RSH CONSULTING

FTP Passphrases and Certificates

RUGONE – October 2020

RSH Consulting – Robyn E. Gilchrist

RSH CONSULTING

RSH Consulting, Inc. is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050

Robyn E. Gilchrist is a Senior RACF and CA ACF2 Consultant. She assists clients with conducting penetration and vulnerability tests to evaluate z/OS controls and with enhancing access controls. As a systems programmer and network engineer, Ms. Gilchrist has installed, configured, and maintained the z/OS Communications Server and WebSphere Application Server (WAS) for z/OS in Network Deployment (ND) mode with associated ACF2 and RACF controls. She has converted CPF-connected ACF2 databases to RRSF-connected RACF databases.

- 617-977-9090
- R.Gilchrist@rshconsulting.com
- www.linkedin.com/in/robyn-e-gilchrist/

Sources and References

- z/OS Communications Server - IP Configuration Guide (SC27-3650)
- WinSCP - https://winscp.net/eng/download.php
- SimpleAuthority - http://simpleauthority.com/

FTP protocols

- FTP – File Transfer Protocol
  - A TCP/IP application that uses TCP and Telnet to bulk-transfer data between hosts
  - Described by Request For Comment (RFC) 959 from the Internet Engineering Task Force (IETF)
    - Implemented on many platforms
    - FTP on z/OS has a unique feature of interfacing with JES and SQL
- FTPS – File Transport Protocol with Secure SSL
  - Built into z/OS FTP server
  - Integrated with IBM System SSL support
    - Can access cryptographic hardware
  - Incompatible with SFTP
- SFTP – SSH File Transfer Protocol
  - An extension of the SSH (Secure SHell) cryptographic protocol
    - A port of Open Source Software's OpenSSH to z/OS
    - A unique protocol, not SSH over FTP
  - Not integrated with IBM System SSL support
    - Can't use IBM cryptographic hardware
  - Incompatible with FTPS

FTP client and Certificate Authority

- MS-Windows FTP client is very basic
  - No certificate support, i.e. no encryption
  - Can only connect to server port 21 (default)
- WinSCP supports certificates
  - Free download
  - Can use non-default server port
  - FTP, SFTP, FTPS, and other file transfer protocols
- Certificate Authority (CA) is SimpleAuthority
  - Free download
  - A full function CA used as a demonstration
  - Mimics non-RACF certificate signer like Entrust or Verisign

FTP.DATA for Passphrases

- Set by the PASSPHRASE keyword
  - DEFAULT=TRUE
  - FTP passphrases are enabled by default, no system modifications required
- If PASSPHRASE set to FALSE
  - FTP server truncates password to first eight characters
- FTP Server recycle required to change keyword values

FTP Server limitations

- No mechanism to change expired passwords or passphrases with FTP
  - Set passwords/passphrases with NOEXPIRE or change by other means (TSO, CICS, batch)

- FTP Server does not honor spaces in passphrases
  - Space character delimits password to first “word”
  - “Dog Cat Bird wolf 73” is a valid passphrase but not valid for FTP use

Setting the FTP client passphrase

```
ALU REGTEST PHRASE('Thispassphrasehas30characters!') nopassword noexpire

 READY
lu regtest
 USER=REGTEST  NAME=ROBYN E TEST          OWNER=TSTOWNR       CREATED=18.136
  DEFAULT-GROUP=GRPTRMNU PASSDATE=N/A    PASS-INTERVAL=180 PHRASEDATE=20.302
  ATTRIBUTES=NOPASSWORD PASSPHRASE
  REVOKE DATE=NONE   RESUME DATE=NONE
  LAST-ACCESS=20.303/13:00:43
  CLASS AUTHORIZATIONS=NONE
  NO-INSTALLATION-DATA
.
.

READY
 TIME-01:01:39 PM. CPU-00:00:02 SERVICE-302399 SESSION-06:40:33 OCTOBER
29,2020
READY
```

FTP Logon with passphrase

```
C:\Users\Robyn>ftp 172.29.122.148
Connected to 172.29.122.148.
220-FTP 18:00:18 on 2020-10-29.
220 Connection will close if idle for more than 5 minutes.
501 command OPTS aborted -- no options supported for UTF8
User (172.29.122.148:(none)): regtest
331 Send password please.
Password:
230 REGTEST is logged on.  Working directory is "REGTEST.".
ftp>
```

Required z/OS components for FTPS

- z/OS Communication Server (TCP/IP)
  - TCPCONFIG TTLS statement in TCP.PROFILE
- z/OS Communications Server Policy Agent (PAGENT)
  - PAGENT Started Task configures security policy into TCP/IP
    - Application Transparent – Transport Layer Security (AT-TLS)
    - TLS protocols provide communication privacy over the internet in a way designed to prevent eavesdropping, tampering or message forgery
  - PAGENT must have READ access to SERVAUTH EZB.INITSTACK.sysname.tcpname
    - If profile does not exist (RC=4), PAGENT socket requests will fail
  - PAGENT policy configuration either …
    - IBM Configuration Assistant for z/OS Communications Server in z/OSMF
    - Manually coding statements in a z/OS UNIX file or MVS dataset
- z/OS Communications Server Syslog Daemon (syslogd)
  - SYSLOGD Started Task logs events for Unix System Services (USS)
    - telnet, TN3270/E, FTP, SMTP, etc.

FTP.DATA statements required for certificate authentication

```
;
; TLS parameters for FTPS

EXTENSIONS AUTH_TLS                ; Enable TLS authentication
TLSMECHANISM ATTLS                 ; Server-specific or ATTLS
SECURE_FTP REQUIRED                ; Security required/optional
SECURE_LOGIN REQUIRED              ; Authenticate client certificates
SECURE_PASSWORD OPTIONAL            ; Password requirement
SECURE_CTRLCONN PRIVATE             ; Minimum level of security CTRL
SECURE_DATACONN PRIVATE            ; Minimum level of security DATA
TLSRFCLEVEL RFC4217                ; SSL/TLS RFC Level supported
TLSTIMEOUT 500                     ; SSL/TLS RFC Level supported
TLSPORT 0                          ; use explicit secure FTP (disable implicit)
KEYRING RSHKEYRING                 ; Name of key ring
FTPKEEPALIVE 0
FTPLOGGING TRUE
```

FTP Server Site certificate – RACF signed

```
racdcert list (label('FTPTST SITE CERT')) ID(FTPTST)
Digital certificate information for user FTPTST:
Label: FTPTST SITE CERT
   Certificate ID: 2QbG49fj4uPG49fj4uNA4snjxUDDxdnj
   Status: TRUST
   Start Date: 2020/01/22 01:00:00
   End Date:   2022/02/01 00:59:59
   Serial Number:
        >03<
   Issuer's Name:
        >CN=RSH RACF Certificate Authority.O=RSH Consulting Inc..L=MA.C=US<
   Subject's Name:
        >CN=XXXXXXXXXXXXXXXXXXXXXXX.COM.O=RSH Consulting Inc.SP=MA.C=US<
   Signing Algorithm: sha256RSA
   Key Usage: HANDSHAKE, DATAENCRYPT, DOCSIGN
   Key Type: RSA
   Key Size: 2048
   Private Key: YES
   Ring Associations:
     Ring Owner: FTPTST
     Ring:
        >RSHKEYRING<
```

FTP Server keyring – Demo Server

```
racdcert listring(*) ID(FTPTST)

 Digital ring information for user FTPTST:

   Ring:
        >RSHKEYRING<
   Certificate Label Name                 Cert Owner     USAGE      DEFAULT
   -------------------------------------  ------------   --------   -------
   RSH RACF CA                            CERTAUTH       CERTAUTH     NO
   FTPTST SITE CERT                       ID(FTPTST)     PERSONAL     YES
   RSH SIMPLEAUTHORITY TEST CA            CERTAUTH       CERTAUTH     NO
```

Starting the FTP demo server – Port 1073

```
//FTPD   PROC MODULE='FTPD',PARMS='PORT 1073'
//*************************************************************
//* 09/11/2018.254 REG: CREATED FOR TESTING ON PORT 1073      *
//*                                                           *
//*************************************************************
//FTPD   EXEC PGM=&MODULE,REGION=4096K,TIME=NOLIMIT,
//       PARM='POSIX(ON) ALL31(ON)/&PARMS'
//*
//*  STEPLIB CONTAINS FTCHKCMD CODED TO DENY FILETYPE=JES     *
//*TEPLIB DD  DSN=REG.TSO.LOAD,DISP=SHR
//*
//CEEDUMP  DD SYSOUT=*
//*
//SYSFTPD DD DISP=SHR,DSN=VENDOR.TCPPARMS(FTPDATAT)
//SYSTCPD DD DISP=SHR,DSN=TCPIP.TCPIP.DATA
```

FTPS – Generating the client certificate CSR

- Cut and paste the CSR file into a txt file on the PC. Send the text file to the Certificate Authority for signing.

```
RACDCERT ID(REGTEST) GENCERT -
  SUBJECTSDN( -
  CN('Robyn Test Cert - REGTEST') -
  O('RSH Consulting Inc') -
  SP('MA') -
  C('US') ) -
  SIZE(2048) -
  NOTBEFORE(DATE(2020-10-27)) -
  NOTAFTER(DATE(2022-10-31)) -
  WITHLABEL('REGTEST 3rd party cert')

  RACDCERT GENREQ(LABEL('REGTEST 3rd party cert')) -
   ID(REGTEST) -
  DSN('REG.TSO.CERT.CSR')
```

FTPS – Generating the private key

- Binary upload the file from the CA that contains the signed certificate. Upload it into a file with RECFM=VB

```
RACDCERT ID(REGTEST) ADD('REG.TSO.CERT.SIGNED') -
WITHLABEL('REGTEST 3rd party cert')
```

- The password set here secures the private key in the PKCS#12 file. It can not be reset and if it is forgotten a new certificate will be needed.

```
RACDCERT ID(REGTEST) -
EXPORT(LABEL('REGTEST 3rd party cert')) -
DSN('REG.TSO.CERT.FTP.CLIENT.P12') PASSWORD('PSWDDAT1') -
FORMAT(PKCS12DER)
```

- Verify the export file is signed by the proper CA and the private key exists

```
RACDCERT CHECKCERT('REG.TSO.CERT.FTP.CLIENT.P12') PASSWORD('PSWDDAT1’)
```

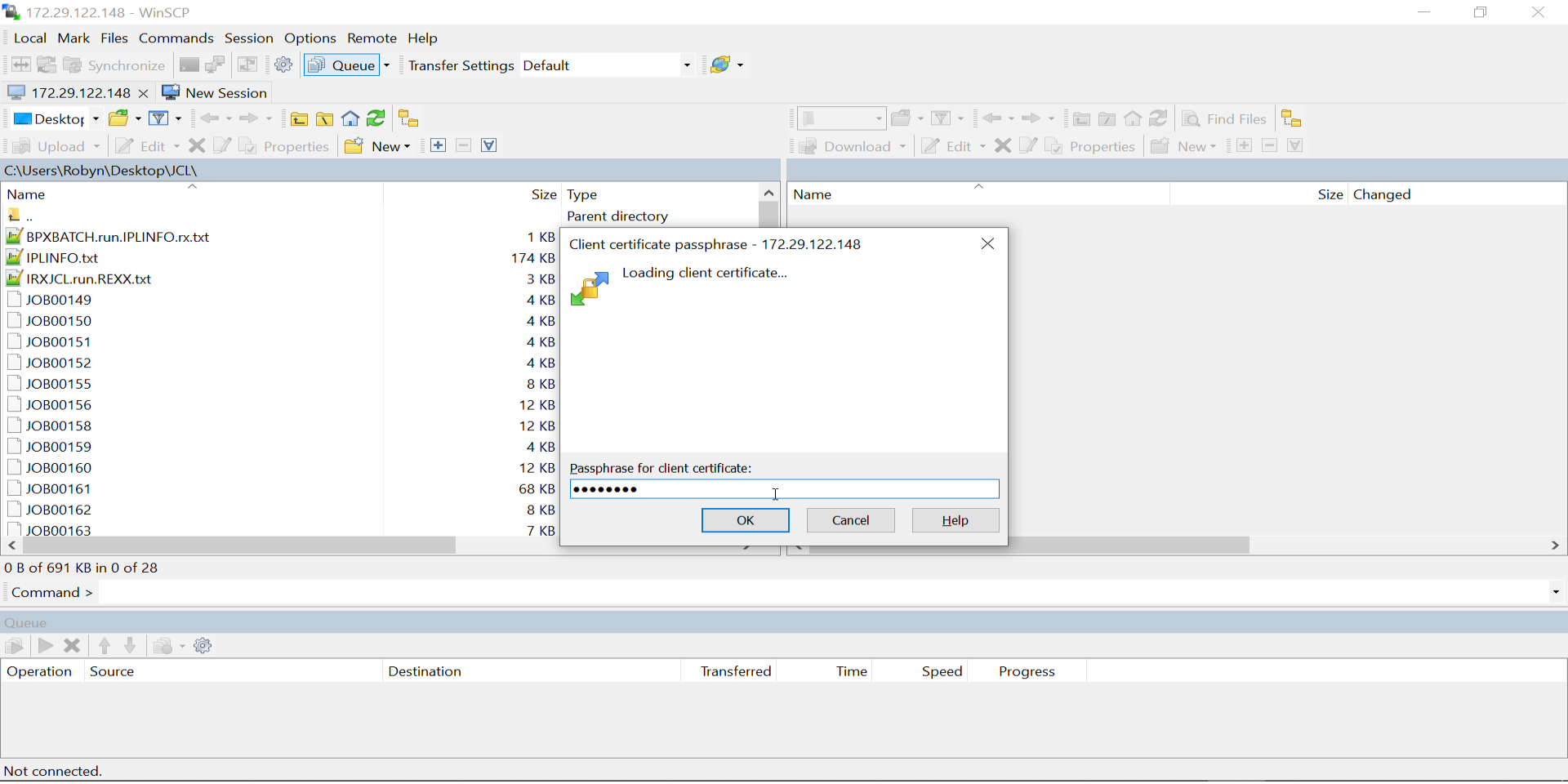
- Binary download the P12 dataset to the machine with the FTP client

FTPS client connection – setting client certificate and connection port

- Notice the port is FTP demo server port 1073, TLS/SSL Explicit encryption

FTPS client connection – using the private key

- The private key passphrase is required, not the 30 character RACF passphrase



FTPS client connection – connected!

- Note the gold key in the lower right corner indicating encryption is active

JCL - 172.29.122.148 - WinSCP

Local Mark Files Commands Session Options Remote Help

Synchronize | Queue | Transfer Settings Default

172.29.122.148 | New Session

Desktop | Upload | Edit | Properties | New

'REGTE: | Download | Edit | Properties | New | Find Files

C:\Users\Robyn\Desktop\JCL\

Name	Size	Type
..		Parent directory
BPXBATCH.run.IPLINFO.rx.txt	1 KB	TXT File
IPLINFO.txt	174 KB	TXT File
IRXJCL.run.REXX.txt	3 KB	TXT File
JOB00149	4 KB	File
JOB00150	4 KB	File
JOB00151	4 KB	File
JOB00152	4 KB	File
JOB00155	8 KB	File
JOB00156	12 KB	File
JOB00158	12 KB	File
JOB00159	4 KB	File
JOB00160	12 KB	File
JOB00161	68 KB	File
JOB00162	8 KB	File
JOB00163	7 KB	File

0 B of 691 KB in 0 of 28

/'REGTEST.'/

Name	Size	Changed
..		
S0W1.ISPF.ISPPROF		8/14/2020
TSO.TESTLIB		10/28/2020
COSVCCSI	1 KB	5/23/2019
FDNDEEOF	1 KB	5/23/2019
IRXJCL.TXT	1 KB	5/23/2019
RACF.ICHPSOUT.KDFAES	1 KB	2/11/2020
RACF.ICHPSOUT.KDFAES2	1 KB	2/11/2020
RACF.ICHPSOUT.LEGACY	1 KB	2/11/2020
RACF.PHRHISTS.KDFAES	1 KB	2/11/2020
RACF.PHRHISTS.KDFAES2	1 KB	2/11/2020
RACF.PHRHISTS.LEGACY	1 KB	2/11/2020
RACF.PWDHISTS.KDFAES	1 KB	2/11/2020
RACF.PWDHISTS.KDFAES2	1 KB	2/11/2020
RACF.PWDHISTS.LEGACY	1 KB	2/11/2020
TDUMP.REGTEST.D180913.T134726	1 KB	5/23/2019

0 B of 1.66 KB in 0 of 19

Command >

Queue

Operation	Source	Destination	Transferred	Time	Speed	Progress

FTP | 0:01:01

FTPS with Client Authentication - summary

- Unique protocol from SFTP
- Ensure z/OS Communication Server components are in place
  - TCP.PROFILE, PAGENT, syslogd
- Update FTP.DATA for TLS activation and client authentication
- Use TLSPORT 0 to disable implicit secure FTP
  - Explicit secure FTP
  - FTPS will run on PORT defined at FTP Server startup
- Use an FTP client that supports TLS
- Create client certificate with a USERID that will be certificate owner
- Passphrase required to access private key on FTP client machine

FTP-JES Interface

- z/OS offers the opportunity for FTP to submit jobs and retrieve output form the JES SPOOL
- Carefully consider the controls governing use of JES by FTP
  - JESINTERFACELEVEL = 2 allows any FTP user to read the entire SPOOL
- Access to JES allows FTP to run TSO commands, REXX programs, issue system commands,etc.
- WinSCP is a challenge for JES
  - WINSCP looks for file names and type
  - Can’t determine from JES
- Easy for Windows FTP client, so that is what we will use

FTP-JES Interface

```
C:\Users\Robyn\Desktop\JCL>ftp 172.29.122.148
Connected to 172.29.122.148.
220-FTP 18:59:49 on 2020-10-29.
220 Connection will close if idle for more than 5 minutes.
501 command OPTS aborted -- no options supported for UTF8
User (172.29.122.148:(none)): regtest
331 Send password please.
Password:
230 REGTEST is logged on.  Working directory is "REGTEST.".
ftp> cd /tmp
250 HFS directory /tmp is the current working directory
ftp> put IPLINFO.txt IPLINFO.rx
200 Port request OK.
125 Storing data set /tmp/IPLINFO.rx
250 Transfer completed successfully.
ftp: 177990 bytes sent in 0.94Seconds 189.15Kbytes/sec.
ftp> quote site chmod 755 /tmp/IPLINFO.rx
200 SITE command was accepted
ftp> quote site filetype=jes
200 SITE command was accepted
ftp> put BPXBATCH.run.IPLINFO.rx.txt
200 Port request OK.
125 Sending Job to JES internal reader FIXrecfm 80
250-It is known to JES as JOB00209
250 Transfer completed successfully.
ftp: 795 bytes sent in 0.08Seconds 9.46Kbytes/sec.
ftp> get JOB00209 JOB00209.txt
```

FTP-JES Interface

- Doing an MGET * with JESINTERFACELEVEL 2 will download the JES SPOOL

```
ftp> quote site jesowner=*
200 SITE command was accepted
ftp> quote site jesjobname=*
200 SITE command was accepted
ftp> quote stat
<snip>
211-JESINTERFACELEVEL is 2
ftp> mget *
200 Representation type is Ascii NonPrint
200 Port request OK.
125 Sending all spool files for requested Jobid
250 Transfer completed successfully.
ftp: 3250 bytes received in 1.25Seconds 2.60Kbytes/sec.
200 Port request OK.
125 Sending all spool files for requested Jobid
250 Transfer completed successfully.
ftp: 3252 bytes received in 1.24Seconds 2.62Kbytes/sec.
200 Port request OK.
```

FTP-JES Interface blocking

- The STEPLIB contains FTP exit FTCHKCMD. For this demonstration, the library has been added to APF. The library containing FTCHKCMD must be PROGRAM protected, if PROGRAM is active.

```
//FTPD   EXEC PGM=&MODULE,REGION=4096K,TIME=NOLIMIT,
//       PARM='POSIX(ON) ALL31(ON)/&PARMS'
//*
//*  STEPLIB CONTAINS FTCHKCMD CODED TO DENY FILETYPE=JES                *
//STEPLIB DD  DSN=REG.TSO.LOAD,DISP=SHR
```

FTP-JES Interface blocking

```
C:\Users\Robyn\Desktop\JCL>ftp 172.29.122.148
Connected to 172.29.122.148.
220-FTP 19:08:56 on 2020-10-29.
220 Connection will close if idle for more than 5 minutes.
501 command OPTS aborted -- no options supported for UTF8
User (172.29.122.148:(none)): regtest
331 Send password please.
Password:
230 REGTEST is logged on.  Working directory is "REGTEST.".
ftp> cd /tmp
250 HFS directory /tmp is the current working directory
ftp> quote site filetype=jes
500-UX-FILETYPE=JES change denied by installation exit
500 User Exit denies Userid 'REGTEST' from using Command 'SITE'.
ftp> quote site filet=jes
500-UX-FILETYPE=JES change denied by installation exit
500 User Exit denies Userid 'REGTEST' from using Command 'SITE'.
ftp> quote site filetype=sql
200 SITE command was accepted
ftp> quote site filetype=seq
200 SITE command was accepted
ftp>
```

IBM Request For Enhancement

- An IBM Request For Enhancement (RFE) has been created by RSH Consulting to improve the FTP to JES interface security

- RFE 125660 – Increasing Security and Control for FTP JES Interface
  - Requests JESINTERFACELEVEL=0 parameter in FTP.DATA to disable the FTP to JES interface
  - Requests a SAF resource to restrict job submission and sysout retrieval via FTP for installations that require the FTP to JES interface

- See RSH RACF Tips article on entering, examining, and voting on RFEs
  - https://www.rshconsulting.com/racftips/RSH_Consulting__RACF_Tips__January_2016.pdf

- Be sure to vote!