

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

**"Reviewing Certificate Repositories and  
Removing Old Entries"**

**Hands-on Lab Guide -- Windows 10 Version**

**(Key Rings, Key Databases, and Digital Certificates)**



## Table of Contents

<b>Part 0: Lab Description (Examining Certificate Repositories) .....</b>	<b>- 3 -</b>
<i>Specific Lab Description: Maintain Certificate Repositories .....</i>	<i>- 3 -</i>
<b>Part 1: Examining and Optionally Deleting Certificates from RACF Repository at MVS .....</b>	<b>- 5 -</b>
<i>You May Review this Section or Skip to Part 2.....</i>	<i>- 6 -</i>
Cleaning up the Server Key Ring Environment at Each MVS .....	- 6 -
Cleaning up the Client Key Ring Environment at Each MVS that Remained after the Previous Class.....	- 6 -
Cleaning up the Certificates at Each MVS .....	- 7 -
<b>End of Required MVS Certificate Removal Lab.....</b>	<b>- 7 -</b>
<b>Part 2 : Examining and Optionally Deleting Certificates from Repository on Microsoft Windows (Windows 10) .....</b>	<b>- 8 -</b>
Locating Certificate Management in the Microsoft Management Console (MMC) .....	- 8 -
<b>End of the Lab .....</b>	<b>- 17 -</b>

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.

## Part 0: Lab Description (Examining Certificate Repositories)

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.

LEGEND for the TEAM Number:

TEAMnx, where “n” represents your ZOS suffix and “x” represents your userid suffix.

EXAMPLE: TEAM53 means ZOS5 and USERID of USER3.

### Specific Lab Description: Maintain Certificate Repositories

Each team on a single ZOS (MVS) system uses RACF as the certificate repository on MVS (Z/OS).

Our labs do **not** use UNIX System Services as the security certificate repository for MVS.

Individual applications can also maintain different certificate repositories. For example, on your Workstation, PCOMM and your Browser have their own way of pointing to the equivalent of a RACF key ring. Even Microsoft Windows has a separate certificate repository that some applications use instead of relying on an application-specific store.

In preparation for your labs that use certificates, you are going to look at these certificate repositories and delete the certificates that the previous attendees at this course may have left in RACF and in your workstation.

**We are assuming a separate RACF Database and Repository on each MVS. That is, we are assuming for this exercise that the RACF database is NOT shared across all MVS images.**

**The workstation certificate stores are all individually maintained and are not shared.**

*The lab is divided into several sections:*

- *Part 1: Examining the Procedures to Remove Certificates from the RACF Repository on MVS*
- *Part 2: Examining and Optionally Deleting Certificates from Microsoft Windows Certificate Repository.*

## Part 1: Examining and Optionally Deleting Certificates from RACF Repository at 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**
4. Move to the ISPF command options screen when you see the READY prompt:
  - a. **ISPF 6**
5. Enter the command to see whether the previous teams left any old certificates or Key rings out there. CAREFUL: Substitute your Team suffix for “nx” or “—” in the following commands. (Example: USER13 or GBGCAS13 if you are Team13.)
  - a. **RACDCERT ID(USERnx) LIST(LABEL('USERnx on MVSn'))**
    - i. Does it exist? **Yes or No?** \_\_\_\_\_
  - b. **RACDCERT ID(TN3270) LIST(LABEL('TN3270 on MVSn'))**
    - i. Does it exist? **Yes or No?** \_\_\_\_\_
  - c. **RACDCERT CERTAUTH LIST(LABEL('GBGCASnx LABS Server CA'))**
    - i. Does it exist? **Yes or No?** \_\_\_\_\_
  - d. **RACDCERT CERTAUTH LIST(LABEL('GBGCACnx LABS Client CA'))**
    - i. Does it exist? **Yes or No?** \_\_\_\_\_
  - e. **RACDCERT ID(USERnx) LISTRING(USERnxRing)**
    - i. Does it exist? **Yes or No?** \_\_\_\_\_
  - f. **RACDCERT ID(TN3270) LISTRING(MyServernRing)**
    - i. Where **n** is the MVS team number.
    - ii. Does it exist? **Yes or No?** \_\_\_\_\_
6. **If any one of these exists, please notify instructor so that they can be removed prior to the lab in which you will recreate them.**
7. Move to ISPF 3.4, by entering the following on the ISPF Command Line:
  - a. **=3.4**
8. Enter the High Level Qualifier of **USER.CS.TEAM\***
  - a. If you find any datasets out there with names similar to the following, *please notify the instructor to remove them:*
    - i. **USER.CS.TEAMnx.SERVERCA.DER**

- ii. **USER.CS.TEAMnx.CLIENTCA.DER**
- iii. **USER.CS.TEAMnx.P12**
- iv. **USER.CS.TEAMnx.IPSECR**
- b. The first three dataset types were used to contain x.509 certificates and optionally keys in various export formats. The last dataset was used to hold one of the configuration files produced by z/OS Configuration Assistant.

## ***You May Review this Section or Skip to Part 2***

These are the steps the instructors take to remove the certificates from the key rings, the key rings themselves, and then the certificates at MVS.

### **Cleaning up the Server Key Ring Environment at Each MVS**

1. The instructor removed the TN3270 Server Certificate from the Server's Key Ring, where "n" or "-" is the MVS Suffix and "nx" is the Suffix of the student team USERID:  
RACDCERT REMOVE(ID(TN3270)  
    LABEL('TN3270 on MVS-') RING('MyServer-Ring')) ID(TN3270)
2. The instructor removed the CA Certificate that signed the Server Certificate from the Server's Key Ring:  
RACDCERT REMOVE(CERTAUTH  
    LABEL('GBGCASnx LABS Server CA') RING('MyServer-Ring'))  
    ID(TN3270)
3. The instructor removed the CA Certificate that signed the Client Certificate from the Server's Key Ring:  
RACDCERT REMOVE(CERTAUTH  
    LABEL('GBGCACnx LABS Client CA') RING('MyServer-Ring'))  
    ID(TN3270)
4. The instructor removed the Server Key Ring from the RACF Repository:  
RACDCERT ID(TN3270) DELRING(MyServer-Ring)

### **Cleaning up the Client Key Ring Environment at Each MVS that Remained after the Previous Class**

Just read through the next steps to see the commands the instructors used to remove any certificates and keyring created by the previous class. You do not have to execute these commands.

1. The instructor has already removed the Client Certificate from the Client's Key Ring, where "n" is the MVS Suffix and "nx" is the Suffix of the student team USERID:  
RACDCERT REMOVE(ID(USERnx)  
    LABEL('USERnx on MVS2') RING('USERnxRing')) ID(USERnx)
2. The instructor has already removed the CA Certificate that signed the Client Certificate from the Client's Key Ring:  
RACDCERT REMOVE(CERTAUTH

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

```
LABEL('GBGCACnx LABS Client CA') RING('USERnxRing'))  
ID(USERnx)
```

3. The instructor has already removed the CA Certificate that signed the Server Certificate from the Client's Key Ring:

```
RACDCERT REMOVE(CERTAUTH  
    LABEL('GBGCASnx LABS Server CA') RING('USERnxRing'))  
ID(USERnx)
```

4. The instructor has already removed the Client Key Ring from the RACF Repository:

```
RACDCERT ID(USERnx) DELRING(USERnxRing)
```

### **Cleaning up the Certificates at Each MVS**

1. The instructor has already removed the Server Certificate, the Client Certificate, Client CA Certificate, and the Server CA Certificate from the RACF Repository; then the raclisted DIGTCERT class was refreshed:

```
RACDCERT ID(TN3270) DELETE(LABEL('TN3270 on MVS-'))  
RACDCERT ID(USERnx) DELETE(LABEL('USERnx on MVS-'))  
RACDCERT CERTAUTH DELETE(LABEL('GBGCACnx LABS Client CA'))  
RACDCERT CERTAUTH DELETE(LABEL('GBGCASnx LABS Server CA'))  
setropts raclist(DIGTCERT) refresh
```

### **End of Required MVS Certificate Removal Lab**

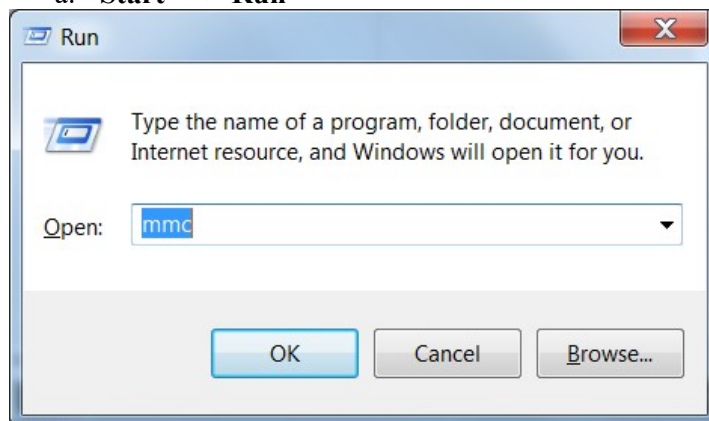
## Part 2 : Examining and Optionally Deleting Certificates from Repository on Microsoft Windows (Windows 10)

### Background:

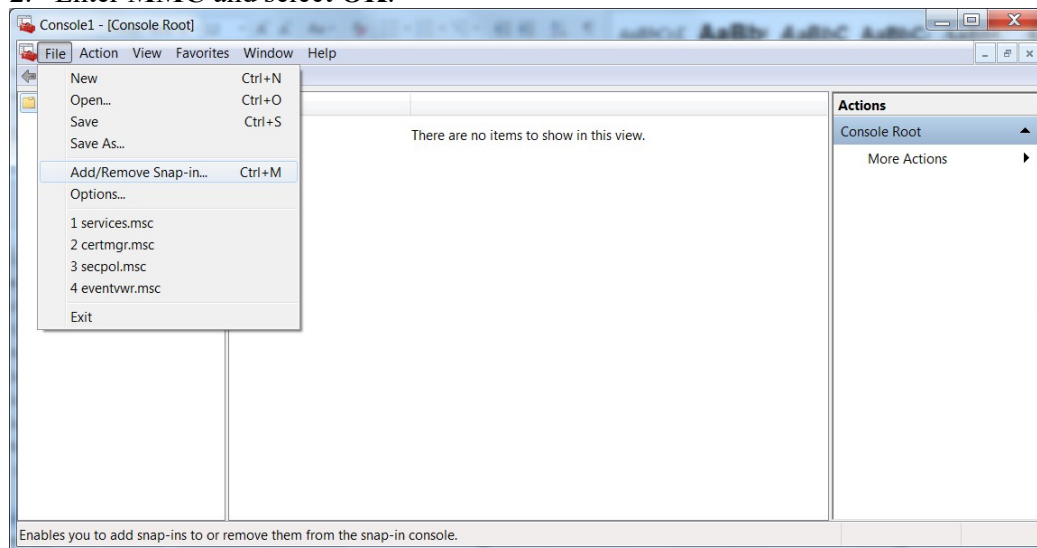
- Some applications have their own Certificate Management utilities, as does PCOMM.
- Other applications, like IPsec in Windows or some SSL/TLS FTP Client programs, take advantage of the Microsoft Certificate Management Utility.
- Others, like PCOMM 5.9.4, permit you to use either an imbedded certificate management utility or to exploit the Microsoft Certificate Management Utility.

### Locating Certificate Management in the Microsoft Management Console (MMC)

1. At your workstation:
  - a. **Start >>> Run**



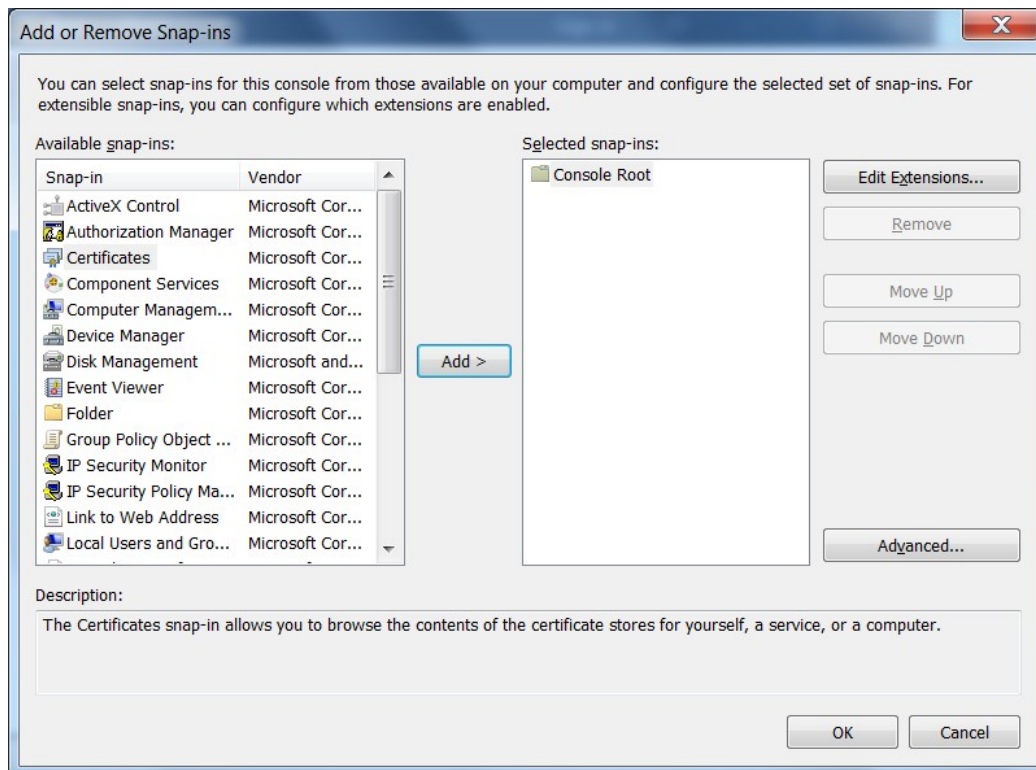
2. Enter **MMC** and select **OK**.



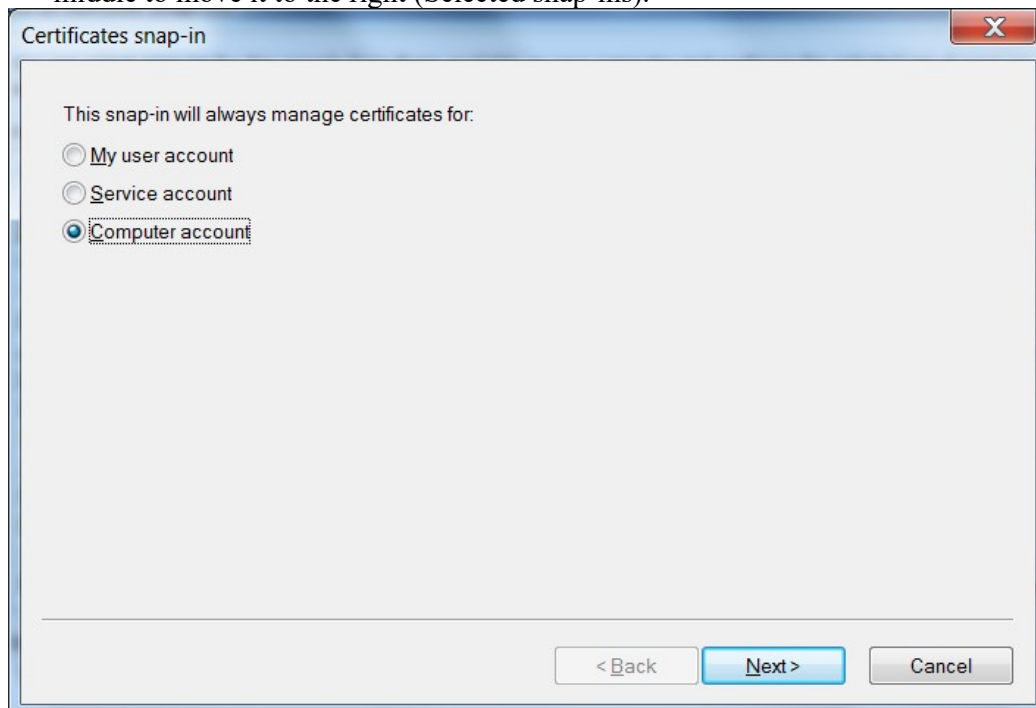
3. **File >>> Add/Remove Snap-in**



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

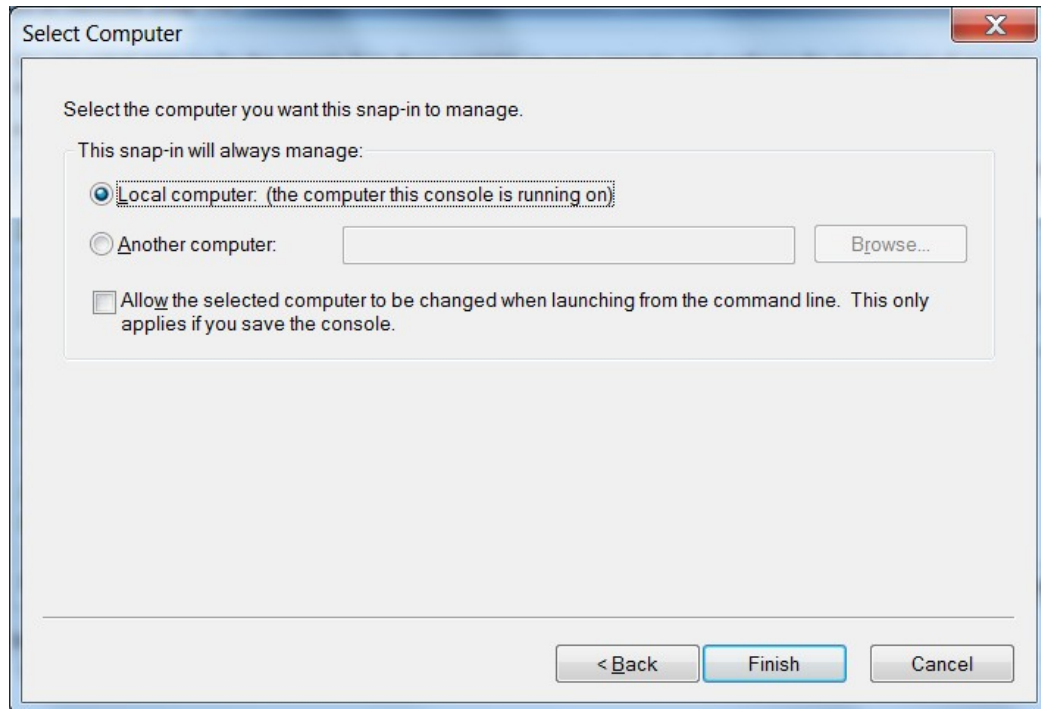


4. Select **Certificates** on the left (Available snap-ins) and use the **Add** button in the middle to move it to the right (Selected snap-ins).

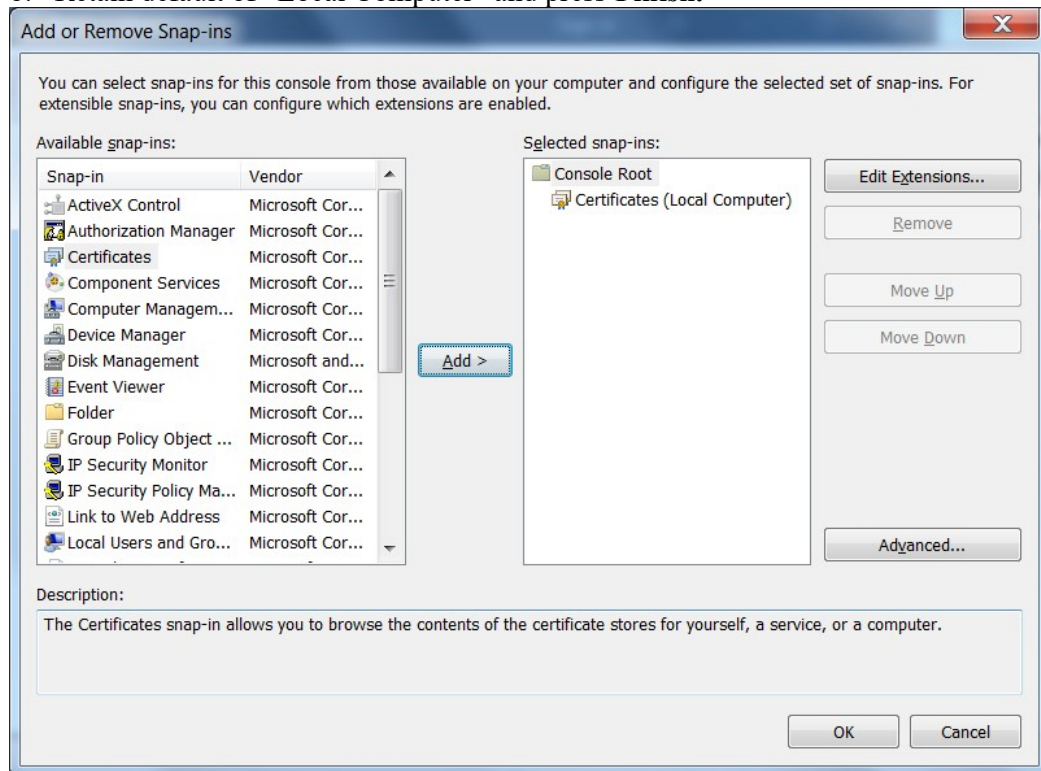


5. On the "Certificates snap-in" screen, select Radio Button for **Computer Account**.
  - a. **Next**

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

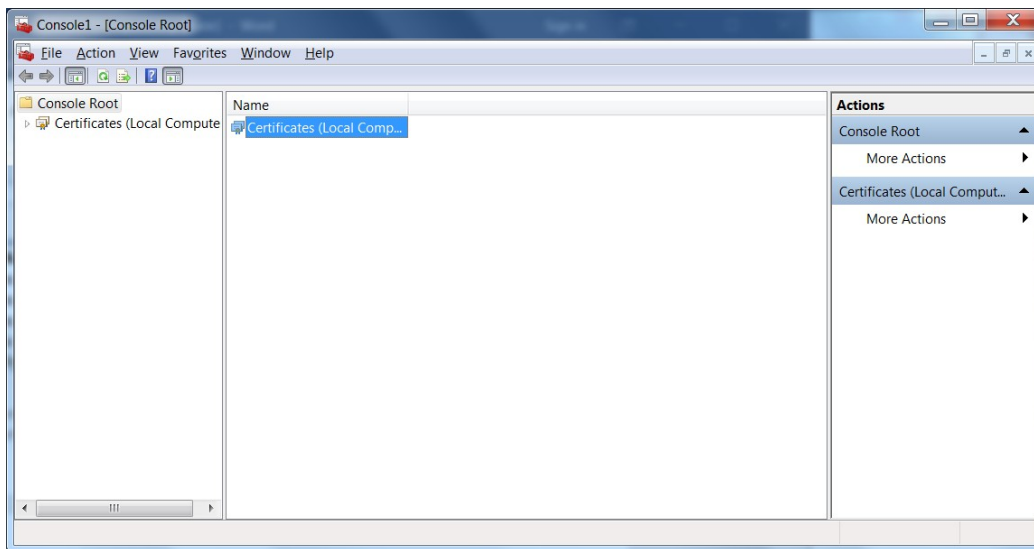


b. Retain default of “Local Computer” and press **Finish**.

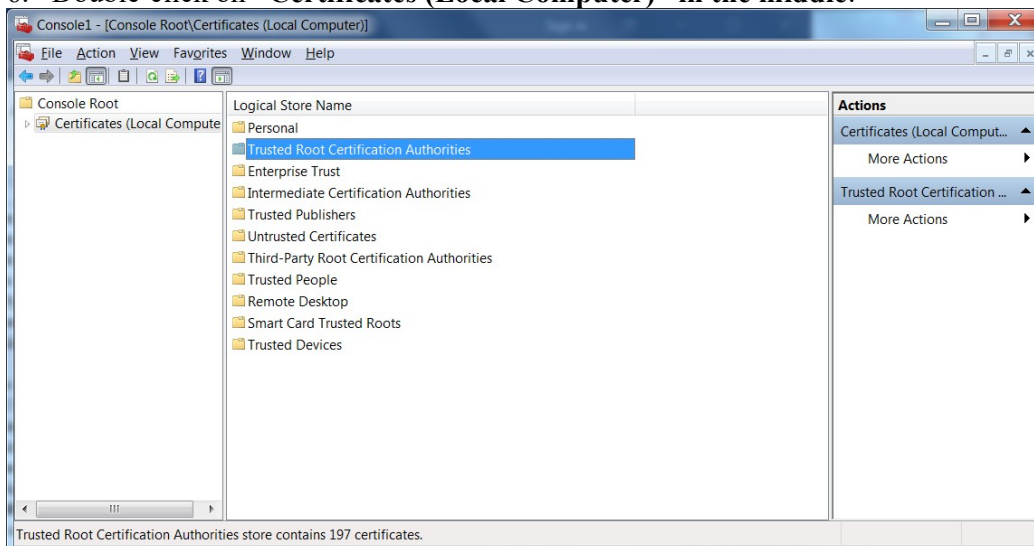


c. Click on **OK**

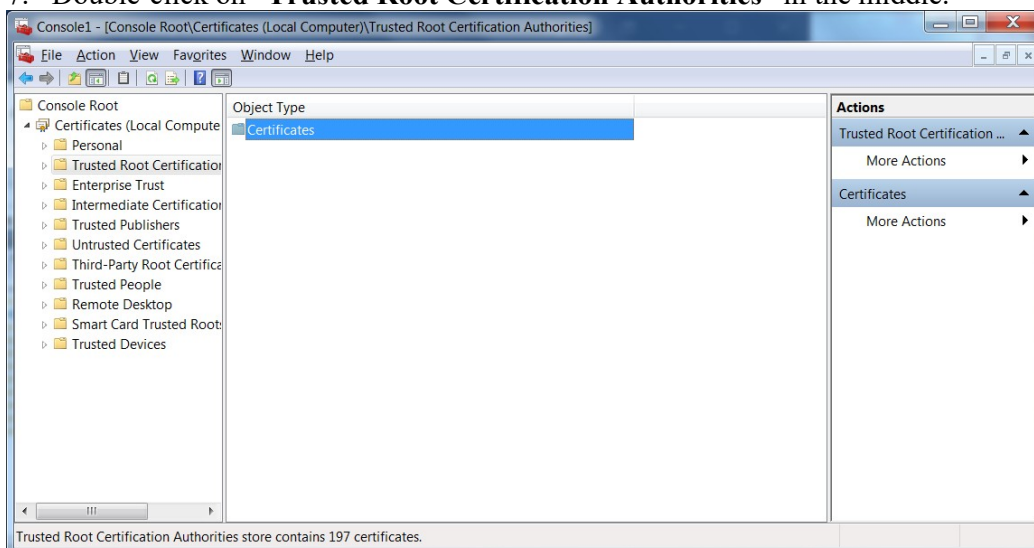
## Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent



6. Double-click on **“Certificates (Local Computer)”** in the middle.



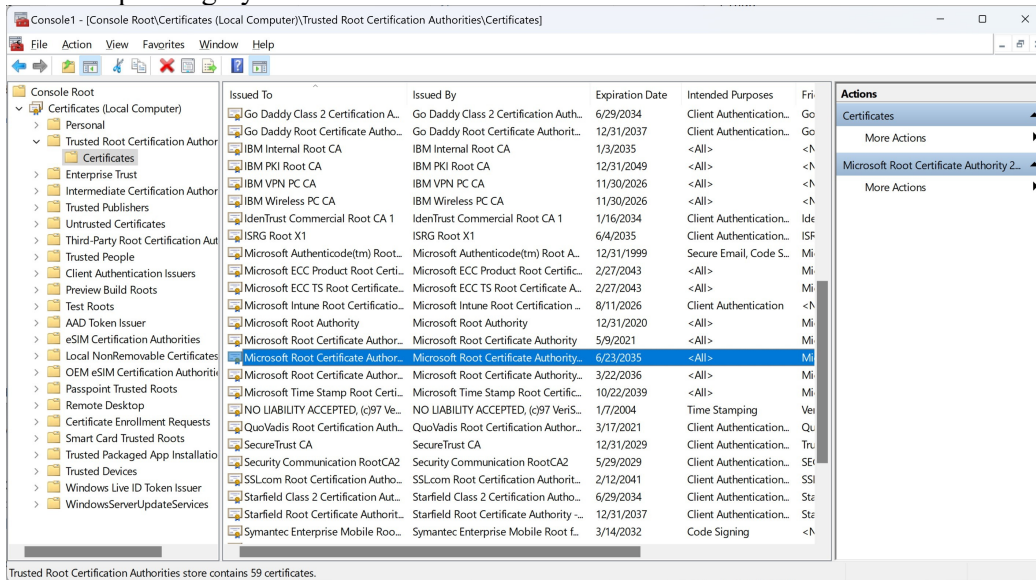
7. Double-click on **“Trusted Root Certification Authorities”** in the middle.



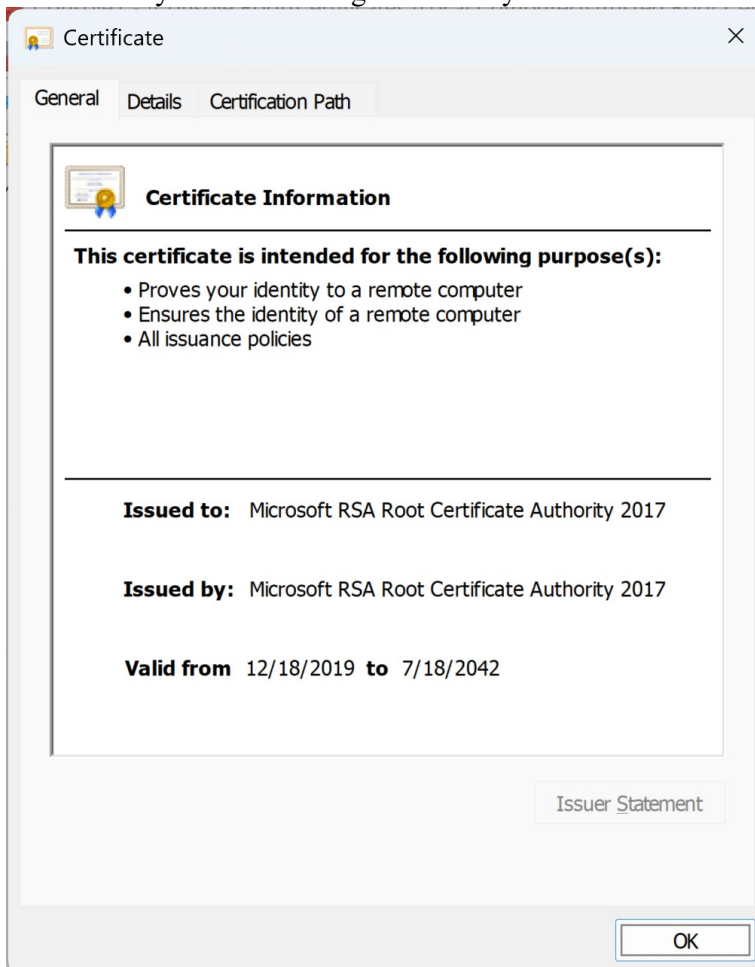
8. Double-click on **“Certificates”** in the middle.

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

- a. This reveals to you the certificates that were included with the Microsoft Operating System.

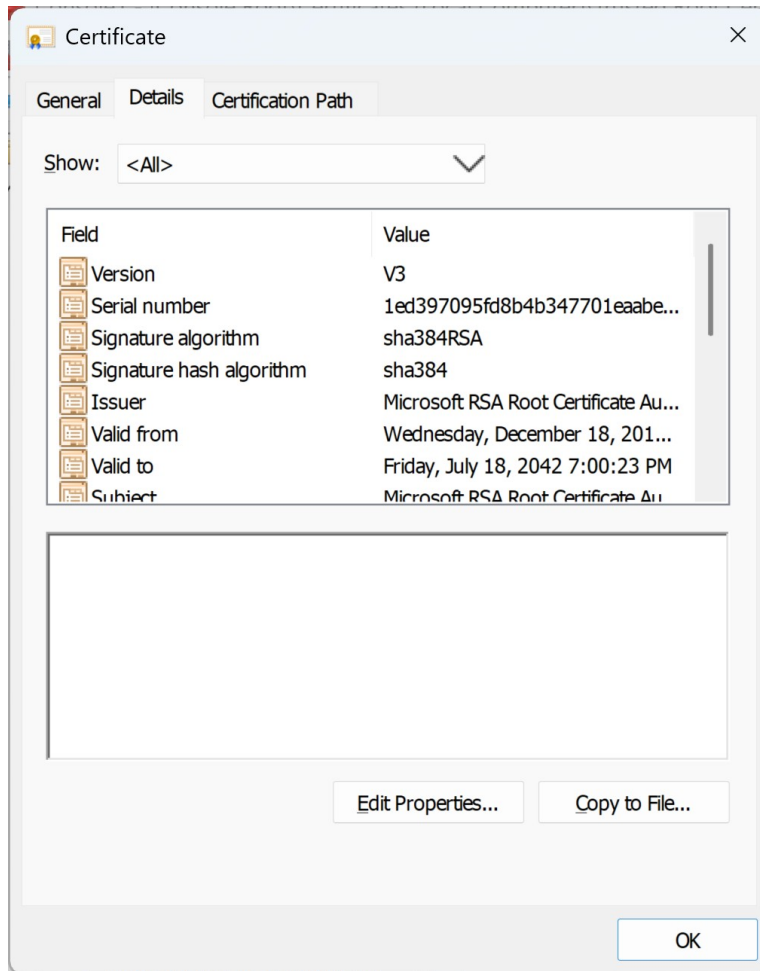


9. Examine the contents of the first **Microsoft Root Certificate Authority 2017** in the list by double-clicking on the entry.



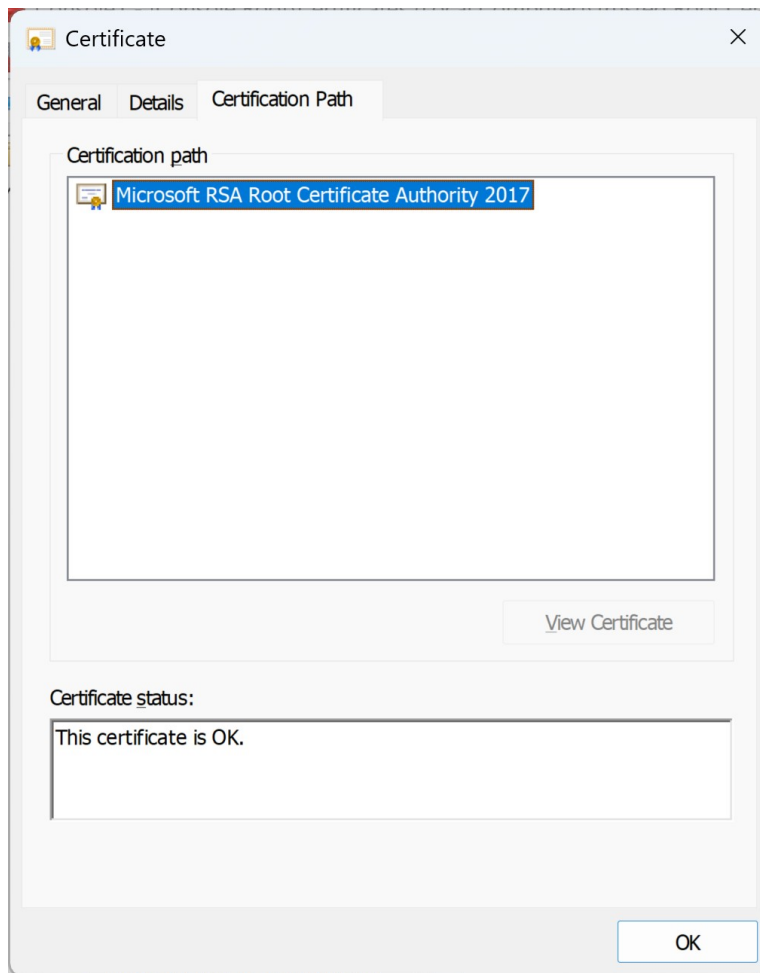
10. Select the **Detail** tab.

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



11. Select the **Certification Path** Tab.

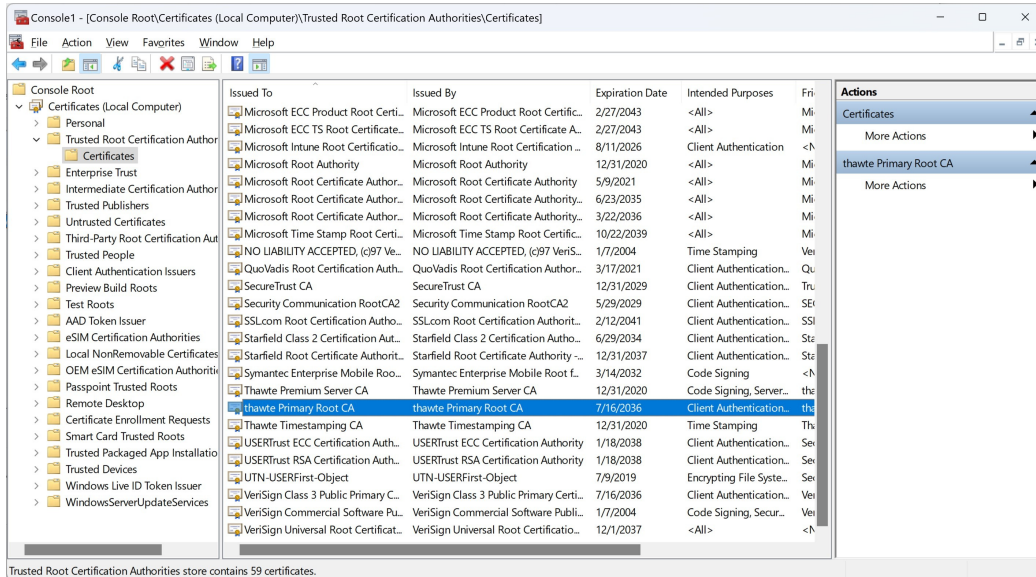
## Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent



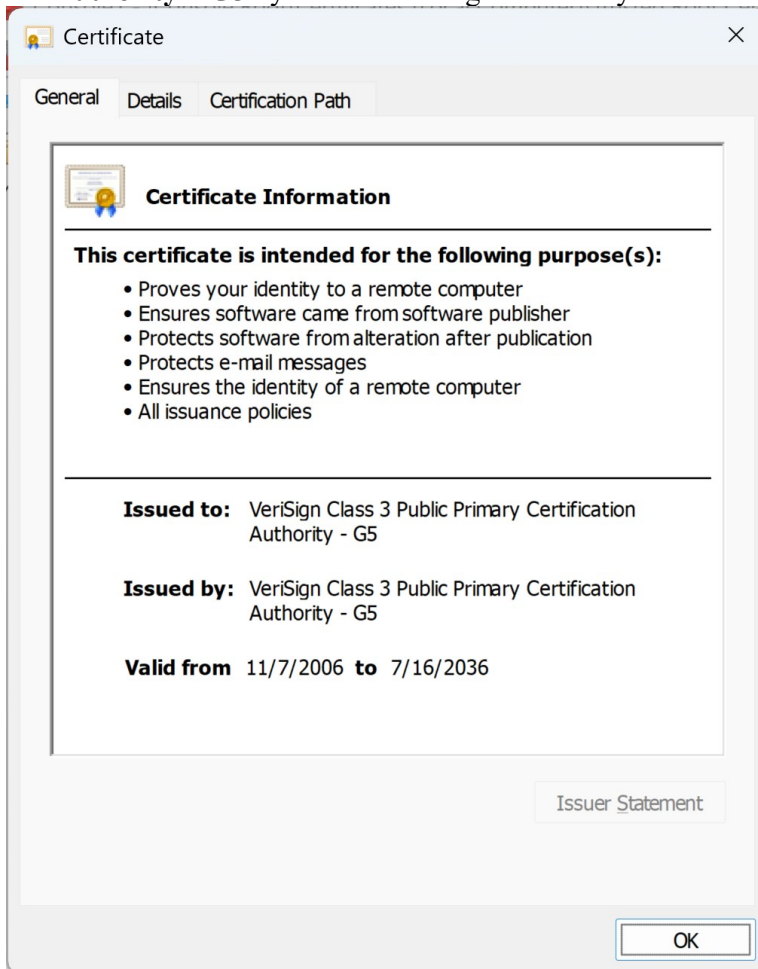
12. Answer these questions:
- a. How many certificates are in the “chain of trust” for this certificate?
    - i. \_\_\_\_\_
      - 1) This tells you that this is a Root CA certificate (a self-signed certificate)
13. Exit from the view of this Certificate by selecting **OK**.



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

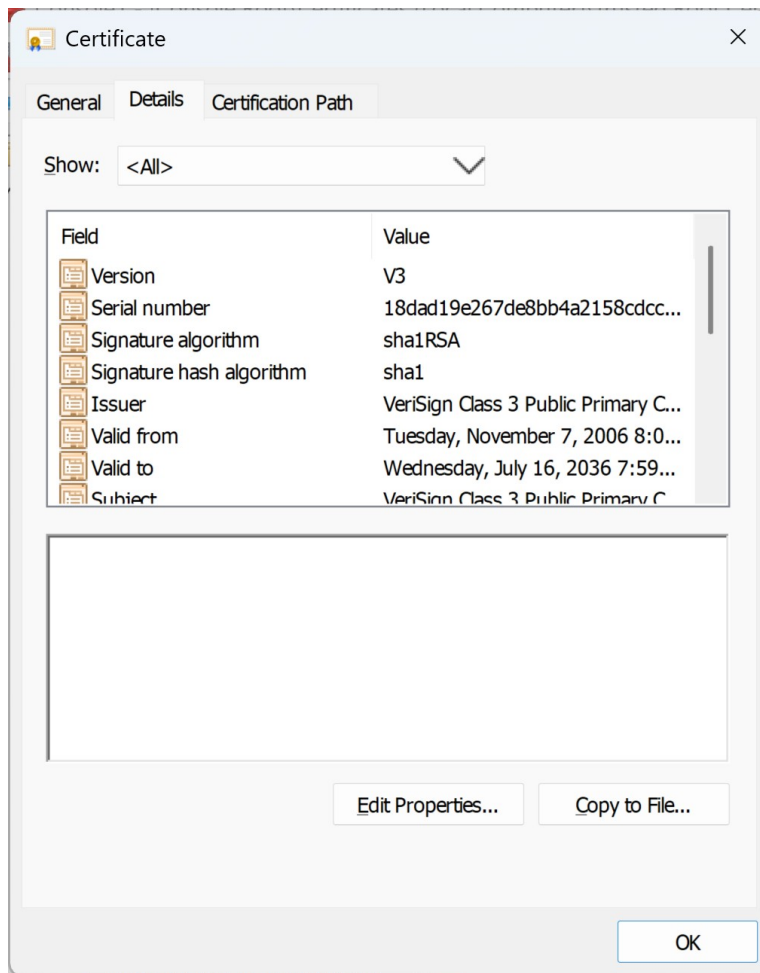


14. Examine the contents of the **VeriSign Class 3 Public Primary Certification Authority – G5** by double-clicking on the entry.



15. Select the **Detail** tab.

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



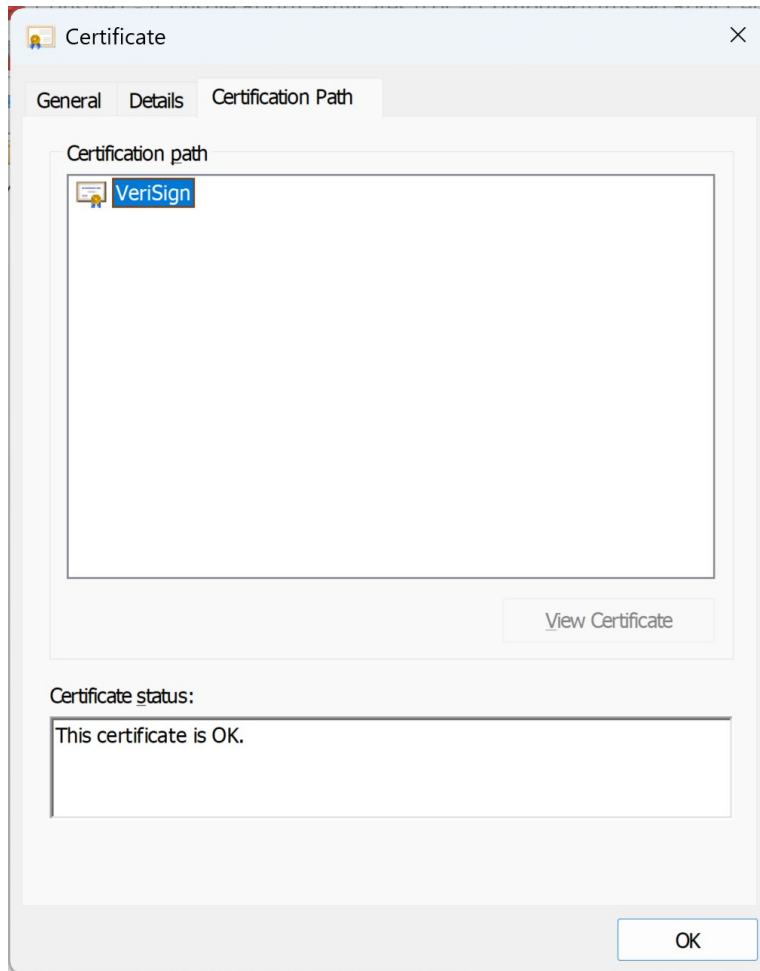
16. Answer these questions:

- a. What is this certificate being used for? (Key Usage)
  - i. Certificate Signing \_\_\_\_\_
  - ii. Off-line CRL Signing \_\_\_\_\_
  - iii. CRL Signing \_\_\_\_\_

17. Select the **Certification Path** tab.



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



18. Answer these questions:
- How many certificates are in the “chain of trust” for this certificate?
    - \_\_\_\_\_1) This tells you that this is a Root CA certificate (a self-signed certificate)
19. Exit from the view of this Certificate by selecting **OK**.
20. Exit from the MMC by selecting:
- File >>> Exit >>> No** (Do not Save)

## End of the Lab

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

