



12895: Rekeying and Renewing Your Expired Digital Certificates in RACF

Hands-on Lab Intro

Gwen Dente, IBM Advanced Technical Skills
(gdente@us.ibm.com)

Tuesday, February 5, 2013: 09:30 AM - 10:30 AM,
HIL, Union Square 23-24, Fourth Floor
Session Number 12895

In this 1st Document:

- Read Descriptions of 2 required Scenarios (pp. 9-12).

- Find your team's IPv4 interfaces and addresses (pp. 15-29).

In the 2nd Document:

- Lab starts on page 15

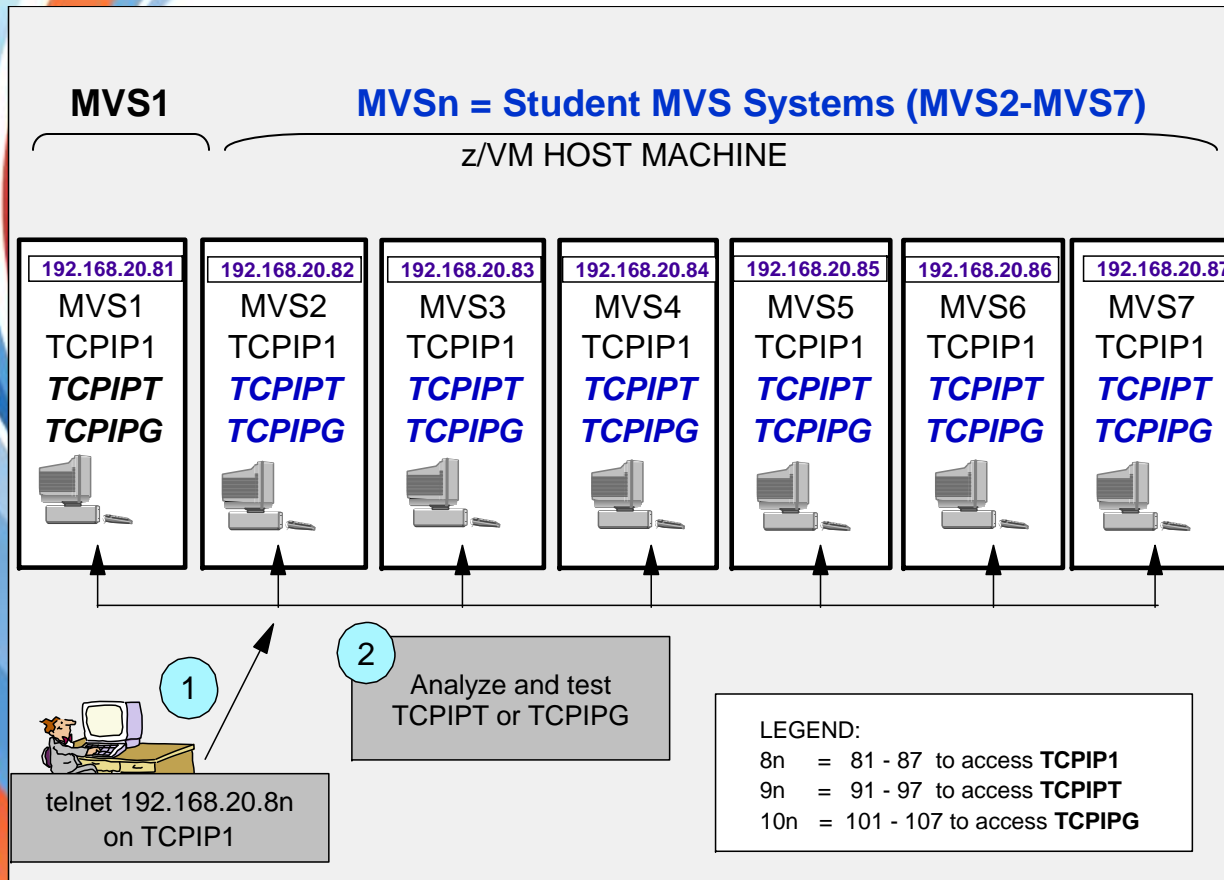


Abstract

- You finally succeeded in establishing a secure environment for FTP on z/OS using security certificates and keyrings. But you forgot one thing: certificates and keys can expire and no longer be usable. In this lab you will learn how to manage your keys and certificates in order to avoid downtime incurred due to expired certificates.

PREREQUISITE: This lab is self-driven and assumes that the attendee already understands x.509 certificate processing and Public Key Infrastructure. The knowledge can be gained by lectures or through previous experience.

Student MVS_n Tests with MVS1; 2 Student TCP/IP Stacks (TCPIPT,TCPIPG)

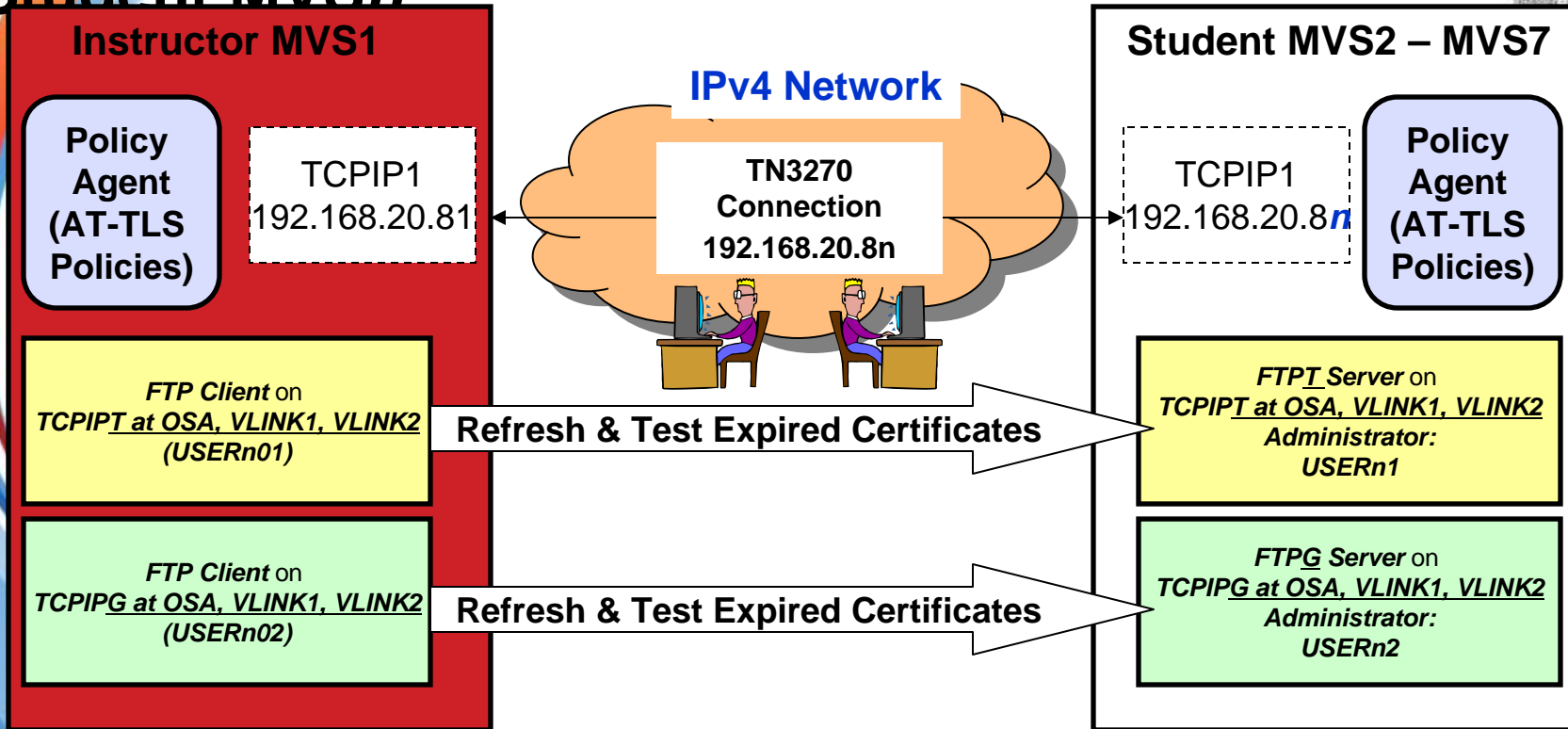


LEGEND:
 "n" represents MVS suffix (1-7)
 Example: MVS_n = MVS1-7
 Example: 8_n = 81-87

LEGEND:
 8n = 81 - 87 to access **TCPIP1**
 9n = 91 - 97 to access **TCPIPT**
 10n = 101 - 107 to access **TCPIPG**

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

Scenarios for Testing between MVS1 & Student MVS_n



1. Test successful secured FTP client connection from MVS1 to your AT-TLS FTP Server at TCPIPT or TCPIPG stack in MVS_n. Testing between Source and Destination OSA Port addresses.
2. Test same connection using expired FTP Server certificate on key ring associated with your FTP Server.
 1. Refresh the expired Server certificate and re-test. Testing between Source and Destination VLINK1 addresses.
3. Test same connection again using expired CA and FTP Server certificates on key ring associated with your FTP Server.
 1. Refresh both expired certificates and re-test the connection. Testing between Source and Destination VLINK2 addresses.

Assignment of Student IDs to TCPIPT or TCPIPG Stacks in MVS_n

TEAM_{n1} / USER_{n1}

TCPIPT Stack

<u>Primary Userid</u>	<u>Alternate Userid</u>
MVS1: USER11	USER101
MVS2: USER21	USER201
MVS3: USER31	USER301
MVS4: USER41	USER401
MVS5: USER51	USER501
MVS6: USER61	USER601
MVS7: USER71	USER701

TEAM_{n2} / USER_{n2}

TCPIPG Stack

<u>Primary Userid</u>	<u>Alternate Userid</u>
MVS1: USER12	USER102
MVS2: USER22	USER202
MVS3: USER32	USER302
MVS4: USER42	USER402
MVS5: USER52	USER502
MVS6: USER62	USER602
MVS7: USER72	USER702

•“n” = Suffix of MVS Image

•Password: gbguser

•z/OS hlq: USER.CS.xxx

•UNIX Subdirectory: /u/user_{nx} (“nx” is suffix of userid)

Assignment of Student IDs to TCPIPT in MVS_n (TEAM_{n1})

TEAM_{n1} / USER_{n1}

Users at TCPIPT Stack

<u>Primary Userid</u>	<u>Telnet into TCPIP1 for Maintenance:</u>	<u>Alternate Userid</u>
MVS1: USER11	192.168.20.81	USER101
MVS2: USER21	192.168.20.82	USER201
MVS3: USER31	192.168.20.82	USER301
MVS4: USER41	192.168.20.84	USER401
MVS5: USER51	192.168.20.85	USER501
MVS6: USER61	192.168.20.86	USER601
MVS7: USER71	192.168.20.87	USER701

- “n” = Suffix of MVS Image
- Password: gbguser
- z/OS hlq: USER.CS.xxx
- UNIX Subdirectory: /u/user_{nx} (“nx” is suffix of userid)

Assignment of Student IDs to TCPIPG in MVS_n (TEAM_{n2})

#SHAREorg



TEAM_{n2} / USER_{n2}

Users at TCPIPG Stack

<u>Primary Userid</u>	<u>Telnet into TCPIP1 for Maintenance:</u>	<u>Alternate Userid</u>
MVS1: USER12	192.168.20.81	USER102
MVS2: USER22	192.168.20.82	USER202
MVS3: USER32	192.168.20.82	USER302
MVS4: USER42	192.168.20.84	USER402
MVS5: USER52	192.168.20.85	USER502
MVS6: USER62	192.168.20.86	USER602
MVS7: USER72	192.168.20.87	USER702

- “n” = Suffix of MVS Image
- Password: gbguser
- z/OS hlq: USER.CS.xxx
- UNIX Subdirectory: /u/user_{nx} (“nx” is suffix of userid)

Key Ring Repository Scenarios (Key Rings and their Certificates)

Two Choices: Renew Expiring Certificate or Replace Private Key



- **Renewing an expiring certificate**

- When a certificate approaches its expiration date, you can renew the certificate and continue using it. You can choose to renew the certificate using the same private key, thereby extending the life of the private key.

- **Retiring a private key**

- Or you can retire the private key and replace it with a new private key (also called certificate *rekeying* or *key rollover*).

- **Scenarios**

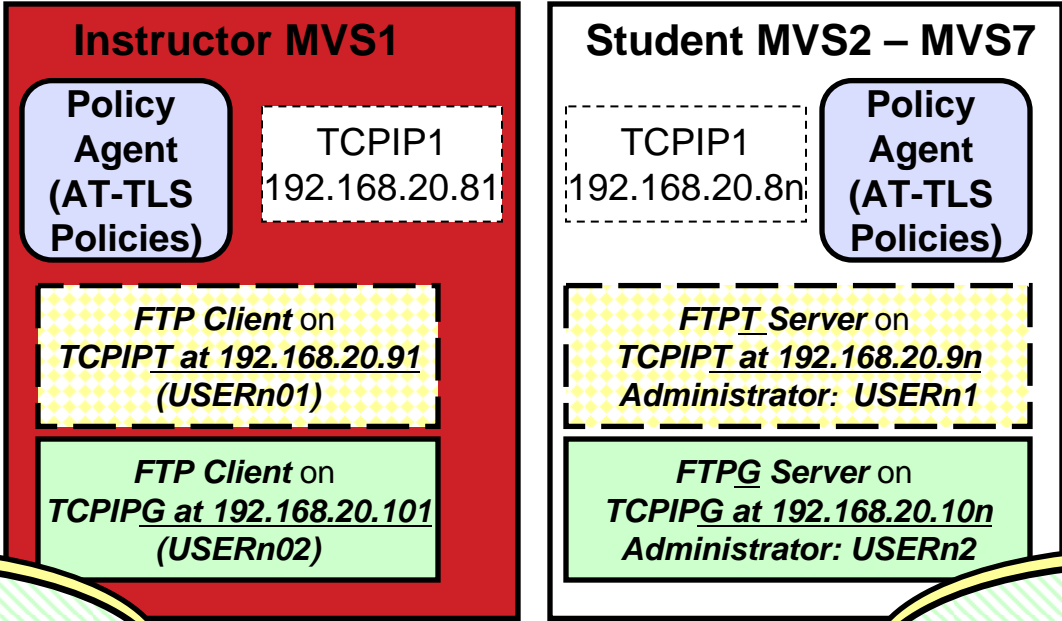
- In **Scenario 1** while using a discrete AT-TLS policy for address ranges 192.168.20.91-97 for TCPIPT and 192.168.20.101-107 for TCPIPG your AT-TLS connections work fine. Certificates are still valid.
- In **Scenario 2** and using a 2nd discrete AT-TLS policy for address ranges 192.168.20.111-117 for TCPIPT and 192.168.20.121-127 for TCPIPG your AT-TLS connections fail with SSL Return Code of 401.
- In **Optional Scenario 3** we ask you to rekey (“rollover”) the FTP Server Certificate and test it.
- In **Optional Scenario 4** while using a 3rd discrete AT-TLS policy for address ranges 172.16.20.111-117 for TCPIPT and 172.16.20.121-127 for TCPIPG your AT-TLS connections fail with SSL Return Code of 401.

- **RACF Prerequisites**


- Authorization to the RACDCERT ROLLOVER, GENCERT, GENREQ, ALTER, REKEY commands and the SETROPTS command.
 - Only the Instructor has authorization to the SETROPTS command, but the PROC named “SPECUSER” can issue the command on a student’s behalf.
 - Prior to the class, students are permitted appropriate temporary access to the facility classes for ALTER, REKEY, and ROLLOVER.

Scenario 1: Successful Key Ring and its Certificates

**FTP.DATA specifies
Server Authentication Only**



TCPIP/Client_RING
•MVS1 LABS Certificate Authority

FTPD/Server_RING 
•FTP Server on MVS1-MVS7
•MVS1 LABS Certificate Authority

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

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

#SHAREorg



**FTP.DATA specifies
Server Authentication Only**

FTPD/FTPEXPn1_RING
 •FTPServer_{n1} EXP
 •MVS1 LABS Certificate Authority

Instructor MVS1

Policy Agent (AT-TLS Policies)
 TCPIP1
 192.168.20.81

FTP Client on TCPIPT at 192.168.20.111 (USERn01)

FTP Client on TCPIPG at 192.168.20.121 (USERn02)

Policy Agent (AT-TLS Policies)
 TCPIP1
 192.168.20.8n

FTPT_Server on TCPIPT at 192.168.20.11n Administrator: USERn1

FTPG_Server on TCPIPG at 192.168.20.12n Administrator: USERn2

TCPIP/Client_RING
 •MVS1 LABS Certificate Authority

SSL RC 401

FTPD/FTPEXPn2_RING
 •FTPServer_{n2} EXP
 •MVS1 LABS Certificate Authority

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



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

**FTP.DATA specifies
Server Authentication Only**

FTPD/FTPEXPn1_RING
 •FTPServer_{n1} EXP
 •[FTPServer_{n1} EXP-2]
 •MVS1 LABS Certificate Authority

Instructor MVS1

Policy Agent (AT-TLS Policies)
 TCPIP1
 192.168.20.81

FTP Client on TCPIPT at 192.168.20.111 (USERn01)

FTP Client on TCPIPG at 192.168.20.121 (USERn02)

Policy Agent (AT-TLS Policies)
 TCPIP1
 192.168.20.8n

FTPT Server on TCPIPT at 192.168.20.11n Administrator: USERn1

FTPG Server on TCPIPG at 192.168.20.12n Administrator: USERn2

TCPIP/Client_RING
 •MVS1 LABS Certificate Authority

FTPD/FTPEXPn2_RING
 •FTPServer_{n2} EXP
 •[FTPServer_{n2} EXP-2]
 •MVS1 LABS Certificate Authority

1. The separate FTP Server Certificates are associated with Private Keys that have been compromised. The FTP Client Key Ring is shared.
2. You must correct this certificate with a RENEW and then with a ROLLOVER and test. Addresses are VLINK1 addresses:
TCPIPT: 192.168.20.111-117; TCPIPG: 192.168.20.121-127

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

**FTP.DATA specifies
Server Authentication Only**

TCPIP/ClientEXP_{n1}_RING
•ZOS_{n1} EXPCA
•[ZOS_{n1} EXPCA-2]

FTPD/FTPCAX_{n1}_RING
•FTPServer_{n1} EXPCA
•ZOS_{n1} EXPCA
•[ZOS_{n1} EXPCA-2]

Instructor MVS1

Policy Agent (AT-TLS Policies)
TCPIP1
192.168.20.81

FTP Client on TCPIPT at 172.16.20.111 (USER_{n1})

FTP Client on TCPIPG at 172.16.20.121 (USER_{n2})

Student MVS2 – MVS7

Policy Agent (AT-TLS Policies)
TCPIP1
192.168.20.8n

FTPT_Server on TCPIPT at 172.16.20.11n Administrator: USER_{n1}

FTPG_Server on TCPIPG at 172.16.20.12n Administrator: USER_{n2}

TCPIP/ClientEXP_{n2}_RING
•ZOS_{n2} EXPCA
•[ZOS_{n2} EXPCA-2]

FTPD/FTPCAX_{n2}_RING
•FTPServer_{n2} EXPCA
•ZOS_{n2} EXPCA
•[ZOS_{n2} EXPCA-2]

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

TCPIPT: 172.16.20.111-117; TCPIPG: 172.16.20.121-127

APPENDIX A: Addresses for MVS1 – MVS7 in TCPIPT and TCPIPG

MVS1 Addresses and (Sub)Networks - Instructor MVS - TCPIPT



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.81

- **At Customizable TCPIPT:**

- **Static VIPAs:**

- VLINK2 172.16.20.111 / 24
- VLINK1 192.168.20.111 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.91 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS 10.1.1.11 / 24
- IQDIOLNK0101010n 10.1.1.11 / 24

- **Predefined HiperSocket:**

- HSDELNK 172.16.20.11 / 24

- **Loopback:**

- LOOPBACK 127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

MVS1 Addresses and (Sub)Networks - Instructor MVS - TCPIPG



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.82

- **At Customizable TCPIPG:**

- **Static VIPAs:**

- VLINK2 172.16.20.121 / 24
- VLINK1 192.168.20.121 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.101 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS 10.1.1.21 / 24
- IQDIOLNK0101010n 10.1.1.21 / 24

- **Predefined HiperSocket:**

- HSDELNK 172.16.20.21 / 24

- **Loopback:**

- LOOPBACK 127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

Student MVS2 Addresses and (Sub)Networks

- TCPIPT

#SHAREorg



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.82

- Student USERID = USER21
- TSO Password = gbguser
- UNIX Subdirectory = /u/user21
- Telnet to 192.168.20.82
- Alternate USERID = USER201

- **At Customizable TCPIPG:**

- **Static VIPAs:**
 - VLINK2 172.16.20.112 / 24
 - VLINK1 192.168.20.112 / 24
- **1000Base-T OSA Interface:**
 - GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.92 / 24
- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**
 - EZASAMEMVS 10.1.1.12 / 24
 - IQDIOLNK0101010n 10.1.1.12 / 24
- **Predefined HiperSocket:**
 - HSDELNK 172.16.20.12 / 24
- **Loopback:**
 - LOOPBACK 127.0.0.1 / 24
- **Default Gateway:** 192.168.20.1 / 24

Student MVS2 Addresses and (Sub)Networks

- TCPIP



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.82

- Student USERID = USER22
- TSO Password = gbguser
- UNIX Subdirectory = /u/user22
- Telnet to 192.168.20.82
- Alternate USERID = USER202

- **At Customizable TCPIP:**

- **Static VIPAs:**

- VLINK2 172.16.20.122 / 24
- VLINK1 192.168.20.122 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.102 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS 10.1.1.22 / 24
- IQDIOLNK0101010n 10.1.1.22 / 24

- **Predefined HiperSocket:**

- HSDELNK 172.16.20.22 / 24

- **Loopback:**

- LOOPBACK 127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

Student MVS3 Addresses and (Sub)Networks

- TCPIPT



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.83

- Student USERID = USER31
- TSO Password = gbguser
- UNIX Subdirectory = /u/user31
- Telnet to 192.168.20.83
- Alternate USERID = USER301

- **At Customizable TCPIPG:**

- ***Static VIPAs:***

- **VLINK2** 172.16.20.113 / 24
- **VLINK1** 192.168.20.113 / 24

- ***1000Base-T OSA Interface:***

- **GIG1F/LGIG1F**
(aka OSDGIG1F) 192.168.20.93 / 24

- ***Dynamic XCF Interfaces (incl. Dynamic HiperSocket):***

- **EZASAMEMVS** 10.1.1.13 / 24
- **IQDIOLNK0101010n** 10.1.1.13 / 24

- ***Predefined HiperSocket:***

- **HSDELNK** 172.16.20.13 / 24

- ***Loopback:***

- **LOOPBACK** 127.0.0.1 / 24

- ***Default Gateway:***

192.168.20.1 / 24

Student MVS3 Addresses and (Sub)Networks

– TCPIP

#SHAREorg



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.83

- Student USERID = USER32
- TSO Password = gbguser
- UNIX Subdirectory = /u/user32
- Telnet to 192.168.20.83
- Alternate USERID = USER302

- **At Customizable TCPIP:**

- **Static VIPAs:**

- VLINK2
- VLINK1

172.16.20.123 / 24
192.168.20.123 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F
(aka OSDGIG1F)

192.168.20.103 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS
- IQDIOLNK0101010n

10.1.1.23 / 24
10.1.1.23 / 24

- **Predefined HiperSocket:**

- HSDELNK

172.16.20.23 / 24

- **Loopback:**

- LOOPBACK

127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

Student MVS4 Addresses and (Sub)Networks

- TCPIPT



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.84

- Student USERID = USER41
- TSO Password = gbguser
- UNIX Subdirectory = /u/user41
- Telnet to 192.168.20.84
- Alternate USERID = USER401

- **At Customizable TCPIPG:**

- **Static VIPAs:**

- VLINK2 172.16.20.114 / 24
- VLINK1 192.168.20.114 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.94 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS 10.1.1.14 / 24
- IQDIOLNK0101010n 10.1.1.14 / 24

- **Predefined HiperSocket:**

- HSDELNK 172.16.20.14 / 24

- **Loopback:**

- LOOPBACK 127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

Student MVS4 Addresses and (Sub)Networks

– TCPIP



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.84

- Student USERID = USER42
- TSO Password = gbguser
- UNIX Subdirectory = /u/user42
- Telnet to 192.168.20.84
- Alternate USERID = USER402

- **At Customizable TCPIP:**

- **Static VIPAs:**
 - VLINK2 172.16.20.124 / 24
 - VLINK1 192.168.20.124 / 24
- **1000Base-T OSA Interface:**
 - GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.104 / 24
- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**
 - EZASAMEMVS 10.1.1.24 / 24
 - IQDIOLNK0101010n 10.1.1.24 / 24
- **Predefined HiperSocket:**
 - HSDELNK 172.16.20.24 / 24
- **Loopback:**
 - LOOPBACK 127.0.0.1 / 24
- **Default Gateway:** 192.168.20.1 / 24

Student MVS5 Addresses and (Sub)Networks

- TCPIPT



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.85

- Student USERID = USER51
- TSO Password = gbguser
- UNIX Subdirectory = /u/user51
- Telnet to 192.168.20.85
- Alternate USERID = USER501

- **At Customizable TCPIPG:**

- **Static VIPAs:**

- VLINK2 172.16.20.115 / 24
- VLINK1 192.168.20.115 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.95 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS 10.1.1.15 / 24
- IQDIOLNK0101010n 10.1.1.15 / 24

- **Predefined HiperSocket:**

- HSDELNK 172.16.20.15 / 24

- **Loopback:**

- LOOPBACK 127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

Student MVS5 Addresses and (Sub)Networks

- TCPIP



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.85

- Student USERID = USER52
- TSO Password = gbguser
- UNIX Subdirectory = /u/user52
- Telnet to 192.168.20.85
- Alternate USERID = USER502

- **At Customizable TCPIP:**

- **Static VIPAs:**

- VLINK2 172.16.20.125 / 24
- VLINK1 192.168.20.125 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.105 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS 10.1.1.25 / 24
- IQDIOLNK0101010n 10.1.1.25 / 24

- **Predefined HiperSocket:**

- HSDELNK 172.16.20.25 / 24

- **Loopback:**

- LOOPBACK 127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

Student MVS6 Addresses and (Sub)Networks

- TCPIPT



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.86

- Student USERID = USER61
- TSO Password = gbguser
- UNIX Subdirectory = /u/user61
- Telnet to 192.168.20.86
- Alternate USERID = USER601

- **At Customizable TCPIPG:**

- **Static VIPAs:**

- VLINK2
- VLINK1

172.16.20.116 / 24
192.168.20.116 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F
(aka OSDGIG1F)

192.168.20.96 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS
- IQDIOLNK0101010n

10.1.1.16 / 24
10.1.1.16 / 24

- **Predefined HiperSocket:**

- HSDELNK

172.16.20.16 / 24

- **Loopback:**

- LOOPBACK

127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

Student MVS6 Addresses and (Sub)Networks

– TCPIP



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.86

- Student USERID = USER62
- TSO Password = gbguser
- UNIX Subdirectory = /u/user62
- Telnet to 192.168.20.86
- Alternate USERID = USER602

- **At Customizable TCPIP:**

- **Static VIPAs:**

- VLINK2 172.16.20.126 / 24
- VLINK1 192.168.20.126 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.106 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS 10.1.1.26 / 24
- IQDIOLNK0101010n 10.1.1.26 / 24

- **Predefined HiperSocket:**

- HSDELNK 172.16.20.26 / 24

- **Loopback:**

- LOOPBACK 127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

Student MVS7 Addresses and (Sub)Networks

- TCPIPT



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.87

- Student USERID = USER71
- TSO Password = gbguser
- UNIX Subdirectory = /u/user71
- Telnet to 192.168.20.87
- Alternate USERID = USER701

- **At Customizable TCPIPG:**

- **Static VIPAs:**

- VLINK2 172.16.20.117 / 24
- VLINK1 192.168.20.117 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.97 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS 10.1.1.17 / 24
- IQDIOLNK0101010n 10.1.1.17 / 24

- **Predefined HiperSocket:**

- HSDELNK 172.16.20.17 / 24

- **Loopback:**

- LOOPBACK 127.0.0.1 / 24

- **Default Gateway:**

192.168.20.1 / 24

Student MVS7 Addresses and (Sub)Networks

– TCPIP



- **At Control or Maintenance TCPIP1:**

- Telnet Address is 192.168.20.87

- **At Customizable TCPIP:**

- Student USERID = USER72
- TSO Password = gbguser
- UNIX Subdirectory = /u/user72
- Telnet to 192.168.20.87
- Alternate USERID = USER702

- **Static VIPAs:**

- VLINK2 172.16.20.127 / 24
- VLINK1 192.168.20.127 / 24

- **1000Base-T OSA Interface:**

- GIG1F/LGIG1F (aka OSDGIG1F) 192.168.20.107 / 24

- **Dynamic XCF Interfaces (incl. Dynamic HiperSocket):**

- EZASAMEMVS 10.1.1.27 / 24
- IQDIOLNK0101010n 10.1.1.27 / 24

- **Predefined HiperSocket:**

- HSDELNK 172.16.20.27 / 24

- **Loopback:**

- LOOPBACK 127.0.0.1 / 24

- **Default Gateway:**

- 192.168.20.1 / 24



APPENDIX B: Setup Jobs & References

Instructor-run Jobs Prior to Lab

At MVS1:

- SYS1.CS.CNTL(RACFPSEC) -- against shared RACF Database from one system
- SYS1.CS.CNTL(RACFP100) -- against shared RACF Database from one system
- SYS1.CS.CNTL(RACFSIZE) -- against shared RACF Database "*****"
- NOTE: Your instructor will already have initialized the following procedures at MVS1 – the system from which you will be testing:
 - /s TCPIP1 and /s TN3270 and /s FTPCCL
 - /s PAGENTT
 - /S TCPIPT,PROF=TCPSn1,CS=SYS1
 - /V TCPIP,TCPIPT,O,SYS1.CS.TCPPARMS(TLSON)
 - /s FTPT,cs=sys1,fdat=ftpSAUTH,data=dat1a
 - /S TCPIPG,PROF=TCPSn2,CS=SYS1
 - /V TCPIP,TCPIPT,O,SYS1.CS.TCPPARMS(TLSON)
 - /s FTPG,cs=sys1,fdat=ftpSAUTH,data=datag
 - /S tn3270t
 - TN3270T PROC PARMS='CTRACE(CTIEZBTN)',PROF=TN&CL1.A,CS=SYS1, DATA=DAT&CL1.A

**FTP.DATA of FTPSAUTH
specifies
Server Authentication Only**

UNIX Copy Jobs for Policy Agent Setup and Policies at all systems

- /BACKUP/CSPOLICY/CERTREFRESH/ussCERTREFRESH.sh

On Your MVS:

- 1) Your instructor will also have run one script to clear out the student directories from a previous lab offering.
 - 1) EMPTYCER (copies skeletons into student datasets on unique volumes)
 - 1) Must be run at each MVS: MVS2-MVS7
 - 2) /s TCPIP1 and /s TN3270 and /s FTPCCL
- 2) /s PAGENTT
 - /S TCPIPT, CS=SYS1,PROF=TCPSn1
 - /V TCPIP,TCPIPT,O,SYS1.CS.TCPPARMS(TLSON)
 - /s FTPT,cs=sys1,fdat=FTPSAUTH,data=dat1a
 - /S TCPIPG, CS=SYS1,PROF=TCPSn2
 - /V TCPIP,TCPIPT,O,SYS1.CS.TCPPARMS(TLSON)
 - /s FTPG,cs=sys1,fdat=FTPSAUTH,data=datag

OTHER INFORMATION:

- SCENARIO 1 Command for TEST: ==> ftp -r TLS -f "//sys1.cs.tcparms(ftpclsec)" -p TCPIPT -s 192.168.20.91
- /s SPECUSER = procedure to execute SETROPTS with Special User Authority

Instructor Jobs Used to Create Pre-Existing Certificates and Rings

At MVS1 – Shared RACF Database:

- **SYS1.CS.CNTL(RACDCLR1)**
//****FOR EXERCISE ON REKEYING/REFRESHING CA and Server CERTS *****
//* Creates Generic Client Ring with only CA connected to it *
//* Creates Individual Client Rings with only CA connected to them *
//*****
• **SYS1.CS.CNTL(RACDFTPX)**
//****FOR EXERCISE ON REKEYING/REFRESHING SERVER CERTIFICATES *****
//* TCPIPT: Create Individual Personal Certificate for FTP Server 11 *
//* USER11 .. USING EXPIRED FTP Server Certificate *
//* TCPIPG: Create Individual Personal Certificate for FTP Server 12 *
//* USER12 .. USING EXPIRED FTP Server Certificate *
//*****
• **SYS1.CS.CNTL(RACDCAX)**
//****FOR EXERCISE ON REKEYING/REFRESHING CA and Server CERTS *****
//* TCPIPT: Create CA and FTP Server Certs that are both expired *
//* USER11 .. USING EXPIRED FTP Server Certificate *
//* TCPIPG: Create CA and FTP Server Certs that are both expired *
//* USER12 .. USING EXPIRED FTP Server Certificate *
//*****

Instructor Jobs Used to Create Pre-Existing Certificates and Rings

At MVS1 – Shared RACF Database:

- **SYS1.CS.CNTL(RACDFTPA)**
//****FOR EXERCISE ON REKEYING/REFRESHING CA and Server CERTS *****
//* Creates Generic SERVER CERT for FTP SERVER on MVS1-7 *
//* Creates Generic SERVER Ring with CACERT and Generic FTP SRVCERT *
//***** THIS NEVER NEEDS A CLEANUP *****
//*****
- **SYS1.CS.CNTL(RACDFTPX)**
//****FOR EXERCISE ON REKEYING/REFRESHING SERVER CERTIFICATES *****
//* TCPIPT: Create Individual Personal Certificate for FTP Server 11 *
//* USER11 .. USING EXPIRED FTP Server Certificate *
//* TCPIPG: Create Individual Personal Certificate for FTP Server 12 *
//* USER12 .. USING EXPIRED FTP Server Certificate *
//*****
- **SYS1.CS.CNTL(RACDCAX)**
//****FOR EXERCISE ON REKEYING/REFRESHING CA and Server CERTS *****
//* TCPIPT: Create CA and FTP Server Certs that are both expired *
//* USER11 .. USING EXPIRED FTP Server Certificate *
//* TCPIPG: Create CA and FTP Server Certs that are both expired *
//* USER12 .. USING EXPIRED FTP Server Certificate *
//*****

Instructor Jobs Used to Create Pre-Existing Certificates and Rings



At MVS1 – Shared RACF Database:

```
• SYS1.CS.CNTL(RACDDEL2)
//****FOR SCENARIO 2 REKEYING/REFRESHING CA and Server CERTS *****
//* Deletes the student Server Key Rings from previous class *
//* Deletes the student FTPServer Certificates from RACF Repository *
//***** RERUN THE JOB RACDFTPX TO DO the FOLLOWING *****
//* Recreates student FTPServer Certificate with Expired Dates *
//* Recreates the Server Key Rings and connects certificates *
//*****

• SYS1.CS.CNTL(RACDDEL4)
//****FOR SCENARIO 4 REKEYING/REFRESHING CA and Server CERTS *****
//* Deletes the student Client Key Rings from previous class *
//* Deletes the student Server Key Rings from previous class *
//* Deletes the student FTPServer Certificates from RACF Repository *
//* Deletes the old and rolled over CA Certificates (RACF Repository) *
//* Recreates the CA Certificate which students later rollover *
//* Recreates student FTPServer Certificate with Expired Dates *
//* Recreates the Client Key Rings and connects certificates *
//* Recreates the Server Key Rings and connects certificates *
//*****

• SYS1.CS.CNTL(RACDCLR2)
//****FOR EXERCISE ON REKEYING/REFRESHING CA and Server CERTS *****
//* Creates INDIVIDUAL Client Rings with only CA connected to them *
//***** THE CLIENTS WILL NEED TO REFRESH THIS KEYRING *****
//***** with a renewed and rekeyed certificate *****
//*****
```



END OF LAB

12895: Rekeying and Renewing Your Expired Digital Certificates in RACF *Hands-on Lab Intro*

Gwen Dente, IBM Advanced Technical Skills
(gdente@us.ibm.com)

Tuesday, February 5, 2013: 09:30 AM - 10:30 AM,
HIL, Union Square 23-24, Fourth Floor
Session Number 12895

In this 1st Document:

- Read Descriptions of 2 required Scenarios (pp. 9-12).
- Find your team's IPv4 interfaces and addresses (pp. 15-29).

In the 2nd Document:

- Lab starts on page 15

