

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

**"Optional: Exporting x.509 Digital Certificates"**

**"Optional: Testing with TN3270 AT-TLS"**

**Hands-on Lab Guide**

**(Optional Lab: Digital Certificate and TN3270 AT-TLS)**



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

Revision date -

Sunday, 22 June 2025

This edition applies to IBM z/OS Configuration Assistant running in z/OSMV 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

Part 0: Lab Description (Configuring Policy Agent for AT-TLS and FTP).....	4
Specific Lab Description: Exporting x.509 Certificates and Using them on a TN3270 Workstation .....	5
Part 1: Exporting the Certificates for Your Workstation to Sequential Datasets on MVS; Receiving Them at Workstation .....	7
Part 2: Add TN3270 to Your Existing AT-TLS Policy .....	10
Part 3: Customize TN3270T at Your MVSn for AT-TLS .....	18
Part 4: Import Certificates to Windows Certificate Store on Your Workstation .....	19
Part 5: Create a PCOMM (TN3270 Emulator) Definition for Client and Server Authentication with z/OS.....	28
End of AT-TLS TN3270 Lab .....	30

## **Part 0: Lab Description (Configuring Policy Agent for AT-TLS and FTP)**

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).

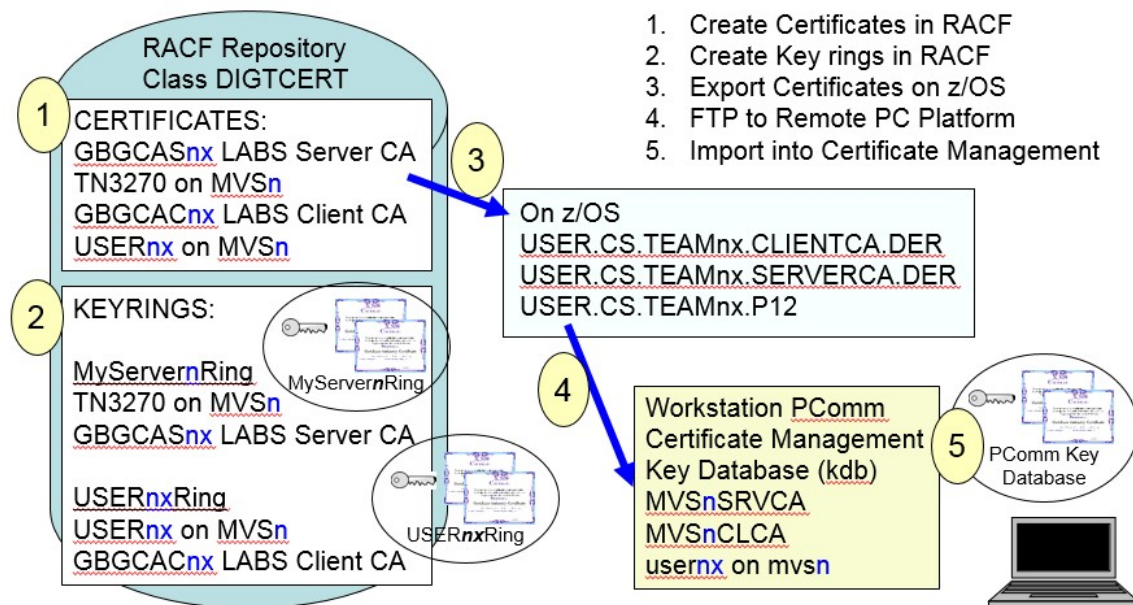
In our labs you use TCPIP1 for basic maintenance on ZOS until you have finished building your own student TCP/IP stacks and procedures. You telnet into TCPIP1 to reach ISPF and UNIX for building the procedures that should run together with the student TCP/IP stack.

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.

## Specific Lab Description: Exporting x.509 Certificates and Using them on a TN3270 Workstation

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**.

1. All self-signed certificates have a serial number of zero.
2. Other signed certificates have a serial number of one or higher.
3. 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.
4. Any time a RACDCERT GENCERT with the SIGNWITH parameter command is entered, a certificate is created and the serial number gets incremented.
5. Given this algorithm, collisions can occur with the profile name if the signing certificate gets deleted and recreated while 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 an IRRD109I message.



## Shared RACF Database between all MVS images in this lab.

In a previous lab you generated:

- Two CA certificates (one to sign the TN3270T server certificate and one to sign the TN3270 client certificate)
- A TN3270T server certificate
- A client certificate for your user ID
- A Client Key ring
  - You attached the appropriate certificates to the key ring.
- A TN3270 Server Key ring
  - You attached the appropriate certificates to the key ring.

The shared RACF Repository now contains a PERSONAL Certificate for the TN3270T Server, a General USERnx Client PERSONAL Certificate, and the signing authority Certificates (CA Certificates) for both types of PERSONAL certificates.

The repository contains many Key rings. One is for the TN3270 Server; the key ring is owned by user ID TN3270. Other key rings for the Local Users owned by user IDs USERnx. A local TSO or UNIX user may require a Local User key ring for connections to multiple server types.

In our lab example, the Local User (USERnx) needs to extend his SSL/TLS/AT-TLS connection capability to his workstation. Management requires both Server and Client Authentication. Therefore, the USER (or an Administrator) needs to **export** the appropriate certificates to a Text or Binary file on MVS.

The choice of the type of export format depends on whether Private Keys need to be included and on the type of certificate format that is acceptable to the workstation SSL/TLS application. In this case the application is Personal Communications (PCOMM), and it can accept

- Text (CERTB64)
- Binary (CERTDER)
- Binary with Private Key (PKCS12DER)

PComm at the level we are using in this course cannot accept the following format:

- Text with Private Key (PKCS12B64)

Other platforms cannot accept:

- Binary with Certificate Chain (PKCS7DER)

The user FTPs the appropriate certificates to the remote workstation and imports those certificates into the Key Management repository of the remote application – Windows in our lab.

Then the teams configure their TN3270 Workstation emulator program and their TN3270 Server for secured TLS connections.

The teams are to connect to the TN3270 Server on their MVS at 192.168.20.101-107. The teams will also need to configure the AT-TLS policy for the TN3270 Server so that it supports both Server and Client Authentication.

Once the teams load the new policy and recycle the TN3270 Server, they then test the connection from the PComm client.

*The lab is divided into several sections:*

- *Part 1: Export the certificates created in an earlier Optional Lab (i.e., last part of the first Digital Certificate lab and ftp from the workstation to transfer the certificates to your workstation C: \temp directory.*
- *Part 2: Create a TN3270 Policy at Configuration Assistant by adding a new TN3270 requirement map to the existing AT-TLS Policy*
- *Part 3: Customize the TN3270 Server at your MVS for AT-TLS*
  - *Change the TN3270 Profile to invoke AT-TLS*
  - *Add a TN3270 AT-TLS Policy to Your Existing FTP AT-TLS Policy which you named TMxx\_ATTLS.policy.*
- *Part 4: Import the exported certificates into the “Windows Certificate Store”*
- *Part 5: Create a PCOMM Emulator profile that connects to your TN3270T at your MVS and requests a TLS connection. Test the AT-TLS connection and diagnose it.*

## **Part 1: Exporting the Certificates for Your Workstation to Sequential Datasets on MVS; Receiving Them at Workstation**

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

1. Create a PCOMM session to connect to TN3270 at TCPIP1 on your assigned MVS system.
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>**

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

- b. Press **ENTER**
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 you are the owner of and which rings your certificate is associated with:
  - a. **RACDCERT ID(USERnx) LISTRING(\*)**
6. You should see at least Two Keyrings:
  - a. **LabClientRing** (Ring Used for FTP Client)
    - i. You used this ring for the FTP AT-TLS Lab.
  - b. **USERnxRing** (Ring Used for Generic Local Client)
    - i. You created this ring in a previous x.509 Digital Certificate Lab.
    - ii. You will use this ring for this TN3270 AT-TLS Lab.
7. You should see 3 certificates on the USERnxRing. Mark **in the spaces** provided whether these certificates are **CERTAUTH** certificates or **PERSONAL** and/or **DEFAULT** certificates.
  - a. **USERnx on MVS**  
\_\_\_\_\_
  - b. **GBGCACnx LABS Client CA**  
\_\_\_\_\_
  - c. **GBGCASnx LABS Server CA**  
\_\_\_\_\_
8. Enter the command to see the contents of the Generic Server Ring (which happens to be owned by TN3270):
  - a. **RACDCERT ID(TN3270) LISTRING(MyServer#Ring)**
    - i. where the “#” between “MyServer” and “Ring” is your z/OS (MVS) number, ZOS2, ZOS3, ZOS4, ZOS5, ZOS6, MVS7, MVS8 or ZOS9.
9. You should see 3 certificates on the MyServer#Ring. Mark **in the spaces** provided whether these certificates are **CERTAUTH** certificates or **PERSONAL** and/or **DEFAULT** certificates.
  - a. **TN3270 on MVS**  
\_\_\_\_\_
  - b. **GBGCACnx LABS Client CA**  
\_\_\_\_\_
  - c. **GBGCASnx LABS Server CA**  
\_\_\_\_\_
10. *In the next steps you are going to export the appropriate certificates into sequential datasets on z/OS so that you can FTP them later to your workstation.*
11. Check to see if the following members are in your dataset “USER.CS.SOURCE”:
  - a. **GBGXDEnx**
  - b. **GBGX12nx**
12. Create the **EXPORT** Jobs:
  - a. Edit **GBGXDEnx** and **GBGX12nx**,
    - i. Change all the “-” characters in the skeleton to your team **suffix**.
    - ii. Change “MVS-” to match your MVS name (**MVS1, MVS2, MVS3, MVS4, MVS5, MVS6, MVS7, MVS8, MVS9**).
13. Answer the following questions about **GBGXDEnx**:
  - a. In what format are the CA Certificates being exported?  
**FORMAT(\_\_\_\_\_)**
  - b. Does the PCOMM application on the workstation need to have access to the private keys of the CA Certificates? Why or Why not?  
\_\_\_\_\_  
\_\_\_\_\_



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

- c. Why is this Certificate Package Export format chosen?  
\_\_\_\_\_
- d. Does this format export in Text or Binary mode?  
\_\_\_\_\_
14. Answer the following questions about **GBGX12nx**:
- a. In what format is the Client Certificate being exported?  
**FORMAT**(\_\_\_\_\_)
- b. Does the PCOMM application on the workstation need to have access to the private keys of the Client Certificates?  
\_\_\_\_\_
- c. Why is this Certificate Package Export format chosen?  
\_\_\_\_\_
- d. Does this format export in Text or Binary mode?  
\_\_\_\_\_
- e. Is the protected password in Upper Case or Lower Case? \_\_\_\_\_
15. Submit the two jobs by entering at the command line:
- a. **sub**
16. Examine the output and determine if any of the commands failed to run because of missing authority.
17. Open a DOS Window at your workstation and position yourself in the /temp directory so that you can ftp the sequential datasets onto the workstation:
- a. **cd /temp**
- b. or **cd /tmp**
- c. If there is no **/temp** or **/tmp** directory just use the root directory, **cd /**
18. Ftp to the Maintenance FTP at your MVS- and switch to BINARY (Image) mode to transfer binary files:
- a. **ftp 192.168.20.8n**
- b. Respond to the prompts to login.
- c. **Enter the command to transmit in binary: "binary"**
19. "Get" the CA certificate sequential datasets and rename them:
- a. **get 'USER.CS.TEAMnx.SERVERCA.DER' MVSnrSRVCA.der**
- b. **get 'USER.CS.TEAMnx.CLIENTCA.DER' MVSnrCLCA.der**
20. "Get" the Client certificate sequential dataset and rename it:
- a. **get 'USER.CS.TEAMnx.P12' MVSnrTMnx.p12**
21. Exit from your FTP connection with MVSnr:
- a. **quit**
- b. **exit**

## Part 2: Add TN3270 to Your Existing AT-TLS Policy

1. Your current AT-TLS policy references FTP only. You now need to add TN3270 to the policy.
2. Open a Web Browser window and go to URL:  
**<https://192.168.20.81:443/zosmf>**
3. Logon using your Team Information Sheet to determine your z/OS User ID and password (the same ones as your TSO logon to your z/OS system).
4. Expand the “**Configuration**” section in the list on the left side of the page if it is not already expanded (“>” means it is not expanded and “V” means that it is already expanded), and click on “**Configuration Assistant**” which is the only option in the expanded section.
5. Use the pull-down if necessary, to select your team’s backing store file and click on the **Open** button.

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

6. If necessary use the technology pull-down to select **AT-TLS**. Use the radio button to select TCP/IP stack **TCPIPT**.
7. Use the **Actions** pull-down to select **Rules**.
8. Select the **Default\_TN3270-Server** rule.
9. Use the **Actions** pull-down to select **View Details**.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant interface. The browser address bar shows the URL 192.168.20.81/zosmf/. The page title is "Network Configuration Assistant". The breadcrumb trail is "Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > View Details".

**View Details**

Buttons: Close, Printable page

**Selected Row**

Status	Name	Local Data Endpoint	Remote Data Endpoint	Application / Requirement Map	Key Ring
Disabled	Default_TN3270-Server	All_IP_Addresses	All_IP_Addresses	TN3270-Server	FTPD/ServerRing1

=====

**Traffic Details**

=====

**Traffic Settings**

Application Name	Local Port	Remote Port	Connect Direction	Jobname	User ID
TN3270-Server	23	1024-65535	Inbound	---	---

Handshake Role	Application Controlled	Secondary Map	Key Ring	Certificate Label	Specify Server Certificate Labels	Server Certificate Labels
Server	Enabled	Disabled	Use default	---	----	----

End - Traffic Details

=====

**Security Level Details**

=====

**Security Level: Default\_Ciphers - IBM supplied: 3DES, AES-256 bit, AES-128 bit encryption**

Type: AT-TLS

**Version**

Use TLS Version 1.3 (Available beginning with z/OS V2R8): No  
Use TLS Version 1.2: No  
Use TLS Version 1.1: Yes  
Use TLS Version 1.0 (not recommended): Yes  
Use SSL Version 3 (not recommended): Yes  
Use SSL Version 2: No

**SSL Version 3 Ciphers**

Entire TLS Version 1.X / SSL Version 3 Cipher Suite in Preferred Order:  
TLSv1.2: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384, TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA, TLS\_RSA\_WITH\_RC4\_128\_SHA, TLS\_RSA\_WITH\_RC4\_128\_MD5, TLS\_RSA\_WITH\_IDEA\_CBC\_SHA, TLS\_RSA\_WITH\_NULL\_SHA, TLS\_RSA\_WITH\_NULL\_MD5, TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV

Buttons: Close, Back to Top

10. Notice the following:
  - a. Status is Disabled.
  - b. Key Ring is FTPD/ServerRing1.
    - i. You need a different key ring defined – one that is specific to TN3270.
  - c. Inbound traffic to remote port 23.
  - d. Handshake Role is Server.
  - e. This rule does not completely suit your needs.
  - f. You will need to create your own TN3270 Server Traffic rule.
11. **Close** the View panel when you are finished reviewing the information.

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

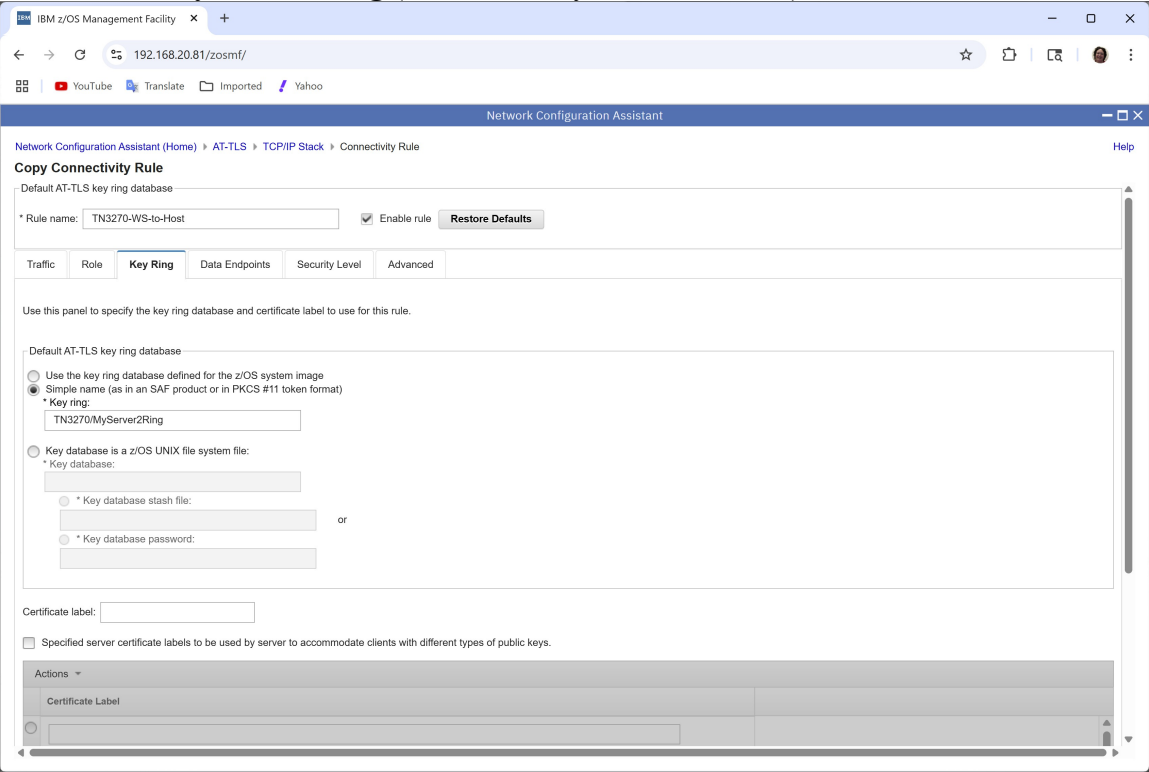
12. Use the **Actions** pull-down to select **Copy...**
13. Change the Rule name to **TN3270-WS-to-Host**.
14. Select **Enable rule**.
15. Enter Application name **TN3270DiffKeyring**.

The screenshot shows the 'Network Configuration Assistant' window. The breadcrumb trail is 'Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule'. The main title is 'Copy Connectivity Rule'. Below it, the text 'Default AT-TLS key ring database' is visible. The 'Rule name' field contains 'TN3270-WS-to-Host'. The 'Enable rule' checkbox is checked. There is a 'Restore Defaults' button. Below this, there are tabs for 'Traffic', 'Role', 'Key Ring', 'Data Endpoints', 'Security Level', and 'Advanced'. The 'Traffic' tab is selected. The text 'Use this panel to specify the traffic settings.' is displayed. The 'Application name' field contains 'TN3270DiffKeyring'. There are two sections for port configuration: 'Local Port' and 'Remote Port'. Each has radio buttons for 'All ports', 'All ephemeral ports', and 'Ports:'. The 'Ports:' option is selected for both. The 'Local Port' 'Ports:' field contains '23'. The 'Remote Port' 'Ports:' field is empty. Below these are checkboxes for 'Indicate the TCP connect direction' (with 'Inbound only' selected) and 'Specify jobname and user ID' (with 'Jobname:' and 'User ID:' fields). At the bottom are 'OK' and 'Cancel' buttons. The bottom status bar shows 'user21' and various icons.

16. Review the **Role** tab if you would like but leave the defaults.

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

- 17. Select the **Key Ring** tab.
- 18. Select **Simple name** and enter your TN3270 Server key ring name **TN3270/MyServernRing** (where “n” is your MVS suffix).



- 19. You viewed the TN3270 key ring previously in this lab.  
Digital ring information for user TN3270:

Ring:

```
>MyServer2Ring<
```

Certificate Label Name	Cert Owner	USAGE	DEFAULT
TN3270 on MVS2	ID (TN3270)	PERSONAL	YES
GBGCAC23 LABS Client CA	CERTAUTH	CERTAUTH	NO
GBGCAS23 LABS Server CA	CERTAUTH	CERTAUTH	NO

- 20. Select the **Data Endpoints** tab.

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

21. Enter Local data endpoint range **192.168.20.100-192.168.20.108**
22. Enter Remote data endpoint subnet range **192.168.0.0/16** (the subnet range that includes the class workstations).

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant. The browser address bar shows the URL 192.168.20.81/zosmf/. The page title is "Network Configuration Assistant". The breadcrumb navigation shows "Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule". The "Copy Connectivity Rule" dialog box is open, showing the "Data Endpoints" tab. The "Rule name" is "TN3270-WS-to-Host". The "Enable rule" checkbox is checked. The "Data Endpoints" tab is selected, showing the "Local data endpoint" and "Remote data endpoint" fields. The "Local data endpoint" field contains "192.168.20.100-192.168.20.108" and the "Remote data endpoint" field contains "192.168.0.0/16".

23. Select the **Security Level** tab.

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

24. Use the pull-down to select the **ATTLSGoldwClientAuth** security level.

The screenshot shows the IBM z/OS Management Facility Network Configuration Assistant web interface. The browser address bar shows the URL 192.168.20.81/zosmf/. The page title is "Network Configuration Assistant". The breadcrumb navigation shows "Network Configuration Assistant (Home) > AT-TLS > TCP/IP Stack > Connectivity Rule". The main heading is "Copy Connectivity Rule". Below this, there is a section for "Default AT-TLS key ring database" with a text input field for "Rule name" containing "TN3270-WS-to-Host", an "Enable rule" checkbox which is checked, and a "Restore Defaults" button. Below this is a tabbed interface with tabs for "Traffic", "Role", "Key Ring", "Data Endpoints", "Security Level", and "Advanced". The "Security Level" tab is currently selected. It contains the instruction "Select the security level that will protect this traffic descriptor" and a dropdown menu labeled "Select a security level" with the selected option "ATTLSGoldwClientAuth - AT-TLS Encryption with Client Authentication". At the bottom of the tab are "OK" and "Cancel" buttons.

25. Review the Advanced tab if you would like but leave all the defaults.

26. Click the **OK** button. This returns you to the Rules panel.

27. Notice the Connectivity Rule that you just created shows up as Enabled in the list.

28. Click on the **Close** button. This returns you to the AT-TLS perspective panel.

29. Click on the **Save** button. Optionally enter a comment and click on the **OK** button.

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

## 30. Use the **Actions** pull-down to select **Install Configuration Files**.

The screenshot shows a web browser window with the URL 192.168.20.81/zosmf/. The page title is "Network Configuration Assistant". The breadcrumb navigation is "Network Configuration Assistant (Home) > AT-TLS > Configuration Files". The main heading is "List of Configuration Files for Stack TCP/IP In Group Default". Below this, there is a sub-heading "List of Configuration Files for Stack TCP/IP In Group Default". A table is displayed with the following columns: Stack, Configuration Type, Status, Last Install, Configured File Name, Configured Host Name, and Configured Installation Method. The table contains one row for "TCP/IP" with the following values: AT-TLS Policy, Needs install, 2025-06-22 00:36:57, /u/user21/TM21\_ATTLS\_FTP.policy, 192.168.20.82, and FTP to user21. Below the table, there is a "Total: 1 Selected: 1" summary and a "Close" button.

Stack	Configuration Type	Status	Last Install	Configured File Name	Configured Host Name	Configured Installation Method
TCP/IP	AT-TLS Policy	Needs install	2025-06-22 00:36:57	/u/user21/TM21_ATTLS_FTP.policy	192.168.20.82	FTP to user21

Total: 1 Selected: 1

Close



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

### 31. Use the **Actions** pull-down to select **Install...**

IBM z/OS Management Facility x +

192.168.20.81/zosmf/

Network Configuration Assistant

Network Configuration Assistant (Home) > AT-TLS > Configuration Files > Install Help

**Install File for Default.ZOS2.TCPIPT**

\* Install file name:  
/u/user21/TM21\_ATTLS\_FTPandTN3270.policy

Installation method  
☐ Save to disk  
☒ FTP

FTP information  
\* Host name: 192.168.20.82  
\* Port number: 21  
User ID: user21 ☒ Save User ID  
\* Password: \*\*\*\*\* ☒ Save Password  
☐ Use TLS/SSL  
Guideline: If Application Transparent TLS (AT-TLS) is being used to protect FTP connections between this z/OSMF server and the target z/OS system, clear this check box.  
☐ Create the directories if they do not exist

Data transfer mode  
☒ Default ☐ Passive ☐ Active  
☐ Propagate this FTP configuration to all files on this image

Comment for the configuration file prologue (optional)

Selecting the GO button may do an automatic save of backing store before the install, based on your preference setting.

Go Close View FTP Log

32. Change the Install file name to **/u/user~~nx~~/TM~~nx~~\_ATTLS\_FTP~~and~~TN3270.policy**

33. Click on the **Go** button.

34. Click on **OK** on the next two panel pop-ups.

35. Click on **Close** button twice to return to the AT-TLS panel.

36. Return to z/OS and use what you have learned in this class to incorporate the new policy.

a. **TSO OMVS**

b. **su**

c. **oedit pagentt.conf**

d. Change the AT-TLS policy name to

**/u/user~~nx~~/TM~~nx~~\_ATTLS\_FTP~~and~~TN3270.policy**

e. Copy the policy agent main configuration file from your local directory to the production directory.

**cp pagentt.conf /etc/PAGT1/**

f. **exit**

g. **exit**

h. **Enter**

i. Update the running policies.

**=D.LOG**

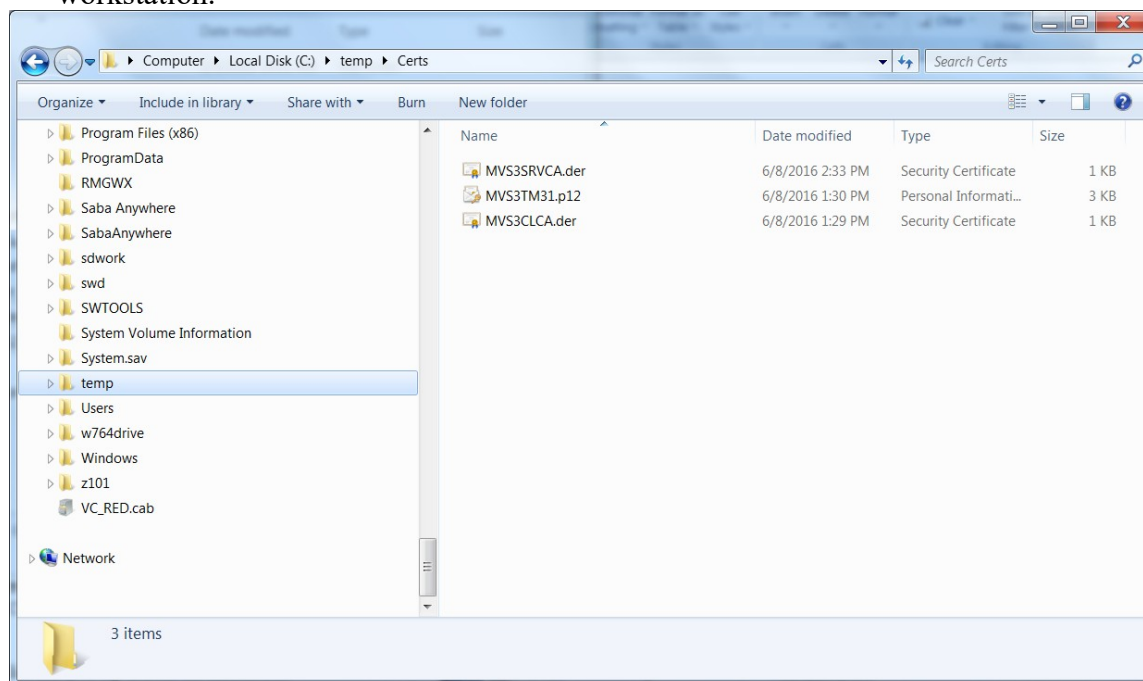
**/F PAGENTT,UPDATE**

## Part 3: Customize TN3270T at Your MVSn for AT-TLS

1. On ZOSn, verify that TTLS is enabled.  
**/D TCPIP,TCPIPT,NETSTAT,CONFIG**
2. If it is not, enable TTLS using your OBEYFILE member **TLSONnx** from an earlier lab.
3. The instructors have provided you with a sample TN3270 profile for AT-TLS support, **USER.CS.TCPPARMS(TNnATTLS)**.
4. Use **=3.4** to view your **USER.CS.TCPPARMS** dataset.
5. Edit the **TNnATTLS** member to include the appropriate entries for TN3270 with AT-TLS. (Use your class notes to add or comment out what you do and do not need.)
  - a. HINT: Look for entries that contain the characters “- - -...” either before or after a keyword.
  - b. In addition, uncomment the **DEBUG CONN DETAIL** to receive useful messages in the MVS log.
6. Return to the MVS Console and recycle TN3270T (or start it if it is not yet started):  
**/S TN3270T,CS=USER,PROF=TNnATTLS**
7. Return to the job that created the USER Certificate EXPORT job:  
**USER.CS.SOURCE(GBGX12nx)**
8. Remind yourself of the **PASSWORD** you assigned in order to protect the **PRIVATE KEY** of this exported certificate:
  - a. **My Private Key password is:** \_\_\_\_\_
  - b. ***You need this password in the next Part of this lab!***

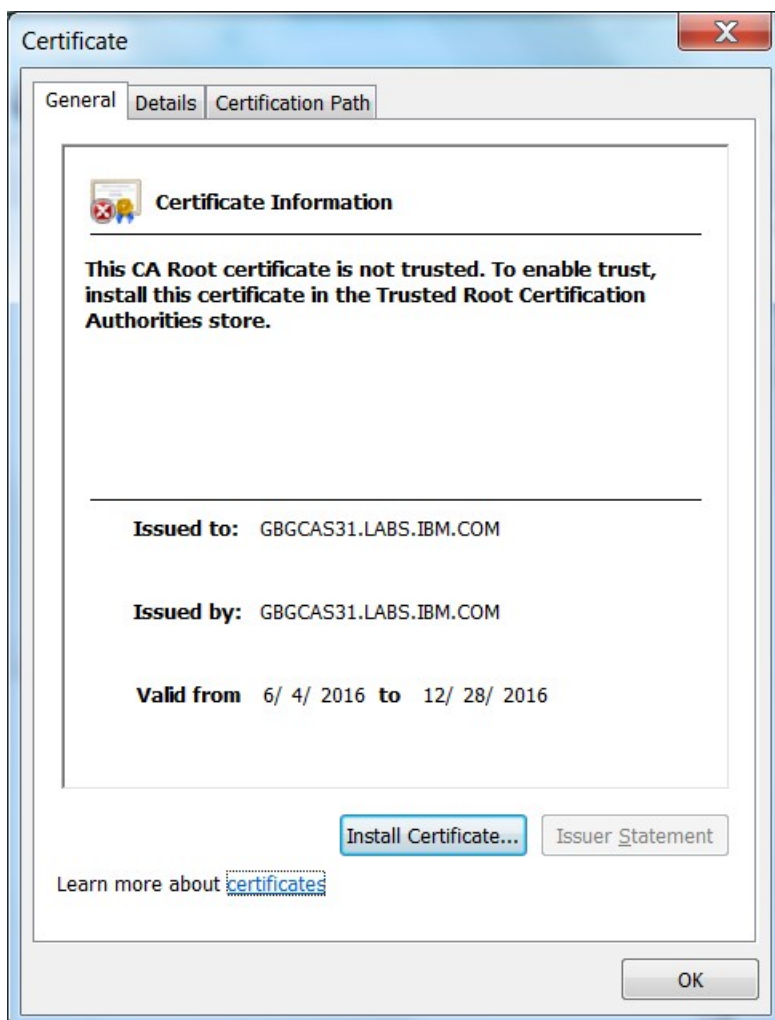
## Part 4: Import Certificates to Windows Certificate Store on Your Workstation

1. Open Windows Explorer list of the certificates that you downloaded to your workstation.



2. Double click on the first certificate **MVS***n***SRVCA.der** where *n* is your MVS number.

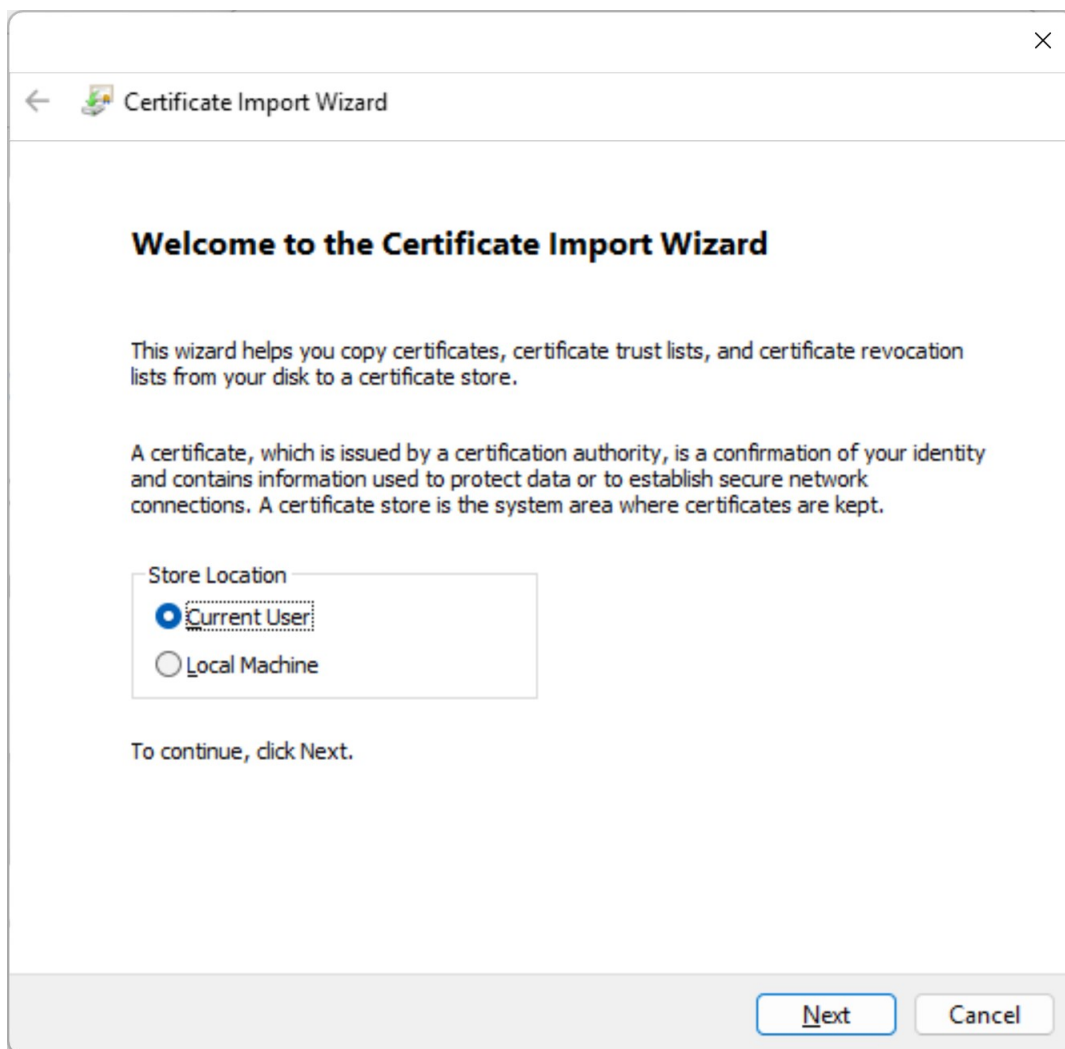
## Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent



3. Click on the **Install Certificate** button.

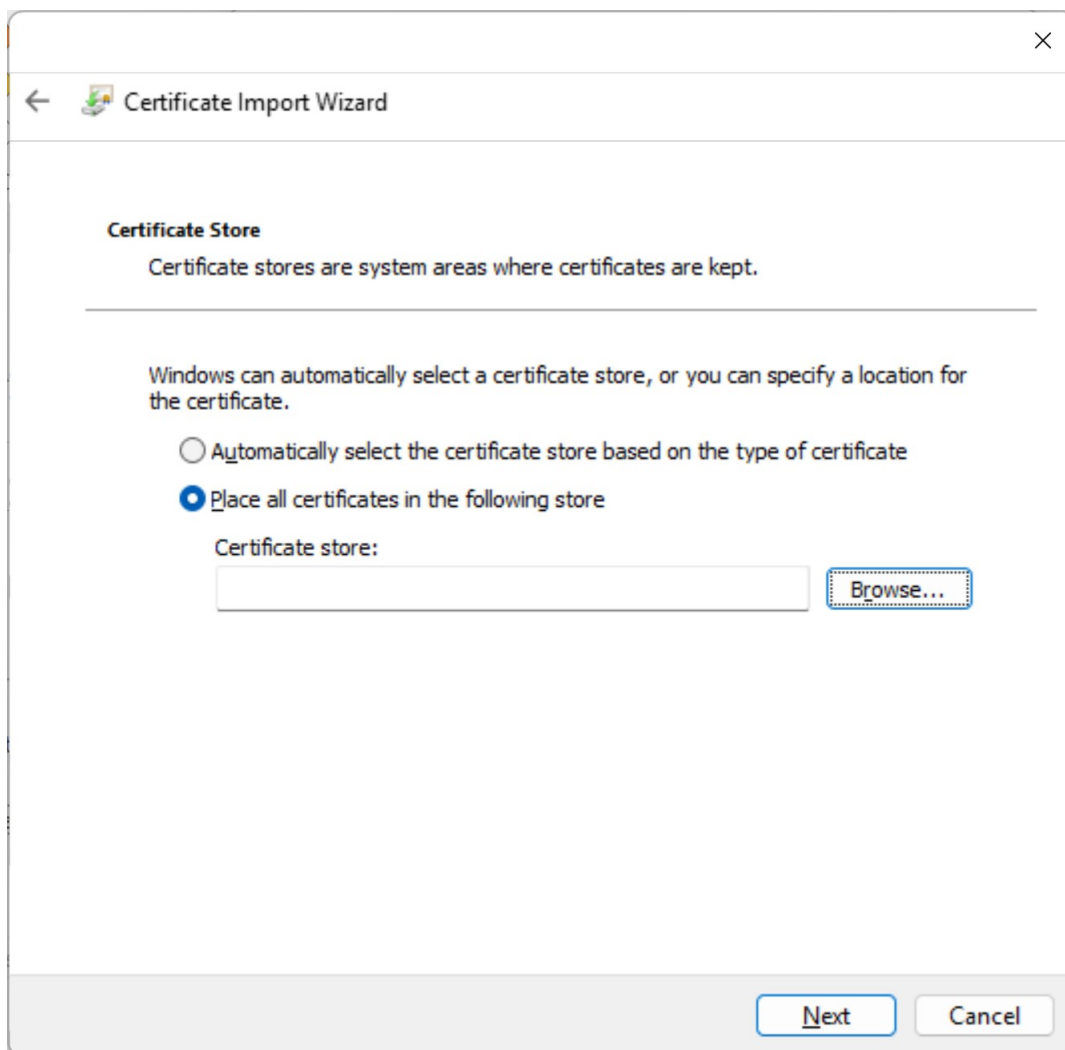
## Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

4. The Certificate Import Wizard is started. You should receive one of the following panels.



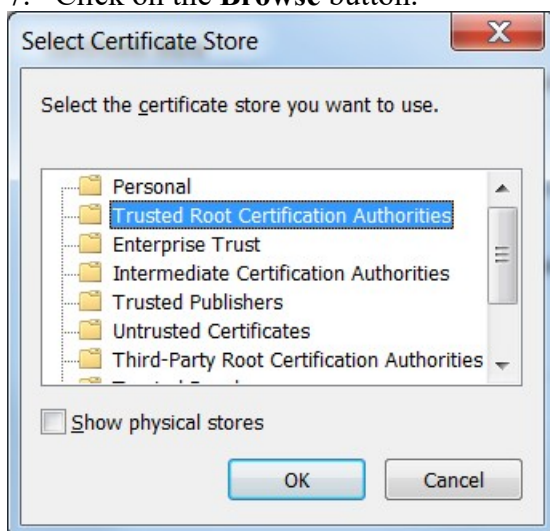
5. Click on **Next**.

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



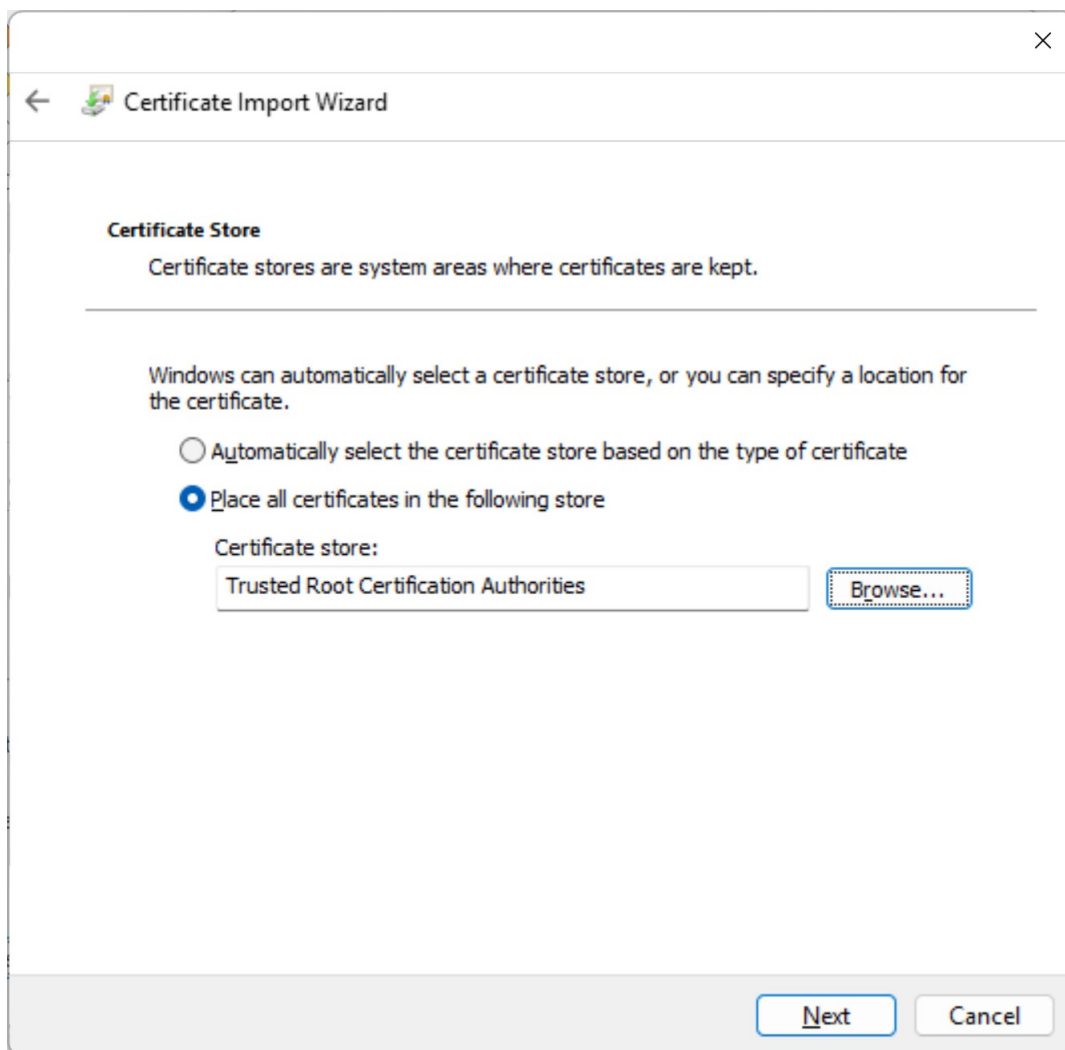
6. Use the radio button to select **Place all certificates in the following store**.

7. Click on the **Browse** button.

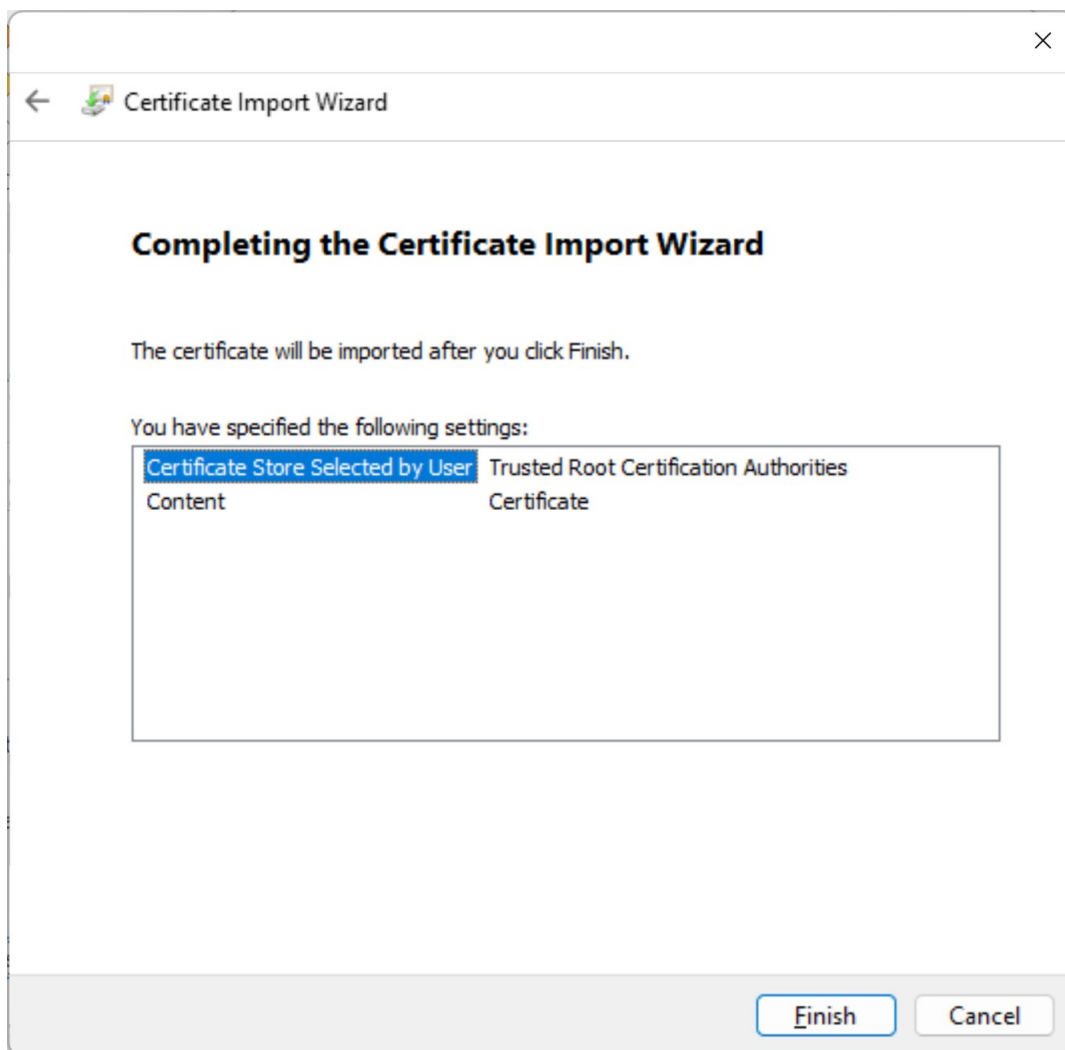


8. Select **Trusted Root Certification Authorities** and click on the **OK** button.

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



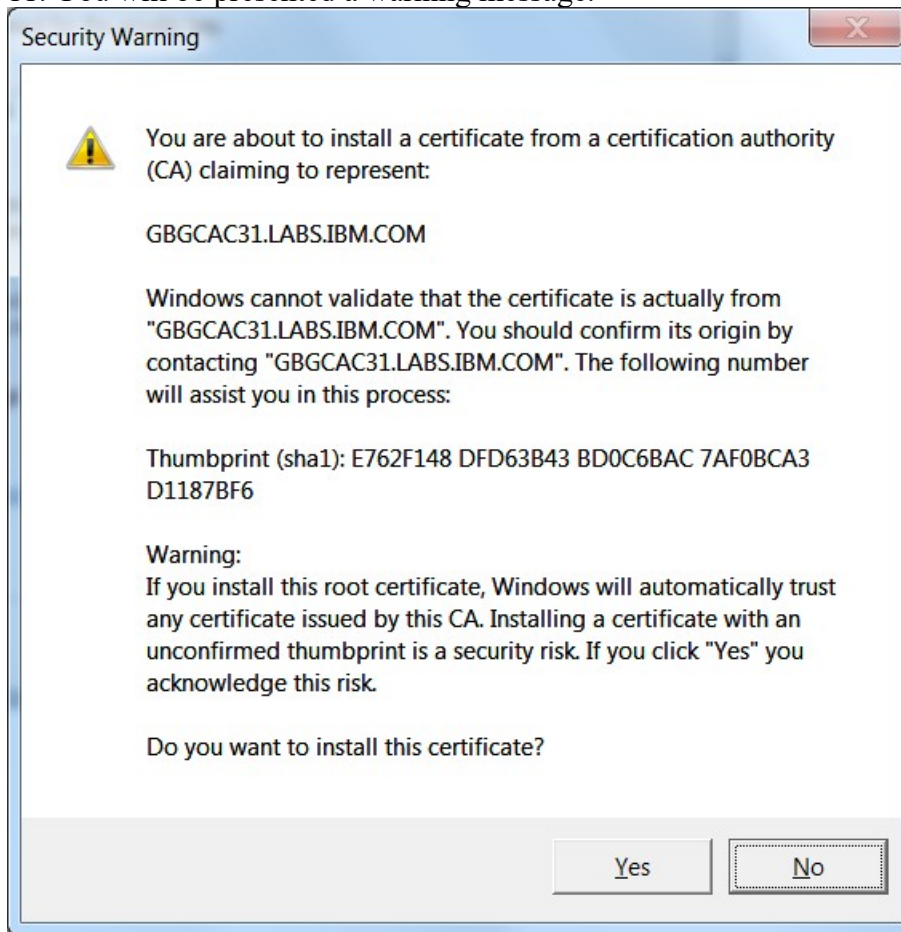
9. Click on the **N**ext button.



10. Click on the **Finish** button.



11. You will be presented a warning message.



12. Click on the **Yes** button.

13. You should be presented with a successful message.



14. Click on the **OK** button twice.

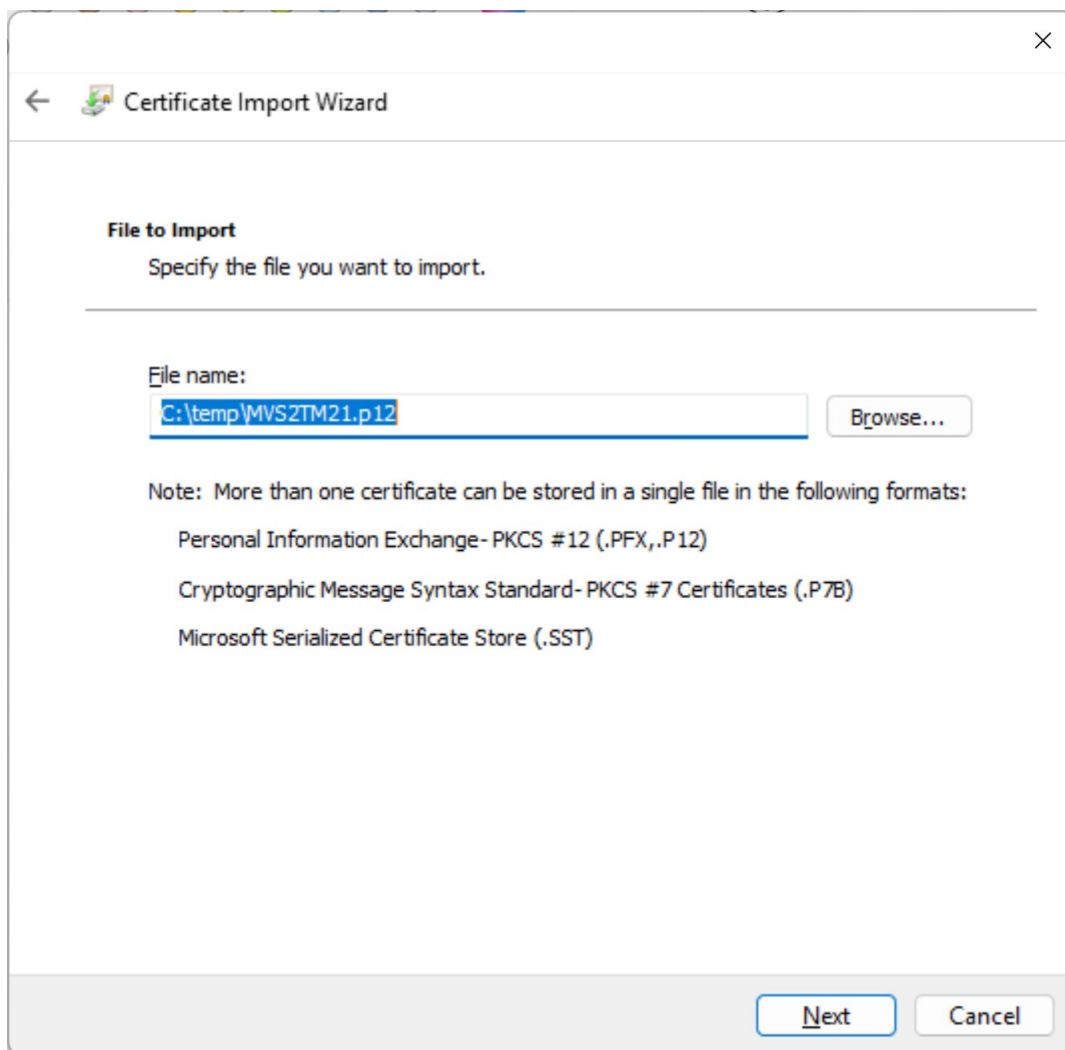
15. Repeat for the other CA certificate file, **MVS<sub>n</sub>CLCA.der**.

16. Double click on the client certificate **MVS<sub>n</sub>TM<sub>n</sub>.p12** where **n** is your MVS number.

17. The Certificate Import Wizard is started.

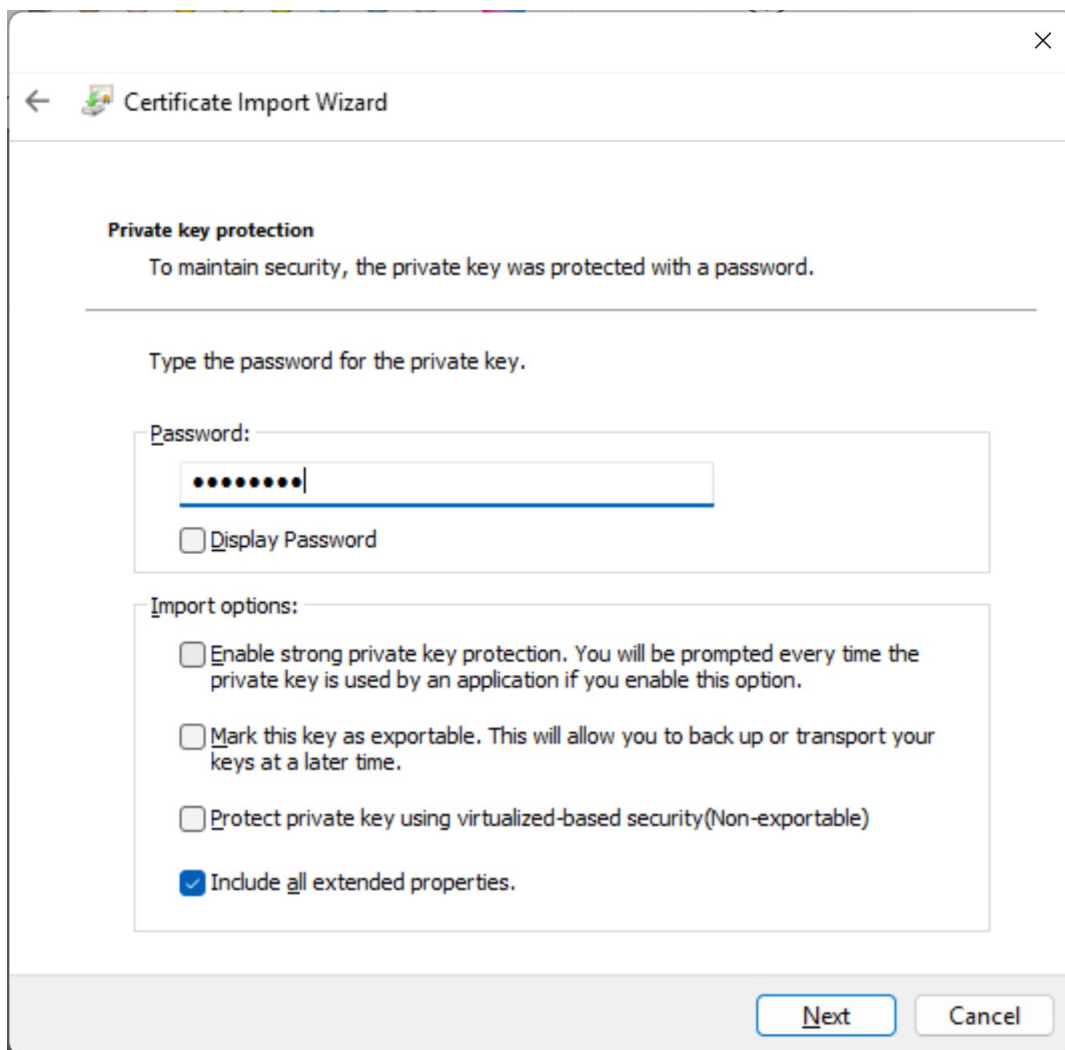
18. Click on the **Next** button.

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



19. Click on the **N**ext button.

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



20. Provide the password to open the P12 file that was created during your EXPORT job at MVS.
  - a. Click on **Next**.
21. Accept the default certificate store by clicking on the **Next** button.
22. Click on the **Finish** button.
23. If you are presented with a warning message click on the **Yes** button.
24. You should be presented with a successful message.
25. Click on the **OK** button twice.

## Part 5: Create a PCOMM (TN3270 Emulator) Definition for Client and Server Authentication with z/OS

1. At your workstation create a new PCOMM Session:
  - a. **Start >>> All Programs >>> Personal Communications >>> Start or Configure Sessions >>> New Session**
2. On the **Host Definition** Tab, fill in **Link Parameters** with
  - a. **IP Address of 192.168.20.1ab.**
  - b. Select **Port 23**
3. On the Security Setup Tab
  - a. Examine the contents of the HELP panels to understand what the configuration is asking you to specify.
  - b. Click on **Enable Security**
  - c. Use the Microsoft Crypto API (MSCAPI) and accept the default **Advanced** options.
  - d. For **Security Protocol**, select **TLS 1.1**
  - e. In **Client Authentication** section, select **Send Personal Certificate to Server if it is Requested**
  - f. Click on **Send or Prompt for Personal Client Certificate.**
  - g. Click on **Select Now** button.
  - h. Select your client certificate and click on the **OK** button three times.
  - i. **Login** under a different user ID (e.g., USER11-USER13).
  - j. **If the session succeeds skip the next Step.**
4. **If the session does not succeed**, look for messages at your MVS and diagnose the problem. Correct the problem and then continue with Step **Error! Reference source not found.**
  - a. For Diagnosis:
    - i. Raise AT-TLS Trace levels to 255
      1. Edit the ATTLS text file to raise trace from 2
    - ii. Enable DEBUG DETAIL
      1. Use command
      2. Or add to TN3270 Profile
    - iii. For more help, consult the TN3270 and AT-TLS chapters of the IP Diagnosis Guide.
5. **If you like, save this PCOMM session for later use so that you need not recreate it if you need it again.**
6. Connect to your MVS with the new TLS PCOMM session.
  - a. You are already logged on with a USERID of USER11, USER12, or USER13. So pick any other user ID, they are all defined on all systems (shared RACF database).
7. Proceed to the MVS Console if you are not already there:
  - a. **ISPF D.LOG or =D.LOG**
8. Execute the telnet command to view the new TN3270T profile:
  - a. **/D TCP/IP,TN3270T,TELNET,PROFILE,DETAIL**
  - b. Examine the **Security fields** of the display.

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

- i. What is the CONNTYPE: \_\_\_\_\_
  - ii. What is the Port's Key Ring name? \_\_\_\_\_
    - 1) Why is the name of the Key Ring not displayed?  
\_\_\_\_\_
  - iii. What is the Encryption Type: \_\_\_\_\_
  - iv. What type of CLIENTAUTH is valid: \_\_\_\_\_
9. Execute the telnet commands to view your TN3270 session:
  - a. **/D TCPIP,TN3270T,T,CONN**
10. Write down the Connection ID number of your TN3270 session:  
\_\_\_\_\_
11. Issue the command to see the detail for your TN3270 connection:
  - a. **/D TCPIP,TN3270T,T,CONN,CONN=<connection id>,DETAIL**
  - b. Is Client Authentication in Use? \_\_\_\_\_
  - c. What is the USERID that is associated with the TN3270 ATTLS Connection?  
\_\_\_\_\_
  - d. What type of Access is coded for this TN3270 Port? Secure or Non-Secure?  
\_\_\_\_\_
  - e. To the right of the "ACCESS" is the Encryption Type or Cipher Spec. Which Cipher Specs are represented? (Look in the IP Configuration Reference.)
    - i. \_\_\_\_\_
  - f. What is the name of the TTLS Rule?  
\_\_\_\_\_
12. Find the names of the LU and the APPL in use for this TN3270 connection:
  - a. **LUNAME:** \_\_\_\_\_
  - b. **APPL:** \_\_\_\_\_
13. Display the LUNAME:
  - a. **/D NET,E,ID=<LUNAME>**  
(where E means SCOPE=ALL)
14. After reviewing the VTAM display, enter **omvs** to examine the SYSLOG and the entries for your secure login:
  - a. **TSO OMVS**
  - b. **su**
  - c. **cd /var/CSLOG**
  - d. **obrowse syslogall.log**
15. After reviewing the messages in the syslog file, exit from the browse with **PF3**.
  - a. The amount of trace data you see depends on whether you changed the trace level for ATTLS from level 2 to level 255.
16. Exit from Superuser mode with **exit**
17. Exit from OMVS with **exit**
18. **Enter** to complete exit from OMVS.
19. **PF3** out of ISPF.
20. **Logoff**

## **End of AT-TLS TN3270 Lab**

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

