

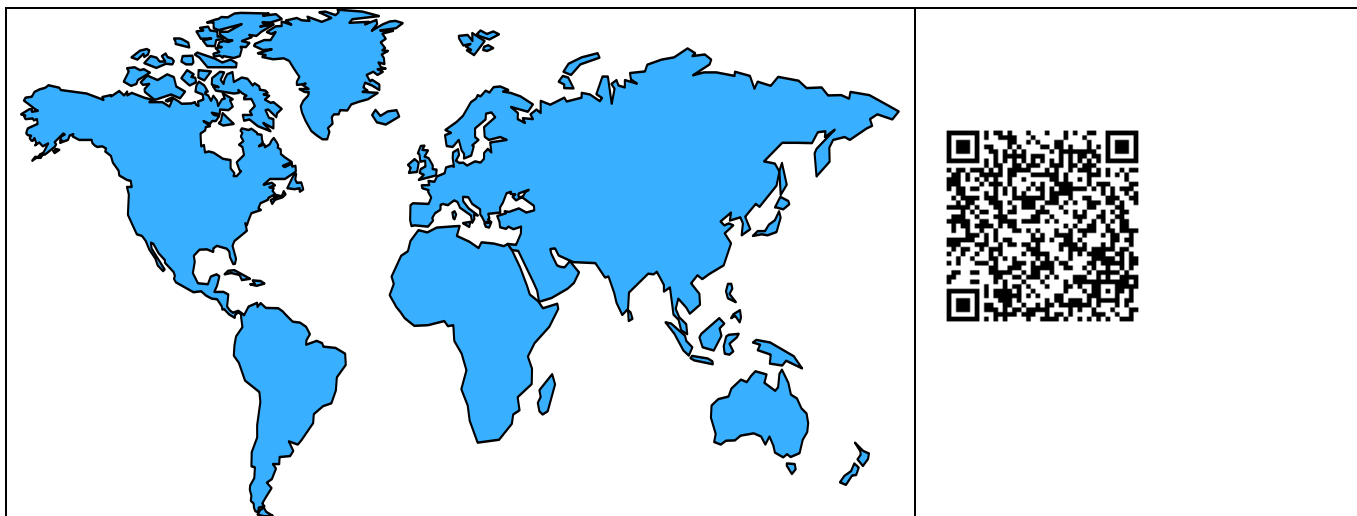
"Creating, Renewing, and Testing x.509 Digital Certificates with RACF" **Hands-on Lab - Part 1 of 2**

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

SHARE 16073

Hands-on Lab Guide

(Digital Certificate Exercises: Creating Certificates)



(USER201-2, USER301-2, USER401-2, USER501-2, USER601-2, USER701-2)

Revision date -

Thursday, 10 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 for suggestions they have made to enhance the user experience with this lab.

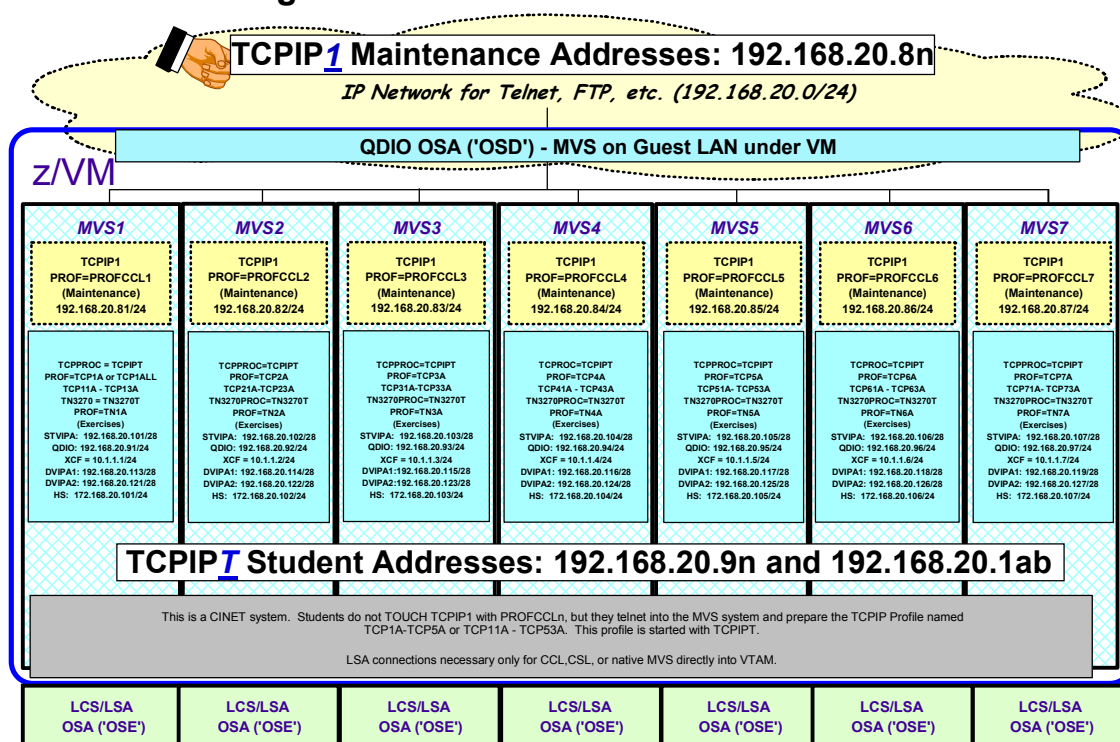
Table of Contents

Table of Contents.....	- 3 -
Introduction: Lab Description (Analyzing and Creating x.509 Digital Certificates)	- 4 -
<i>General Lab Diagram.....</i>	<i>- 4 -</i>
<i>Specific Lab Description: Creating x.509 Certificates</i>	<i>- 5 -</i>
Scenario 0: Getting Started with the Lab.....	- 9 -
Scenario 1 (Optional): Analyzing Some Key Rings and Certificates in the Shared RACF Database	- 10 -
<i>End of Scenario 1.....</i>	<i>- 14 -</i>
Scenario 2: Building Certificates and Key Rings of Your Own for Server Authentication.....	- 15 -
<i>End of Scenario 2.....</i>	<i>- 18 -</i>
Scenario 3: Testing your Certificates and Key Rings over Secured FTP Connections	- 19 -
<i>End of the Lab.....</i>	<i>- 25 -</i>
APPENDIX: Lab Documentation	- 26 -
<i>Scenario 1: Documentation for Certificate Lab</i>	<i>- 26 -</i>
Output from: racdcert ID(USER22) list	- 26 -
Output from: racdcert ID(USER22) listring(LabClientRing)	- 26 -
Output from: racdcert certauth list(label('WSC LABS Certificate Authority')).....	- 26 -
<i>Scenario 2: CERTIFICATE LAB: Jobs Run for FTP_X Certificate Creation Lab with AT-TLS</i>	<i>- 27 -</i>
JCL: CA Certificate for Signing FTP_X Server Certificates	- 27 -
JCL: FTP_X Server PERSONAL Certificate	- 28 -
JCL: Creating Server and Client Key Rings and Connecting Certificates	- 28 -
<i>Scenario 3: FTP_X Procedure for Port 2021 and FTP.DATA Files.....</i>	<i>- 29 -</i>
JCL: FTP_X Initialization Procedure.....	- 29 -
FTP.DATA File for FTP_X Server (Server Authentication Only)	- 29 -
FTP.DATA File for FTP_X Client (Server Authentication Only).....	- 31 -
Answers	- 33 -
<i>Scenario 1:.....</i>	<i>- 33 -</i>
<i>Scenario 2:.....</i>	<i>- 33 -</i>
<i>Scenario 3:.....</i>	<i>- 33 -</i>

Introduction: Lab Description (Analyzing and Creating x.509 Digital Certificates)

If you feel that you already understand the lab logistics, you may skip this introduction and proceed to the optional Scenario 1 of this lab handout, where you will analyze x.509 certificates that have already been created for you.

General Lab Diagram



Each student ZOS (MVS) system has three TCP/IP stacks running in it: TCPIP1, TCPIPT, and TCPIPG.

The basic TCPIP stack is used for access only and not testing and is named TCPIP1. The TN3270 procedure that has affinity to the access TCPIP1 is named TN3270. The FTP procedure that has affinity to TCPIP1 is named FTPCCL(1).

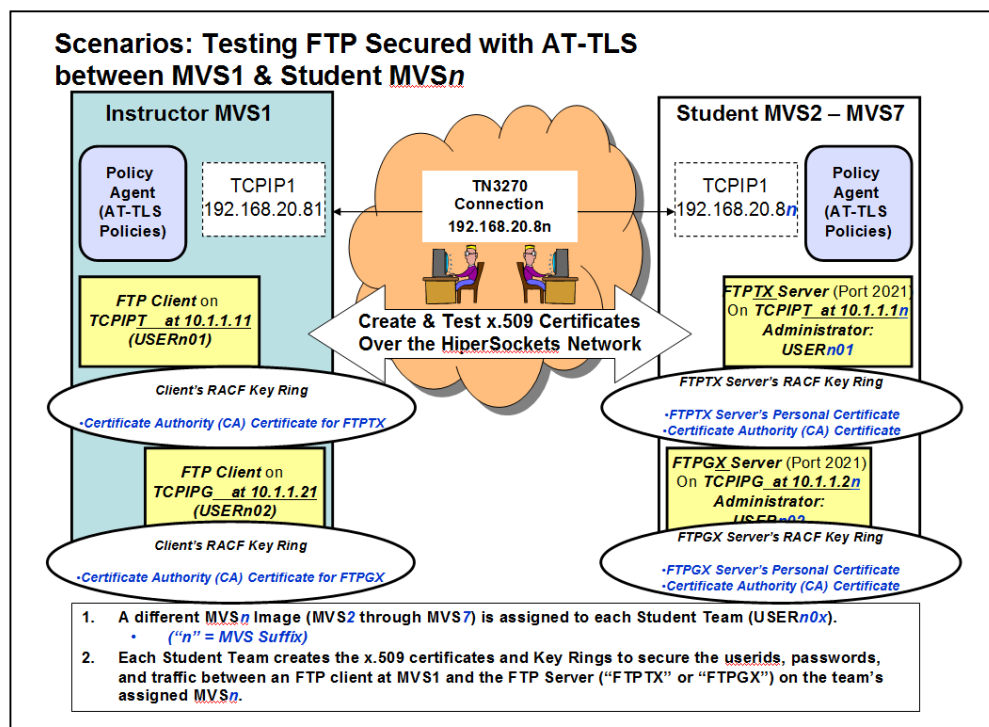
In our labs you use TCPIP1 for basic maintenance on your MVS_n until you have finished building your own student TCP/IP stacks and procedures. You telnet into TCPIP1 to reach ISPF and UNIX for building the procedures that should run together with the student TCP/IP test stack.

There are six “Student z/OS (MVS) systems” that you will be working on: MVS2-MVS7. The student TCP/IP stacks on these systems are named TCPIPT and TCPIPG. The students customize a test stack and *not* the instructor “maintenance” stack. The students also customize any other procedures that are part of the security labs and that are to have affinity with TCPIPT and TCPIPG.

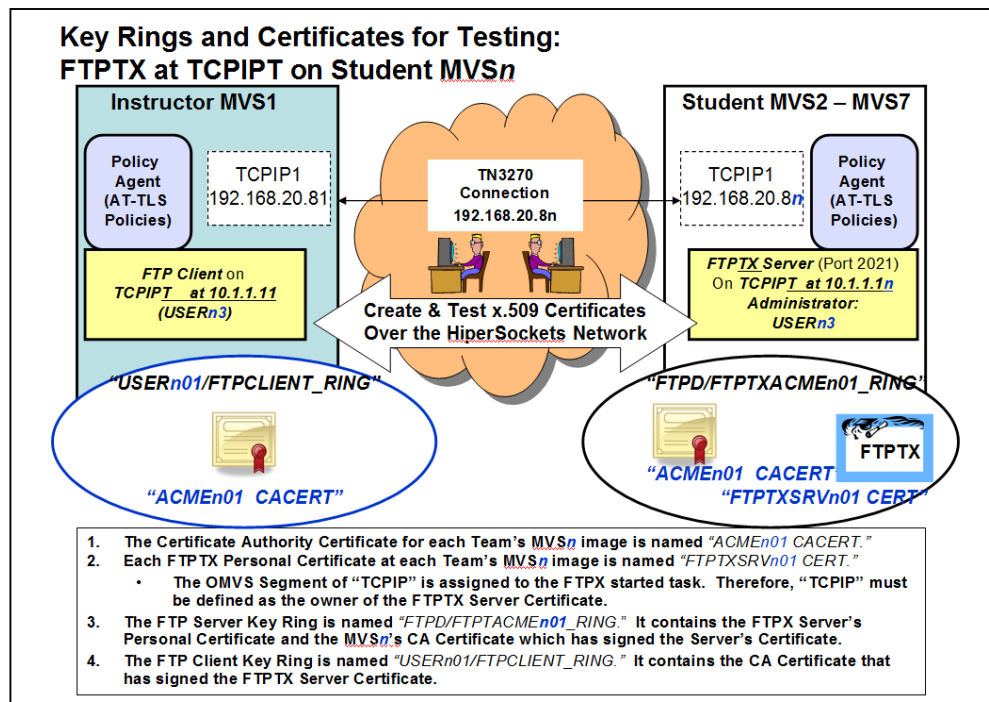
Specific Lab Description: Creating x.509 Certificates

The lab's RACF Database is shared by all 7 MVS images: MVS1 through MVS7. Because the database is shared, you may create Certificates and Key Rings for all systems from a single MVS image instead of having to sign onto each image to create its own Key Rings and Certificates.

The visual below provides a **general overview** of the lab topology. You will sign onto your assigned MVS using TN3270 over an IPv4 LAN network (192.168.20.0/24). You will create the necessary RACF Key Rings and Certificates from your userid at your assigned MVS. Then you will sign onto MVS1 to test the certificates in an FTP secured session over a HiperSockets network (10.1.1.0/24).



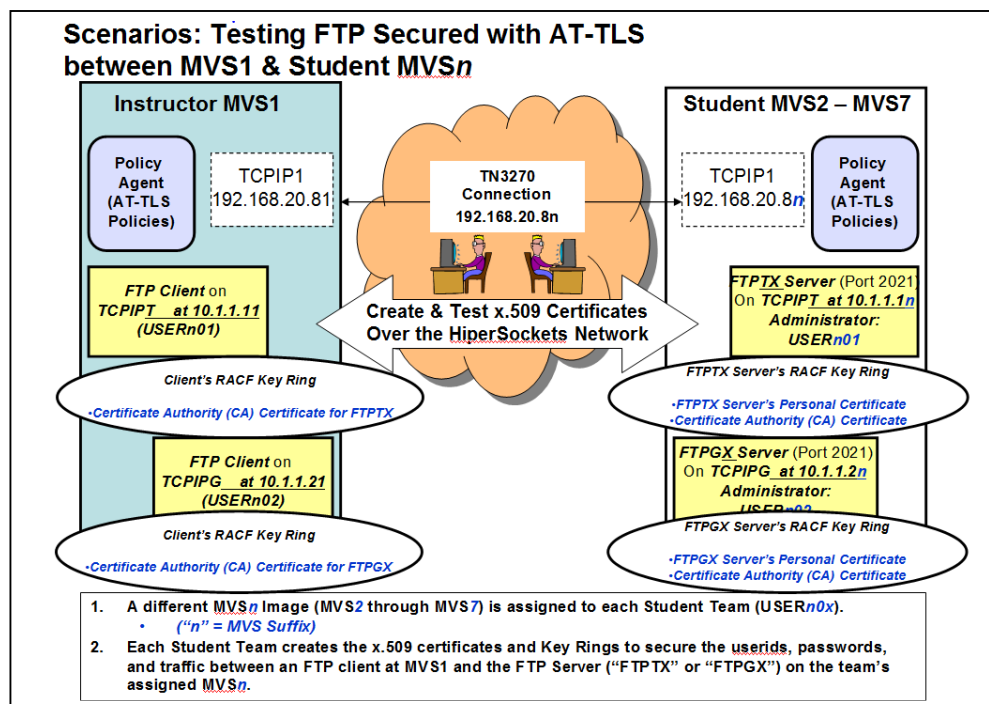
The next visual shows you the naming conventions for the Key Rings and Certificates that you will be creating *if you are assigned to a TCPIPT* stack. User IDs of **USER201**, **USER301**, **USER401**, **USER501**, **USER601**, and **USER701** are assigned to the *TCPIPT* stack.



As the visual above illustrates, if your userid ends in "1", as with **USERn01**, you will perform the following tasks for the *TCPIPT* stack on MVS_n:

1. Create a Certificate Authority Certificate for your User ID.
 - a. "ACME01 CERT"
2. Create a Personal FTP Server Certificate for your assigned FTPTX procedure:
 - a. 'FTPTXSRVn01 CERT'
3. Create a Key Ring that contains the appropriate certificates for your FTPTX procedure:
 - a. "FTPTXACME01_RING" (owned by FTPD) which contains:
 - i. "ACME01 CERT"
 - ii. 'FTPTXSRVn01 CERT'
4. Create a Key Ring for your assigned userid that contains the CA certificate that will be used to authenticate the FTPTX server during AT-TLS negotiation.
 - a. "FTPCLIENT_RING" (owned by you) which contains:
 - i. "ACME01 CERT"
5. Test your Key Rings and x.509 certificates.

The next visual shows you the naming conventions for the Key Rings and Certificates that you will be creating *if you are assigned to a TCPIPG* stack. User IDs of **USER202**, **USER302**, **USER402**, **USER502**, **USER602**, and **USER702** are assigned to the *TCPIPG* stack.



As the visual above illustrates, if your user id ends in "2", as with **USERn02**, you will perform the following tasks for the *TCPIPG* stack on MVS_n:

1. Create a Certificate Authority Certificate for your user id.
 - a. "ACME_n02 CERT"
2. Create a Personal FTP Server Certificate for your assigned FTGPX procedure:
 - b. 'FTPGXSRVn02 CERT'
3. Create a Key Ring that contains the appropriate certificates for your FTGPX procedure:
 - c. "FTPGXACME_n02_RING" (owned by FTPD) which contains:
 - i. "ACME_n02 CERT"
 - ii. 'FTPGXSRVn02 CERT'
4. Create a Key Ring for your assigned user id that contains the CA certificate that will be used to authenticate the FTPTX server during AT-TLS negotiation.
 - a. "FTPCIENT_RING" (owned by you) which contains:
 - i. "ACME_n02 CERT"
5. Test your Key Rings and x.509 certificates.

Shared RACF Database with shared Key Rings and Certificates.

Both the Server and the Client certificates are signed by the same Certificate Authority (CA). The CA assigns a sequence number to each certificate as it signs it. In RACF certificates are stored under the DIGTCERT class. Profile names for the certificates stored there are in the form of : ***Serial-number.Issuer's Distinguished-name.***

All self-signed Certificates have a serial number of zero. Signed Certificates have a serial number of one or higher. The serial number of a signed Certificates depends on the CA Certificate that signs it. The last used serial number for the CA Certificate is stored in the CA's profile. Any time a RACDCERT GENCERT with the SIGNWITH parameter command is entered, a Certificate is created and the serial number gets incremented. Given this algorithm, collisions can occur with the profile name if the signing Certificate is deleted and the signed Certificates do not get deleted. Collisions can also occur if CA Certificates are exported with their keys to multiple nodes where they will be allowed to continue creating server and client Certificates. The collisions are externalized with the IRRD109I message.

The lab is divided into several sections:

- ***Scenario 1 (Optional): Analyzing the Key Rings and Certificates in the Shared RACF Database***
- ***Scenario 2: Creating a new CA Certificate, a new server Certificate, new Key Rings at your MVS_n system.***
- ***Scenario 3: Testing your Certificates and Key Rings over a Secured FTP connection between MVS1 (FTP client) and your FTP Server at MVS_n.***
 - ***At the TCPIPT stack, the FTP server is “FTPTX”.***
 - ***At the TCPIPG stack, the FTP server is “FTPGX”.***

Scenario 0: Getting Started with the Lab

You have **three separate documents** for each lab:

- 1) A **Userids Sheet** that shows you your assigned MVS system, userid, password, and more.
- 2) **Diagrams** that contain a page for your assigned userid or team which explains the configuration of your TCP/IP stack.
- 3) 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 illustrate 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:
 - 1) **MVS****n****CS** (where “n” is the suffix of the MVS/ZOS system).
5. If you do not see such an icon, create a PCOMM session to connect to TN3270 at TCPIP/ on your assigned MVS system. You should be telnetting into TCPIP/ on your MVS system at **192.168.20.8n** (where “n” is the suffix of the MVS/ZOS system).
 - 1) Team 20x telnets as User20x to TCPIP1 in MVS2 at **192.168.20.82**
 - 2) Team 30x telnets as User30x to TCPIP1 in MVS3 at **192.168.20.83**
 - 3) Team 40x telnets as User40x to TCPIP1 in MVS4 at **192.168.20.84**
 - 4) Team 50x telnets as User50x to TCPIP1 in MVS5 at **192.168.20.85**
 - 5) Team 60x telnets as User60x to TCPIP1 in MVS6 at **192.168.20.86**
 - 6) Team 70x telnets as User70x to TCPIP1 in MVS7 at **192.168.20.87**
6. When you see the Message 10 screen from the TN3270 server, provide your userid with the logon command that has been built for this system. (The logon command is named “TSO”, but it is a VTAM LOGON nevertheless).
 - 1) **TSO <userid>**
7. On the ISPF signon screen, provide the password you were given in class.
 - 1) **<password>**
 - 2) **Press ENTER**
8. Move to the SDSF log screen when you see the **READY** prompt:
 - 1) **ispf d.log**
9. Use your team’s page from the **Diagrams** to verify that your TCP/IP stack is running with the correct network interfaces and IP addresses:
 - 1) **For TCPIPT Teams: /d tcpip,tcpiPT,n,home**
 - 2) **For TCPIPG Teams: /d tcpip,tcpiPG,n,home**
10. Notify instructor if the output is not correct for your assigned TCP/IP stack.

Scenario 1 (Optional): Analyzing Some Key Rings and Certificates in the Shared RACF Database

If you feel that you already understand x.509 certificate contents well enough without having to review your knowledge, you may skip the rest of Scenario 1 and proceed to Scenario 2 of this lab handout, where you will create and test your own certificates.

1. Move to the ISPF command options screen. Enter the following at the SDSF Command Line:
 - a. = 6

- Later in this lab you will create YOUR OWN CA and FTP Server Certificates for use with “SSL Server Authentication.”
- For now, examine entirely different Certificates and Key Rings that are used for “SSL Server and Client Authentication.” **We want you to understand the contents of the Key Rings and Certificates if you are unfamiliar with this material or need a refresher course.**
- You will be examining:
 - An FTP Server’s Key Ring that contains the Server’s Personal Certificate and the Certificate of the Certificate Authority (CA) that signed the FTP Server’s Certificate..
 - A Client Key Ring that contains the Client’s Personal Certificate and the Certificate of the CA that signed the Client’s Certificate.
 - For Server Authentication only, a Client Key Ring need contain only the CA Certificate or Certificates that have signed any Server Certificates the Client may receive during SSL/TLS/AT-TLS Negotiation and Authentication.
 - For Client and Server Authentication, a Client Key Ring must contain the Client’s Personal Certificate and the CA Certificate or Certificates that have signed its Personal Certificate and that of any Server Certificates the Client may receive during SSL/TLS/AT-TLS Negotiation and Authentication.

2. Enter the command to see which Certificates the USER ID of “TCPIP” owns:
 - a. **RACDCERT ID(TCPIP) LIST**

- We have already authorized your USER IDs in RACF to perform certain RACDCERT LIST commands.

3. Answer the following questions about the following FTP Server Certificate owned by the USER ID named "TCPIP." (Label is "FTP on ANY ZOS".)
 - a. Does the Certificate have a unique Certificate number? _____
 - b. Is the Certificate in TRUST Status? _____
 - c. What is the Serial Number assigned by the CA issuer? _____
 - d. What is the Issuer's Name, that is, who signed this Certificate? _____
 - e. What is the Subject's Full Distinguished Name (in sequence)?
>CN=_____.WSC.LABS.IBM.COM.O=IBM.C=US<
 - f. What is the size of the keys in the PKI key pair? _____
 - g. Is this certificate associated with a Private Key? _____
 - h. What Key Ring is the certificate connected to (owner/ringname)?
i. _____ / _____
4. Terminate the display of the remaining certificates with an **ATTENTION** by pressing the **ESC** key of your TN3270 keyboard.
 - a. Then press **ENTER** to return to ISPF option 6.
5. Display the Key Ring that this particular FTP Certificate resides on and remember that the certificate names and rings are case-sensitive:
 - a. **RACDCERT ID(FTPD) LISTRING(ServerRing1)**
NOTE: If a process or a user owns the Key Ring, this process or user may reference the Key Ring without including the Key Ring's owner ID as part of the Key Ring name:
 1. Example: "ServerRing1"*NOTE: If a process or a user does not own the Key Ring, this process or user must reference the Key Ring by including the Key Ring's owner ID as part of the Key Ring name:*
 2. Example: "FTPD/ServerRing1"
6. **Fill in the missing information** about "Cert Owner" from the display that you see:

Certificate Label Name	Cert Owner	USAGE	DEFAULT
-----	-----	-----	-----
FTP on ANY ZOS	ID (_____) PERSONAL		YES
WSC LABS Certificate Authority	CERTAUTH CERTAUTH		NO

- A Started Task -- like an FTP -- is associated with an OMVS segment assigned to a USER ID.
- If the Started Task is to own a PERSONAL certificate, that certificate must be owned by the Started Task's USER ID.
- The FTP servers that you will be working with on z/OS are owned by "TCPIP." That is, this FTP Server's Started Task is associated with user id "TCPIP."
- Therefore, the x.509 Certificate must also be owned by "TCPIP" as you see in the display above.

7. Enter the command to see which PERSONAL Certificates the USER ID of USER13 owns and which Key Rings this Certificate is associated with:
 - a. **RACDCERT ID(USER13) LIST**
8. Looking at only the first certificate in the display, answer the following questions about USER13's PERSONAL Certificate:
 - a. **Does the Certificate have a unique Certificate number?** _____
 - b. **Is the Certificate in TRUST Status?** _____
 - c. **What is the Serial Number assigned by RACF, the CA issuer?** _____
 - d. **What is the Issuer's Name, that is, who signed this Certificate?** _____
 - e. **What is the Subject's Full Distinguished Name (in sequence)?**
 >CN=USER_____.WSC.LABS.IBM.COM.O=IBM.C=US<
 - f. **What is the size of the keys in the PKI key pair?** _____
 - g. **Is this certificate associated with a Private Key?** _____
 - h. **What Key Rings is the Certificate connected to ("owner"/"ringname")?**
 - i. _____ / _____
 - ii. _____ / _____
9. Terminate the display of the remaining certificates with an **ATTENTION** by pressing the **ESC** key of your TN3270 keyboard.
 - a. Then press **ENTER** to return to ISPF option 6.
10. Enter the command to see what is on one of the Key Rings that USER13's Certificate is connected to:
 - a. **RACDCERT ID(USER13) LISTRING(LabClientRing)**

Digital ring information for user USER13:

Ring:

>LabClientRing<

Certificate Label Name	Cert Owner	USAGE	DEFAULT
USER13 on ANY ZOS	ID (USER13)	PERSONAL	YES
WSC LABS Certificate Authority	CERTAUTH	CERTAUTH	NO

11. Answer the following questions about this Key Ring:
 - a. **How many default Certificates are on the ring?** _____
 - b. **Who owns the default Certificate?** _____
 - c. Can the owner of this default Certificate find his Certificate by pointing to the Key Ring name alone? **Yes or No?**

 - d. **How many CA Certificates are on the ring?** _____
12. Normally a client ring must also contain a copy of the CA Certificate of the Server and so we should be seeing **two CA Certificates** on this ring: one CA that signed the FTP Server certificate and one CA Certificate that signed the USER13 certificate. Why is there **only one CA Certificate on this ring?**
 - a. *Because the same CA Certificate has signed both the Personal Server Certificate and the Personal Client Certificate.*
13. Notice the RACF Label of the CA Certificate on this Key Ring:
 - a. "WSC LABS Certificate Authority"
 - b. This is the same CA Certificate that was on the FTP server Key Ring that you displayed earlier.
 - c. You will display the contents of USER13's Certificate later. But, for now...
14. Enter the command to see what is on the other client Key Ring:
 - a. **RACDCERT ID(FTPD) LISTRING(ClientRing1)**
15. Answer the following questions about this Key Ring:
 - a. **Who owns this Key Ring?** That is, which user id is associated with this Key Ring? _____
 - b. **How many default Certificates are on the ring?** _____
 - c. **Who owns the default Certificate?** _____
NOTE: The owner of the default certificate identifies only the Key Ring in his security definitions in order to find the certificate he should use. He does not have to specify a certificate label to find his Certificate.
 - d. **How many individual user clients can point to this Key Ring if they are permitted to the Key Ring and are asked to present a client Certificate?**
 - i. _____
 - e. **How do the other users of this Key Ring have to identify their Certificate if they cannot use the DEFAULT certificate?**
 - i. *They must identify their own Certificate by specifying the Label name of the Certificate.*
 - f. **How many CA Certificates are on the ring?** _____
16. Now issue the command to see the contents of the Certificate Authority Certificate that signed your Client Certificate and the FTP Server Certificate:
 - a. **RACDCERT CERTAUTH LIST (LABEL('WSC LABS Certificate Authority'))**
 - i. You have CONTROL access to the facility class IRR.DIGTCERT.LIST and should be able to execute this command.

17. Answer these questions about the Certificate Authority Certificate:
- a. **Does the Certificate have a unique Certificate ID?** _____
 - b. **Is the Certificate in TRUST Status?** _____
 - c. **What is the Serial Number assigned to this Root CA Certificate?** _____
 - d. **What is the Issuer's Name?**
 - ii. >CN=_____.LABS.IBM.COM.O=MVS1 CA.C=US<
 - e. **What is the Subject's Name?**
 - iii. >CN=_____.LABS.IBM.COM.O=IBM.C=US<
 - f. **What is this Certificate used for?** (That is, what is its "Key Usage"?)

 - g. **What is the size of the Private Key?** _____
 - h. **Does this CA Certificate reside on the FTP Client Ring owned by USER13?** (The name of this Key Ring is "USER13/LabClientRing.") _____
 - i. **Does this CA Certificate reside on the Server Ring named "FTPD/ServerRing1" which is owned by user id FTPD?**

18. **Why do the ServerRing1 and the LabClientRing require only one CA Certificate** when one usually sees the CA Certificate that has signed the client certificate and another CA Certificate that has signed the server certificate on a single ring?
- j. *Because the same CA Certificate has signed both the Personal Server Certificate and the Personal Client Certificate.*
19. **Press ENTER to review the other Key Rings on which this CA Certificate resides.** With the last ENTER you will be returned to ISPF Option 6.

End of Scenario 1

Scenario 2: Building Certificates and Key Rings of Your Own for Server Authentication

1. Enter the ISPF Data Set List Utility screen from the ISPF command line entry:
 - a. = **3.4**
2. At the “User DSName Level” enter the name of your dataset:
 - a. **USER.CS.SOURCE**
 - b. Press **ENTER**
3. Select USER.CS.SOURCE with an “m” in the left-hand column:

DSLST - Data Sets Matching USER.CS.SOURCE
Command ==>

Command - Enter "/" to select action

m USER.CS.SOURCE

- a. Then press **ENTER**.
4. You may see many members here, some of which do not apply to the current lab. However, you must find the following members in the dataset:
 - a. ACFTTn0x **or** ACFTGn0x (“n0x” is Team Suffix: n01 or n02)
 - b. ACMCTn0x **or** ACMCGn0x (“n0x” is Team Suffix: n01 or n02)
 - c. ACRNTn0x **or** ACRNGn0x (“n0x” is Team Suffix: n01 or n02)
5. *If you do not see the aforementioned members, immediately ask your Instructor to correct this omission.*
6. Next, one by one, you will edit YOUR team’s members. Do not edit until you are asked to do so in this booklet. **PAY ATTENTION TO THE MEMBERS YOUR USER ID IS TO EDIT!!!!**

- a. Instructions for User IDs **USER201** – **USER701** assigned to TCPIPT stack:

_____ ACFT**T**n01 (“n” is MVS number)
_____ ACMC**T**n01 (“n” is MVS number)
_____ ACRN**T**n01 (“n” is MVS number)

- b. Instructions for User IDs **USER202** – **USER702** assigned to TCPIPG stack:

_____ ACFT**G**n02 (“n” is MVS number)
_____ ACMC**G**n02 (“n” is MVS number)
_____ ACRN**G**n02 (“n” is MVS number)

7. Now begin editing. First, edit the job for a Certificate Authority (CA) that will sign your Server Certificate:
 - a. Edit either **ACMCTⁿ⁰¹** or **ACMCGⁿ⁰²**.
 - i. **Change** all the “- - -” **characters** in the skeleton to the last three digits of your User ID.
 - ii. **Replace** the “NOTBEFORE” date with today’s date.
 - iii. **Replace** the IP “ALTNAME” of **10.1.1.¹ⁿ** or **10.1.1.²ⁿ** with the correct DynamicXCF HiperSockets (IQDIO) address in your TCP/IP stack.
 - iv. **Re-examine** the RACDCERT commands to **verify your changes** and to **understand what the commands** are generating.
8. Submit the job by entering at the command line:
 - a. **sub**
 - i. **Even if you receive a Return Code of 0, there could still be something wrong on an individual command. Always examine your output!**
9. Examine the output
 - a. **=d.o**
Select your submitted job with “s” and verify that the Certificate Status is **TRUST**
 - i. If NOTRUST, ask the instructor for help.
10. Examine the rest of the output and determine if any commands failed to run because of missing authority.
 - 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.**
 - b. Since you do not have authority to issue SETROPTS, please submit the PROC that will do this on your behalf.
 - i. **=d.log**
 - ii. **/s specuser**
11. **While you are at the console, display the owner of the existing FTP Started Tasks** on these MVS systems. (All the FTP Started Tasks are owned by the same User ID, a fact you must know to generate the Personal Certificate of the FTP server assigned to your team.)
 - a. **/d a,ftp***
 - b. **Example of Output:**

```

D A,FTP*
IEE115I 10.02.31 2012.267 ACTIVITY 595
JOBS      M/S    TS USERS    SYSAS    INITS    ACTIVE/MAX VTAM    OAS
00006    00012    00001    00031    00022    00001/00030
00014
FTPCC11  STEP1    TCPIP    OWT  AO  A=0037  PER=NO  SMC=000
                PGN=N/A  DMN=N/A  AFF=NONE
                CT=000.019S  ET=00263.55
                WUID=STC11395  USERID=TCPIP
  
```

- c. **With which OMVS Segment and USER ID is the Started Task associated?**
 - i. **HINT: The *TS USERS* column and the *USERID=* field provide this answer.**

12. Return with =3.4 to USER.CS.SOURCE.

13. Next create the Server Certificate for your FTP Server and sign it with the CA Certificate that you just created.

- a. **Edit either ACFTT*n01* or ACFTG*n02***
 - i. **Change** all the “---“ characters in the skeleton to the last three digits of your user id.
 - ii. **Replace the IP “ALTNAME” of 10.1.1.*1n* or 10.1.1.*2n*** with the correct DynamicXCF HiperSockets (IQDIO) address in your TCP/IP stack.
 - iii. **Replace the “NOTBEFORE” date** with today’s date.
 - iv. **Re-examine the RACDCERT commands to verify your changes and to understand what the commands are generating!**
 - 1. *For example, the User ID of “TCPIP” must own this Certificate because it will be used by the FTPTX or FTPGX procedure.*

- o We have already authorized your User IDs in RACF to perform certain RACDCERT commands contained in this JCL.

14. Submit the job by entering at the command line:

- a. **sub**
 - i. **Even if you receive a Return Code of 0, there could still be something wrong on an individual command. Always examine your output!**
- b. **=d.o**
- c. Select your submitted job with “s” and verify that the Certificate Status is **TRUST**
 - i. If NOTRUST, ask the instructor for help.

15. Examine the output and determine if any commands failed to run because of missing authority.

- 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.***
- b. **Since you do not have authority to issue SETROPTS, please submit the PROC that will do this on your behalf.**
 - i. **=d.log**
 - ii. **/s specuser**

16. Return with =3.4 to USER.CS.SOURCE

17. Finally, **create** the Key Rings for the Client at MVS1 and the FTP Server at your MVS*n*. Then **connect** the appropriate certificates to the Key Rings.

- a. **Edit either ACRNTⁿ⁰¹ or ACRNGⁿ⁰²**
 - i. **Change** all the “---“ **characters** in the skeleton to the last three digits of your User ID.
 - ii. **Re-examine** the RACDCERT commands to verify your changes and to understand what the commands are generating!
 - 1. **These commands can be confusing because TWO USER IDs are named in the RACDCERT CONNECT command:**
 - a. **The USER ID / OWNER of the Key Ring**
 - b. For connecting a CA Certificate, “**CERTAUTH**” identifies the CA Certificate’s Label.
 - c. For connecting a Personal Certificate, “**ID(TCPIP)**” identifies the Personal Server Certificate’s Label.

- o We have already authorized your USERIDs in RACF to perform certain RACDCERT commands contained in this JCL.

- 18. Submit the jobs by entering at the command line:
 - a. **sub**
 - b. Then use **PF3 to save and exit** the member under your name.
- 19. Examine the output and determine if any commands failed to run because of missing authority.
 - 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.**
 - b. **Since you do not have authority to issue SETROPTS, please submit the PROC that will do this on your behalf.**
 - i. **=d.log**
 - ii. **/s specuser**

End of Scenario 2

Scenario 3: Testing your Certificates and Key Rings over Secured FTP Connections

You will be testing using an AT-TLS implementation of SSL/TLS. This means that...

- a. We have already created AT-TLS policies using the z/OS Communications Server Configuration Assistant.
 - b. We have started the TCP/IP stacks with TLS capability.
 - c. Policy Agent has loaded the policies for your FTP Client and FTP Server into the running TCP/IP stacks on the MVS systems.
 - d. We have created the FTP Client parameter file ("FTPCLSEC") and a parameter file ("FTPSAUTH") for your FTP server. You will initiate the FTPTX or the FTPGX Server on YOUR MVS_n and then test the connection and the Key Rings from MVS1.
1. Verify that the Policy Agent Procedure is running at your MVS_n, *where you should still be in the log (=d.log)*:
 - a. **/d a,pagantt**
 - i. If it is not running, please start it
 1. **/s pagantt**
 2. Verify that the your test TCP/IP stack is running with the command:
 - a. **/d tcpip**
 - i. **User IDs of USER_{n01} work with the TCPIPT stack.**
 - ii. **User ids of USER_{n02} work with the TCPIPG stack.**
 - b. If either stack is not running, advise the instructor to start the stack.
 3. At your MVS_n, you will recycle the Secure version of the FTP Server with affinity to your TCP/IP stack and point to the Server's **FTP.DATA** parameter file that we customized for you. First determine if your FTP server is active:
 - a. **/d a,ftp_{TX}*** or **/d a,ftp_{GX}***
 - a. to determine if the FTPTX or FTPGX Server is running
 - b. **CAREFUL: Look only for your assigned FTP-X Server.**
Other Servers should continue to run if they are up:
 - i. FTPCCL1 (leave this one up)
 - ii. FTPT1 (leave this one up)
 - iii. FTPG1 (leave this one up)
 - b. **/p FTP_{TXI}** or **/p FTP_{GXI}** (bring down FTPTX or FTPGX server – UNIX forked address space -- if it is running)
 - a. **Wait for the FTP server to end before proceeding.**

IMPORTANT: In the next step you will start the FTP server again. For this lab, it is quicker to recycle the FTP Server in order to pick up the changed Key Rings and Certificates. If we were teaching you AT-TLS operations, we would only need to update the "instance ID" in the AT-TLS policy in order to load the refreshed Key Ring.

- c. **/s FTP_{TX}** or **/s FTP_{GX}**

4. Verify that your FTP server is running on Port 2021:
 - a. If you are **USERn01**:
 - a. **/D TCPIP,TCPIP,T,N,CONN,SERVER** (affinity with **TCPIPT**)

USER ID	CONN	LOCAL SOCKET	FOREIGN SOCKET	STATE
BPXOINIT	00000017	0.0.0.0..10007	0.0.0.0..0	LISTEN
FTPTX1	000015F4	0.0.0.0..2021	0.0.0.0..0	LISTEN <<

- b. If you are **USERn02**:
 - a. **/D TCPIP,TCPIPG,N,CONN,SERVER** (affinity with **TCPIPG**)

USER ID	CONN	LOCAL SOCKET	FOREIGN SOCKET	STATE
BPXOINIT	00000011	0.0.0.0..10007	0.0.0.0..0	LISTEN
FTPGX1	000015F0	0.0.0.0..2021	0.0.0.0..0	LISTEN <<

5. Display which traces are running for the FTP Server:
 - a. **/F FTPTX1,DEBUG=? **or** /F FTPGX1,DEBUG=?**
 - i. **Which traces are running?**

6. Enable access, basic, and security tracing at the FTP Server:
 - a. If you are **USERn01**:
 - i. **/F FTPTX1,DEBUG=(ACC,BAS,SEC)**
 NOTE: Later ... not now ... you will disable the trace with
 1. **F FTPTX1,DEBUG=(NONE)**
 - b. If you are **USERn02**:
 - i. **/F FTPGX1,DEBUG=(ACC,BAS,SEC)**
 NOTE: Later ... not now ... you will disable the trace with
 1. **F FTPGX1,DEBUG=(NONE)**

7. Next move to a second TN3270 emulator session **that is connected to MVS1, which is NOT your assigned MVS system.**

- a. You should be telnetting into **MVS1 (ZOS1)** at **192.168.20.81**.

8. When you see the Message 10 screen from the TN3270 server, provide your User ID with the logon command that has been built for this system. (The logon command is named "TSO", but it is a VTAM LOGON nonetheless.)

- a. **TSO <userid>** (User id is "**USERn0x**")

9. On the ISPF signon screen, provide the password you were given in class.

- a. **<password>** (Use standard password.)
 - b. Press **ENTER**

10. Move to the Console of MVS1:

- a. **ISPF D.LOG**

11. User**n01**: Verify that TCPIPT and PAGENTT are running:

- a. At command line: **/D A,L**
 - i. **Examine** the display to verify that the procedures are running.
 - ii. If they are not, advise the instructor to start them.

12. User **n02**: Verify that TCPIP **G** and PAGENTT are running:
 - a. At command line: **/D A,L**
 - i. **Examine** the display to verify that the procedures are running.
 - ii. If they are not, advise instructor to start them.

13. At the command line, move to Option 6 of ISPF:

- a. **=6**

14. On the command line of **MVSI**, enter the following FTP client command as a client of the TCPIP **T** or TCPIP **G** stack.

Request that AT-TLS point to the FTP Client Data File (which specifies AT-TLS security is allowed), connect to the dynamically created DynamicXCF HiperSockets address in your own MVS system as the Source IP address, **and specify the FTPTX or FTPGX Server port of 2021!**
DO NOT LOGIN to the FTP SESSION until you answer the initial questions further below.

- a. *If you are User **n01** on the TCPIP **T** stack:*

```
FTP -r TLS -f "//SYS1.CS.TCPPARMS(FTPCLSEC)" -p
TCPIPT
-s 10.1.1.11 10.1.1.1n 2021
```

("n" is last digit of YOUR MVSn's dynamicXCF HiperSockets address)

- b. *If you are User **n02** on the TCPIP **G** stack:*

```
FTP -r TLS -f "//SYS1.CS.TCPPARMS(FTPCLSEC)" -p
TCPIPG
-s 10.1.1.21 10.1.1.2n 2021
```

("n" is last digit of YOUR MVSn's dynamicXCF HiperSockets address)

NOTE: Whether or not the connection fails, "quit" and re-execute the command -- with tracing (debugging= "-d") enabled -- as follows:

- a. At TCPIP **T**: `ftp -r TLS -d -f "//sys1.cs.tcparms(ftpclsec)" -p TCPIPT -s 10.1.1.11 10.1.1.1n 2021`
- b. At TCPIP **G**: `ftp -r TLS -d -f "//sys1.cs.tcparms(ftpclsec)" -p TCPIPG -s 10.1.1.21 10.1.1.2n 2021`

15. Examine the Client Connection Messages that you receive **before you login**.

- a. Note the messages about the AT-TLS policies for the client.
- b. Note the >>> AUTH TLS message that appears.
- c. Answer the following questions – the messages appear if you have coded DEBUG SEC in the client's FTP data file:
 - i. **What version of SSL or TLS has been negotiated?** _____
 - ii. **What cipherspec was chosen?** _____
 - iii. **Has FTP with AT-TLS been enabled for FIPS-140?** _____
 - iv. **What is the meaning of this cipherspec? (e.g., AES, or DES or 3DES, or??)** _____

RESPONSE : This is documented in the z/OS Cryptographic Services System SSL Programming at

<http://publib.boulder.ibm.com/infocenter/zos/v1r13/index.jsp?topic=%2Fcom.ibm.zos.r13.gska100%2Fcsdcwh.htm>

0A 168-bit Triple DES encryption with SHA-1 message authentication and RSA key exchange

16. Next login to the FTP session with your user id and password.
 - a. **<USER n 0x>**
 - b. **<password>**
 - c. **ENTER**
 - a. We have specified the following in the Client Data File to capture messages in the SYSLOGD log:
 - i. **DEBUG SEC ; security processing**
 - ii. **LOGCLIENTERR TRUE ; Report err EZZ9830I**
 - b. NOTE: We are collecting error messages for AT-TLS in /var/CSLOG/syslogall.log.
 - c. NOTE: We have already raised the AT-TLS trace level for this exercise to a value of **255** in order to examine the SSL error Return Codes. Once this system is moved into production, you would want to lower the tracing level in order to improve performance.
17. Issue the “dir” command to test the data connection.
 - a. **dir**
18. Issue the command to view the connection status from the client perspective:
 - a. **locstat**
 - i. Find the security messages on the last screen that prove this is a secure connection:
EZA2889I Authentication mechanism: TLS
EZA2890I Control connection protection: Private
EZA2891I Data connection protection: Private
EZA2860I Secure Hostname is: OPTIONAL
19. Issue the command to view the connection status from the server perspective:
 - a. **status**
 - i. Find the 211 response messages that prove this is a secure connection.
211-Authentication type: TLS
211-Control protection level: Private
211-Data protection level: Private
211-TLS security is supported at the RFC4217 level
20. While your FTP connection is still running, **return to your own MVS console log at MVS n** and issue the command to see if TTLS sessions are running:
 - a. **/D TCPIP,TCPIPT,N,TTLS or /D TCPIP,TCPIPG,N,TTLS**
 - b. **What is the session count (“CONNS”)?** _____
21. Display the connections and Connection ID associated with your FTP server:
 - a. **/D TCPIP,TCPIPT,N,CONN,CLIENT=FTP TXI or**

- b. /D TCPIP,TCPIP,N,CONN,CLIENT=FTP**GX**I
- i. **Example:** The connection ID in the display below is “15FF”

```
D TCPIP,TCPIPT,N,CONN,CLIENT=FTPTX1
EZZ2500I NETSTAT CS V1R12 TCPIPT 144
USER ID  CONN      LOCAL SOCKET      FOREIGN SOCKET      STATE
FTPTX1   000015FF  10.1.1.12..2021   10.1.1.11..1085    ESTBLSH
FTPTX1   000015C0  0.0.0.0..2021    0.0.0.0..0         LISTEN
2 OF 2 RECORDS DISPLAYED
END OF THE REPORT
```

- c. Write down the connection id (“xxxx”) of your connection, because you will need it in the next step: _____
22. Then issue the details connection display for this Connection ID “xxxx”:
- a. /D TCPIP,TCPIP,N,TTLS,CONN=xxxx,DETAIL ****or****
- b. /D TCPIP,TCPIP,N,TTLS,CONN=xxxx,DETAIL
23. Examine the output and answer these question:
- a. Which version of TLS is this connection exploiting? TLS V _____
- b. Is the connection abiding by FIPS140 standards? _____
- c. Which 2-digit Cipher Type is the connection using for encryption?
- _____
- i. What cryptographic algorithm is indicated? _____
- d. What is the name of the AT-TLS Rule that the Server is using?
- i. TTLSRULE: FTP_X____@2021@10.1.1.____/24
- e. What Key Ring name is defined in the AT-TLS Policy Rule?
- i. KEYRING: _____FTPD/FTPXACME_____
- _____RING

Sample Output from Command:

```
D TCPIP,TCPIPT,N,TTLS,CONN=15FF,DETAIL
EZD0101I NETSTAT CS V1R12 TCPIPT 146
CONNID: 000015FF
JOBNAME:      FTPTX1
LOCALSOCKET:  10.1.1.12..2021
REMOTESOCKET: 10.1.1.11..1085
SECLEVEL:     TLS VERSION 1.1
CIPHER:       0A TLS_RSA_WITH_3DES_EDE_CBC_SHA
CERTUSERID:   N/A
MAPTYPE:      PRIMARY
FIPS140:      OFF
TTLSRULE: FTPTXn010N2021@10.1.1.12/24 4
PRIORITY:     252
LOCALADDR:    10.1.1.12
LOCALPORT:    2021
REMOTEADDR:   10.1.1.11
REMOTEPORTFROM: 1024      REMOTEPORTTO: 65535
DIRECTION:    INBOUND
TTLSGRP ACTION: GACT1
GROUPID:      00000004
TTLSENABLED:  ON
CTRACECLEARTEXT: OFF
TRACE:        7
SYSLOGFACILITY: DAEMON
SYSLOGFACILITY: DAEMON
SECONDARYMAP:  OFF
FIPS140:      OFF
```

```

TTLSENVACTION:  EACT4 FTPXSRV23_P2021_TCPIPT
ENVIRONMENTUSERINSTANCE:  0
HANDSHAKEROLE:  SERVER
KEYRING:  FTPD/FTPXACME23_RING
SSLV2:  OFF
SSLV3:  ON
TLSV1:  ON
TLSV1.1:  ON
RESETCIPHERTIMER:  0
APPLICATIONCONTROLLED:  OFF
HANDSHAKETIMEOUT:  10
TRUNCATEDHMAC:  OFF
CLIENTMAXSSLFRAGMENT:  OFF
SERVERMAXSSLFRAGMENT:  OFF
CLIENTHANDSHAKESNI:  OFF
SERVERHANDSHAKESNI:  OFF
CLIENTAUTHTYPE:  REQUIRED
CERTVALIDATIONMODE:  ANY
TTLSCONNCTION:  CACT1
HANDSHAKEROLE:  SERVER
V3CIPHERSUITES:  0A TLS_RSA_WITH_3DES_EDE_CBC_SHA
                  2F TLS_RSA_WITH_AES_128_CBC_SHA

CTRACECLEARTXT:  OFF
TRACE:  255
APPLICATIONCONTROLLED:  ON
SECONDARYMAP:  ON
1 OF 1 RECORDS DISPLAYED
END OF THE REPORT

```

24. Log off the FTP session on MVS1:

a. **Quit**

25. Enter OMVS at MVS1 to view the Syslog Daemon log for messages about the client FTP connection:

a. **tso omvs**

b. **su**

c. **obrowse /var/CSLOG/syslogall.log**

26. Toward the bottom of the log, look for messages relating to your connection to 10.1.1.1n or 10.1.1.2n.

a. **f 10.1.1.1n or f 10.1.1.2n**

27. You have just completed testing the Secure FTP Server on your MVS_n system.

28. Exit OMVS:

a. **Exit** twice and press **ENTER**

29. **Log off** MVS1 and return to your own MVS_n system.

30. At your own MVS_n, browse the SYSLOG Daemon log to see if there are any messages about your FTP session.

a. **tso omvs**

b. **su**

i. **obrowse /var/syslogall.log** (or possibly: **obrowse /var/CSLOG/syslogall.log**)

31. Exit OMVS:

- c. After looking at the log **Exit** twice and press **ENTER**
- 32. When you have finished, return to the MVS console display and disable the FTP Server tracing:
 - a. = **D.LOG**
 - b. /F **FTPTX1,DEBUG=(NONE)** or /F **FTPGX1,DEBUG=(NONE)**
- 33. Log off MVS. **CONGRATULATIONS! Your Certificates and Key Rings are working and you have successfully finished this lab.**

End of the Lab

If you like and have time, proceed to the advanced lab that involves ... RENEWING CERTIFICATES and

APPENDIX: Lab Documentation

Scenario 1: Documentation for Certificate Lab

Output from: racdcert ID(USER22) list

Digital certificate information for user USER22:

```

Label: USER22 on ANY ZOS
Certificate ID: 2Qbk4sXZ8vLk4sXZ8vJAlpVAwdXoQOnW4kBA
Status: TRUST
Start Date: 2009/08/05 00:00:00
End Date: 2013/02/09 23:59:59
Serial Number:
    >04<
Issuer's Name:
    >CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
Subject's Name:
    >CN=USER22.WSC.LABS.IBM.COM.O=IBM.C=US<
Subject's AltNames:
    EMail: USER22 at WSC.LABS.IBM.COM
Private Key Type: Non-ICSF
Private Key Size: 1024
Ring Associations:
    Ring Owner: FTPD
    Ring:
        >ClientRing1<
    Ring Owner: USER22
    Ring:
        >LabClientRing<

```

Output from: racdcert ID(USER22) listring(LabClientRing)

racdcert id(USER22) listring(LabClientRing)

Digital ring information for user USER22:

```

Ring:
    >LabClientRing<
Certificate Label Name      Cert Owner      USAGE      DEFAULT
-----
USER22 on ANY ZOS          ID(USER22)      PERSONAL    YES
WSC LABS Certificate Authority CERTAUTH        CERTAUTH    NO

```

Output from: racdcert certauth list(label('WSC LABS Certificate Authority'))

racdcert certauth list(label('WSC LABS Certificate Authority'))

Digital certificate information for CERTAUTH:

```

Label: WSC LABS Certificate Authority
Certificate ID:
2QiJmZmDhZmjgebiw0DTwcLiQMOFmaOJhomDgaOFQMGko4iWmYmjQEBA
Status: TRUST
Start Date: 2009/02/09 00:00:00
End Date: 2013/02/09 23:59:59
Serial Number:
    >00<
Issuer's Name:

```

```

      >CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
Subject's Name:
      >CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
Subject's AltNames:
      IP: 192.168.20.0
      EMail: ZOS at WSC.LABS.IBM.COM
      Domain: WSC.LABS.IBM.COM
Key Usage: CERTSIGN
Private Key Type: Non-ICSF
Private Key Size: 1024
Ring Associations:
      Ring Owner: FTPD
      Ring:
        >ClientRing1<
      Ring Owner: FTPD
      Ring:
        >ServerRing1<
      Ring Owner: USERnx
      Ring:
        >LabClientRing<

```

Scenario 2: CERTIFICATE LAB: Jobs Run for FTP_X Certificate Creation Lab with AT-TLS

JCL: CA Certificate for Signing FTP_X Server Certificates

```

***** Top of Data *****
//ACMECA13 JOB MSGCLASS=X,NOTIFY=&SYSUID
//ACMECA13 EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//*****
//*      Create Certificate Authority for Certificate Creation LAB      *
//*      THIS CA SIGNS THE SERVER CERTIFICATES                        *
//*      CHANGE ALL "--" Characters to your team Suffix                *
//*      CHANGE THE ALTNAME IP ADDR 4TH OCTET TO 101 through 107      *
//*      START CERTIFICATE VALIDITY TODAY; END IN 6 MONTHS            *
//*****
//*****
//*      USERIDS, HFS Datasets, UNIX directories created with        *
//*      (JOB ADDUSER)                                                *
//*      FTP These files to other z/OS Systems                        *
//*      FTP with  BINARY, RECFM=VB, LRECL=84, BLOCKSIZE=27998      *
//*****
//*****
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
RACDCERT  CERTAUTH  GENCERT
            SUBJECTSDN (O('ACME')
                        CN('ACMECA13')
                        C('US'))
            ALTNAME (IP(10.1.1.11)
                     DOMAIN('ACME.LABS.IBM.COM')
                     EMAIL('ACMECA13@ACME.LABS.IBM.COM'))
            NOTBEFORE (DATE(2012-09-22))
            NOTAFTER (DATE(2020-09-22))
            KEYUSAGE (CERTSIGN)
            SIZE(1024)
            WITHLABEL('ACME13 CACERT')
            setropts raclist(DIGTCERT) refresh
            racdcert CERTAUTH list(label('ACME13 CACERT'))
/*
      F1=Help      F3=Exit      F4=Return      F5=Rfind      F12=CRetrieval
***** Bottom of Data *****

```

JCL: FTP_X Server PERSONAL Certificate

```

***** Top of Data *****
//ACFTPX13 JOB MSGCLASS=X,NOTIFY=&SYSUID
//ACFTPX13 EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//*****
//*      Create Individual Personal Certificate for FTP Server
//*****
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(TCPIP) GENCERT
      SUBJECTSDN (CN('FTPXSRV13'))
      OU('ACME')
      C('US'))
      ALTNAME (IP(10.1.1.11)
              DOMAIN('ACME.LABS.IBM.COM')
              EMAIL('FTPX13@ACME.LABS.IBM.COM'))
      NOTBEFORE(DATE(2012-09-22))
      NOTAFTER(DATE(2016-09-22))
      WITHLABEL('FTPXSRV13 CERT')
      SIZE(1024)
      SIGNWITH(CERTAUTH
      Label('ACME13 CACERT'))
      setropts raclist(DIGTCERT) refresh
      racdcert ID(TCPIP) list(label('FTPXSRV13 CERT'))
/*
***** Bottom of Data *****

```

JCL: Creating Server and Client Key Rings and Connecting Certificates

```

***** Top of Data *****
*****
//ACRING13 JOB MSGCLASS=X,NOTIFY=&SYSUID
//ACRING13 EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//*****
//*      Create Client and Server Key Rings and Connect Certificates
//*****
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
RACDCERT ID(FTPD) ADDRING(FTPXACME13_RING)
RACDCERT ID(FTPD) CONNECT(ID(TCPIP) LABEL('FTPXSRV13 CERT'))
      RING(FTPXACME13_RING) USAGE(PERSONAL) DEFAULT)
RACDCERT ID(FTPD) CONNECT(CERTAUTH
      LABEL('ACME13 CACERT'))
      RING(FTPXACME13_RING) USAGE(CERTAUTH))
RACDCERT ID(USER13) ADDRING(FTPCLIENT_RING)
RACDCERT ID(USER13) CONNECT(CERTAUTH
      LABEL('ACME13 CACERT'))
      RING(FTPCLIENT_RING) USAGE(CERTAUTH))
      setropts generic(DIGTCERT) refresh
      setropts raclist(DIGTCERT) refresh
      racdcert ID(FTPD) listring(FTPXACME13_RING)
      racdcert ID(USER13) listring(FTPCLIENT_RING)
/*

```

Scenario 3: FTP_X Procedure for Port 2021 and [FTP.DATA](#) Files

JCL: FTP_X Initialization Procedure

```
***** Top of Data *****
//FTPX PROC MODULE='FTPD',CS=SYS1,DATA=DAT&CL1.A,PARMS='PORT 2021'
//FTPD EXEC PGM=&MODULE,REGION=0M,TIME=NOLIMIT,
//      PARM=('POSIX(ON) ALL31(ON)',
//      'ENVAR("_BPXK_SETIBMOPT_TRANSPORT=TCPIPT"',
//      '"TZ=EST5EDT")/&PARMS')
/* THIS FTP PROC RUNS ON PORT 2021 FOR BASIC SERVER AUTHENTICATION
/* CS=USER
/* CS=SYS1
/* FDAT=FTPSAUTH (SERVER AUTHENTICATION ONLY)
/* FDAT=FTPDATA (NO AUTHENTICATION)
/* FDAT=FTPSEC (SERVER AND CLIENT AUTHENTICATION)
/* FTPT PROC MODULE='FTPD',CS=SYS1,PARMS=''
/* PARM=('POSIX(ON) ALL31(ON)',
/*
/* ENVAR("RESOLVER_CONFIG=/'TCPIVP.TCPPARMS(TCPDATA)'/")/&PARMS')
/*
/* PARM=('POSIX(ON) ALL31(ON) ENVAR("_BPX_JOBNAME=MYFTP")/',
/* '&PARMS')
/*
/* PARM=('POSIX(ON) ALL31(ON) ENVAR("KRB5_SERVER_KEYTAB=1")/',
/* '&PARMS')
/*
/*YSFTPD DD DISP=SHR,DSN=&CS..CS.TCPPARMS(&FDAT)
//CEEDUMP DD SYSOUT=*
//SYSFTPD DD DISP=SHR,DSN=&CS..CS.TCPPARMS(FTPSAUTH)
//SYSTCPD DD DISP=SHR,DSN=&CS..CS.TCPPARMS(&DATA)
***** Bottom of Data *****
```

[FTP.DATA](#) File for FTP_X 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.
```

Share in Pittsburgh, PA Session 16073

```

;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

```

FTP.DATA File for FTP_X 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
                                           ; FTP or ATTLS

TLSMECHANISM 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)

```

Share in Pittsburgh, PA Session 16073

```

; 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,
;                               ; (S) Specify what level of RFC 4217,
;                               ; On Securing ; FTP with TLS, is
;                               ; supported
;                               ; DRAFT (D) Internet Draft level
;                               ; RFC4217 RFC level

```

Answers

Scenario 1:

- 3.a. Yes, as per the Introduction, each certificate has a unique Certificate number per CA.
- 3.b. Yes
- 3.c. 36
- 3.d. >CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
- 3.e. FTP
- 3.f. 1024
- 3.g. Yes
- 3.h. FTPD/ServerRing1
- 6. TCPIP
- 8.a. Yes, as per the Introduction, each certificate has a unique Certificate number per CA.
- 8.b. Yes
- 8.c. 40
- 8.d. >CN=WSCCA.LABS.IBM.COM.O=IBM.C=US<
- 8.e. 13
- 8.f. 1024
- 8.g. Yes
- 8.h.i. FTPD/Clientring1
- 8.h.ii. USER13/LabClientRing
- 11.a. One
- 11.b. ID(USER13)
- 11.c. Yes
- 11.d. One
- 15.a. FTPD
- 15.b. One
- 15.c. ID(USER1)
- 15.d. All of them but all except USER1 must use the cert label name as well.
- 15.f. One
- 17.a. Yes
- 17.b. Yes
- 17.c. 008C
- 17.d. MVS1CA
- 17.e. WSCCA
- 17.f. CERTSIGN
- 17.g. 1024
- 17.h. Yes
- 17.i. Yes

Scenario 2:

- 11.c. TCPIP

Scenario 3:

- 5.a.i. None
- 15.c.i. TLSv1.1

15.c.ii. 0A
15.c.iii. No
15.c.iv. 3DES
20.b. 1
21.c. 64F
23.a. 1.1
23.b. No
23.c. 0A
23.c.i. 3DES
23.d.i. FTPTX201@2021@10.1.1.0/24~4
23.e.i. 201

