Share in Pittsburgh, PA Session 16074

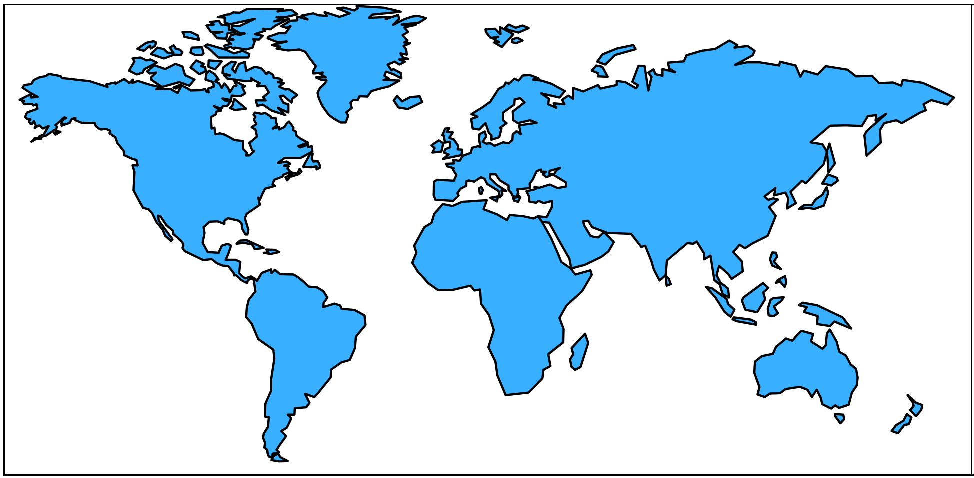
"Creating, Renewing, and Testing x.509 Digital Certificates with RACF" Hands-on Lab - Part 2 of 2

Part 1: CREATE and TEST Certificates
Part 2: RENEW Keys & ROLLOVER Certificates

SHARE 16074

Hands-on Lab Guide

(Digital Certificate Exercises: Extending Expiration Dates & Keys)



(USER21-22, USER31-32, USER41-42, USER51-52, USER61-62, USER71-72)

Revision date - Friday, 12 July. 2014

This edition applies to IBM z/OS Configuration Assistant V1R13 running on a Windows 7 platform.
The Configuration Assistant was downloaded from the IBM Communications Server website named: http://www.ibm.com/software/network/commserver/zos/support/
Attention:
Information in this document was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

Acknowledgements: Many thanks to Wai Choi of IBM PKI Development and Linda Harrison, Johnny Chi, Mahyar Imanian, and Sean O’Brien of IBM Advanced Technical Skills for suggestions they have made to enhance the user experience with this lab.

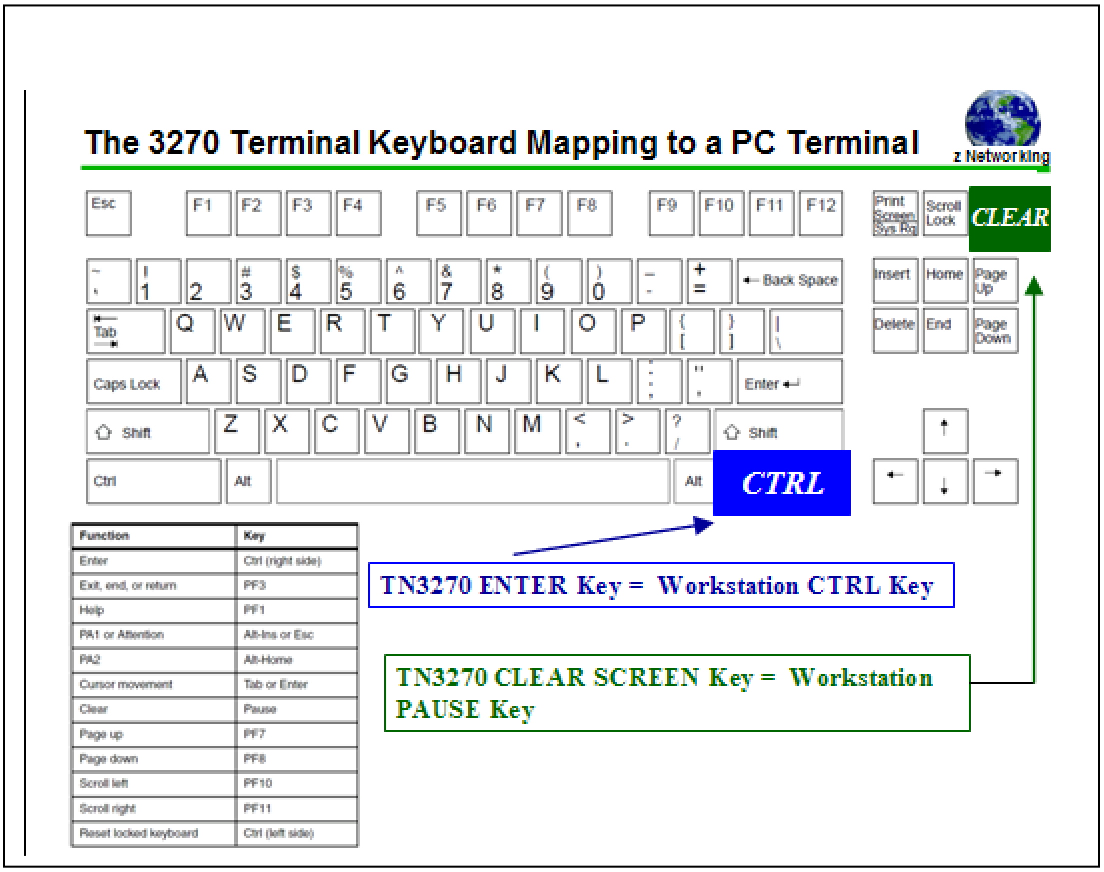
Table of Contents

Lab Topology and Organization: Lab Description (Configuring Policy Agent for AT-TLS and FTP)

Hands-on Lab Guide (z/OS Exercises – Two Hours)
2 Members per Team (Max Members = 36)

The lab is divided into several sections:

- *Scenario 0: Getting Started with the Lab*
- *Scenario 1 (Optional): Successful Key Ring and its Certificates*
- *Scenario 2: Key Ring and Renewal of Expired FTP Server Certificate*
- *Scenario 3 (Optional): Rekeying &"Rollover" of Personal FTP Certificate*
- *Scenario 4 (Optional): Rekeying &"Rollover" of Certificate Authority & FTP Server Personal Certificates*
- *APPENDIX: Lab Definition Samples*



The 3270 Terminal Keyboard Mapping to a PC Terminal

Function	Key
Enter	Ctrl (right side)
Exit, end, or return	PF3
Help	PF1
PA1 or Attention	Alt-Ins or Esc
PA2	Alt-Home
Cursor movement	Tab or Enter
Clear	Pause
Page up	PF7
Page down	PF8
Scroll left	PF10
Scroll right	PF11
Reset locked keyboard	Ctrl (left side)

TN3270 ENTER Key = Workstation CTRL Key

TN3270 CLEAR SCREEN Key = Workstation PAUSE Key

WORKSHOP POLICY RULES

Please maintain the integrity of the lab systems!

Do NOT customize the z/OS systems beyond what is asked of you in the labs.

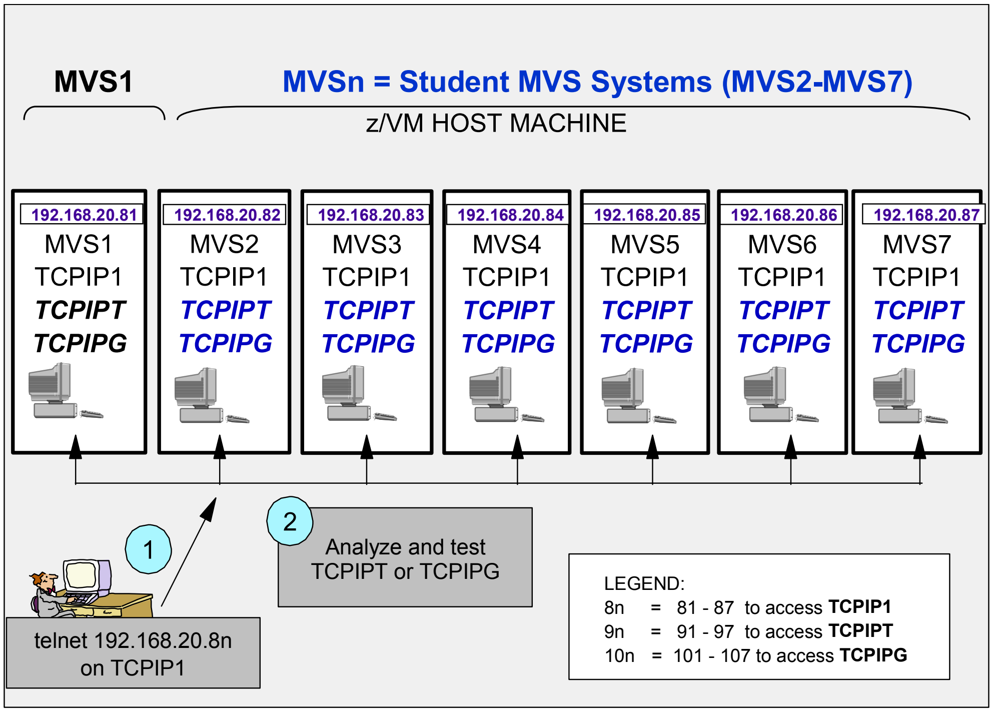
If you do so, you will negatively impact the labs not only for yourself but also for the other lab participants.

You are not authorized to copy or reproduce the lab materials for any purpose outside of this Workshop other than for no-charge training.

Introduction: Lab Environment, User IDs, Passwords, and Logging into MVS Images

If you feel that you already understand the lab logistics, you may skip this introduction and proceed to Optional Scenario 1 of this lab handout, where you will see what a successful secured FTP connection should look like. (Later Scenarios allow you to experience failures caused by invalid certificates and you will correct these situations.)

General Lab Diagram



1. Telnet into Maintenance Stack (TCPIP1) at the MVSn Guest Machine.
   A. Initialize and Test your TCPIPT or TCPIPG stack with the instructor profile.
   B. Edit TCP/IP configurations for Test Stack (TCPIPT or TCPIPG) with ISPF editor under TSO
2. Initialize and Test your TCPIPT or TCPIPG with your new profile.
3. You will test your connections against the Instructor MVS: MVS1.

MVS1 is the instructor "Control" system against which you will test the configurations that you build in your own MVS. The six "Student ZOS (MVS) systems" are labelled MVS2 – MVS7. In the lab book we refer to the student MVS systems as "MVS***n***" where ***"n"*** denotes the last digit of the MVS name. You will test against your own TCPIP***T*** or

TCPIP*G* stack in your MVS and you will also test against both stacks in the “Control” MVS image named MVS*1*.

Each ZOS (MVS) system has three TCP/IP stacks running in it: TCPIP*1*, TCPIP*T*, and TCPIP*G*. The basic TCPIP stack belonging to the instructors on each MVS image is named TCPIP1. The TCPIP stacks that the students customize are named TCPIP*T* and TCPIP*G*.

In our labs you use TCPIP*1* for basic maintenance on your ZOS until you begin working with your own student TCP/IP stacks and procedures. You telnet into “TN3270” at TCPIP*1* to reach ISPF and UNIX for building the procedures that should run together with the student TCP/IP stacks named TCPIP*T* and TCPIP*G*. The TN3270 procedure has affinity to the maintenance TCPIP*1*. The FTP procedure that has affinity to TCPIP*1* is named FTPCCL(1). Depending on the labs you execute you may find yourself also building a TN3270*T* or TN3270*G* procedure and an FTP*T* or FTP*G* procedure that have affinity to your student stack of TCPIP*T* or TCPIP*G*.

<u>SUMMARY:</u> The student TCP/IP stack is named either TCPIP*T* or TCPIP*G*. The students customize this stack at their assigned MVS (MVS*2* – MVS*7*) and *not* the instructor “maintenance” stack at MVS1. The students also customize any other procedures that are part of the labs and that are to have affinity with TCPIP*T* or TCPIP*G*.

Each MVS system may have up to three students configuring the TCP/IP environment. The three students work as a single Team.

Note that the labs are behind a firewall that performs Network Address Translation (NAT). On the lab systems themselves you will configure addresses in the 192.168.20.0/24 network.

Your workstations are also behind a firewall.

Please note that you have access to the INTERNET but NOT to the IBM INTRANET in these labs.

User IDs and Passwords

At the start of the class you will be assigned a Team User ID, in the form “USER***nx***,” where ***“n”*** stands for the MVS number you are to work on and “x” represents your team suffix. Password for the TSO User IDs will be handed out before the lab.

Workstation Configuration

You will be taking advantage of Personal Communications (PCOMM) for TN3270 connections to your MVS system.

Lab Booklets

Lab Booklets are handed out at the beginning of the lab.

Access to Files on z/OS

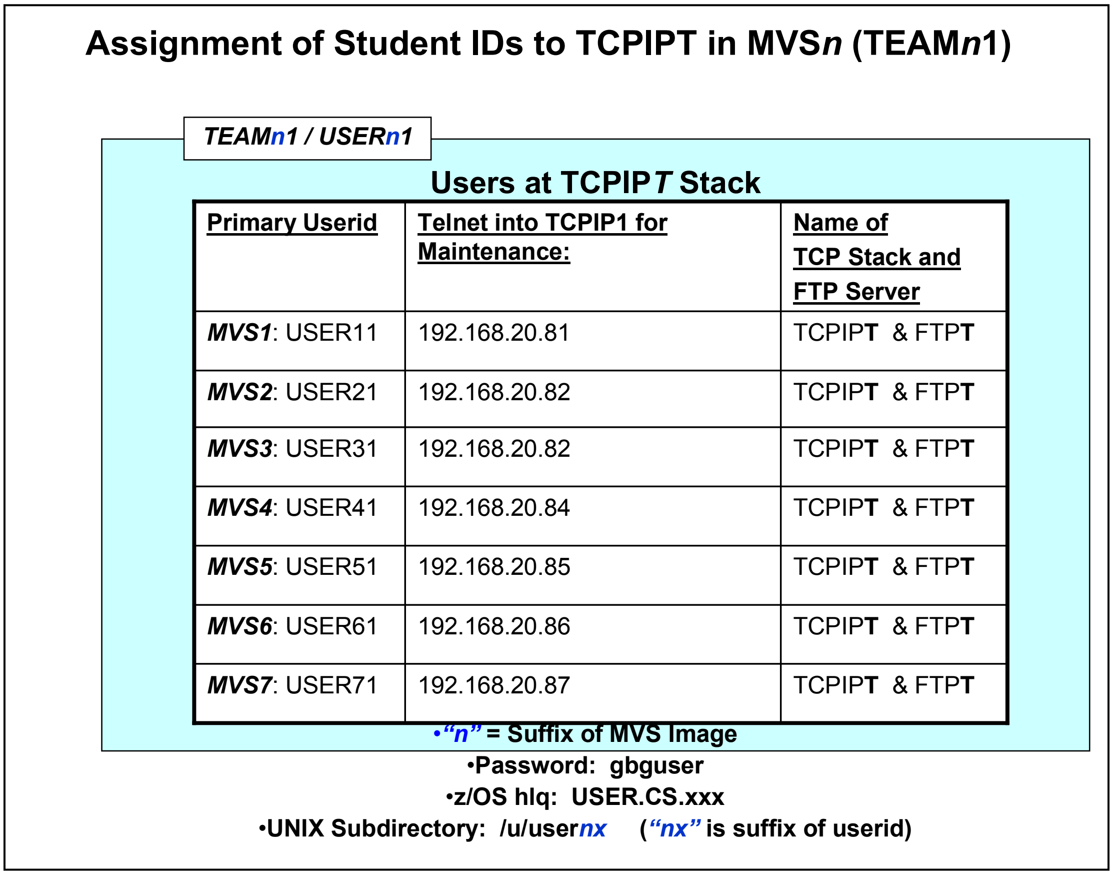
Your MVS (z/OS) system is set up to allow you full access to the MVS datasets that begin with the high-level qualifiers of USER.CS. …. You have READ access to the datasets that start with "SYS1." In UNIX you have permission to switch to SuperUser mode and will be told to do so during the labs.

You have UNIX identities on the MVS systems and you have a directory in /u/usernx (where "nx" is the number of your team). You are not a SuperUser, but you are permitted to BPX.SUPERUSER. (UNIXPRIV and RACF Access Control Lists – ACLs – are preferred over BPX.SUPERUSER in a highly secure UNIX environment, but these are lab systems that don't require that kind of control.)

User IDs and Assigned MVS Images

1. LEGEND for the TEAM Number and User ID value:
    a. USER***nx***, where ***"n"*** represents your MVS (ZOS) suffix number (e.g., ***1*** through *7*) and ***"x"*** represents a suffix of ***1*** for the TCPIP***T*** stack or ***2*** for the TCPIP***G*** stack).
    b. EXAMPLE:
        i. USER*72* means you are assigned to MVS*7* and to the TCPIP***G*** stack (i.e., ***2nd*** student stack on an MVS).
2. Up to two separate teams may be working on the same MVS system. You need not coordinate with the other teams.
3. Examine the Full Network Logical Diagram above and note the TN3270 and FTP Addresses of the "maintenance" stack named **TCPIP*1***.
    a. If you are assigned to MVS1, you connect to IP @ 192.168.20.81
    b. If you are assigned to MVS2, you connect to IP @ 192.168.20.82
    c. If you are assigned to MVS3, you connect to IP @ 192.168.20.83
    d. If you are assigned to MVS4, you connect to IP @ 192.168.20.84
    e. If you are assigned to MVS5, you connect to IP @ 192.168.20.85
    f. If you are assigned to MVS6, you connect to IP @ 192.168.20.86
    g. If you are assigned to MVS7, you connect to IP @ 192.168.20.87

4. If you are a member of TEAM*n1* with logon of USER*n1*, you are assigned to the ***TCPIPT*** stack on MVS***n*** and will be working on the FTP server named FTP***T***.
   a. (***"n"*** is the MVS suffix of MVS***2*** through MVS*7*.)
   b. See the diagram that follows.



Assignment of Student IDs to TCPIPT in MVS*n* (TEAM*n*1)

TEAMn1 / USERn1

Users at TCPIP*T* Stack

Primary Userid	**Telnet into TCPIP1 for Maintenance:**	**Name of TCP Stack and FTP Server**
MVS1: USER11	192.168.20.81	TCPIP**T** & FTP**T**
MVS2: USER21	192.168.20.82	TCPIP**T** & FTP**T**
MVS3: USER31	192.168.20.82	TCPIP**T** & FTP**T**
MVS4: USER41	192.168.20.84	TCPIP**T** & FTP**T**
MVS5: USER51	192.168.20.85	TCPIP**T** & FTP**T**
MVS6: USER61	192.168.20.86	TCPIP**T** & FTP**T**
MVS7: USER71	192.168.20.87	TCPIP**T** & FTP**T**

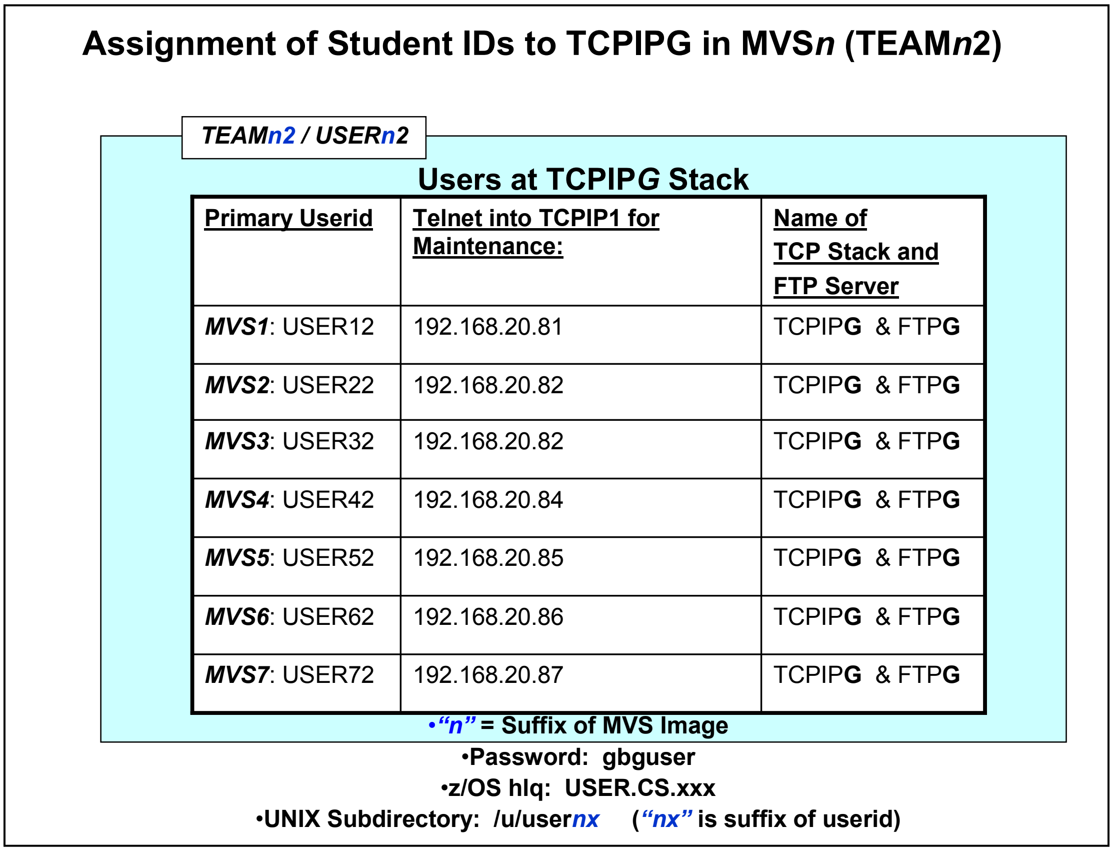
•*"n"* = Suffix of MVS Image

•Password: gbguser

•z/OS hlq: USER.CS.xxx

•UNIX Subdirectory: /u/user*nx* (*"nx"* is suffix of userid)

5. If you are a member of TEAM*n2* with logon of USER*n2*, you are assigned to the ***TCPIPG*** stack on MVS***n*** and will be working on the FTP server named FTP***G***.
   a. (***"n"*** is the MVS suffix of MVS***2*** through MVS*7*.)
   b. See the diagram that follows.



Assignment of Student IDs to TCPIPG in MVS*n* (TEAM*n*2)

TEAMn2 / USERn2

Users at TCPIP*G* Stack

Primary Userid	**Telnet into TCPIP1 for Maintenance:**	**Name of TCP Stack and FTP Server**
MVS1: USER12	192.168.20.81	TCPIP**G** & FTP**G**
MVS2: USER22	192.168.20.82	TCPIP**G** & FTP**G**
MVS3: USER32	192.168.20.82	TCPIP**G** & FTP**G**
MVS4: USER42	192.168.20.84	TCPIP**G** & FTP**G**
MVS5: USER52	192.168.20.85	TCPIP**G** & FTP**G**
MVS6: USER62	192.168.20.86	TCPIP**G** & FTP**G**
MVS7: USER72	192.168.20.87	TCPIP**G** & FTP**G**

•*"n"* = Suffix of MVS Image
•Password: gbguser
•z/OS hlq: USER.CS.xxx
•UNIX Subdirectory: /u/user*nx* (*"nx"* is suffix of userid)

NOTE: Your instructor will already have initialized the following procedures ***at MVS1*** – the system against which you will be testing. Do NOT EXECUTE or SUBMIT THESE – YOU MAY BE ASKED TO CREATE YOUR OWN VERSIONS of some of these in this lab.

- At MVS1:
  - SYS1.CS.CNTL(RACFPSEC) and SYS1.CS.CNTL(RACFP100) -- against shared RACF Database from one system
  - SYS1.CS.CNTL(RACFSIZE) -- against shared RACF Database """"""""""
  - NOTE: Your instructor will already have initialized the following procedures at MVS1 – the system from which you will be testing:
  - /s PAGENTT
  - /S *TCPIPT*,PROF=TCPSn1,CS=SYS1
    - /V TCPIP,TCPIPT,O,SYS1.CS.TCPPARMS(TLSON)
  - /S *TCPIPG,*PROF=TCPSn2,CS=SYS1
    - /V TCPIP,TCPIPG,O,SYS1.CS.TCPPARMS(TLSON)
  - /S tn3270t
    - TN3270T PROC PARMS='CTRACE(CTIEZBTN)',PROF=TN&CL1.A,CS=SYS1, DATA=DAT&CL1.A
  - /s FTPT,cs=sys1,fdat=ftpsauth,data=dat1a
  - /s FTPG,cs=sys1,fdat=ftpsauth,data=datag

- On Your MVS:
  - Your instructor will also have run one script to clear out the student directories from a previous lab offering on all 7 MVS volumes.
    - EMPTYCRE (for CREATE and for ROLLOVER LABS)
    - (copies skeletons into student datasets on unique volumes)
  -
- **UNIX Copy Jobs for Policy Agent Setup and Policies at all systems**
  - /BACKUP/CSPOLICY/CERTREFRESH/ussCERTCreateRefresh.sh

Scenario 0: Getting Started with the Lab

Logging into and Verifying Your MVSn (z/OS) System ("n" = MVS Suffix)

> You have **three separate documents** for each lab:
>
> a. **A Userids Sheet** that shows you your assigned MVS system, userid, password, and more.
> b. **Diagrams** that contains a page for your assigned userid or team which explains the configuration of your TCP/IP stack.
> c. **A Lab Booklet**. (This is the booklet you are now reading.)

1. Examine your **Userids Sheet** to determine your assigned MVS system, userids, passwords, and so on.
2. Open the **Diagrams** that illustrates the lab flow. Find the page that relates to the TCP/IP stack configuration with which you will be working.
3. **NOW YOU ARE READY TO BEGIN.**
4. If you have a PCOMM Folder or set of ICONs on your Desktop that points to the MVS systems for this lab, double-click on the ICON for your assigned MVS. The ICON name may be something like:
    a. **MVSnCS** (where "n" is the suffix of the MVS/ZOS system).
        a. If you can connect to your MVS, **skip to Step 6.**
5. If you do not see such an icon, create a PCOMM session to connect to TN3270 at TCPIP*1* on your assigned MVS system. Ensure that you are using code page IBM-1047, which is required by Policy Agent prior to z/OS V1R11.
    a. You should be telnetting into TCPIP*1* on some MVS system at **192.168.20.8n** (where "n" is the suffix of the MVS/ZOS system).
    b. Team1x telnets as User1x to TCPIP1 in MVS1 at **192.168.20.81**
    c. Team 2x telnets as User2x to TCPIP1 in MVS2 at **192.168.20.82**
    d. Team 3x telnets as User3x to TCPIP1 in MVS3 at **192.168.20.83**
    e. Team 4x telnets as User4x to TCPIP1 in MVS4 at **192.168.20.84**
    f. Team 5x telnets as User5x to TCPIP1 in MVS5 at **192.168.20.85**
    g. Team 6x telnets as User6x to TCPIP1 in MVS6 at **192.168.20.86**
    h. Team 7x telnets as User7x to TCPIP1 in MVS7 at **192.168.20.87**
6. When you see the TN3270 logon ("Message 10") screen from the TN3270 server – which can take a couple of seconds – enter the TSO logon command together with your User ID (USER***nx*** - where "***nx***" is the two-digit suffix assigned to your team and User ID).
    a. **TSO <userid>**
        i. Our "LOGON" command is named "TSO"
            1. Example for Team72: **TSO USER72**
        ii. Press 3270 keyboard's **ENTER** key (= Windows **'Ctrl'** key)

7. On the ISPF signon screen, provide the password you were given in class.
    a. **<password>**
    b. **Press ENTER** (= Windows **'Ctrl'** key)
8. When you see the ***Ready*** prompt, enter …
    a. **"ispf d.log"**
        i. This takes you to a view of the MVS console for your MVS image.
9. From the SDSF command line of the MVS log enter the command to verify that you are using the correct User ID and are logged into the correct MVS system:
    a. **"WHO"**
        i. You should see **USERID=USER*nx*** and **MEMBER=MVS*n***

10. From the MVS log enter the command to see how many TCP/IP stacks are currently running at your assigned MVS system:
    a. **"/D TCPIP"**
        i. You may see one to three active stacks:
            1. **TCPIP*1*** (the maintenance stack)
            2. **TCPIP*T*** (for User IDs ending in ***n1***)
            3. **TCPIP*G*** (for User IDs ending in ***n1***)
        ii. **If your assigned TCPIP stack is running, skip to Step 11.**
    b. USER***n1***: ***If*** **the TCPIP*T* stack is *not active***, please start it with:
        i. **/S TCPIP*T*,PROF=TCPS*n1*** ***("n"*** = your MVS suffix)
            1. When the stack completes initialization, activate an OBEYFILE to enable AT-TLS:

        /V TCPIP,TCPIP*T*,O,SYS1.CS.TCPPARMS(TLSON)
    c. USER***n2***: ***If*** **the TCPIP*G* stack is *not active***, please start it with:
        1. **/S TCPIP*G*,PROF= TCPS*n2*** ***("n"*** = your MVS suffix)
            1. When the stack completes initialization, activate an OBEYFILE to enable AT-TLS:

        /V TCPIP,TCPIP*G*,O,SYS1.CS.TCPPARMS(TLSON)

11. Use your team's assigned MVS and TCPIP page from the **Diagrams** to verify that your TCP/IP stack is running with the **correct network interfaces and IP addresses:**
    a. **For TCPIPT Teams: /D TCPIP,TCPIPT,N,HOME**
    b. **For TCPIPG Teams: /D TCPIP,TCPIPG,N,HOME**

12. Notify instructor if the output is not correct for your assigned TCP/IP stack.

13. If everything looks right, enter the command to determine whether Policy Agent ("PAGENTT") has been initialized:
    a. **/D A,PAG***
        i. If it is ***not*** running, please start it with:
            1. **/S PAGENTT**
14. If everything looks right, enter the command to determine whether your FTP Server ("FTPTx") is running:
    a. **/D A,FTP***
        i. **USER*n1*:** Look for **FTP*T1***

ii. **USER*n2*:** Look for **FTP*G1***

15. **If your FTP Server is *not* running, please start it with the following command:**
    a. USER***n1***:
        i. **/S FTP*T*,FDAT=FTPSAUTH**
            1. ***("n"*** = your MVS suffix)
    b. USER***n2***:
        ii. **/S FTP*G*,FDAT=FTPSAUTH**

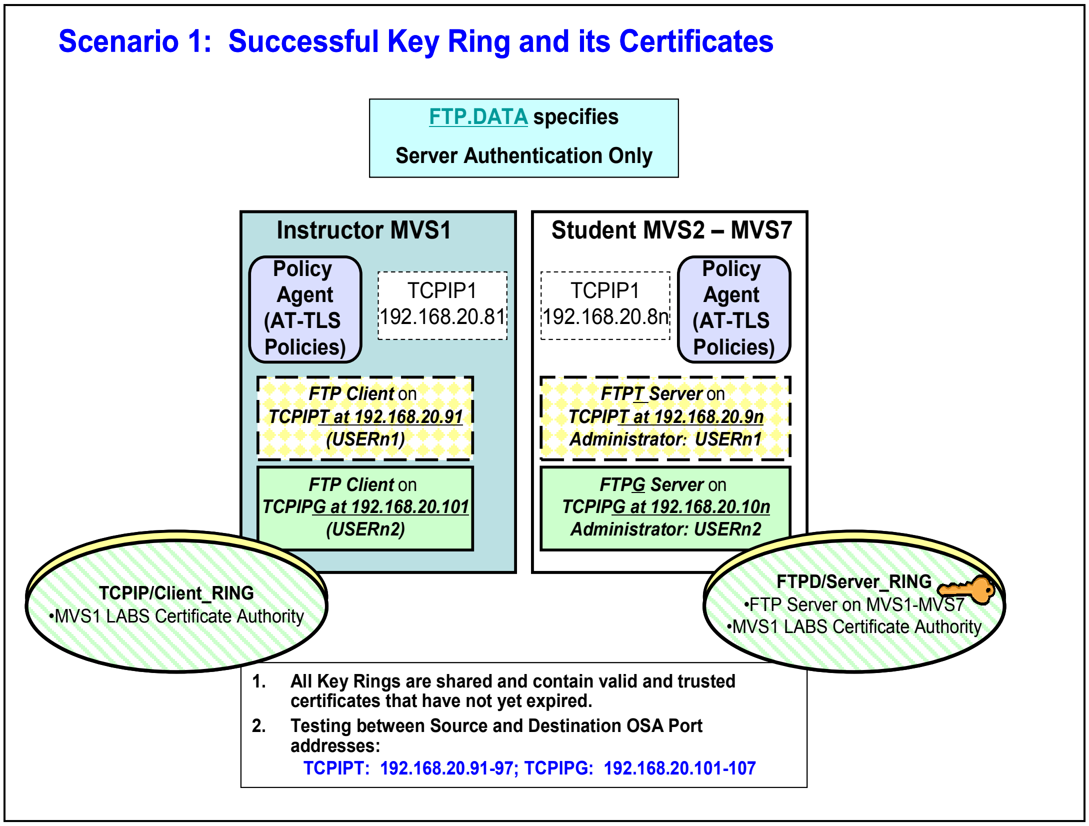
Examining the z/OS Image

1. From the command line enter the command to start browsing the contents of the Student Datasets:
    a. **=3.4**
    b. At the DSNAME field of the next panel enter the high-level qualifier for the student datasets:
        i. **SYS1.CS.TCPPARMS**
        ii. Press **ENTER**
            - Then enter a **"b"** next to **"SYS1.CS.TCPPARMS"** and press **ENTER** again to browse the dataset.
2. You should see at least the following members for the first part of the lab:
    a. **SYS1.CS.TCPPARMS:**
    a. **TCPSn1** (TCP/IP Profile Dataset) - ("n" = MVS Suffix)
    b. **TCPSn2** (TCP/IP Profile Dataset) - ("n" = MVS Suffix)
    c. **DATnA** (TCP.DATA file to establish affinity with the TCPIP***T*** stack)
    d. **DATAG** (TCP.DATA file to establish affinity with the TCPIP***G*** stack)
    e. **TLSON**
    f. **FTPSAUTH**
    g. **FTPCLSEC**
    b. Enter **PF3 (F3)** to exit from this screen

3. Enter **PF3 (F3)** again to return you to the DSLIST screen.
    a. At the DSNAME field of the panel enter the high-level qualifier for the student datasets:
        i. **USER.CS.SOURCE**
    b. Press **ENTER**
        i. Then enter a **"b"** next to **"USER.CS.SOURCE"** and press **ENTER** again to browse the dataset.
        ii. You may see many members, but for this part of the lab we will need the following two members:
            1. **SKRENU*nx*** (nx is your TEAM's suffix)
            2. **SKROLL*nx*** (nx is your TEAM's suffix)

4. **If you fail to see the specified members, notify your instructor.**

Scenario 1 (OPTIONAL): Successful Connection -- Key Ring and its Certificate


Scenario 1: Successful Key Ring and its Certificates
FTP.DATA specifies
Server Authentication Only
Instructor MVS1
Policy Agent (AT-TLS Policies)
TCPIP1
192.168.20.81
FTP Client on TCPIPT at 192.168.20.91 (USERn1)
FTP Client on TCPIPG at 192.168.20.101 (USERn2)
Student MVS2 – MVS7
TCPIP1
192.168.20.8n
Policy Agent (AT-TLS Policies)
FTPT Server on TCPIPT at 192.168.20.9n Administrator: USERn1
FTPG Server on TCPIPG at 192.168.20.10n Administrator: USERn2
TCPIP/Client_RING
•MVS1 LABS Certificate Authority
FTPD/Server_RING
•FTP Server on MVS1-MVS7
•MVS1 LABS Certificate Authority

1. All Key Rings are shared and contain valid and trusted certificates that have not yet expired.
2. Testing between Source and Destination OSA Port addresses:
   TCPIPT: 192.168.20.91-97; TCPIPG: 192.168.20.101-107

<u>Explanation of Scenario</u>: In this optional lab scenario you will be verifying FTP Connections with VALID (Unexpired) Certificates and Keys.

IMPORTANT: Screen captures are APPROXIMATE EXAMPLES of what you may see. Always follow the lab instructions for what to enter on the GUI screens and ignore the entries in the EXAMPLE unless you are told to use those entries.

> If you feel that you already understand the basics of working with x.509 certificates, you may skip this brief Scenario which illustrates and explains what a successful FTP connection should look like and proceed to Scenario 2 of this lab handout. There you will see FTP connection failures and then correct the problems that were caused by invalid certificates.

Running the Optional Lab in Scenario 1

1. If not still logged into **<u>your</u>** MVS***n***, use PCOMM to log in to it with the address ***at 192.168.20.8n.***
2. **Next login to *MVS1*** with **your** User ID: "USER***nx.***"

3. MVS***1 is at 192.168.20.81. (Find an ICON for MVSCS1 or, if necessary, create a second PCOMM session per previous instructions.)***

4. Position yourself at ISPF Option 6 in order to test a **working FTP connection** that has been defined with AT-TLS.
5. **=6**

6. From TSO enter the command to open an FTP connection between the source IP address of 192.168.20.***91*** or ***101*** and the destination FTP server address of 192.168.20.***9n*** or ***10n*** connected to ***Port 21*** on the target system. The "ftp" command is requesting Transport Layer Security (TLS) over the OSD OSA port and is using the client FTP parameter file named "ftpclsec".

   a. USERS with ID of **USER*n1* at TCPIP*T*:**
      ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*T* -s 192.168.20.91 192.168.20.9*<u>n</u>*
      (*<u>"n"</u>* = <u>your</u> MVS suffix)
   b. USERS with ID of **USER*n2* at TCPIP*G*:**
      ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*G* -s 192.168.20.101 192.168.20.10*<u>n</u>*
      (*<u>"n"</u>* = <u>your</u> MVS suffix)

```
EZY2640I Using 'SYS1.CS.TCPPARMS(FTPCLSEC)' for local site
configuration parame
         ters.
EZYFT25I Using //'SYS1.TCPIP.STANDARD.TCPXLBIN' for FTP translation
tables for
         the control connection.
EZYFT31I Using //'SYS1.TCPIP.STANDARD.TCPXLBIN' for FTP translation
tables for the data connection.
EZA1450I IBM FTP CS V1R13
EZA1466I FTP: using TCPIPT
EZYFT18I Using catalog '/usr/lib/nls/msg/C/ftpdmsg.cat' for FTP
messages.
EZA1554I Connecting to:   192.168.20.92 port: 21.
220-FTPT1 IBM FTP CS V1R13 at MVSS2T.dmz, 14:14:31 on 2012-09-18.
220 Connection will close if idle for more than 5 minutes.
FC0242 ftpAuth: security values: mech=TLS, tlsmech=ATTLS, sFTP=R,
sCC=P, sDC=P <<<<<<<<<<<<<<<<<<<<<<<<<<
FC2656 ftpAuthAttls: AT-TLS policy set as application controlled.
FU1367 TTLSRule: FTPTClientat192.168.20.9n~4
FU1373 TTLSGroupAction: gAct1
FU1379 TTLSEnvironmentAction: eAct4
FU1386 TTLSConnectionACtion: cAct3
```

```
EZA1701I >>> AUTH TLS   <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
234 Security environment established - ready for negotiation <<<<<
FC2811 authServerAttls: Start Handshake     <<<<<<<<<<<<<<<<<<<<<<
FC2842 authServerAttls: FIPS140 not enabled
FC2863 authServerAttls: Using TLSv1.1 protocol <<<<<<<<<<<<<<<<<<<
FC2874 authServerAttls: SSL cipher: 0A
EZA2895I Authentication negotiation succeeded   <<<<<<<<<<<<<<<<<<
FC1754 setdlevel: entered
FC1911 setpbsz: entered
EZA1701I >>> PBSZ 0
200 Protection buffer size accepted
EZA1701I >>> PROT P
200 Data connection protection set to private    <<<<<<
EZA2906I Data connection protection is private   <<<<<<
EZA1459I NAME (192.168.20.92:USER21):  <<<<<<<<<<<<<<<<<<<<<<<<<<
```

7. Notice in the output display the lines marked with “<<<<<<”
8. These show you a successful SSL/TLS/AT_TLS negotiation and Server Authentication for FTP using TLSv1.1 . Both the control connection and the data connection are set to private – that is, are being secured.

9. Enter your User ID and Password when requested. Here is an example of what you will see:

```
EZA1701I >>> USER USER21
331 Send password please.
EZA1789I PASSWORD:


EZA1701I >>> PASS
230 USER201 is logged on.  Working directory is "USER21.".
EZA1460I Command:
```

10. Observe how this control connection over which User IDs, Passwords, and commands are sent is successful.

11. Test the data connection next by executing the FTP directory subcommand:
    a. **dir**

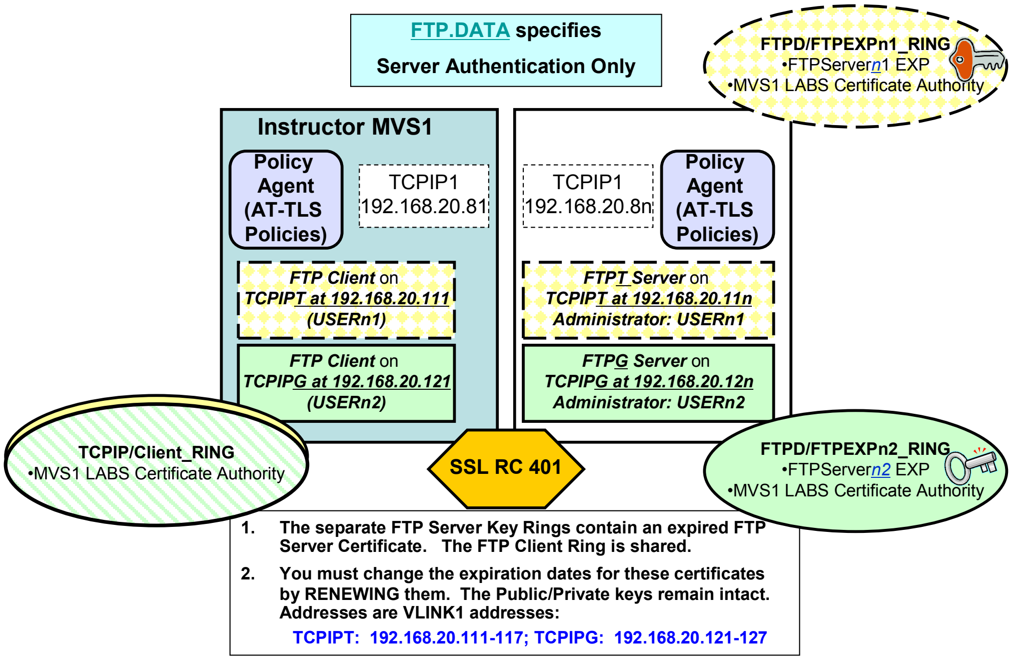
```
 EZA1460I Command:
dir
 EZA1701I >>> PORT 192,168,20,91,4,8
 200 Port request OK.
 EZA1701I >>> LIST
 125 List started OK
 FU1130 protDataConnAttls: Issuing SIOCTTLSCTL to query policy state
 FU1172 protDataConnAttls: AT-TLS policy set as application controlled.
 FU1367 TTLSRule: FTPTClientat192.168.20.9n~4
 FU1373 TTLSGroupAction: gAct1
 FU1379 TTLSEnvironmentAction: eAct4
 FU1386 TTLSConnectionACtion: cAct3
 FU1206 protDataConnAttls: Issuing SIOCTTLSCTL to start handshake
 FU1230 protDataConnAttls: FIPS140 not enabled
 FU1251 protDataConnAttls: Using TLSv1.1 protocol  <<<<<<<<<<<<<<<<
 FU1263 protDataConnAttls: SSL cipher: 0A          <<<<<<<<<<<<<<<<
 EZA2284I Volume Unit    Referred Ext Used Recfm Lrecl BlkSz Dsorg
Dsname
 EZA2284I ZOSUSR 3390   2012/09/18  1   15  U        0      0  PO  HFS
 EZA2284I ZOSUSR 3390   2012/09/18  2    2  FB      80 27920  PO
ISPF.ISPPROF
 250 List completed successfully.
 EZA1460I Command:
```

12. Notice in the output display the lines marked with "<<<<<<"
13. These show you successful secured data transfer over the data connection using the TLSV1.1 protocol and employing the 3DES ("triple DES") encryption algorithm ***(="0A").***
14. Exit from the FTP connection with the following subcommand:
15. **quit**

Next you will test Scenario 2 of the lab.

Scenario 2: A Failed Connection -- Key Ring and Renewal of Expired FTP Server Certificate

Scenario 2: Key Ring and Renewal of Expired FTP Server Certificate



FTP.DATA specifies
Server Authentication Only

FTPD/FTPEXPn1_RING
•FTPServern1 EXP
•MVS1 LABS Certificate Authority

Instructor MVS1

Policy Agent (AT-TLS Policies)

TCPIP1
192.168.20.81

TCPIP1
192.168.20.8n

Policy Agent (AT-TLS Policies)

FTP Client on TCPIPT at 192.168.20.111 (USERn1)

FTPT Server on TCPIPT at 192.168.20.11n Administrator: USERn1

FTP Client on TCPIPG at 192.168.20.121 (USERn2)

FTPG Server on TCPIPG at 192.168.20.12n Administrator: USERn2

TCPIP/Client_RING
•MVS1 LABS Certificate Authority

SSL RC 401

FTPD/FTPEXPn2_RING
•FTPServern2 EXP
•MVS1 LABS Certificate Authority

1. The separate FTP Server Key Rings contain an expired FTP Server Certificate. The FTP Client Ring is shared.
2. You must change the expiration dates for these certificates by RENEWING them. The Public/Private keys remain intact. Addresses are VLINK1 addresses:
   TCPIPT: 192.168.20.111-117; TCPIPG: 192.168.20.121-127

Explanation of Scenario: In this lab scenario your attempt to establish a secured FTP connection will fail, because the FTP Server Certificate at your MVS has expired. You will use RACF to extend the expiration date of the FTP Server Certificate. Subsequently you will establish a successful FTP connection.

IMPORTANT: Screen captures are APPROXIMATE EXAMPLES of what you may see. Always follow the lab instructions for what to enter on the GUI screens and ignore the entries in the EXAMPLE unless you are told to use those entries.

The Connection Fails with SSL RC401

1. You can stay logged in at YOUR MVS, but position yourself at your second TN3270 emulator session logged into MVS*1 at 192.168.20.81.*

2. Position yourself at ISPF Option 6 at MVS*1* in order to test a connection between two Static VIPAs (VLINK1) that *will fail* with SSL Return Code of 401. ***SSL RC 401 indicates that a Certificate has expired.***

   a. For TCPIP*T* Client (USER*n1*):
   ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*T* -s 192.168.20.111 192.168.20.11*n*
   (***"n"*** = your MVS suffix)

   b. For TCPIP*G* Client (USER*n2*):
   ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*G* -s 192.168.20.121 192.168.20.12*n*
   (***"n"*** = your MVS suffix)

3. You will see error messages that look something like this:

```
EZY2640I Using 'SYS1.CS.TCPPARMS(FTPCLSEC)' for local site
configuration parame
         ters.
EZYFT25I Using //'SYS1.TCPIP.STANDARD.TCPXLBIN' for FTP translation
tables for
         the control connection.
EZYFT31I Using //'SYS1.TCPIP.STANDARD.TCPXLBIN' for FTP translation
tables for the data connection.
EZA1450I IBM FTP CS V1R13
EZA1466I FTP: using TCPIPT
EZYFT18I Using catalog '/usr/lib/nls/msg/C/ftpdmsg.cat' for FTP
messages.
EZA1554I Connecting to:   192.168.20.112 port: 21.
220-FTPT1 IBM FTP CS V1R13 at MVSS2T.dmz, 16:26:46 on 2012-09-18.
220 Connection will close if idle for more than 5 minutes.
FC0242 ftpAuth: security values: mech=TLS, tlsmech=ATTLS, sFTP=R,
sCC=P, sDC=P <<<<<<<<<<<<<<<<<<<<<<<<<<<<
FC2656 ftpAuthAttls: AT-TLS policy set as application controlled.
FU1367 TTLSRule: FTPTClient@192.168.20.11n~5
FU1373 TTLSGroupAction: gAct1
FU1379 TTLSEnvironmentAction: eAct4
FU1386 TTLSConnectionAction: cAct3
EZA1701I >>> AUTH TLS     <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
234 Security environment established - ready for negotiation
FC2811 authServerAttls: Start Handshake   <<<<<<<<<<<<<<<<<<<<<<<<<<
FC2820 authServerAttls: ioctl() failed on SIOCTTLSCTL - EDC8121I
Connection reset. (errno2=0x77A9733D)
EZA2897I Authentication negotiation failed  <<<<<<<<<<<<<<<<<<<<<<<<
EZA1534I *** Control connection with 192.168.20.112 dies.   <<<<<<<<
SC3945 SETCEC code = 10
```

```
SC3406 endSession: recv() failed - EDC8121I Connection reset.
(errno2=0x76650446)
EZA1457I You must first issue the 'OPEN' command
PC1017 logClientErrMsg: entered  <<<<<<<<<<<<<
PC0915 setClientRC: entered
PC0985 setClientRC: std_rc=10234, rc_type=STD, rc=10234  <<<<<<<<
EZZ9830I USER201 FTP failed - Cmd = 10(open) Reply = 234 NX STD RC =
10234 <<<<<<<<<<<<<<<<<<<
EZA1460I Command:
```

4. Note how you were using AT-TLS to send an *AUTH TLS* command to establish the security environment, but the FTP Server authentication negotiation failed. (Relevant messages are highlighted above in blue with “<<<<<<<<<<<<<”.)
   a. Then the control connection failed. You will learn why it failed in the next steps.
   b. Note also that we enabled client messages to gather more data:
      ```
      (i)      PC1017 logClientErrMsg: entered
      ```
   c. Note that the Client Return Codes in this case give us little information:
      ```
      (i)      PC0985 setClientRC: std_rc=10234, rc_type=STD,
         rc=10234
         1. 10:  The standard FTP client return code is 10234,
            indicating that a subcommand was sent by the
            client (10 = OPEN command); the last response from
            the server was 234.
         2. 234:  Means that we received FTP Server Reply code
            of 234 which indicates:
            a. 234 Security environment established - ready for negotiation
      NOTE:  Client code 10 is found in the Communications
      Server IP User's Guide and Commands(SC31-8780) and
      Server Reply Code 234 is found in the z/OS
      Communications Server IP and SNA Codes(SC31-8791).
      ```

5. Exit from the FTP session:
   a. **Quit**

6. We have enabled a high level of TLS tracing in our policy files and so you will find the relevant error message in the UNIX SYSLOG Daemon logs at the client and or the server side of the connection. We look at the SYSLOG Daemon log next.

Researching the Problem

1. From the command line of ISPF at MVS***1*** enter:
    a. **tso omvs**
        i. This takes you to the UNIX shell

2. Switch into SUPERUSER in order to be authorized to view the log:
    a. **su**

3. Browse the SYSLOG Daemon log file of MVS***n*** by entering the following command:
    a. **obrowse /var/CSLOG/syslogall.log**
        i. If this does not yield log messages, we might be recording inn a different file today. Try **obrowse /var/syslogall.log**

4. Find the address of your remote FTP server:
    a. TCPIP***T*** Target:
        f 192.168.20.11n (***"n"*** = your MVS suffix)
    b. TCPIP***G*** Target:
        f 192.168.20.12n (***"n"*** = your MVS suffix)

5. The messages surrounding this message look something like this:

```
EZD1284I TTLS Flow  GRPID: 00000001 ENVID: 00000006 CONNID: 000000CA
RC:  401 Call GSK_SECURE_SOCKET_INIT - 7EB3C318

EZD1283I TTLS Event GRPID: 00000001 ENVID: 00000006 CONNID: 000000CA
RC:  401 Initial Handshake 00000000 7EB9C798

EZD1286I TTLS Error GRPID: 00000001 ENVID: 00000006 CONNID: 000000CA
LOCAL: 192.168.20.111..1038 REMOTE: 192.168.20.112..21 JOBNAME:
USER21 USERID: USER21 RULE: FTPTClient@192.168.20.11n~5
RC:  401 Initial Handshake 00000000 7EB9C798
```

You have received an SSL Return Code of 401. The description in the Cryptographic Services System Secure Sockets Layer Programming (SC24-5901-09) is :

> **401 Certificate is expired or is not valid yet.**
> **Explanation:** The current time is either before the Certificate start time or after the Certificate end time.
> **User response:** Obtain a new Certificate if the Certificate is expired or wait until the Certificate becomes valid if it is not valid yet.

6. You might also see an EZD1287I message on the MVS Console of the target FTP Server (i.e., your FTP Server at your MVS**n**):

```
EZD1287I TTLS Error RC:  401 Initial Handshake 036
  LOCAL: 192.168.20.112..21
  REMOTE: 192.168.20.111..1038
  JOBNAME: FTPT1 RULE: FTPT@192.168.20.112 2
  USERID: TCPIP GRPID: 00000002 ENVID: 00000009 CONNID: 000000AD
```

7. During the handshake the FTP Server sent you its Certificate and this Certificate is not valid. At either MVS, display the Certificate on the shared RACF database to determine what the validity dates are. *(The certificate is documented on your diagrams.)*

   a. TCPIP***T*** of your MVSn: From ISPF Option 6 enter:
   RACDCERT ID(TCPIP) LIST(LABEL('FTPServer*n*1 EXP'))
   (***"n"*** = your MVS suffix)

   b. TCPIP***G*** of your MVSn: From ISPF Option 6 enter:
   RACDCERT ID(TCPIP) LIST(LABEL('FTPServer*n*2 EXP'))
   (***"n"*** = your MVS suffix)

8. You will see output with **expired dates** similar to the following:

```
Digital certificate information for user TCPIP:
  Label: FTPServer22 EXP
  Certificate ID: 2QXjw9fJ18bj1+KFmaWFmfLyQMXn10BA
  Status: TRUST
  Start Date: 2007/11/15 00:00:00     <<<<<<<<<<<<<<<<<<<<<<<<
  End Date:   2011/10/07 23:59:59     <<<<<<<<<<<<<<<<<<<<<<<<
  Serial Number:
       >1D<
  Issuer's Name:
       >CN=MVS1CA.LABS.IBM.COM.O=MVS1 CA.C=US<
  Subject's Name:
       >CN=FTPServer22 EXP.OU=WSC.C=US<
  Subject's AltNames:
    IP: 192.168.20.101
    EMail: FTPG at ZOS1
    Domain: WSC.IBM.COM
  Key Type: RSA
  Key Size: 1024
  Private Key:  YES
  Ring Associations:
    Ring Owner: FTPD
    Ring:
       >FTPEXP22_RING<
```

9. You must update the expiration date and refresh the policy to cause the change in the Key Ring to be re-read. YOU MUST RETAIN THE ORIGINAL START DATE. Write that date here: ____

Correcting the Problem in Scenario 2

1. Open your original TN3270 emulator (PCOMM) session that is connected to YOUR MVS**n** system at:
    a. 192.168.20.8***n*** (***"n"*** = your MVS suffix)

2. Login to the emulator session with your User ID if you are not still logged in:
    a. TCPIP***T*** is USER***n1***
    b. TCPIP***G*** is USER***n2***

3. Use ISPF Option 3.4 to work with the contents of USER.CS.SOURCE.
    a. **=3.4**
    b. Insert name of USER.CS.SOURCE for the dataset
        i. **USER.CS.SOURCE**
    c. Place an **"m"** next to the dataset.
    d. Place an **"e"** for **"edit"** next to the member named
        i. SKRENU***nx***
            1. ***"nx"*** is the suffix of your Team ID: 21, 22, or 31, 32, etc.
    e. To renew the expiration dates of a Certificate, look for the following steps in the JCL:
        i. Generate a Certificate Request for the Certificate with the invalid dates ***("RACDCERT GENREQ" command)***
        ii. Generate a new Certificate, keeping the original old date, but extending the new date by one year from today. ***("RACDCERT GENCERT" command)***
            1. Your Task: Exchange the date marked with Question Marks for a date one year from today.
        iii. Verify that the Certificate is TRUSTed – since the old date will cause it to default to UNTRUSTED. ***("RACDCERT ALTER" command)***

4. Finally submit the job. (Because of the SETROPTS command you may see a Return Code of 08.)
    a. **sub**
    b. Then use **PF3 to save and exit** the member under your name.

5. Review the output.
    a. **=D.O from the ISPF command line**
        i. Select your job log for review.
        ii. *IMPORTANT:* Verify that all commands except for the SETROPTS have been accepted. If the job fails to run cleanly, you may not proceed since it will cause errors for future steps. Ask the instructor for help if this happens.
    b. **Your output will look similar to the following: marked as TRUSTed and with an end date that is in the future.**

```
Digital certificate information for user TCPIP:

  Label: FTPServer31 EXP
  Certificate ID: 2QXjw9fJ18bj1+KFmaWFmfPxQMXn10BA
  Status: TRUST
  Start Date: 2011/01/07 00:00:00
  End Date:   2014/07/28 23:59:59    <<<<<<<<<<<<<<<<<<<<<<<<
  Serial Number:
     >70<
  Issuer's Name:
     >CN=MVS1CA.LABS.IBM.COM.O=MVS1 CA.C=US<
  Subject's Name:
     >CN=FTPServer31 EXP.OU=WSC.C=US<
  Subject's AltNames:
    IP: 192.168.20.93
    EMail: FTPT at ZOS3
    Domain: WSC.IBM.COM
  Key Type: RSA
  Key Size: 1024
  Private Key: YES
  Ring Associations:
    Ring Owner: FTPD
    Ring:
     >FTPEXP31_RING<
```

6. **Notice the following in the output:**
   a. The label of the Certificate remains the same.
   b. The Issuer Name in the Certificate remains the same.
   c. The Subject Name in the Certificate remains the same.
   d. The expiration date in the Certificate has changed.
   e. Note how the FTP Server Key Ring looks the same as before. ***The association of your renewed FTP Server Certificate with the existing Key Rings has been retained!***

7. You are not authorized to execute the SETROPTS command directly. Instead, run the following procedure at SDSF. It will execute the SETROPTS commands for you on your behalf:
   a. **/S SPECUSER**

8. Correct any errors in the ***SKRENUnx*** job and resubmit if necessary

9. Return to the Console Log of YOUR MVS***n***:
   a. **=D.LOG**

IMPORTANT: In the next step you will restart your FTP server. When you are using AT-TLS, it is not necessary to recycle the FTP server disruptively in order to refresh in memory the changed Key Rings and Certificates. However, for this lab, it is quicker to recycle the FTP server like this in order to accomplish the refresh.

10. Stop your FTP Server and restart it so that it rereads the refreshed Key Ring:
    a. For TCPIP***T***:
        i. **/P FTP*T1*** (wait till the FTP server stops)
        ii. **/S FTP*T*,FDAT=FTPSAUTH**
    b. For TCPIP***G***:
        i. **/P FTPG1** (wait till the FTP server stops)
        ii. **/S FTPG,FDAT=FTPSAUTH**

11. Now return to your TN3270 session at MVS***1*** where you will test your changes.

Testing the Correction in Scenario 2

1. You should be signed on at MVS1.
    a. TCPIP***T***: USER***n***1 (***“n”*** = your MVS suffix)
    b. TCPIP***G***: USER***n***2 (***“n”*** = your MVS suffix)

2. Move to ISPF Option 6 where you enter the following FTP command:

    a. For TCPIP***T*** Client (USER***n***1):
    ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*T* -s 192.168.20.111 192.168.20.11*n*
    (***“n”*** = your MVS suffix)
    b. For TCPIP***G*** Client (USER***n***2):
    ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*G* -s 192.168.20.121 192.168.20.12*n*
    (***“n”*** = your MVS suffix)

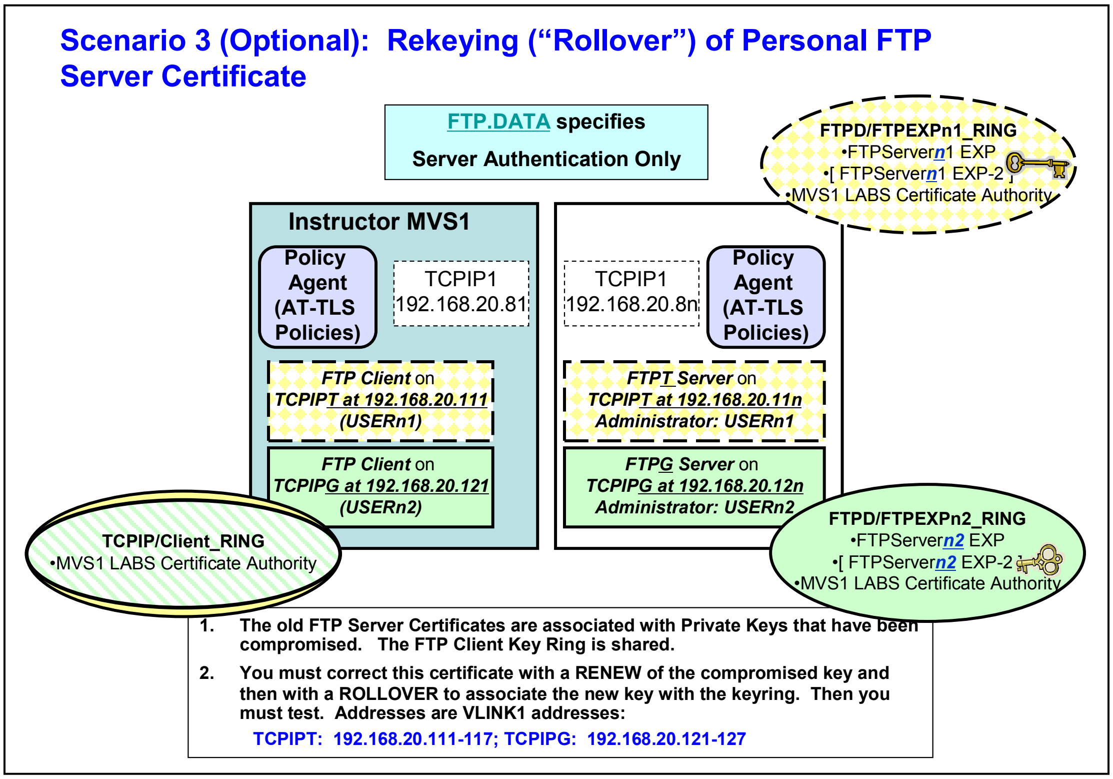
3. The FTP connection ***should not fail***. If it does, examine the manner in which you executed the command and try again. You may need to ask the instructor for help or look at the SYSLOGD log in OMVS to determine why the failure took place.
    a. For testing purposes we have set a very high level of tracing for AT-TLS so that you may see all messages. Once testing is complete, the tracing levels should be reduced in a production environment.

What you have learned in Scenario 2 of this lab:

You have learned how to extend the lifetime (expiration date) of the certificate and its private key without changing the private key.

4. **If you have time – i.e., if this is a 2-hour lab – you may test Optional Scenario 3 of the lab. In scenario 3 you renew (i.e., regenerate) the private/public key pair. This is called "rolling over" or "renewing" a certificate.**

Scenario 3 (Optional): Rekeying ("Rollover") of Personal FTP Certificate



Scenario 3 (Optional): Rekeying ("Rollover") of Personal FTP Server Certificate

FTP.DATA specifies

Server Authentication Only

FTPD/FTPEXPn1_RING
•FTPServer*n*1 EXP
•[FTPServer*n*1 EXP-2]
•MVS1 LABS Certificate Authority

Instructor MVS1

Policy Agent (AT-TLS Policies)

TCPIP1
192.168.20.81

FTP Client on
TCPIPT at 192.168.20.111
(USERn1)

FTP Client on
TCPIPG at 192.168.20.121
(USERn2)

TCPIP1
192.168.20.8n

Policy Agent (AT-TLS Policies)

FTPT Server on
TCPIPT at 192.168.20.11n
Administrator: USERn1

FTPG Server on
TCPIPG at 192.168.20.12n
Administrator: USERn2

TCPIP/Client_RING
•MVS1 LABS Certificate Authority

FTPD/FTPEXPn2_RING
•FTPServer*n2* EXP
•[FTPServer*n2* EXP-2]
•MVS1 LABS Certificate Authority

1. The old FTP Server Certificates are associated with Private Keys that have been compromised. The FTP Client Key Ring is shared.
2. You must correct this certificate with a RENEW of the compromised key and then with a ROLLOVER to associate the new key with the keyring. Then you must test. Addresses are VLINK1 addresses:

TCPIPT: 192.168.20.111-117; TCPIPG: 192.168.20.121-127

Explanation of Scenario: The Security Auditor at your site indicates that the key pairs for the FTP Server Certificate are more than one year old. Your company's new security policy demands that keys be regenerated at least once a year, and so now you must rekey the FTP Server Certificate that you just finished renewing.

Editing and Execution of the Job to Re-key the FTP Certificate

1. You should be signed on at YOUR MVS***n*** with your User ID:
   a. TCPIP***T***: USER***n***1 (***"n"*** = your MVS suffix)
   b. TCPIP***G***: USER***n***2 (***"n"*** = your MVS suffix)

2. Use ISPF Option 3.4 to work with the contents of USER.CS.SOURCE.
   a. **=3.4**
   b. Insert name of USER.CS.SOURCE for the dataset
      i. **USER.CS.SOURCE**
   c. Place an **"m"** next to the dataset.
   d. Place an **"e"** for **"edit"** next to the member named
      i. SKROLL***nx*** (***"nx"*** = your User ID suffix)

3. There is nothing to edit here, but take note of the following RACF commands in this dataset member:
    1. You are removing the private key associated with the old FTP Server Certificate and you are generating a new public/private key pair to the copy of the Certificate that now bears a new label name. *("RACDCERT REKEY" command)*
    2. You are generating a Certificate Request for the rekeyed Certificate and placing the request in a dataset (DSN). *("RACDCERT GENREQ" command)*
    3. You are generating the new Certificate with the output dataset now as input, and the original Certificate Authority is signing the rekeyed FTP Server Certificate. *("RACDCERT GENCERT" command)*
    4. You are rolling the newly signed and rekeyed Certificate into all Key Rings that previously held the old version of the Certificate. *("RACDCERT ROLLOVER" command)*

4. Submit the job. (Because of lack of authorization for issuing the SETROPTS command you may see a Return Code of 08.)
    a. **sub**
    b. Then use **PF3 to save and exit** the member under your name.

5. Review the output of the job
    a. **=D.O**
        i. Select your job for review.
        ii. ***IMPORTANT:*** **Verify that all commands except for the SETROPTS have been accepted. If the job fails to run cleanly, you may not proceed since it will cause errors for future steps.**

6. Notice the contents of the FTP Server Key Ring (FTPEXP21_RING) that are printed in the job log. Does it now contain the OLD or the NEW FTP Server Certificate?
    a. **Answer:** Old or New?
        i. (The old FTP certificate name was "FTPServer*nx* EXP".)

```
Digital ring information for user FTPD:

  Ring:
       >FTPEXP21_RING<
  Certificate Label Name                Cert Owner     USAGE      DEFAULT
  --------------------------------      ------------   --------   -------
  MVS1 LABS Certificate Authority       CERTAUTH       CERTAUTH     NO

  FTPServer21 EXP-2                     ID(TCPIP)      PERSONAL     YES
```

7. Notice the two output displays of FTP Server Certificates:
   a. The original label (‘FTPServer*nx*_EXP ‘) no longer has a private key and no longer belongs to any Key Ring, as this example shows you:

```
Digital certificate information for user TCPIP:

   Label: FTPServer21 EXP
   Certificate ID: 2QXjw9fJ18bj1+KFmaWFmfLxQMXn10BA
   Status: TRUST
   Start Date: 2011/01/07 00:00:00
   End Date:   2013/09/18 23:59:59
   Serial Number:
        >30<
   Issuer's Name:
        >CN=MVS1CA.LABS.IBM.COM.O=MVS1 CA.C=US<
   Subject's Name:
        >CN=FTPServer21 EXP.OU=WSC.C=US<
 ***
Subject's AltNames:
  IP: 192.168.20.101
  EMail: FTPT at ZOS1
  Domain: WSC.IBM.COM
  Key Type: RSA
  Key Size: 1024
Private Key: NO       <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Ring Associations:
*** No rings associated *** <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

NOTE: **Since this is a PERSONAL Certificate, the old Certificate is replaced on the Key Ring with the new one.**

   b. The command with the rekeyed label name displays the Certificate, as you see in this example:

```
   Digital certificate information for user TCPIP:

   Label: FTPServer21 EXP-2    <<<<<<<<<<<<<<<<<<<<<<<<<<<
   Certificate ID: 2QXjw9fJ18bj1+KFmaWFmfLxQMXn12Dy
   Status: TRUST
   Start Date: 2012/09/19 00:00:00
   End Date:   2013/09/19 23:59:59
   Serial Number:
        >31<
   Issuer's Name:
        >CN=MVS1CA.LABS.IBM.COM.O=MVS1 CA.C=US<
   Subject's Name:
        >CN=FTPServer21 EXP.OU=WSC.C=US<    <<<<<<<<<<<<<<<<<<<
   Subject's AltNames:
     IP: 192.168.20.101
     EMail: FTPT at ZOS1
     Domain: WSC.IBM.COM
   Key Type: RSA
   Key Size: 1024
   Private Key: YES   <<<<<<<<<<<<<<
```

```
Ring Associations:            <<<<<<<<<<<<<<<<<<<<<<<<<<<<<
  Ring Owner: FTPD
  Ring:
     >FTPEXP21_RING<
```

8. Observe in the output display that you now have a Private Key and the renewed and rolled over certificate is now associated with the original key ring.

```
Key Type: RSA
   Key Size: 1024
   Private Key: YES  <<<<<<<<<<<<<<
   Ring Associations: <<<<<<<<<<<<<<<<<<<<<<<<<<<<<
     Ring Owner: FTPD
     Ring:
     >FTPEXP21_RING<
```

9. Return to the Console Log of YOUR MVS***n***:
   a. **=D.LOG**

10. You are not authorized to execute the SETROPTS command directly. Instead, run the following procedure which will execute the commands for you on your behalf:
    a. **/S SPECUSER**

IMPORTANT: In the next step you will restart your FTP server. When you are using AT-TLS, it is not necessary to recycle the FTP server in order to refresh in memory the changed Key Rings and Certificates. However, for this lab, it is quicker to recycle the FTP server like this in order to accomplish the refresh.

11. Stop your FTP Server and restart it so that it rereads the refreshed Key Ring:
    a. For TCPIP***T***:
       i. **/P FTP*T1***
       ii. **/S FTP*T*,FDAT=FTPSAUTH**
    b. For TCPIP***G***:
       i. **/P FTP*G1***
       ii. **/S FTP*G*,FDAT=FTPSAUTH**

12. Now return to your TN3270 session with MVS1 where you will test your changes.

Testing the Correction in Scenario 3

1. You should be signed on at MVS***1*** with your User ID:
   a. TCPIP***T***: USER***n***1 (**"*n*"** = your MVS suffix)
   b. TCPIP***G***: USER***n***2 (**"*n*"** = your MVS suffix)

2. Our systems are not a full SYSPLEX. Therefore you must refresh the RACLIST class at MVS1 to pick up the changes in the shared RACF Database. At the SDSF Console command line enter the following:
   a. **/S SPECUSER**

3. Move to ISPF Option 6 where you enter the following FTP command:
   a. For TCPIP***T*** Client (USER***n***1):

      ```
      ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p
      TCPIPT -s 192.168.20.111    192.168.20.11n
      ```

      (**"*n*"** = your MVS suffix)

   b. For TCPIP***G*** Client (USER***n***2):

      ```
      ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p
      TCPIPG -s 192.168.20.121    192.168.20.12n
      ```

      (**"*n*"** = your MVS suffix)

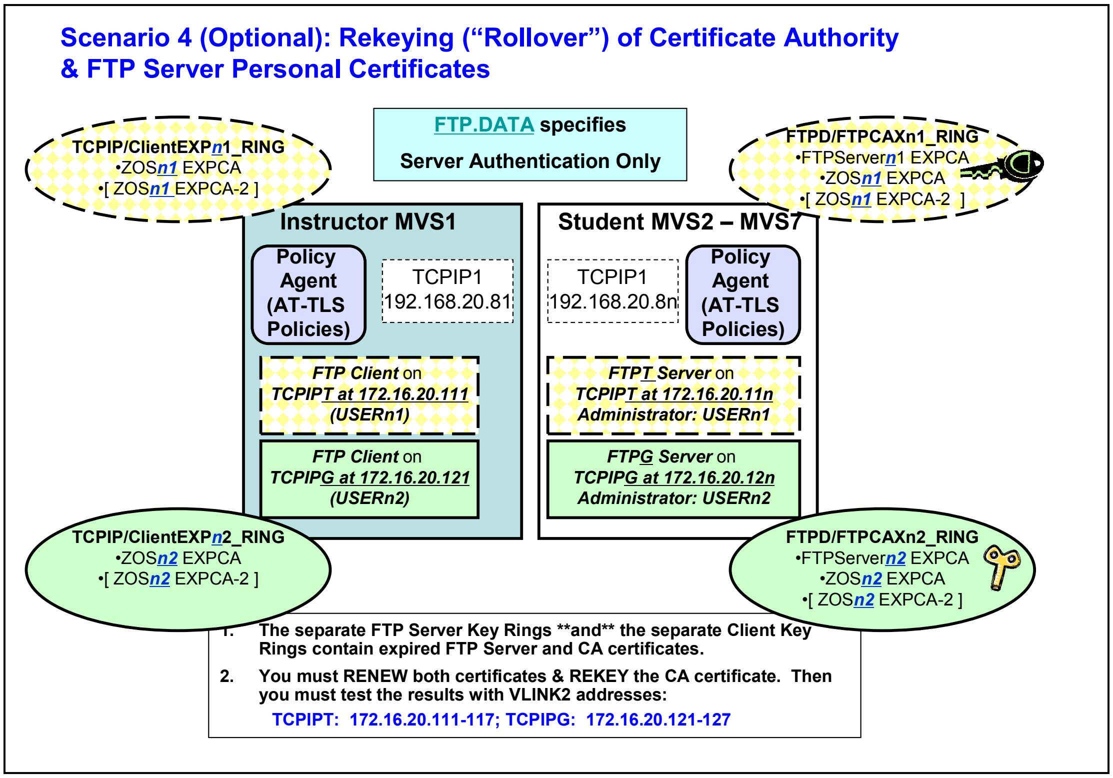
4. The FTP connection with the new re-keyed Certificate should not fail.
   a. If it does, examine the manner in which you executed the command and try again.
      i. You may need to ask the instructor for help or look at the SYSLOGD log in OMVS to determine why the failure took place.
   b. For testing purposes we have set a very high level of tracing for AT-TLS so that you may see all messages. ***Once testing is complete, the tracing levels should be reduced in a production environment.***

What you have learned in Scenario 3 of this lab:

You have learned how to change the public and private key pair associated with a PERSONAL certificate through the rekey and rollover process. You have also seen how the rollover process replaced the contents of the Key Rings associated with the certificate that you have rekeyed.
You have also seen how the old PERSONAL certificate is no longer associated with a private key or with a Key Ring.

If this is a very long lab period, you may be able to test Optional Scenario 4 of the lab. Scenario 4 is a complicated lab involving an expired CA certificate and one that needs rekeying as well.

Scenario 4 (Optional): Rekeying ("Rollover") of Certificate Authority & FTP Server Personal Certificates



Scenario 4 (Optional): Rekeying ("Rollover") of Certificate Authority & FTP Server Personal Certificates

1. The separate FTP Server Key Rings **and** the separate Client Key Rings contain expired FTP Server and CA certificates.
2. You must RENEW both certificates & REKEY the CA certificate. Then you must test the results with VLINK2 addresses:
   TCPIPT: 172.16.20.111-117; TCPIPG: 172.16.20.121-127

Explanation of Scenario: You will be working with a different AT-TLS policy and a different set of Key Rings and Certificates from those with which you have tested before. You are testing Static VIPA (VLINK2) connections over the Predefined HiperSockets network 172.16.20.0/24. ***Remember: These are all new to you: Client Key Rings, FTP Server Key Rings, FTP Server Certificates, and Certificate Authority Certificates.*** *Both Key Rings contain expired Certificates that need to be renewed. But, in addition, the Certificate Authority Certificate must be rekeyed. For the first time in this lab you see that the contents of the Client Key Rings must also be changed. These are local clients working with the same shared RACF Database, and so the jobs that you run will place the new Certificates into the correct repository without further work.*

NOTE: If there were also remote clients, you would need to EXPORT the renewed and rekeyed CA Certificate without its private key to those remote clients for IMPORT into their Certificate repositories. This lab does not use remote clients and so this EXPORT/IMPORT step is unnecessary.

Testing the Connections in Scenario 4 with Expired Certificates

1. You should be signed on at MVS1 with your User ID:
   a. TCPIP***T***: USER***n***1 (***"n"*** = your MVS suffix)
   b. TCPIP***G***: USER***n***2 (***"n"*** = your MVS suffix)

2. Move to ISPF Option 6 where you enter the following FTP command:
   a. For TCPIP***T*** Client (USER***n***1):
      ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*T* -s 172.16.20.111 172.16.20.11*n*
      (***"n"*** = your MVS suffix)
   b. For TCPIP***G*** Client (USER***n***2):
      ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*G* -s 172.16.20.121 172.16.20.12*n*
      (***"n"*** = your MVS suffix)

3. **Observe in the Client FTP messages** that the Security Environment is established and ready for negotiation. However, the Authentication of the Server fails. Example is:

```
EZA1701I >>> AUTH TLS
234 Security environment established - ready for negotiation
FC2811 authServerAttls: Start Handshake
FC2820 authServerAttls: ioctl() failed on SIOCTTLSCTL - EDC8121I
Connection reset. (errno2=0x77A9733D)
EZA2897I Authentication negotiation failed  <<<<<<<<<<<<<<<<<<<<
```

4. Quit out of the FTP session:
   a. **quit**

5. Move to the MVS**1** log to find your FTP Server destination address:
   a. **=D.LOG**
   b. If you are USER***n01***:
      i. **f 172.16.20.11n**
   c. If you are USER***n02***:
      i. **f 172.16.20.12n**

6. You should find a failing message EZD1287I with an appropriate timestamp and an SSL Return Code of 401. Example is:

```
EZD1287I TTLS Error RC:  401 Initial Handshake 410
   LOCAL: 172.16.20.121..1035
   REMOTE: 172.16.20.122..21
   JOBNAME: USER21 RULE: FTPGCLI@Team22_MVS1-MVS2  7
   USERID: USER21 GRPID: 00000003 ENVID: 00000004 CONNID: 000008DA
```

7. Note the failing security rule at the source (client) system (MVS1):
   a. Example: `JOBNAME:`***`USER21 RULE:FTPGCLI@Team22_MVS1-MVS2`***

8. Your next step is to find out (or remember) what an SSL Error of 401 means. The description in the Cryptographic Services System Secure Sockets Layer Programming (SC24-5901-09) is :

   401 Certificate is expired or is not valid yet.
   Explanation: The current time is either before the certificate start time or after the certificate end time.
   User response: Obtain a new certificate if the certificate is expired or wait until the certificate becomes valid if it is not valid yet.

9. Move back to your original TN3270 emulator session at your MVS**n** where you are logged in as
   a. **TCPIP*T* stack:** USER***n1***
   b. **TCPIP*G* stack:** USER***n2***

10. You will observe ALMOST the same MVS log message (EZD1287I) at your MVS target system. An example is:

```
EZD1287I TTLS Error RC:  401 Initial Handshake
  LOCAL: 172.16.20.112..21
  REMOTE: 172.16.20.111..1050
  JOBNAME: FTPT1 RULE: FTPT@172.16.20.112
  USERID: TCPIP GRPID: 00000004 ENVID: 00000015 CONNID: 000008DC
```

11. One of the major differences between the two sets of messages is the AT-TLS rule that was used:
    a. On the target system (MVS***n***) the rule is for the FTP Server (FTPT or FTPG):
       i. Example: `JOBNAME:FTPT1 RULE:FTPT@172.16.20.112`
    b. On the source system (MVS1) the rule that failed is the FTP Client Rule:
       i. Example: `JOBNAME:USER201 RULE:FTPGCLI@Team22 MVS1-MVS2`

    c. **MEANING:** Either one or both Key Rings have expired Certificates (RC 401) or an expired FTP Server Certificate is stored at the FTP Server Key Ring and being received by the Client Key Ring which rejects it.

12. Determine which Certificate or Certificates are invalid.

13. You should be signed on at your MVS***n*** with your User ID:
    a. TCPIP***T***: USER***n***1 (***"n"*** = your MVS suffix)
    b. TCPIP***G***: USER***n***2 (***"n"*** = your MVS suffix)

14. Move to ISPF Option 6 to view the contents and dates associated with the Key Rings and Certificates depicted in your lab visual for Scenario 4.
    a. **=6**

15. Enter the following commands for the Key Rings and Certificates that are documented in the diagrams for this lab. Then review the output for expiration dates. ***PAY ATTENTION TO THE COMMANDS FOR YOUR CLIENT's User ID.***

a. **For TCPIP*T* Client** (USER***n1***):

i. **RACDCERT ID(TCPIP) LISTRING(ClientEXP*n*1_RING)**

EXAMPLE:

```
Digital ring information for user TCPIP:

 Ring:
     >ClientEXP21_RING<
 Certificate Label Name          Cert Owner     USAGE      DEFAULT
 ------------------------------  ------------   --------   -------
 ZOS21 EXPCA                    CERTAUTH      CERTAUTH     NO
```

ii. **RACDCERT CERTAUTH LIST(LABEL('ZOS*n*1 EXPCA'))**

1. **Original Start Date is: ______________________**
2. **Expiration Date is: __________________________**
3. You will later renew the CA Certificate to change the expiration date.
4. **How many Key Rings does this CA Certificate reside on? _________________**
5. You will also ROLLOVER the CA certificate so that it is refreshed in both Key Rings.

iii. **RACDCERT ID(FTPD) LISTRING(FTPCAX*n*1_RING)**

EXAMPLE:

```
Digital ring information for user FTPD:

 Ring:
     >FTPCAX21_RING<
 Certificate Label Name          Cert Owner     USAGE      DEFAULT
 ------------------------------  ------------   --------   -------
 FTPServer21 EXPCA                 ID(TCPIP)    PERSONAL    YES
 ZOS21 EXPCA                    CERTAUTH      CERTAUTH     NO
```

iv. **RACDCERT ID(TCPIP) LIST(LABEL('FTPServer*n*1 EXPCA'))**

1. **Original Start Date is:______________________**
2. **Expiration Date is: __________________________**
3. **On how many Key Rings does this FTP Server Personal Certificate reside? _________________**

b. **For TCPIP*G* Client** (USER***n2***):

   i. **RACDCERT ID(TCPIP) LISTRING(ClientEXP*n*2_RING)**

      EXAMPLE:

```
Digital ring information for user TCPIP:

 Ring:
    >ClientEXP22_RING<
 Certificate Label Name          Cert Owner    USAGE     DEFAULT
 --------------------------      ------------  --------  -------
 ZOS22 EXPCA                    CERTAUTH      CERTAUTH   NO
```

   ii. **RACDCERT CERTAUTH LIST(LABEL('ZOS*n*2 EXPCA'))**

      1. **Original Start Date is: ______________________**
      2. **Expiration Date is: __________________________**
      3. You will later renew the CA Certificate to change the expiration date.
      4. **On how many Key Rings does this CA Certificate reside? _________________**
      5. You will also ROLLOVER the CA certificate so that it is refreshed in both Key Rings.
      6. Does your documentation show whether this CA Certificate resides on other platforms or distributed systems?
         a. *No, and therefore any changes to this CA certificate need not require an export to those other platforms.*

   iii. **RACDCERT ID(FTPD) LISTRING(FTPCAX*n*2_RING)**

      EXAMPLE:

```
Digital ring information for user FTPD:

 Ring:
    >FTPCAX22_RING<
 Certificate Label Name          Cert Owner    USAGE     DEFAULT
 --------------------------      ------------  --------  -------
 FTPServer22 EXPCA                ID(TCPIP)    PERSONAL   YES
 ZOS22 EXPCA                    CERTAUTH      CERTAUTH   NO
```

   iv. **RACDCERT ID(TCPIP) LIST(LABEL('FTPServer*n*2 EXPCA'))**

      1. **Original Start Date is: ______________________**
      2. **Expiration Date is: __________________________**
      3. **On how many Key Rings does this FTP Server Personal Certificate reside? _________________**

2. You already know that you must rekey and rollover this CA Certificate. Now you see you must extend the expiration date as well.

> You must change the expiration date and refresh the policy to cause the change in the Key Ring to be re-read. YOU WILL RETAIN THE ORIGINAL START DATE so that any Certificates that you sign with the new CA Certificate will fall within the lifetime of the CA Certificate.

Editing and Execution of the Job to Renew and Rollover a CA Certificate

1. You should be signed on at YOUR MVS***n*** with your User ID:
   a. TCPIP***T***: USER***n***1 (***"n"*** = your MVS suffix)
   b. TCPIP***G***: USER***n***2 (***"n"*** = your MVS suffix)

2. Use ISPF Option 3.4 to browse the contents of USER.CS.SOURCE.
   a. **=3.4**
   b. Insert name of USER.CS.SOURCE for the dataset
      i. **USER.CS.SOURCE**
   c. Place an **"m"** next to the dataset.
   d. Place an **"e"** for **"edit"** next to the member named
      i. **SKROL4*nx*** (***"nx"*** = your User ID suffix)
      ii. **IMPORTANT: Be sure to select the member that begins with SKROL*4* ! (Other members look similar.)**

3. There is nothing to edit here, but take note of the following RACF commands in this dataset member:
   a. You are removing the private key associated with the old CA and you are generating a new public/private key pair for the copy of the Certificate that now bears a new label name.
   b. At the same time we are extending the expiration date while retaining the start date. ***("RACDCERT REKEY" command)***
   c. You are rolling over the renewed and rekeyed Certificate into all Key Rings that previously held the old version of the Certificate. ***("RACDCERT ROLLOVER" command)***
   d. **Verify whether there is anything to change in this member. (There should not be.)**

4. Submit the job. (Because of the SETROPTS command you may see a Return Code of 08.)
   a. **sub**
   b. Then use **PF3 to save and exit** the member under your name.

5. **Review the output of the job**
   a. **=D.O**

6. Select your job for review.
    a. ***IMPORTANT:*** **Verify that all commands except for the SETROPTS have been accepted. If the job fails to run cleanly, you may not proceed since it will cause errors for future steps.**

7. Notice the contents of the Client and FTP Server Key Rings as you peruse the job log. Do they now contain the OLD or the NEW CA Certificate or BOTH?
    a. **Answer:** Old or New or Both?
    b. NOTE:
        i. **Since this is a Certificate Authority Certificate, the new Certificate is added to the Key Rings together with the old CA Certificate. The answer is "Both."**
        ii. The old Certificate can still be used for authentication **IF** the client accepts expired Certificates. But only the new CA can be used for signing Certificates.

Example of Output:

```
Digital ring information for user FTPD:

  Ring:
       >FTPCAX21_RING<
  Certificate Label Name                Cert Owner     USAGE    DEFAULT
  --------------------------------      ------------   -------- -------
  FTPServer21 EXPCA                     ID(TCPIP)      PERSONAL   YES

  ZOS21 EXPCA                           CERTAUTH       CERTAUTH   NO

  ZOS21 EXPCA-2                         CERTAUTH       CERTAUTH   NO

Digital ring information for user TCPIP:

  Ring:
       >ClientEXP21_RING<
  Certificate Label Name                Cert Owner     USAGE    DEFAULT
  --------------------------------      ------------   -------- -------
  ZOS21 EXPCA                           CERTAUTH       CERTAUTH   NO

  ZOS21 EXPCA-2                         CERTAUTH       CERTAUTH   NO
```

8. Compare the output field named ***"Private Key"*** in the following two CA Certificate displays.

```
Digital certificate information for CERTAUTH:
  Label: ZOS21 EXPCA      <<<<<<<<<<<<OLD CA CERT  <<<<<<<<<<<<<<<<
  Certificate ID: 2QiJmZmDhZmjgenW4vLxQMXn18PB
  Status: TRUST
  Start Date: 2008/10/07 00:00:00
  End Date:   2011/10/07 23:59:59
  Serial Number:
       >00<
  Issuer's Name:
       >CN=ZOS21 EXPCA.OU=WSC.C=US<
  Subject's Name:
       >CN=ZOS21 EXPCA.OU=WSC.C=US<
  Subject's AltNames:
    IP: 172.16.20.121
    EMail: TCPIPTCA at ZOS2
    Domain: WSC.IBM.COM
  Key Usage: CERTSIGN
  Key Type:  RSA
  Key Size:  1024
  Private Key: NO      <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
  Ring Associations:
    Ring Owner: FTPD
    Ring:
       >FTPCAX21_RING<
    Ring Owner: TCPIP
    Ring Owner: TCPIP
    Ring:
       >ClientEXP21_RING<


Digital certificate information for CERTAUTH:

  Label: ZOS21 EXPCA-2    <<<<<<<<< NEW CA CERT <<<<<<<<<<<<<<<<<<<<
  Certificate ID: 2QiJmZmDhZmjgenW4vLxQMXn18PBYPJA
  Status: TRUST
  Start Date: 2012/09/11 00:00:00
  End Date:   2020/12/31 23:59:59
  Serial Number:
       >02<
  Issuer's Name:
       >CN=ZOS21 EXPCA.OU=WSC.C=US<
  Subject's Name:
       >CN=ZOS21 EXPCA.OU=WSC.C=US<
  Subject's AltNames:
    IP: 172.16.20.121
    EMail: TCPIPTCA at ZOS2
    Domain: WSC.IBM.COM
    Domain: WSC.IBM.COM
  Key Usage: CERTSIGN
  Key Type:  RSA
  Key Size:  1024
  Key Type: RSA  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
  Key Size: 1024
  Private Key:  YES   <<<<<<<<<<<<<<<<<<<<<<<<<<<<
  Ring Associations:
    Ring Owner: FTPD
    Ring:
       >FTPCAX21_RING<
    Ring Owner: TCPIP
    Ring:
       >ClientEXP21_RING<
```

OBSERVATION: Only the new CA Certificate can be used to sign Certificates. (See above -- `Private Key: YES`.) The old CA Certificate is still available for authentication of other personal Server or Client Certificates it may have signed in the past.

9. You are not authorized to execute the SETROPTS command directly. Instead, run the following procedure **at both MVS1 and YOUR MVS**n. It will execute the commands for you on your behalf in each MVS Image:
   a. **At MVS1: /S SPECUSER**
   b. **At MVSn: /S SPECUSER**

IMPORTANT: In the next step you will restart your FTP server. When you are using AT-TLS, it is not necessary to recycle the FTP server in order to refresh in memory the changed Key Rings and Certificates. However, for this lab, it is quicker to recycle the FTP server in order to accomplish the refresh.

10. Stop your FTP Server and restart it at your MVS***n*** so that it rereads the refreshed Key Rings:
    a. For TCPIP***T***:
       i. **/P FTP*T1***
       ii. **/S FTP*T*,FDAT=FTPSAUTH**
    b. For TCPIP***G***:
       i. **/P FTP*G1***
       ii. **/S FTP*G*,FDAT=FTPSAUTH**

11. Now return to your TN3270 session with MVS1 where you will test your changes.

Testing the Connections in Scenario 4 with Rolled Over CA Certificate

> At this point you have corrected only the CA Certificate but not the FTP Certificate, which has also expired.

1. You should be signed on at MVS1 with your User ID:
   a. TCPIP***T***: USER***n***1 (***"n"*** = your MVS suffix)
   b. TCPIP***G***: USER***n***2 (***"n"*** = your MVS suffix)

2. Move to ISPF Option 6 where you enter the following FTP command:
   a. For TCPIP***T*** Client (USER***n***1):
      ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*T* -s 172.16.20.111 172.16.20.11*n*
      (***"n"*** = your MVS suffix)
   b. For TCPIP***G*** Client (USER***n***02):
      ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*G* -s 172.16.20.121 172.16.20.12*n*
      (***"n"*** = your MVS suffix)

3. Notice that you are still getting the same errors as before – at least one of the necessary Certificates is still invalid. You already saw in the job log from the previous job that you ran that the CA certificate seems to have been corrected. So now you suspect that there is something wrong with the FTP Server Certificate itself.

> Recall that the FTP Server Certificate has also expired. You have not yet corrected this problem.

4. You must now extend the expiration date of the FTP Server Certificate. In so doing, you will need to sign the Certificate with the new CA, since the old CA no longer has a private key with which to sign the Certificates it issues.

5. Quit out of the FTP session:
   a. **quit**

Editing and Execution of the Job to Renew the FTP Server Personal Certificate

1. You should be signed on at YOUR MVS***n*** with your User ID:
   a. TCPIP***T***: USER***n***1 (***“n”*** = your MVS suffix)
   b. TCPIP***G***: USER***n***2 (***“n”*** = your MVS suffix)

2. Display the FTP Server Certificate again to determine what the validity dates are:
   a. TCPIP***T***: From ISPF Option 6 enter:
   RACDCERT ID(TCPIP) LIST(LABEL(‘FTPServer*n*1 EXPCA’))
   (***“n”*** = your MVS suffix)
   b. TCPIP***G***: From ISPF Option 6 enter:
   RACDCERT ID(TCPIP) LIST(LABEL(‘FTPServer*n*2 EXPCA’))
   (***“n”*** = your MVS suffix)

3. You will see output with expired dates similar to the following example:

```
Digital certificate information for user TCPIP:

   Label: FTPServer21 EXPCA
   Certificate ID: 2QXjw9fJ18bj1+KFmaWFmfLxQMXn18PB
   Status: TRUST
   Start Date: 2008/10/07 00:00:00
   End Date:   2011/10/07 23:59:59   <<<<<<<<< EXPIRED <<<<<<<<<<<<<
   Serial Number:
        >01<
   Issuer's Name:
        >CN=ZOS21 EXPCA.OU=WSC.C=US<
   Subject's Name:
        >CN=FTPServer21 EXPCA.OU=WSC.C=US<
   Subject's AltNames:
     IP: 172.16.20.92
     EMail: FTPT at ZOS2
     Domain: WSC.IBM.COM
   Key Type: RSA
   Key Size: 1024
   Private Key: YES
   Ring Associations:
     Ring Owner: FTPD
     Ring:
        >FTPCAX21_RING<
```

You must change the expiration date and refresh the policy to cause the change in the Key Ring to be re-read. YOU NEED NOT RETAIN THE ORIGINAL START DATE, but you should ensure that the lifetime of this certificate stays within the lifespan of the CA Certificate that signs it.

4. This FTP Certificate has also already expired. It needs to be renewed and signed by the rekeyed Certificate Authority.

5. Use ISPF Option 3.4 to browse the contents of USER.CS.SOURCE.
   a. **=3.4**
   b. Insert name of USER.CS.SOURCE for the dataset
      i. **USER.CS.SOURCE**
   c. Place an **"m"** next to the dataset.
   d. Place an **"e"** for **"edit"** next to the member named
      i. SKFTP4***nx*** (***"nx"*** = your User ID suffix)

6. Edit the member named USER.CS.SOURCE(SKFTP4***nx***)
   a. ***"nx"*** is the suffix of your Team ID: 21, 22, or 31, 32, etc.

7. *YOU NEED NOT CHANGE FIELDS IN THIS MEMBER*. The expiration timeframe will default to one year starting from today. To renew the expiration dates of a Certificate, we are performing the following steps:
   a. Generating a Certificate Request for the Certificate with the invalid dates ***("RACDCERT GENREQ" command)***
   b. Generating a new Certificate, changing the original old date to today's date, but extending the expiration date by the default of one year from today. ***("RACDCERT GENCERT" command)***
   c. Having the Certificate signed by the CA that you just rolled over in the previous exercise.

8. Finally submit the job. (Because of the SETROPTS command you may see a Return Code of 08.)
   a. **sub**
   b. Then use **PF3 to save and exit** the member under your name.

9. Review the output.
   a. **=D.O**
      i. Select your job for review.
      ii. *IMPORTANT:* Verify that all commands except for the SETROPTS have been accepted. If the job fails to run cleanly, you may not proceed since it will cause errors for future steps.

10. Notice the following in the output:
    a. The change to the expiration date.
    b. Note how the FTP Server Key Ring looks ALMOST the same as before. T***he association of your renewed FTP Server Certificate with the existing Key Rings has been retained!***

11. You are not authorized to execute the SETROPTS command directly. Instead, run the following procedure which will execute the commands for you on your behalf:
    a. **/S SPECUSER**
12. Return to the Console Log of YOUR MVS***n***:
    a. **=D.LOG**

> **IMPORTANT:** In the next step you will restart your FTP server. When you are using AT-TLS, it is not necessary to recycle the FTP server in order to refresh in memory the changed Key Rings and Certificates. However, for this lab, it is quicker to recycle the FTP server in order to accomplish the refresh.

13. Stop your FTP Server and restart it so that it rereads the refreshed Key Ring:
    a. For TCPIP***T***:
        i. **/P FTP*T1***
        ii. **/S FTP*T*,FDAT=FTPSAUTH**
    b. For TCPIP***G***:
        i. **/P FTP*G1***
        ii. **/S FTP*G*,FDAT=FTPSAUTH**

14. Now return to your TN3270 session with MVS1 where you will test your changes.

Testing the FTP Server Certificate Corrections in Scenario 4

1. You should be signed on at MVS1 with your User ID:
    a. TCPIP***T***: USER***n***1 (***"n"*** = your MVS suffix)
    b. TCPIP***G***: USER***n***2 (***"n"*** = your MVS suffix)

2. Move to ISPF Option 6 where you enter the following FTP command:
    a. For TCPIP***T*** Client (USER***n***1):
        ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*T* -s 172.16.20.111 172.16.20.11*n*
        (***"n"*** = your MVS suffix)
    b. For TCPIP***G*** Client (USER***n***2):
        ===> ftp -r TLS -f "//'SYS1.CS.TCPPARMS(FTPCLSEC)'" -p TCPIP*G* -s 172.16.20.121 172.16.20.12*n*
        (***"n"*** = your MVS suffix)

Observe that now your FTP connection succeeds.

3. Quit out of the FTP session:
    a. **Quit**

4. You have finished the last part – an optional scenario – of this lab. Please logoff your two TN3270 emulator sessions.

What you have learned in Scenario 4 of this lab:

You have learned how to change the public and private key pair associated with a CERTIFICATE AUTHORITY CERTIFICATE through the rekey and rollover process.

You have seen how the Key Ring after the rekey and rollover of a CA Certificate contains both the old and new CA Certificates. This is so that the old Certificate may continue to validate PERSONAL certificates that it may have signed previously even though it no longer has a Private Key. But you have also seen that the presence of a Private Key on the new CA Certificate permits it to issue and sign new Certificates.

IMPORTANT: *If there were also remote clients, you would need to EXPORT the renewed and rekeyed CA Certificate without its private key to those remote clients for IMPORT into their Certificate repositories. This lab does not use remote clients and so this EXPORT/IMPORT step is unnecessary for this lab.*

End of RACF Certificate Rekeying and Renewing Lab

APPENDIX: Documentation

FTP.DATA File for FTP Client (Server Authentication Only)

This file depicts only the Security Section of the FTP Client's FTP.DATA file. In this lab we are using AT-TLS and so only a few of the parameters in this file are uncommented. The other parameters (e.g., Key Ring and Encryption Algorithms) are contained in the FTP Client Policy built with z/OS Communications Server Configuration Assistant.

```
; ---------------------------------------------------------------------
;
; 7. Security options
;
; ---------------------------------------------------------------------

 SECURE_MECHANISM    TLS             ; Name of the security mechanism
                                     ; that the client uses when it
                                     ; sends an AUTH command to the
                                     ; server.
                                     ; GSSAPI = Kerberos support
                                     ; TLS    = TLS
 TLSMECHANISM ATTLS                  ; FTP or ATTLS
 ;
 SECURE_FTP         ALLOWED          ; Authentication indicator
                                     ; ALLOWED        (D)
                                     ; REQUIRED

;SECURE_CTRLCONN   CLEAR             ; Minimum level of security for
 SECURE_CTRLCONN   PRIVATE           ; Minimum level of security for
                                     ; the control connection
                                     ; CLEAR          (D)
                                     ; SAFE
                                     ; PRIVATE

;SECURE_DATACONN   CLEAR             ; Minimum level of security for
 SECURE_DATACONN   PRIVATE           ; Minimum level of security for
                                     ; the data connection
                                     ; NEVER
                                     ; CLEAR          (D)
                                     ; SAFE
                                     ; PRIVATE

;SECURE_HOSTNAME   OPTIONAL          ; Authentication of hostname in
                                     ; the server certificate
                                     ; OPTIONAL (D)
                                     ; REQUIRED

;SECURE_PBSZ       16384             ; Kerberos maximum size of the
                                     ; encoded data blocks
                                     ; Default value is 16384
                                     ; Valid range is 512 through 32768
; Name of a ciphersuite that can be passed to the partner during
; the TLS handshake. None, some, or all of the following may be
; specified. The number to the far right is the cipherspec id
; that corresponds to the ciphersuite's name.
;CIPHERSUITE       SSL_NULL_MD5      ; 01
;CIPHERSUITE       SSL_NULL_SHA      ; 02
;CIPHERSUITE       SSL_RC4_MD5_EX    ; 03
;CIPHERSUITE       SSL_RC4_MD5       ; 04
;CIPHERSUITE       SSL_RC4_SHA       ; 05
;CIPHERSUITE       SSL_RC2_MD5_EX    ; 06
;CIPHERSUITE       SSL_DES_SHA       ; 09
;CIPHERSUITE       SSL_3DES_SHA      ; 0A
;CIPHERSUITE       SSL_AES_128_SHA   ; 2F
;CIPHERSUITE       SSL_AES_256_SHA   ; 35

;KEYRING           name              ; Name of the Key Ring for TLS
                                     ; It can be the name of an HFS
                                     ; file (name starts with /) or
                                     ; a resource name in the security
                                     ; product (e.g., RACF)

;TLSTIMEOUT        100               ; Maximum time limit between full
                                     ; TLS handshakes to protect data
                                     ; connections
                                     ; Default value is 100 seconds.
                                     ; Valid range is 0 through 86400

;SECUREIMPLICITZOS TRUE              ; Specify whether client will
                                     ; connect to a z/OS FTP server
                                     ; when using the TLS port.
                                     ; TRUE  (D)
                                     ; FALSE  Use FALSE if server is
                                     ; not z/OS or the port is not the
                                     ; TLS port (990).
;TLSRFCLEVEL       DRAFT         ; (S) Specify what level of RFC 4217,
 TLSRFCLEVEL       RFC4217       ; (S) Specify what level of RFC 4217,
                                     ; On Securing ; FTP with TLS, is
                                     ; supported
                                     ; DRAFT (D) Internet Draft level
                                     ; RFC4217   RFC level
```

FTP.DATA File for FTP Server (Server Authentication Only)

This file depicts only the Security Section of the FTP Server's FTP.DATA file. In this lab we are using AT-TLS and so only a few of the parameters in this file are uncommented. The other parameters (e.g., Key Ring and Encryption Algorithms) are contained in the FTPX Server Policy built with z/OS Communications Server Configuration Assistant.

```
************************************* Top of Data ***********************
; ---------------------------------------------------------------------
;
; 12. Security options
;
```

```
; ---------------------------------------------------------------------

;EXTENSIONS        AUTH_GSSAPI       ; Enable Kerberos authentication
                                     ; Default is disabled.

 EXTENSIONS        AUTH_TLS          ; Enable TLS authentication
                                     ; Default is disabled.
;SECURE_MECHANISM   TLS              ; Not used on Server - Client only
 TLSMECHANISM       ATTLS            ; FTP or ATTLS
;

 SECURE_FTP        ALLOWED           ; Authentication indicator
                                     ; ALLOWED        (D)
                                     ; REQUIRED

 SECURE_LOGIN      NO_CLIENT_AUTH    ; Authorization level indicator
;SECURE_LOGIN      REQUIRED          ; Authorization level indicator
                                     ; for TLS
                                     ; NO_CLIENT_AUTH (D)
                                     ; REQUIRED
                                     ; VERIFY_USER

;SECURE_PASSWORD   REQUIRED          ; REQUIRED (D) - User must enter
                                     ;     password
                                     ; OPTIONAL - User does not have to
                                     ;     enter a password
                                     ; This setting has meaning only
                                     ; for TLS when implementing client
                                     ; certificate authentication


;
;SECURE_PASSWORD_KERBEROS  REQUIRED  ; REQUIRED (D) - User must enter
                                     ;     password
                                     ; OPTIONAL - User does not have to
                                     ;     enter a password
                                     ; This setting has meaning only
                                     ; for Kerberos

;SECURE_CTRLCONN   CLEAR             ; Minimum level of security for
 SECURE_CTRLCONN   PRIVATE           ; Minimum level of security for
                                     ; the control connection
                                     ; CLEAR          (D)
                                     ; SAFE
                                     ; PRIVATE

;SECURE_DATACONN   CLEAR             ; Minimum level of security for
 SECURE_DATACONN   CLEAR             ; Minimum level of security for
                                     ; the data connection
                                     ; NEVER
                                     ; CLEAR          (D)
                                     ; SAFE
                                     ; PRIVATE

;SECURE_PBSZ       16384             ; Kerberos maximum size of the
                                     ; encoded data blocks
                                     ; Default value is 16384
                                     ; Valid range is 512 through 32768

; Name of a ciphersuite that can be passed to the partner during
; the TLS handshake. None, some, or all of the following may be
; specified. The number to the far right is the cipherspec id
; that corresponds to the ciphersuite's name.
; the ciphersuites are ignored if AT-TLS is in effect
```

```
;CIPHERSUITE       SSL_3DES_SHA      ; 0A
;CIPHERSUITE       SSL_AES_128_SHA   ; 2F
;CIPHERSUITE       SSL_AES_256_SHA   ; 35
;
;CIPHERSUITE       SSL_NULL_MD5      ; 01
;CIPHERSUITE       SSL_NULL_SHA      ; 02
;CIPHERSUITE       SSL_RC4_MD5_EX    ; 03
;CIPHERSUITE       SSL_RC4_MD5       ; 04
;CIPHERSUITE       SSL_RC4_SHA       ; 05
;CIPHERSUITE       SSL_RC2_MD5_EX    ; 06
;CIPHERSUITE       SSL_DES_SHA       ; 09
;CIPHERSUITE       SSL_3DES_SHA      ; 0A
;CIPHERSUITE       SSL_AES_128_SHA   ; 2F
;CIPHERSUITE       SSL_AES_256_SHA   ; 35

; the Key Ring is ignored if AT-TLS is in effect
;KEYRING           /FTPD/ServerRing1 ; Name of the Key Ring for TLS
                                     ; It can be the name of an hfs
                                     ; file (name starts with /) or
                                     ; a resource name in the security
                                     ; product (e.g., RACF)

; the TLSTIMEOUT is ignored if AT-TLS is in effect
;TLSTIMEOUT        100               ; Maximum time limit between full
                                     ; TLS handshakes to protect data
                                     ; connections
                                     ; Default value is 100 seconds.
                                     ; Valid range is 0 through 86400
;TLSRFCLEVEL       DRAFT             ; Specify what level of RFC 4217,
 TLSRFCLEVEL       RFC4217           ; Specify what level of RFC 4217,
                                     ; On Securing FTP with TLS, is
                                     ; supported.
                                     ; DRAFT    (D) Internet Draft level
                                     ; RFC4217      RFC level
```

Creating the Certificate Authority Certificates

For these labs we decided to be our own certificate authority using the RACF *racdcer*t command within a JCL member.

```
***************************** Top of Data **************************
//RACDCA    JOB MSGCLASS=X,NOTIFY=&SYSUID
//RACDCA   EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//**********************************************************************
//*     Create Individual Personal Certificate for FTP Server          *
//**********************************************************************
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT CERTAUTH GENCERT                                          -
         SUBJECTSDN  (CN('WSC Certificate Authority #1')           -
                      OU('WSC')                                    -
                      C('US'))                                     -
                      ALTNAME (IP(192.168.20.101)                  -
                               EMAIL('CA1@ZOS1')                   -
                               DOMAIN('WSC.IBM.COM'))              -
                      NOTBEFORE(DATE(2008-10-07))                  -
                      NOTAFTER(DATE(2011-10-07))                   -
                      WITHLABEL('WSC Certificate Authority #1')   -
                      SIZE(1024)                                  -
                      KEYUSAGE(CERTSIGN)
  racdcert CERTAUTH list(label('WSC Certificate Authority #1'))
/*
```

```
********************************** Top of Data *************************
//RACDCAX   JOB MSGCLASS=X,NOTIFY=&SYSUID
//RACDCAX  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//****FOR EXERCISE ON REKEYING/REFRESHING CA and Server CERTS *********
//* TCPIPT:  Creating Client and Server Key Rings with Expired CERTS  *
//* TCPIPG:  Creating Client and Server Key Rings with Expired CERTS
*
//* TCPIPT:  Create CA and FTP Server Certs that are both expired     *
//*     USER11 .. USING EXPIRED FTP Server Certificate                *
//* TCPIPG:  Create CA and FTP Server Certs that are both expired     *
//*     USER12 .. USING EXPIRED FTP Server Certificate                *
//*********************************************************************
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT CERTAUTH GENCERT                                         -
         SUBJECTSDN  (CN('ZOS11 EXPCA')                           -
                      OU('WSC')                                   -
                      C('US'))                                    -
                      ALTNAME (IP(172.16.20.111)                  -
                               EMAIL('TCPIPTCA@ZOS1')             -
                               DOMAIN('WSC.IBM.COM'))             -
                      NOTBEFORE(DATE(2008-10-07))                 -
                      NOTAFTER(DATE(2011-10-07))                  -
                      WITHLABEL('ZOS11 EXPCA')                    -
                      SIZE(1024)                                  -
                      KEYUSAGE(CERTSIGN)
RACDCERT CERTAUTH  ALTER(LABEL('ZOS11 EXPCA')) TRUST
RACDCERT ID(TCPIP) GENCERT                                        -
         SUBJECTSDN  (CN('FTPServer11 EXPCA')                     -
                      OU('WSC')                                   -
                      C('US'))                                    -
                      ALTNAME (IP(172.16.20.111)                  -
                               EMAIL('FTPT@ZOS1')                 -
                               DOMAIN('WSC.IBM.COM'))             -
                      NOTBEFORE(DATE(2008-10-07))                 -
                      NOTAFTER(DATE(2011-10-07))                  -
                      WITHLABEL('FTPServer11 EXPCA')              -
                      SIZE(1024)                                  -
                      SIGNWITH(CERTAUTH                           -
                      Label('ZOS11 EXPCA'))
RACDCERT ID(TCPIP) ALTER(LABEL('FTPServer11 EXPCA')) TRUST
RACDCERT ID(FTPD) ADDRING(FTPCAX11_RING)
RACDCERT ID(FTPD) CONNECT(ID(TCPIP) LABEL('FTPServer11 EXPCA')     -
         RING(FTPCAX11_RING) USAGE(PERSONAL) DEFAULT)
RACDCERT ID(FTPD) CONNECT(CERTAUTH                                 -
         LABEL('ZOS11 EXPCA')                                      -
         RING(FTPCAX11_RING) USAGE(CERTAUTH))
RACDCERT ID(TCPIP) ADDRING(ClientEXP11_RING)
RACDCERT ID(TCPIP) CONNECT(CERTAUTH                                -
         LABEL('ZOS11 EXPCA')                                      -
         RING(ClientEXP11_RING) USAGE(CERTAUTH))
  setropts generic(DIGTCERT) refresh
  setropts raclist(DIGTCERT) refresh
  racdcert CERTAUTH list(label('ZOS11 EXPCA'))
  racdcert ID(TCPIP) list(label('FTPServer11 EXPCA'))
  racdcert ID(FTPD) listring(FTPCAX11_RING)
  racdcert ID(TCPIP) listring(ClientEXP11_RING)
```

Creating the FTP Client Certificates and Key Rings

```
********************************* Top of Data *************************
//RACDCLR2  JOB MSGCLASS=X,NOTIFY=&SYSUID
//RACDCLR2 EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//****FOR EXERCISE ON REKEYING/REFRESHING CA and Server CERTS *********
//* Creates INDIVIDUAL Client Rings with only CA connected to them    *
//***********  THE CLIENTS WILL NEED TO REFRESH THIS KEY RING *********
//***********  with a renewed and rekeyed certificate        **********
//**********************************************************************
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT ID(TCPIP) ADDRING(ClientEXP11_RING)
RACDCERT ID(TCPIP) CONNECT(CERTAUTH                                   -
         LABEL('ZOS11 EXPCA')                                         -
         RING(ClientEXP11_RING) USAGE(CERTAUTH))
  setropts generic(DIGTCERT) refresh
  setropts raclist(DIGTCERT) refresh
  racdcert ID(TCPIP) listring(ClientEXP11_RING)
```

```
********************************* Top of Data *************************
//RACDCLR1  JOB MSGCLASS=X,NOTIFY=&SYSUID
//RACDCLR1 EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//****FOR EXERCISE ON REKEYING/REFRESHING CA and Server CERTS *********
//* Creates SHARED Generic Client Ring with only CA connected to it   *
//*********  STUDENTS DO NOT NEED TO CHANGE THIS RING *****************
//**********************************************************************
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT ID(TCPIP) ADDRING(Client_RING)
RACDCERT ID(TCPIP) CONNECT(CERTAUTH                                   -
         LABEL('MVS1 LABS Certificate Authority')                     -
         RING(Client_RING) USAGE(CERTAUTH))
  setropts generic(DIGTCERT) refresh
  setropts raclist(DIGTCERT) refresh
  racdcert ID(TCPIP) listring(Client_RING)
/*
/*
```

Creating the FTP Server Certificates and Key Rings

```
********************************* Top of Data *************************
```

```
//RACDFTPA  JOB MSGCLASS=X,NOTIFY=&SYSUID
//RACDFTPA EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//****FOR EXERCISE ON REKEYING/REFRESHING CA and Server CERTS *********
//* Creates Generic SERVER CERT for FTP SERVER on MVS1-7              *
//* Creates Generic SERVER Ring with CACERT and Generic FTP SRVCERT   *
//****** THIS NEVER NEEDS A CLEANUP  **********************************
//*********************************************************************
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT ID(TCPIP) GENCERT                                        -
         SUBJECTSDN  (CN('FTP Server on MVS1-MVS7')               -
                      OU('WSC')                                   -
                      C('US'))                                    -
                      ALTNAME (IP(192.168.20.0)                   -
                               EMAIL('FTP@ZOS1')                  -
                               DOMAIN('WSC.IBM.COM'))             -
                      NOTBEFORE(DATE(2012-09-08))                 -
                      NOTAFTER(DATE(2015-12-31))                  -
                      WITHLABEL('FTP Server on MVS1-MVS7')        -
                      SIZE(1024)                                  -
                      SIGNWITH(CERTAUTH                           -
                      Label('MVS1 LABS Certificate Authority'))
RACDCERT ID(FTPD) ADDRING(Server_RING)
RACDCERT ID(FTPD) CONNECT(CERTAUTH                                -
         LABEL('MVS1 LABS Certificate Authority')                 -
         RING(Server_RING) USAGE(CERTAUTH))
RACDCERT ID(FTPD) CONNECT(ID(TCPIP)                               -
         LABEL('FTP Server on MVS1-MVS7')                         -
         RING(Server_RING) USAGE(PERSONAL) DEFAULT)
  setropts generic(DIGTCERT) refresh
  setropts raclist(DIGTCERT) refresh
  racdcert ID(FTPD) listring(Server_RING)
/*

********************************* Top of Data *************************
//RACDFTPX  JOB MSGCLASS=X,NOTIFY=&SYSUID
//RACDFTPX EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//****FOR EXERCISE ON REKEYING/REFRESHING SERVER CERTIFICATES *********
//* TCPIPT:  Create Individual Personal Certificate for FTP Server 11 *
//*     USER11 .. USING EXPIRED FTP Server Certificate                *
//* TCPIPG:  Create Individual Personal Certificate for FTP Server 12 *
//*     USER12 .. USING EXPIRED FTP Server Certificate                *
//*********************************************************************
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT ID(TCPIP) GENCERT                                        -
         SUBJECTSDN  (CN('FTPServer11 EXP')                       -
                      OU('WSC')                                   -
                      C('US'))                                    -
                      ALTNAME (IP(192.168.20.91)                  -
                               EMAIL('FTPT@ZOS1')                 -
                               DOMAIN('WSC.IBM.COM'))             -
                      NOTBEFORE(DATE(2011-01-07))                 -
                      NOTAFTER(DATE(2011-10-07))                  -
                      WITHLABEL('FTPServer11 EXP')                -
                      SIZE(1024)                                  -
                      SIGNWITH(CERTAUTH                           -
                      Label('MVS1 LABS Certificate Authority'))
RACDCERT ID(TCPIP) ALTER(LABEL('FTPServer11 EXP')) TRUST
setropts raclist(DIGTCERT) refresh
racdcert ID(TCPIP) list(label('FTPServer11 EXP'))
RACDCERT ID(FTPD) ADDRING(FTPEXP11_RING)
RACDCERT ID(FTPD) CONNECT(ID(TCPIP) LABEL('FTPServer11 EXP')      -
         RING(FTPEXP11_RING) USAGE(PERSONAL) DEFAULT)
RACDCERT ID(FTPD) CONNECT(CERTAUTH                                -
         LABEL('MVS1 LABS Certificate Authority')                 -
         RING(FTPEXP11_RING) USAGE(CERTAUTH))
setropts generic(DIGTCERT) refresh
setropts raclist(DIGTCERT) refresh
racdcert ID(FTPD) listring(FTPEXP11_RING)
```

Renewing the FTP Server Certificates to Change Expiration

```
********************************* Top of Data *************************
//RACDRENU  JOB MSGCLASS=X,NOTIFY=&SYSUID
//RACDRENU EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//****FOR EXERCISE ON REKEYING/REFRESHING SERVER CERTIFICATES *********
//****  This JCL IS USED FOR A SKELETON THAT THE STUDENTS WORK WITH ***
//* TCPIPT:  Renew expired FTP Server Certificate but keep Private Key*
//*     USER11 .. USING EXPIRED FTP Server Certificate                *
//* TCPIPT:  Renew expired FTP Server Certificate but keep Private Key*
//*     USER12 .. USING EXPIRED FTP Server Certificate                *
//*********************************************************************
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT ID(TCPIP) GENREQ(LABEL('FTPServer11 EXP'))                 -
    DSN('USER.FTPSRV11.EXP.REQ')
RACDCERT ID(TCPIP) GENCERT('USER11.FTPSRV11.EXP.REQ')            -
    SIGNWITH(CERTAUTH LABEL('MVS1 LABS Certificate Authority'))
RACDCERT ID(TCPIP) GENREQ(LABEL('FTPServer12 EXP'))                 -
    DSN('USER.FTPSRV12.EXP.REQ')
RACDCERT ID(TCPIP) GENCERT('USER12.FTPSRV12.EXP.REQ')            -
    SIGNWITH(CERTAUTH LABEL('MVS1 LABS Certificate Authority'))
RACDCERT ID(TCPIP) GENREQ(LABEL('FTPServer21 EXP'))                 -
    DSN('USER.FTPSRV21.EXP.REQ')
RACDCERT ID(TCPIP) GENCERT('USER21.FTPSRV21.EXP.REQ')            -
    SIGNWITH(CERTAUTH LABEL('MVS1 LABS Certificate Authority'))
RACDCERT ID(TCPIP) GENREQ(LABEL('FTPServer22 EXP'))                 -
    DSN('USER.FTPSRV22.EXP.REQ')
RACDCERT ID(TCPIP) GENCERT('USER22.FTPSRV22.EXP.REQ')            -
    SIGNWITH(CERTAUTH LABEL('MVS1 LABS Certificate Authority'))
setropts raclist(DIGTCERT) refresh
setropts generic(DIGTCERT) refresh
```

Rekeying (“Rolling Over”) the FTP Server Certificates

```
********************************* Top of Data *************************
//RACDROLL  JOB MSGCLASS=X,NOTIFY=&SYSUID
//RACDROLL  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//****FOR EXERCISE ON REKEYING/REFRESHING SERVER CERTIFICATES *********
```

```
//****  This JCL IS USED FOR A SKELETON THAT THE STUDENTS WORK WITH ***
//* TCPIPT:  Rekey the     FTP Server Certificate                     *
//*     USER11 .. USING renewed FTP Server Certificate                *
//* TCPIPG:  Rekey the     FTP Server Certificate                     *
//*     USER12 .. USING renewed FTP Server Certificate                *
//*********************************************************************
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT ID(TCPIP) REKEY(LABEL('FTPServer11 EXP'))            -
WITHLABEL('FTPServer11 EXP-2')
RACDCERT ID(TCPIP) GENREQ(LABEL('FTPServer11 EXP-2'))         -
DSN('USER11.FTPSRV11.EXP-2.REQ')
RACDCERT ID(TCPIP) GENCERT('USER11.FTPSRV11.EXP-2.REQ')       -
SIGNWITH(CERTAUTH LABEL('MVS1 LABS Certificate Authority'))
RACDCERT ID(TCPIP) ROLLOVER(LABEL('FTPServer11 EXP'))         -
NEWLABEL('FTPServer11 EXP-2')
racdcert ID(FTPD) listring(FTPEXP11_RING)
setropts raclist(DIGTCERT) refresh
setropts generic(DIGTCERT) refresh
```

Renewing and Rolling Over (“Rekeying”) the CA Certificates

```
********************************* Top of Data *************************
//RACDREN4  JOB MSGCLASS=X,NOTIFY=&SYSUID
//RACDREN4 EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//****FOR EXERCISE ON REKEYING/REFRESHING SERVER CERTIFICATES *********
//***This is used as a skeleton for the students to run during lab ****
//* TCPIPT:  Rollover CA certificate to change the private key        *
//*          Extend the expiration of the CA Certificate  (RENEW)     *
//* TCPIPG:  Rollover CA certificate to change the private key        *
//*          Extend the expiration of the CA Certificate  (RENEW)     *
//* TCPIPT:  Renew the FTPServer Cert signed by new CA                *
//* TCPIPG:  Renew the FTPServer Cert signed by new CA                *
//*********************************************************************
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT CERTAUTH  REKEY(LABEL('ZOS11 EXPCA'))            -
     WITHLABEL('ZOS11 EXPCA-2')                           -
     NOTBEFORE(DATE(2012-09-11))                          -
     NOTAFTER(DATE(2020-12-31))
RACDCERT CERTAUTH  ROLLOVER(LABEL('ZOS11 EXPCA'))         -
    NEWLABEL('ZOS11 EXPCA-2')
racdcert ID(FTPD) listring(FTPCAX11_RING)
racdcert ID(TCPIP) listring(ClientEXP11_RING)
racdcert CERTAUTH list(LABEL('ZOS11 EXPCA')
racdcert CERTAUTH list(LABEL('ZOS11 EXPCA-2')
setropts raclist(DIGTCERT) refresh
setropts generic(DIGTCERT) refresh
```

Answers

Scenario 2:

9. 2011/01/07

Scenario 4:

15.a.ii.1. 2008/10/07
15.a.ii.2. 2011/10/07
15.a.ii.4. 2
15.a.iv.1. 2008/10/07
15.a.iv.2. 2011/10/07
15.a.iv.3. 1