

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

**"Analyzing x.509 Digital Certificates and Creating
Certificates and Keyrings"**

Hands-on Lab Guide

(Digital Certificate Exercises)



Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

Revision date -

Friday, 20 June 2025

This edition applies to IBM z/OS Configuration Assistant running in z/OSMF on z/OS V3.1.

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.

Table of Contents

Table of Contents.....3

Part 0: Lab Description (Analyzing and Optionally Creating x.509 Digital Certificates)4

Specific Lab Description: Creating x.509 Certificates 4

Part 1: Analyzing the Keyrings and Certificates at your MVS.....5

End of Part 1..... 8

Part 2: Building Certificates and Keyrings of Your Own.....9

End of the Lab 11

Part 0: Lab Description (Analyzing and Optionally Creating x.509 Digital Certificates)

Each student ZOS (MVS) system has two TCP/IP stacks running in it. The basic TCPIP stack belonging to the instructors is named TCPIP1. The TN3270 procedure that has affinity to the instructor 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 ZOS 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 stack.

The student TCP/IP stack is named TCPIPT. The students customize this 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.

There are eight “Student ZOS (MVS) systems” that you will be working on.

Specific Lab Description: Creating x.509 Certificates

Each team on a single ZOS (MVS) system will examine the certificates used for the AT-TLS labs.

In this lab you will examine certificates and keyrings that have been created for a RACF Database that is shared by 9 MVS images: MVS1 through MVS9. You will then create individual certificates and keyrings on your MVS system that you will use in a later AT-TLS lab.

The RACF Database is shared between the 9 MVS Systems with shared Keyrings 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 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 gets 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 get externalized with the IRRD109I message.

The lab is divided into several sections:

- *Part 1: Analyzing the Keyrings and Certificates at your MVS System*
- *Part 2: Creating a new CA Certificate, a new server certificate, new keyrings at your MVS system.*

Part 1: Analyzing the Keyrings and Certificates at your MVS

1. If you have not already done so, create a PCOMM session to connect to TN3270 at TCPIP1 on your assigned MVS system.
 - a. You should be telnetting into TCPIP1 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**
 - i. Team 8x telnets as User8x to TCPIP1 in MVS8 at **192.168.20.88**
 - j. Team 9x telnets as User9x to TCPIP1 in MVS9 at **192.168.20.89**
2. 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.)
 - a. **TSO <userid>**
3. On the ISPF signon screen, provide the password you were given in class.
 - a. **<password>**
 - b. Press **ENTER**

Securing and Encrypting Network Traffic to z/OS Communications Server with
Policy Agent

4. Move to the ISPF command options screen when you see the READY prompt:
 - a. **ISPF 6**
5. Enter the command to see which certificates the userid of TCPIP owns:
 - a. **RACDCERT ID(TCPIP) LIST**
6. Answer the following questions about the FTP Server Certificate owned by the userid named TCPIP. (Label is "FTP on ANY ZOS".)
 - a. Does the certificate have a unique certificate ID? _____
 - b. Is the certificate in TRUST Status? _____
 - c. Is this certificate expired or not? _____
 - i. (An expired certificate may not be usable depending on the implementation of the platform needing to use it.)
 - d. What is the Serial Number assigned by RACF, the CA issuer?

 - e. What is the Issuer's Name, that is, who signed this certificate?

 - f. What is the Subject's Full Distinguished Name (in sequence)?
>CN=_____.WSC.LABS.IBM.COM.O=IBM.C=US<
 - g. What is the size of the Key? _____
 - h. What key rings is the cert. connected to (owner/ringname)?
_____/_____
7. Display the key ring that the FTP Certificate resides on:
 - a. **RACDCERT ID(FTPD) LISTRING(ServerRing1)**
8. Fill in the missing information 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

9. Enter the command to see which certificates you own and which key rings your certificate is associated with:
 - a. **RACDCERT ID(USERnx) LIST**
10. Answer the following questions about your **PERSONAL** certificate (Label = **USERnx on ANY ZOS**):
 - a. Does the certificate have a unique certificate ID? _____
 - b. Is the certificate in TRUST Status? _____
 - c. Is this certificate expired or not? _____
 - i. (An expired certificate may not be usable depending on the implementation of the platform needing to use it.)
 - d. What is the Serial Number assigned by RACF, the CA issuer? _____
 - e. What is the Issuer's Name, that is, who signed this certificate? _____
 - f. What is the Subject's Fully Distinguished Name (in sequence)?
>CN=USER_____.WSC.LABS.IBM.COM.O=IBM.C=US<
 - g. What is the size of the Key? _____
 - h. What key rings is the certificate connected to (owner/ringname)?
 - i. _____/_____
 - ii. _____/_____
11. Enter the command to see what is on one of the keyrings your certificate is connected to:
 - a. **RACDCERT ID(USERnx) LISTRING(LabClientRing)**

Securing and Encrypting Network Traffic to z/OS Communications Server with
Policy Agent

12. Answer the following questions about this keyring:
- How many default certificates are on the ring? _____
 - Who owns the default certificate? _____
 - Can the owner of this default certificate find his certificate by pointing to the key ring name alone? Yes or No? _____
 - How many CA Certificates are on the ring? _____
13. Normally a client ring must also contain a copy of the CA Certificate of the Server. Why is there only one CA Certificate on this ring?
- _____
- _____
- _____
14. Notice the RACF Label of the CA Certificate on your key ring:
- "WSC LABS Certificate Authority"
 - Is this the same CA Certificate that signed the FTP Server Certificate?
- _____
- c. *You will display the contents of this certificate later. But, for now...*
15. Enter the command to see what is on the other client key ring:
- RACDCERT ID(FTPD) LISTRING(ClientRing1)**
16. Answer the following questions about this keyring:
- Who owns this key ring? That is, which userid is associated with this keyring? _____
 - How many default certificates are on the ring? _____
 - Who owns the default certificate? _____
 - How many individual user clients can point to this key ring if they are permitted to the keyring and are asked to present a client certificate? Choose answer One or Multiple? _____
 - How do these users have to identify which certificate is theirs on the ring? *They must identify their own certificate by specifying the _____ name of the certificate.*
 - How many CA Certificates are on the ring? _____
17. Now issue the command to see the contents of the Certificate Authority certificate that signed your client certificate and the FTP server certificate:
- RACDCERT CERTAUTH LIST(LABEL('WSC LABS Certificate Authority'))**
 - You may receive an error if you have not been permitted with CONTROL access to the facility IRR.DIGTCERT.LIST.
IRRD101I You are not authorized to issue the RACDCERT command.
 - If you receive this error, it is really telling you that you are not authorized for certain RACDCERT functions. You already know that you can execute other RACDCERT functions.
 - If you have limited authorization to RACDCERT CERTAUTH, ask the instructor to execute this command for you.***
18. Answer these questions about the Certificate Authority Certificate:
- Does the certificate have a unique certificate ID? _____
 - Is the certificate in TRUST Status? _____
 - Is this CA Certificate expired or not? _____
 - (An expired certificate may not be usable depending on the implementation of the platform needing to use it.)
 - What is the Serial Number assigned to this Root, CA Certificate? _____
 - What is the Issuer's Name? _____

Securing and Encrypting Network Traffic to z/OS Communications Server with
Policy Agent

- i. >CN=_____.LABS.IBM.COM.O=IBM.C=US<
 - f. What is the Subject's Name?
 - i. >CN=_____.LABS.IBM.COM.O=IBM.C=US<
 - g. What is the size of the Key? _____
 - h. What is this certificate used for? (That is, what is its “Key Usage”?)

 - i. Does this CA Certificate reside on the FTP Client Ring owned by YOUR
Userid, which is named “USERnx/LabClientRing”?

 - j. Does this CA Certificate reside on the Server Ring owned by userid FTPD,
which is named “FTPD/ServerRing1”?

19. **Why do the ServerRing1 and the LabClientRing require only one CA
certificate when one usually has one CA certificate for the client and another
one for the server on a single ring?**

End of Part 1

Part 2: Building Certificates and Keyrings of Your Own

1. Next enter the ISPF Data Set List Utility screen:
 - a. =3.4
2. Display the data set USER.CS.SOURCE. To the right of “Dsname Level” enter:
 - a. **USER.CS.SOURCE**
3. Select USER.CS.SOURCE with an “m” in the left-hand column:

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

Command - Enter "/" to select action

m USER.CS.SOURCE

- a. Then press **ENTER**.
4. You should see all the following members with a suffix that matches your Userid Suffix.

Menu Functions Confirm Utilities Help

DSLIS USER.CS.SOURCE
Command ==>

	Name	Prompt
	GBGCAC61	
<u>e</u>	GBGCAS61	
	GBGCLI61	
	GBGRCS61	
	GBGRGC61	
	GBGSRV61	
	GBGXCE61	
	GBGXDE61	
	GBGX1261	

5. Edit the job for a CA that will sign your Server Certificate:
 - a. **Edit GBGCASnx**, changing all the “- -” **characters** in the skeleton to the last two digits of your userid.
 - b. **Change** the final octet of the **Alternate name** to **100, 101, 102, 103, 104, 105, 106, 107, or 108** to match one of the IP addresses on your TCPIPT stack.
 - i. Example: 192.168.20.nnn becomes 192.168.20.106 (in MVS7).
 - 1) The Policy *may* need to match this value. (It depends on the policy type – i.e., IPsec or AT-TLS policy.)
 - c. **IMPORTANT: Start the Certificate Validity today and end it in 6 months.**
6. Submit the job by entering at the command line:
 - a. **sub**
7. Examine the output and verify that the Certificate Status is **TRUST** and examine the output and determine if any commands failed to run because of missing authority.
 - a. If not TRUST, ask the instructor for help.
 - b. In order to review the output you may wish to split the screen.
 - i. PF2

Securing and Encrypting Network Traffic to z/OS Communications Server with
Policy Agent

- ii. =D.O (to view the held output)
 - iii. “prefix **” and “user **” (may be necessary to see all the jobs)
 - iv. Select your job with an “S” on the left side of the screen.
 - v. PF3 (to exit viewing the job)
 - vi. PF9 (to jump between the split screen images or PF3 to exit split screen view)
8. **Return** to USER.CS.SOURCE
9. Edit the job for a CA that will sign your Client Certificate:
- a. Edit **GBGCACnx**, changing all the “- -” characters in the skeleton to the last two digits of your userid.
 - b. **Change** the final octet of the **Alternate name** to **91, 92, 93, 94, 95, 96, 97, 98, or 99** to match one of the IP Addresses on your TCPIPT stack.
 - i. Example: 192.168.20.**nn** becomes 192.168.20.95 (**in MVS5**).
 - 1) The Policy *may* need to match this value. (It depends on the policy type – i.e., IPsec or AT-TLS policy.)
 - c. **Start the Certificate Validity today and end it in 6 months.**
10. Submit the job by entering at the command line:
- a. **sub**
11. Examine the output and verify that the Certificate Status is **TRUST** and examine the output and determine which commands failed to run because of missing authority.
- a. If not TRUST, ask the instructor for help.
12. Examine the output and determine which commands failed to run because of missing authority.
13. Return to **USER.CS.SOURCE**
14. Next create the Client and Server certificates.
- a. **Edit GBGCLInx and GBGSRVnx**, changing all the “- -” characters in the skeleton to the last two digits of your userid.
 - b. Also change **MVS_n** or **MVS-** to reflect your MVS System: **MVS1, MVS2, MVS3, MVS4, MVS5, MVS6, MVS7, MVS8, MVS9**.
 - c. **Start the Certificate Validity today and end it in 6 months.**
15. Submit the jobs by entering at the command line:
- a. **sub**
16. Examine the output and verify that the Certificate Status is **TRUST** and examine the output and determine which commands failed to run because of missing authority.
- a. If not TRUST, ask the instructor for help.
17. Return to **USER.CS.SOURCE**
18. Finally, create the keyrings for the Client and the Server and connect the appropriate certificates to the keyrings.
- a. Edit **GBGRGCnx and GBGRGSnx**,
 - i. Change all the “- -” characters in the skeleton to the last two digits of your userid.
 - ii. Change **MVS_n** or **MVS-** to reflect your MVS System: **MVS1, MVS2, MVS3, MVS4, MVS5, MVS6, MVS7, MVS8, MVS9**.
 - 1) **WARNING:** Change MyServer-Ring to reflect your MVS System suffix:
i.e., “MyServer2Ring,” “MyServer3Ring,” etc.
 - b. Note that these rings are different from the ones you tested with previously because this TN3270 client and this TN3270 server have DIFFERENT signing authorities.

Securing and Encrypting Network Traffic to z/OS Communications Server with
Policy Agent

- c. **How many CA Certificates need to be on each key ring now?** _____
19. Submit the jobs by entering at the command line:
 - a. **sub**
 20. Examine the output and determine which commands failed to run because of missing authority.
 21. You have reached the end of this lab. We don't expect you to become RACF experts, since there is usually a specialist at your site who performs these types of functions. But we wanted to give you a feel for how you could use RACF to create certificates and keyrings.

End of the Lab

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

