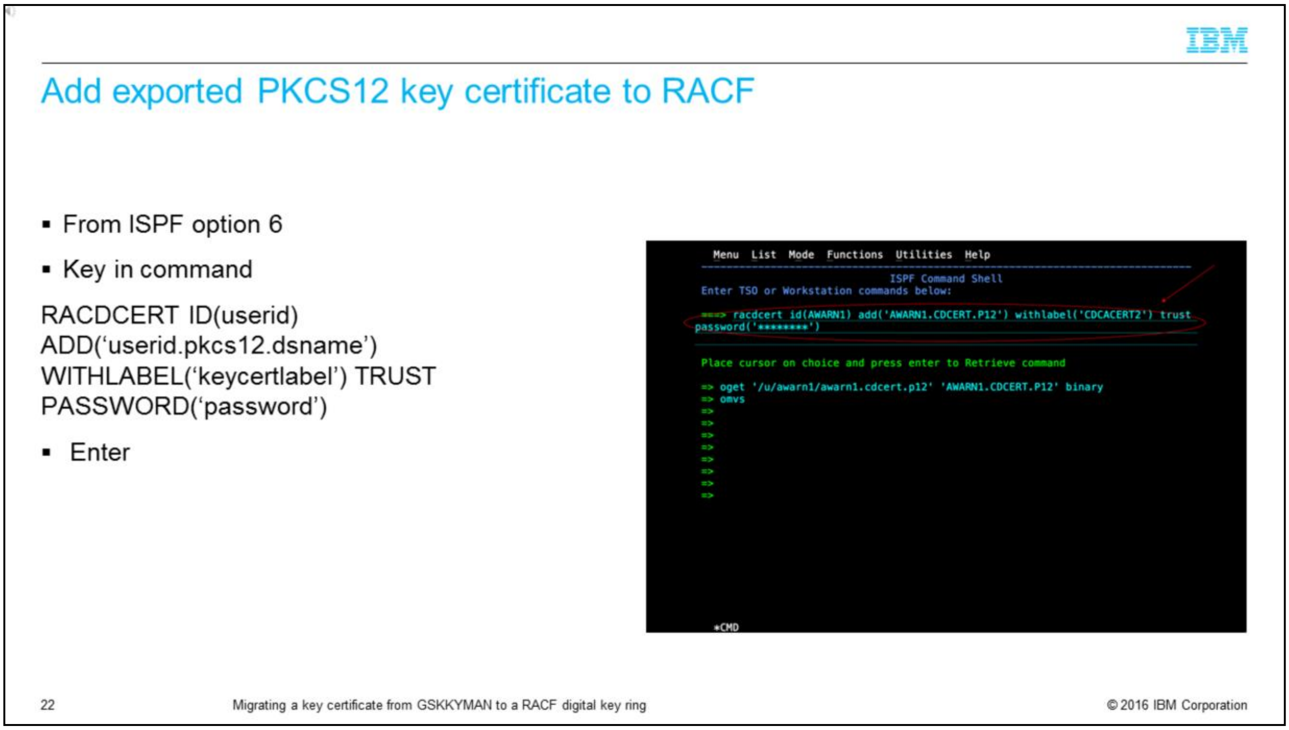
Output from OGET

- Message IGD100I displayed
- Enter

```
  Menu  List  Mode  Functions  Utilities  Help
 ------------------------------------------------------------------------------
                              ISPF Command Shell
 Enter TSO or Workstation commands below:

 ===> oget '/u/awarn1/awarn1.cdcert.p12' 'AWARN1.CDCERT.P12' binary



 Place cursor on choice and press enter to Retrieve command

 => omvs
 =>
 =>
 =>
 =>
 =>
 =>
 =>
 =>
 =>
 IGD100I 9925 ALLOCATED TO DDNAME SYS00023 DATACLAS (        )
 ***
```

21 Migrating a key certificate from GSKKYMAN to a RACF digital key ring

You will receive message IGD100I to confirm that the system created a new data set. You will now add the exported PKCS12 key certificate to RACF. Press enter to continue.



Add exported PKCS12 key certificate to RACF

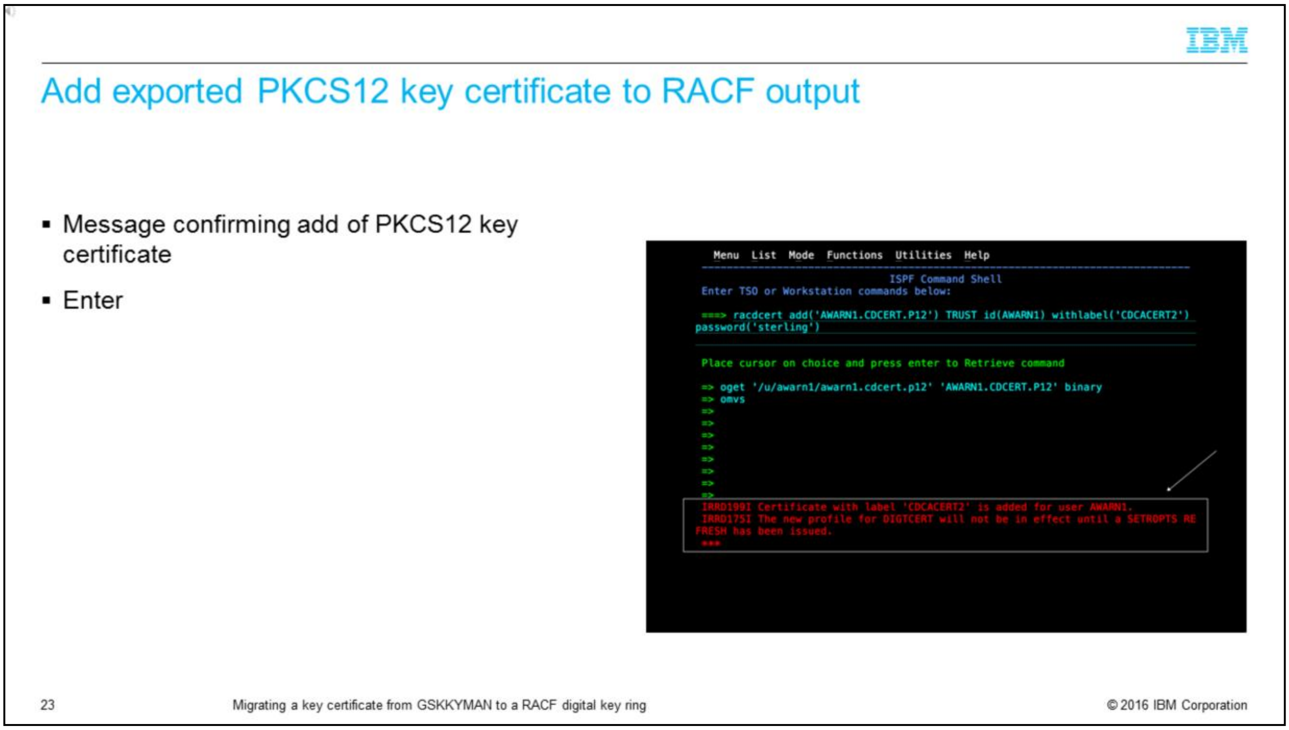
- From ISPF option 6
- Key in command

RACDCERT ID(userid)
ADD(‘userid.pkcs12.dsname’)
WITHLABEL(‘keycertlabel’) TRUST
PASSWORD(‘password’)

- Enter

```
  Menu  List  Mode  Functions  Utilities  Help
 ------------------------------------------------------------------------------
                          ISPF Command Shell
 Enter TSO or Workstation commands below:

 ===> racdcert id(AWARN1) add('AWARN1.CDCERT.P12') withlabel('CDCACERT2') trust
password('********')

 Place cursor on choice and press enter to Retrieve command

 => oget '/u/awarn1/awarn1.cdcert.p12' 'AWARN1.CDCERT.P12' binary
 => omvs
 =>
 =>
 =>
 =>
 =>
 =>
 =>
 =>

  *CMD
```

To add the exported key certificate to RACF, from ISPF option 6, key in the RACDCERT ADD command as displayed on this slide. The data set name is the z/OS data set name to which you moved your exported UNIX System Services file. You must give the key certificate a label and add it as trust. You must key in the password that you chose when you exported the key certificate then press enter to add the key certificate to RACF.

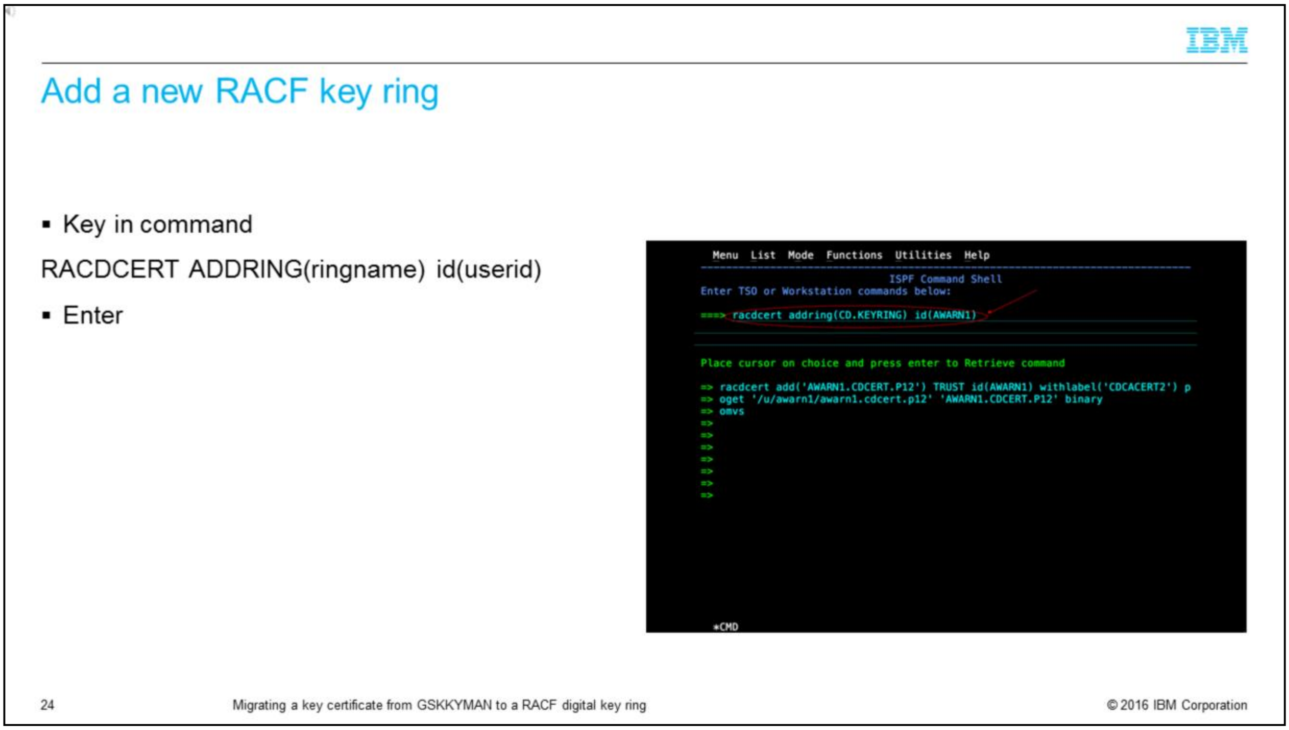


Add exported PKCS12 key certificate to RACF output

- Message confirming add of PKCS12 key certificate
- Enter

```
                              ISPF Command Shell
 Enter TSO or Workstation commands below:

 ===> racdcert add('AWARN1.CDCERT.P12') TRUST id(AWARN1) withlabel('CDCACERT2')
password('sterling')

 Place cursor on choice and press enter to Retrieve command

 => oget '/u/awarn1/awarn1.cdcert.p12' 'AWARN1.CDCERT.P12' binary
 => omvs
 =>
 =>
 =>
 =>
 =>
 =>
 =>
 =>
 IRRD199I Certificate with label 'CDCACERT2' is added for user AWARN1.
 IRRD175I The new profile for DIGTCERT will not be in effect until a SETROPTS RE
FRESH has been issued.
 ***
```

You will receive a message that confirms the PKCS12 key certificate is added. You might need to refresh RACF for the change to be in effect. Press enter to continue.



Add a new RACF key ring

- Key in command

RACDCERT ADDRING(ringname) id(userid)

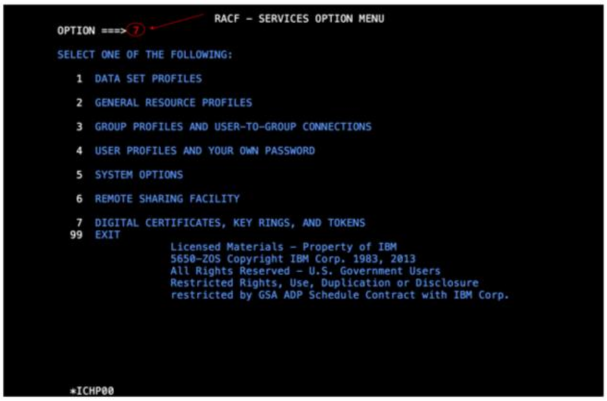
- Enter

```
  Menu  List  Mode  Functions  Utilities  Help
 ------------------------------------------------------------------------------
                              ISPF Command Shell
 Enter TSO or Workstation commands below:

 ===> racdcert addring(CD.KEYRING) id(AWARN1)


 Place cursor on choice and press enter to Retrieve command

 => racdcert add('AWARN1.CDCERT.P12') TRUST id(AWARN1) withlabel('CDCACERT2') p
 => oget '/u/awarn1/awarn1.cdcert.p12' 'AWARN1.CDCERT.P12' binary
 => omvs
 =>
 =>
 =>
 =>
 =>
 =>
 =>





   *CMD
```

In ISPF option 6 key in a RACDCERT ADDRING command to add a new key ring. You will give the key ring a name and associate it with a user ID. Press enter to continue.

Work with RACF certificate, key rings, and tokens

- Key in 7 on the ISPF RACF menu
- Enter

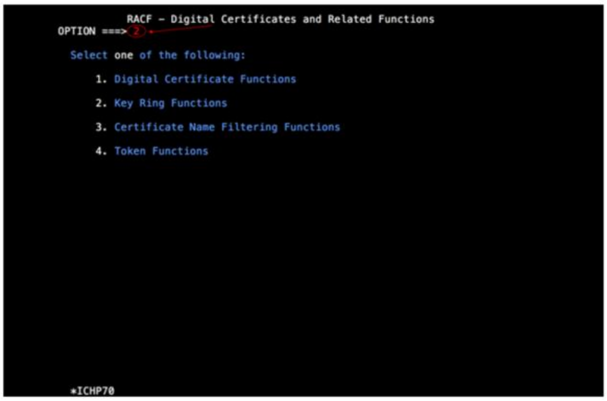


```
                            RACF - SERVICES OPTION MENU
OPTION ===> 7

SELECT ONE OF THE FOLLOWING:

   1  DATA SET PROFILES

   2  GENERAL RESOURCE PROFILES

   3  GROUP PROFILES AND USER-TO-GROUP CONNECTIONS

   4  USER PROFILES AND YOUR OWN PASSWORD

   5  SYSTEM OPTIONS

   6  REMOTE SHARING FACILITY

   7  DIGITAL CERTIFICATES, KEY RINGS, AND TOKENS
  99  EXIT
                Licensed Materials - Property of IBM
                5650-ZOS Copyright IBM Corp. 1983, 2013
                All Rights Reserved - U.S. Government Users
                Restricted Rights, Use, Duplication or Disclosure
                restricted by GSA ADP Schedule Contract with IBM Corp.




  *ICHP00
```

You will now navigate to your ISPF RACF panels. From the RACF services option menu, key in 7. Press enter to continue.

Select Key Ring Functions

- Key in 2 to select Key Ring Functions
- Enter

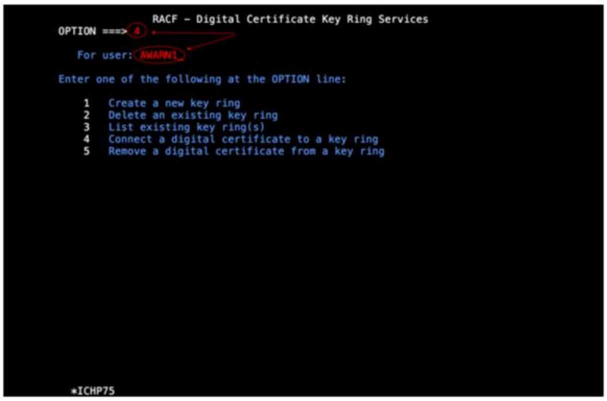


```
             RACF - Digital Certificates and Related Functions
OPTION ===> 2

  Select one of the following:

      1. Digital Certificate Functions

      2. Key Ring Functions

      3. Certificate Name Filtering Functions

      4. Token Functions




  *ICHP70
```

From the RACF digital certificates and related functions panel, you will key in 2 to select key ring functions. Press enter to continue.

Certificate key ring services

- Key in 4 to connect your certificate to you key ring
- Enter

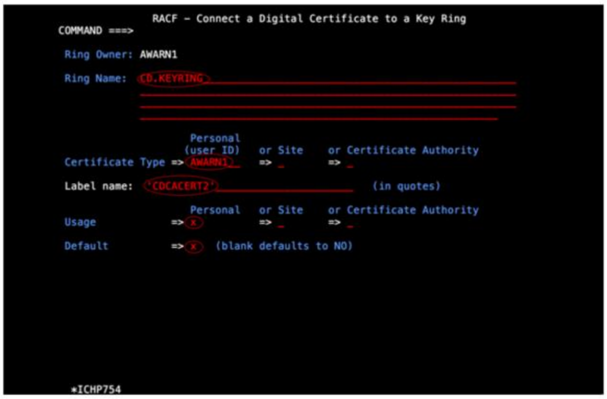


```
                 RACF - Digital Certificate Key Ring Services
OPTION ===> 4

   For user: AWARN1

Enter one of the following at the OPTION line:

    1   Create a new key ring
    2   Delete an existing key ring
    3   List existing key ring(s)
    4   Connect a digital certificate to a key ring
    5   Remove a digital certificate from a key ring




 *ICHP75
```

From the RACF digital certificate key ring services panel, key in 4 on the command line to connect your digital certificate to your key ring. Key in your user ID and press enter to continue.

Connect certificate to a key ring

- Key in the ring name
- Key in your user ID
- Key in the label of your certificate
- Key in ‘x’ for personal usage
- Key in ‘x’ default for key usage
- Enter

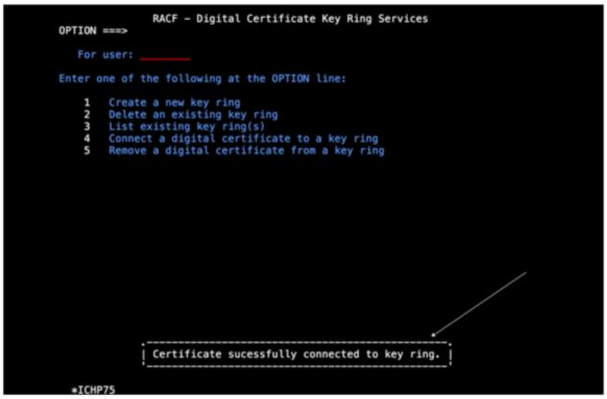


```
                 RACF - Connect a Digital Certificate to a Key Ring
COMMAND ===>

 Ring Owner: AWARN1

 Ring Name:  CD.KEYRING___________________________________________________
             _________________________________________________________________
             _________________________________________________________________
             ______________________________________________________________

                       Personal
                      (user ID)   or Site    or Certificate Authority
 Certificate Type => AWARN1__     => _       => _

 Label name:  'CDCACERT2'_____________________     (in quotes)

                       Personal   or Site    or Certificate Authority
 Usage              => x          => _       => _

 Default            => x   (blank defaults to NO)




  *ICHP754
```

On the RACF panel to connect a digital certificate to your key ring, key in your key ring name, your user ID, key certificate label name and personal for usage. Default designates this certificate as the key ring's default. In this example default is selected. Press enter to add your certificate to your key ring.

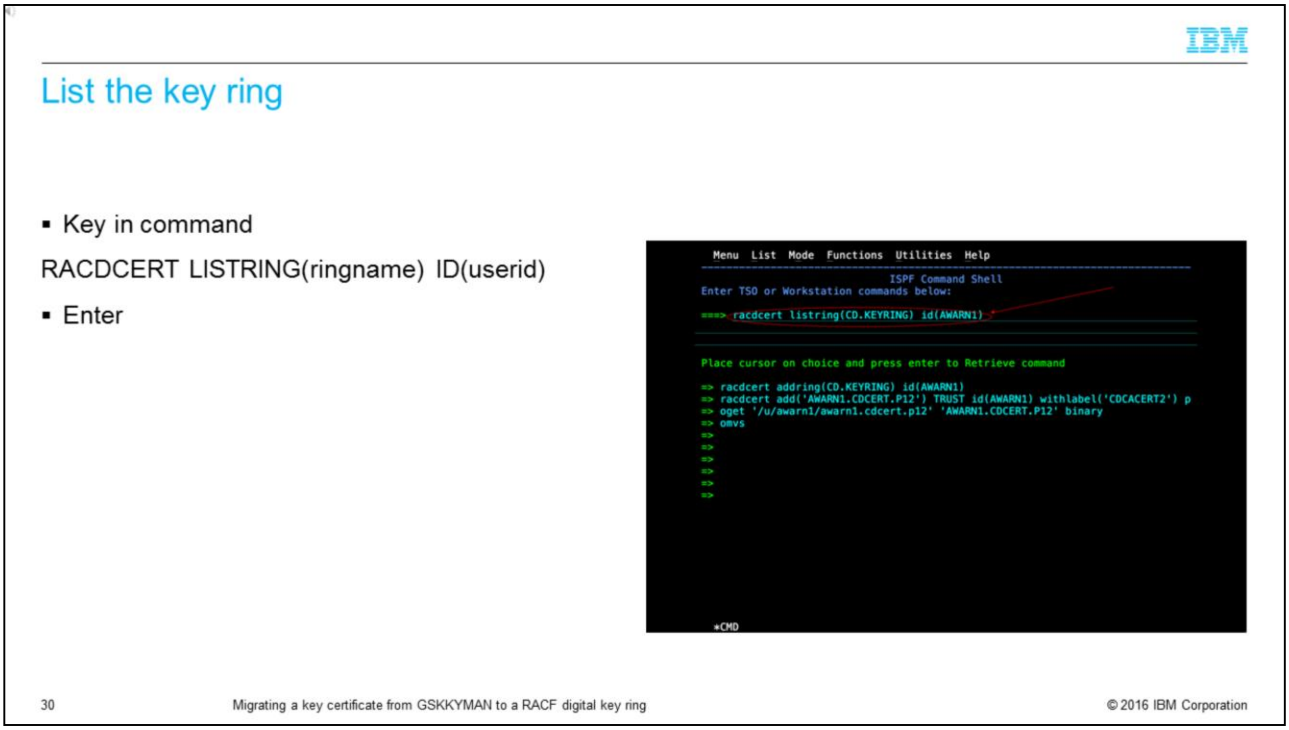
Certificate added to key ring

- Message that is displayed to confirm that your certificate was added to your key ring successfully



```
                 RACF - Digital Certificate Key Ring Services
OPTION ===>

   For user: ________

Enter one of the following at the OPTION line:

    1   Create a new key ring
    2   Delete an existing key ring
    3   List existing key ring(s)
    4   Connect a digital certificate to a key ring
    5   Remove a digital certificate from a key ring



                .----------------------------------------------.
                | Certificate sucessfully connected to key ring. |
                '----------------------------------------------'

   *ICHP75
```

You will see a message that confirms that your key certificate was added to your key ring successfully.



List the key ring

- Key in command

RACDCERT LISTRING(ringname) ID(userid)

- Enter

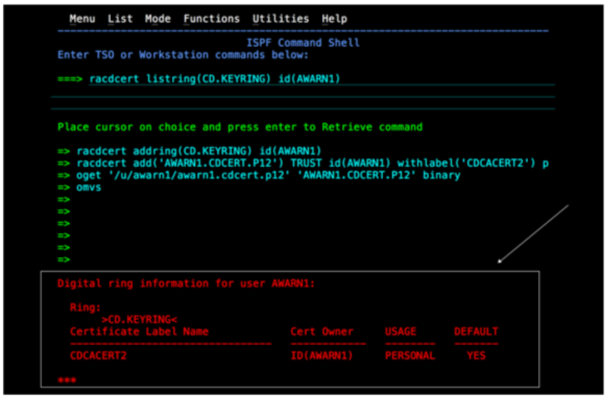
```
  Menu  List  Mode  Functions  Utilities  Help
 ------------------------------------------------------------------------------
                             ISPF Command Shell
 Enter TSO or Workstation commands below:

 ===> racdcert listring(CD.KEYRING) id(AWARN1)



 Place cursor on choice and press enter to Retrieve command

 => racdcert addring(CD.KEYRING) id(AWARN1)
 => racdcert add('AWARN1.CDCERT.P12') TRUST id(AWARN1) withlabel('CDCACERT2') p
 => oget '/u/awarn1/awarn1.cdcert.p12' 'AWARN1.CDCERT.P12' binary
 => omvs
 =>
 =>
 =>
 =>
 =>
 =>



  *CMD
```

30 Migrating a key certificate from GSKKYMAN to a RACF digital key ring © 2016 IBM Corporation

Navigate back to ISPF option 6 and key in the RACDCERT LISTRING command to list your key ring. Enter to continue.

Key ring information displayed

- Message that is displayed to show your key ring information.
- Enter

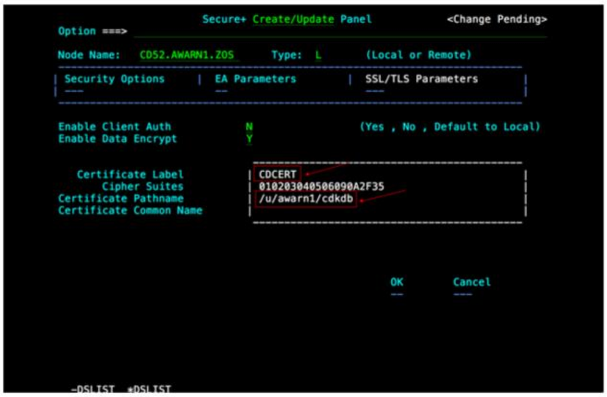


```
   Menu  List  Mode  Functions  Utilities  Help
 ------------------------------------------------------------------------------
                              ISPF Command Shell
 Enter TSO or Workstation commands below:

 ===> racdcert listring(CD.KEYRING) id(AWARN1)



 Place cursor on choice and press enter to Retrieve command

 => racdcert addring(CD.KEYRING) id(AWARN1)
 => racdcert add('AWARN1.CDCERT.P12') TRUST id(AWARN1) withlabel('CDCACERT2') p
 => oget '/u/awarn1/awarn1.cdcert.p12' 'AWARN1.CDCERT.P12' binary
 => omvs
 =>
 =>
 =>
 =>
 =>
 =>
 Digital ring information for user AWARN1:

   Ring:
        >CD.KEYRING<
   Certificate Label Name             Cert Owner     USAGE      DEFAULT
   --------------------------------   ------------   --------   -------
   CDCACERT2                          ID(AWARN1)     PERSONAL     YES

 ***
```

A message is displayed as output from the RACDCERT LISTRING command to display your key ring information. The message includes the key certificate name that you added to your key ring. Enter to continue.

Configure Secure+ replace GSKKYMAN

- Navigate to Secure+



```
                         Secure+ Create/Update Panel            <Change Pending>
Option ===> 

Node Name:   CD52.AWARN1.ZOS      Type:  L       (Local or Remote)
---------------------------------------------------------------------
| Security Options        |  EA Parameters          |  SSL/TLS Parameters    |
---------------------------------------------------------------------

Enable Client Auth            N                  (Yes , No , Default to Local)
Enable Data Encrypt           Y

                                 ------------------------------------------
   Certificate Label            | CDCERT                                   |
       Cipher Suites            | 010203040506090A2F35                     |
Certificate Pathname            | /u/awarn1/cdkdb                          |
Certificate Common Name         |                                          |
                                 ------------------------------------------

                                                     OK        Cancel

          -DSLIST  *DSLIST
```

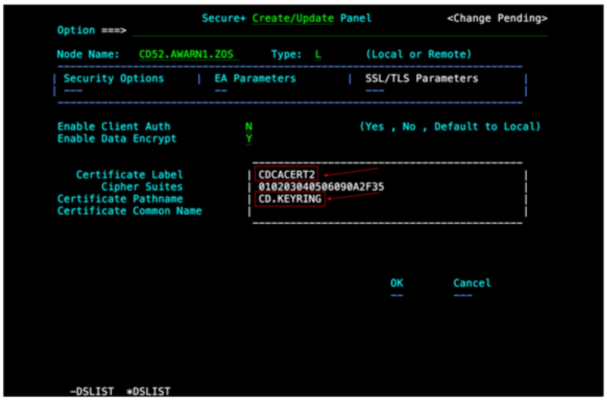
You will navigate to your Sterling Connect:Direct for z/OS IUI Secure+ option, open your Secure+ parmfile and select SSL/TSL parameters. You will see your old key database details display on the Secure+ create/update panel.

Configure Secure+ to use new RACF key ring

- Change certificate label to label used in RACF key ring.
- Change certificate path name to RACF key ring name.

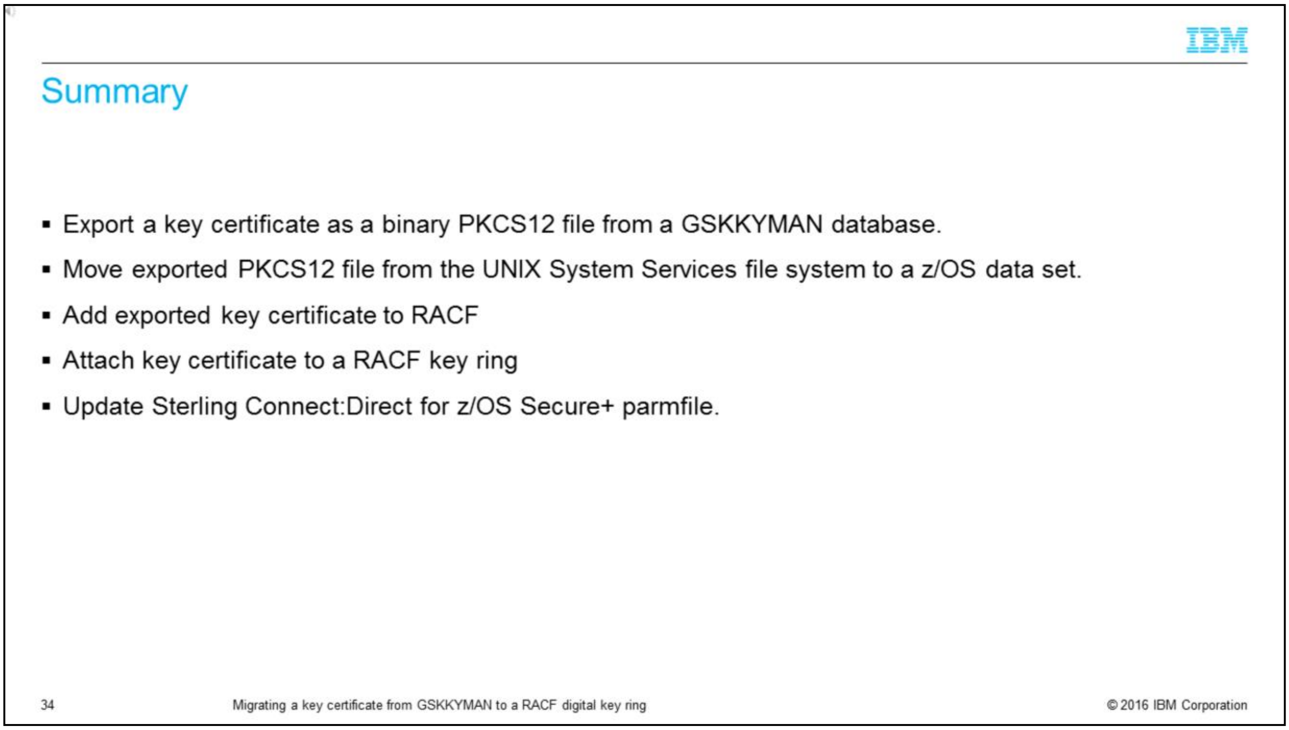
Note Remember to scroll down and remove the old gskkyman database password.

- Enter OK
- Enter File->Save As
- Restart Sterling Connect:Direct for z/OS



```
                              Secure+ Create/Update Panel            <Change Pending>
 Option ===> ______________________________________________________________

 Node Name:   CD52.AWARN1.ZOS      Type:  L        (Local or Remote)
 -------------------------------------------------------------------------
| Security Options       |  EA Parameters          |  SSL/TLS Parameters  |
| ---                    |  --                     |  ---                 |
 -------------------------------------------------------------------------

 Enable Client Auth             N               (Yes , No , Default to Local)
 Enable Data Encrypt            Y

                                  -------------------------------------------
    Certificate Label            | CDCACERT2                                 |
        Cipher Suites            | 010203040506090A2F35                      |
 Certificate Pathname            | CD.KEYRING                                |
 Certificate Common Name         |                                           |
                                  -------------------------------------------



                                                          OK          Cancel
                                                          --          ---



      -DSLIST  *DSLIST
```

You will now configure Secure+ to use the new RACF key ring in place of your GSKKYMAN database. You will place your cursor on certificate label and enter. Change the key certificate label to the key certificate label used in your RACF key ring and enter. You will place your cursor on certificate path name and enter. Change the certificate path name to the RACF key ring name and PF8 to scroll down. Remove the GSKKYMAN database password as it is not needed for a RACF key ring. Move your cursor to OK and press enter to continue. Select File and Save As to update your Sterling Connect:Direct for z/OS Secure+ Parmfile.

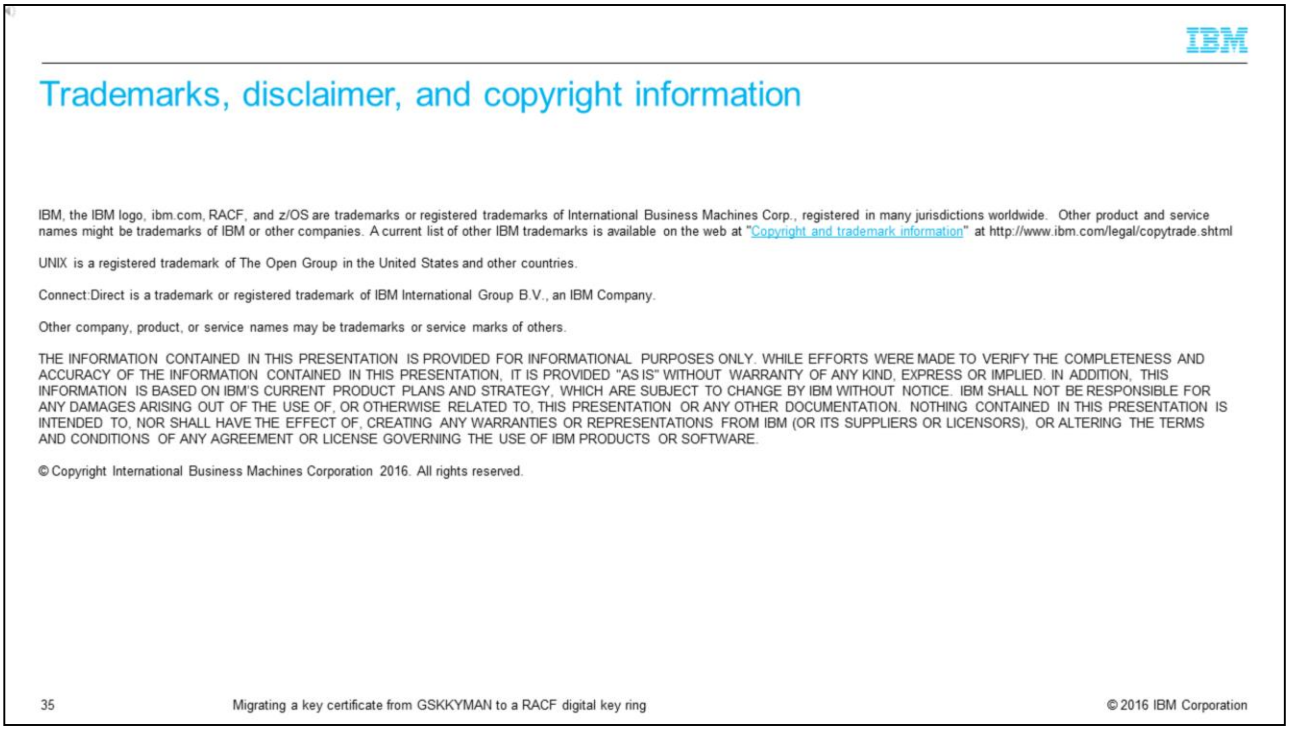


Summary

- Export a key certificate as a binary PKCS12 file from a GSKKYMAN database.
- Move exported PKCS12 file from the UNIX System Services file system to a z/OS data set.
- Add exported key certificate to RACF
- Attach key certificate to a RACF key ring
- Update Sterling Connect:Direct for z/OS Secure+ parmfile.

34 Migrating a key certificate from GSKKYMAN to a RACF digital key ring © 2016 IBM Corporation

In this presentation, you learned how to export a key certificate from a GSKKYMAN database as a PKCS12 binary file. You also learned how to move the file from UNIX System Services to a z/OS data set and add it to RACF. You then learned how to attach the key certificate to a RACF key ring and update to Sterling Connect Direct for z/OS Secure+ parmfile.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, RACF, and z/OS are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

UNIX is a registered trademark of The Open Group in the United States and other countries.

Connect:Direct is a trademark or registered trademark of IBM International Group B.V., an IBM Company.

Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.