RSH
CONSULTING

FTP Passphrases and Certificates

GSE UK
Security Working Group
February 2021

RSH Consulting – Robyn E. Gilchrist

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 used 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
  - Feature of z/OS Communication Server FTP Server
  - Integrated with IBM System SSL support
    - Can access cryptographic hardware
  - Incompatible with SFTP
- SFTP – Secure File Transfer Protocol
  - An extension of 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
  - Not demonstrated in this presentation

FTP Client and Certificate Authority (CA)

- MS-Windows FTP client is very basic
  - No certificate support, i.e. no SFTP, no FTPS
  - Can only connect to well-known server port 21 (default)
  - Does not support spaces in passphrases

- WinSCP supports certificates
  - Free download
  - Supports encryption and non-standard ports
  - Supports spaces in passphrases
  - FTP, FTPS, SFTP and other file transfer protocols

- Certificate Authority (CA) is SimpleAuthority
  - Free download for demonstration
  - Mimics non-RACF certificate signer like Entrust or Verisign

RACF Password Phrases

- Formally referred to as RACF Password Phrases
- Passphrase is informal and is the commonly used term
- Allow mixed case and special characters
- Characteristics
  - Length
    - 14 to 100 characters
    - 9 to 13 characters can be implemented using RACF exit ICHPWX11
    - 9 to 100 characters with PASSWORD ALGORITHIM KDFAES
  - Must not contain the user ID as sequential uppercase or lowercase characters
  - Must contain at least 2 alphabetic characters (A - Z, a - z)
  - Must contain at least 2 non-alphabetic characters (numeric, punctuation, or special characters)
  - Must not contain more than 2 consecutive characters that are identical (e.g., 'aaa')

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 - Passphrase Limitations

- No mechanism to change expired passwords or passphrases with FTP
  - Set passwords/passphrases or change by other means (TSO, CICS, batch) or set with NOEXPIRE keyword
  - NOEXPIRE is used in this demonstration

- Leading and trailing spaces are not honored

- Valid RACF passphrase characters that are FTP control characters are not handled by the server
  - Colon (:)
  - At sign (@)

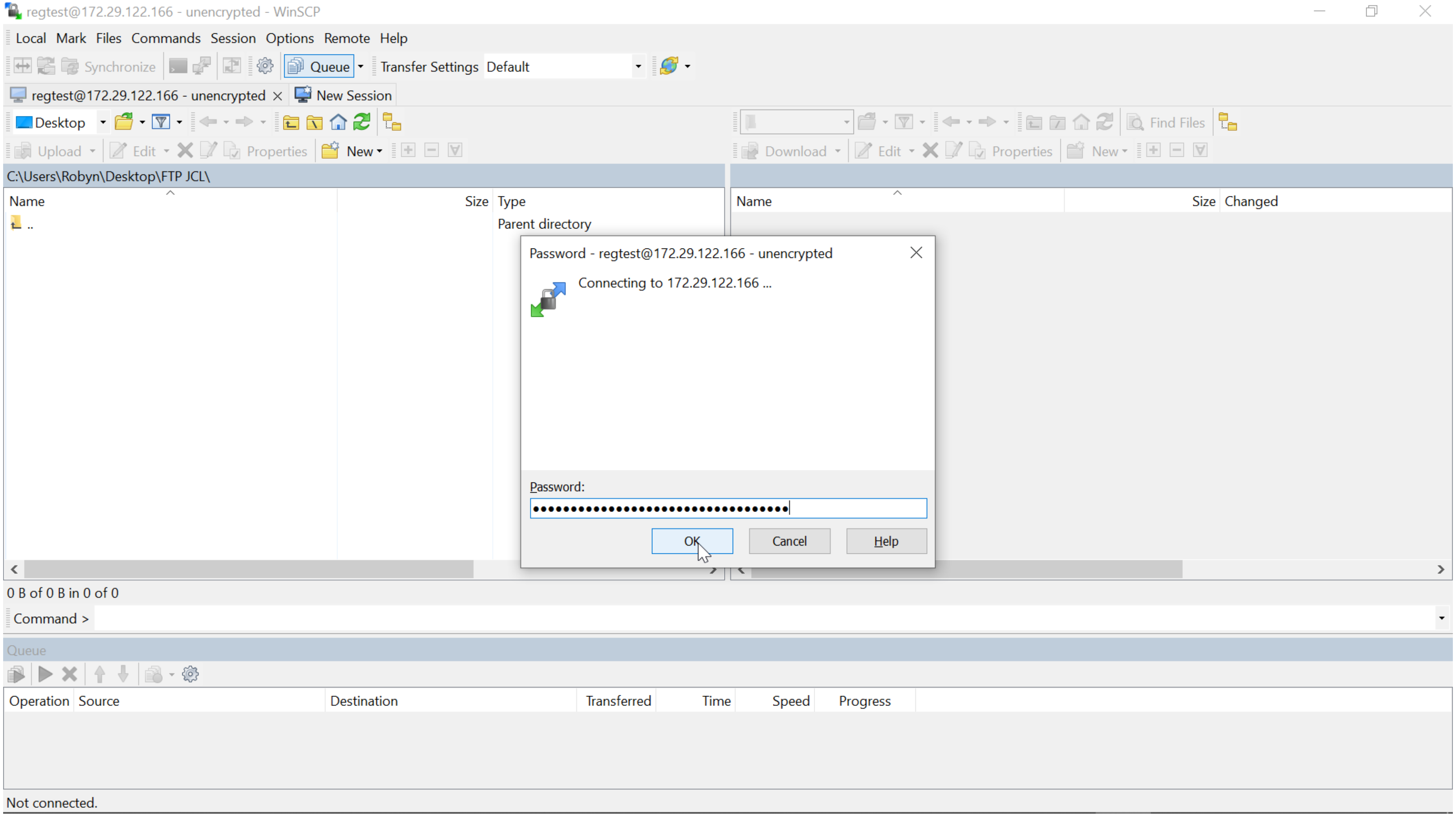
Setting the FTP Client Passphrase

- Setting the USERID passphrase and removing the password

```
ALU REGTEST PHRASE(‘This passphrase has 37 characters!’) noexpire nopassword

 READY
lu regtest
 USER=REGTEST  NAME=ROBYN E TEST         OWNER=TSTOWNR       CREATED=18.136
  DEFAULT-GROUP=TESTGRP PASSDATE=N/A    PASS-INTERVAL=180 PHRASEDATE=21.012
  ATTRIBUTES=NOPASSWORD PASSPHRASE
  REVOKE DATE=NONE   RESUME DATE=NONE
  LAST-ACCESS=21.012/13:00:43
  CLASS AUTHORIZATIONS=NONE
  NO-INSTALLATION-DATA
```

FTP Logon with Passphrase

- Note the 37 character passphrase



regtest@172.29.122.166 - unencrypted - WinSCP

Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
regtest@172.29.122.166 - unencrypted
New Session
Desktop
Find Files
Upload
Edit
Properties
New
Download
Edit
Properties
New

C:\Users\Robyn\Desktop\FTP JCL\

Name	Size	Type
..		Parent directory

Name	Size	Changed

Password - regtest@172.29.122.166 - unencrypted

Connecting to 172.29.122.166 ...

Password:

••••••••••••••••••••••••••••••••••

0 B of 0 B in 0 of 0

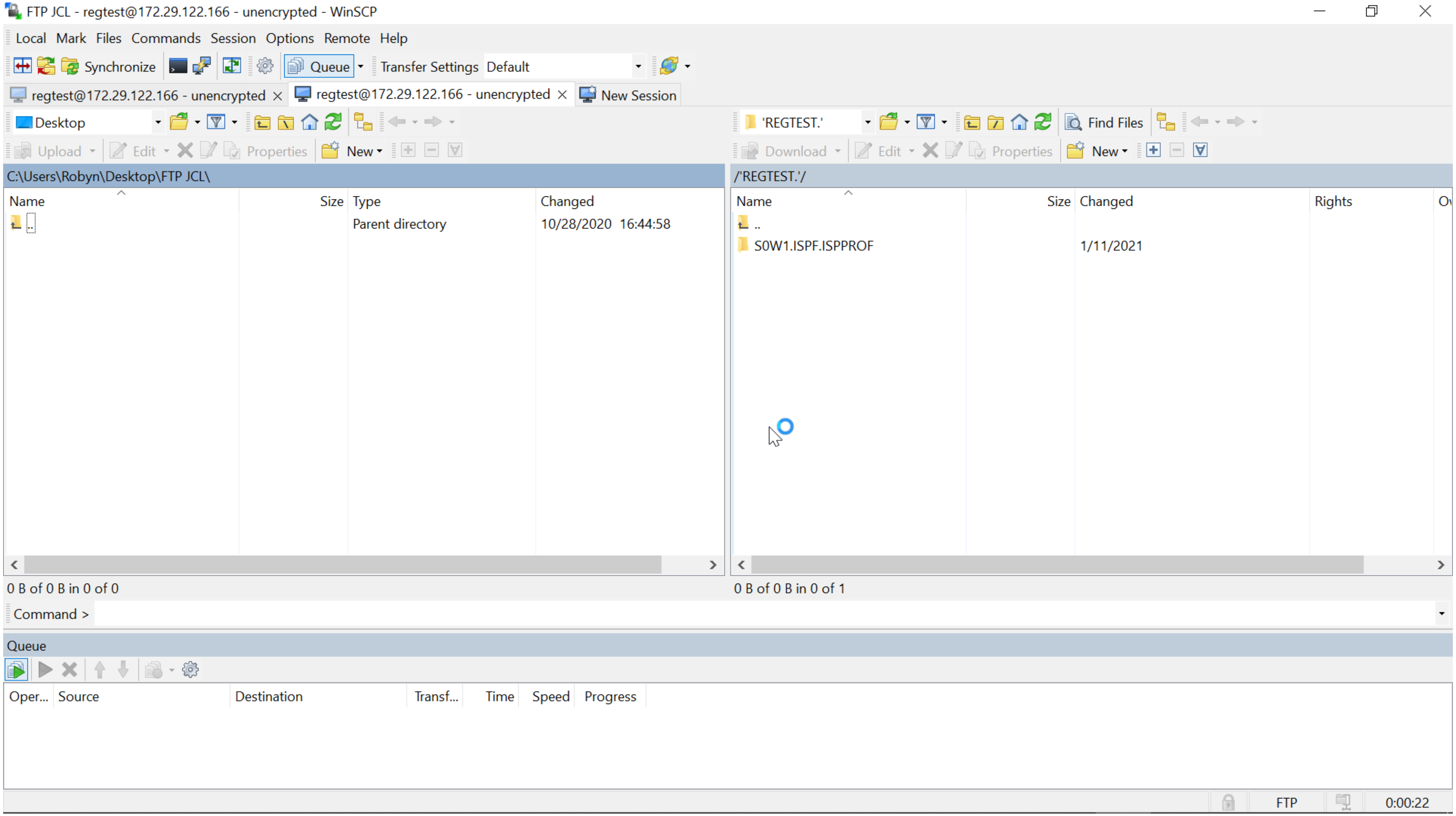
Command >

Operation	Source	Destination	Transferred	Time	Speed	Progress

Not connected.

FTP Logon with Passphrase

- Success! A non-secure logon, note the grey key in the lower right corner



FTP JCL - regtest@172.29.122.166 - unencrypted - WinSCP

Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
regtest@172.29.122.166 - unencrypted
regtest@172.29.122.166 - unencrypted
New Session
Desktop
Upload Edit Properties New
'REGTEST.'
Find Files
Download Edit Properties New

C:\Users\Robyn\Desktop\FTP JCL\

Name	Size	Type	Changed
..		Parent directory	10/28/2020 16:44:58

0 B of 0 B in 0 of 0

/'REGTEST.'/

Name	Size	Changed	Rights	O
..				
S0W1.ISPF.ISPPROF		1/11/2021		

0 B of 0 B in 0 of 1

Oper...	Source	Destination	Transf...	Time	Speed	Progress

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 (STC) logs events for Unix System Services (USS)
    - telnet, TN3270/E, FTP, SMTP, etc.

FTPS Configuration Steps - Server

- Implement required z/OS components
  - PAGENT responsible for specifying FTP server HandshakeRole and Keyring name

- FTP Server certificate setup
  - Obtain server certificate – RACF signed or external CA
  - ADD certificates to RACF
    - Server certificate CA as CERTAUTH
    - Server certificate as ID(<USERID of FTP server STC>)
  - ADDRING to create the FTP server keyring
  - CONNECT server and CA certificates to FTP server keyring
    - Server certificate CA as CERTAUTH
    - Server certificate as ID(<USERID of FTP server STC>) with DEFAULT attribute

- Modify FTP.DATA server configuration to activate security

- Recycle FTP Server to activate configuration changes

FTP Server Certificate – RACF Signed

```
racdcert list (label('FTPTEST SERVER CERT')) ID(FTPTEST)
Digital certificate information for user FTPTST:
Label: FTPTEST SERVER 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=FTP.SERVER.IP.ADDRESS.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: FTPTEST
     Ring:

        >RSHKEYRING<
```

FTP Server Keyring

- Certificate owner is FTP server STC USERID and is set DEFAULT
- Server CA and Client CA are added to FTP server keyring

```
racdcert listring(*) ID(FTPTEST)

 Digital ring information for user FTPTEST:

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

FTP.DATA – Activate FTPS Secure Server

- FTP.DATA configuration statements that enable FTPS

```
EXTENSIONS AUTH_TLS             ; Support TLS authentication

TLSMECHANISM ATTLS              ; TLS implemented by AT-TLS, not FTP
                                ; Preferred method of implementation
                                ; ATTLS specification causes KEYRING keyword to
                                ; be ignored and use PAGENT

SECURE_CTRLCONN PRIVATE         ; Integrity and privacy protection required
                                ; on control connection

SECURE_DATACONN PRIVATE         ; Integrity and privacy protection required
                                ; on data connection

SECURE_FTP REQUIRED             ; REQUIRED keyword disallows clear text login
                                ; ALLOWED keyword permits clear text or TLS login

TLSPORT 0                       ; Explicit secure FTP (disable implicit)
```

FTP.DATA – Activate FTPS Client Authentication

- SECURE_LOGIN configuration statement enables FTPS client authentication

```
SECURE_LOGIN REQUIRED     ; NO_CLIENT_AUTH (default)
                          ; REQUIRED verifies client certificate authentication
                          ; VERIFY_USER verifies client certificate and checks
                          ; authority to
                          ; SERVAUTH EZB.FTP.<sysname>.ftpservername.PORTxxxx
```

FTPS Configuration Steps - Client

- Obtain client certificate with private key
  - RACF generated Certificate Signing Request (CSR) or 3rd party client certificate
  - Demonstration uses RACF CSR

- RACDCERT actions
  - ADD client certificate and CA signer certificate into RACF
    - If completing a RACF Certificate Signing Request, this action generates the private key
  - CONNECT client certificate signer CA to FTP server keyring/virtual keyring
    - Client certificate CA as CERTAUTH
    - Client certificate need not be connected to user's keyring

- Configure FTP client
  - Add P12 file to TLS/SSL configuration
  - Explicit encryption and a non-default port are used in this demonstration

FTPS – Generating Certificate Signing Request

- Use RACDCERT GENCERT and GENREQ commands to create a Certificate Signing Request (CSR) for the client certificate

```
RACDCERT ID(REGTEST) GENCERT –
SUBJECTSDN( -
  CN('Robyn Test Cert – REGTEST') -
  O('RSH Consulting Inc') -
  SP('MA') -
  C('US') ) -
  SIZE(2048) -
  NOTBEFORE(DATE(2021-01-12)) -
  NOTAFTER(DATE(2022-01-11)) -
  WITHLABEL('REGTEST 3rd party cert')

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

FTPS Client – RACF CSR

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

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC0DCCAbgCAQAwWzELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRswGQYDVQQK
ExJSU0ggQ29uc3VsdGluZyBJbmMxIjAgBgNVBAMTGVJvYnluIFRlc3QgQ2VydCAt
IFJFR1RFU1QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDM7Eb+w2Jf
fHIvk/qOkoU9ACmg0doOnbD+nt1bYLMN4Au16OR5scmtDaho98FyETucQbw4RkOP
.
.
.
/pmyAzMw2meIUvQsFYMEBwt2q9mDiLj80pkEZfXJC/P+829gBAYO83KFnWjHo9Sy
AO71iA==
-----END NEW CERTIFICATE REQUEST-----
```

FTPS Client – 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(‘REGTEST.TSO.CERT.SIGNED') -
WITHLABEL('REGTEST 3rd party FTP cert')
```

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

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

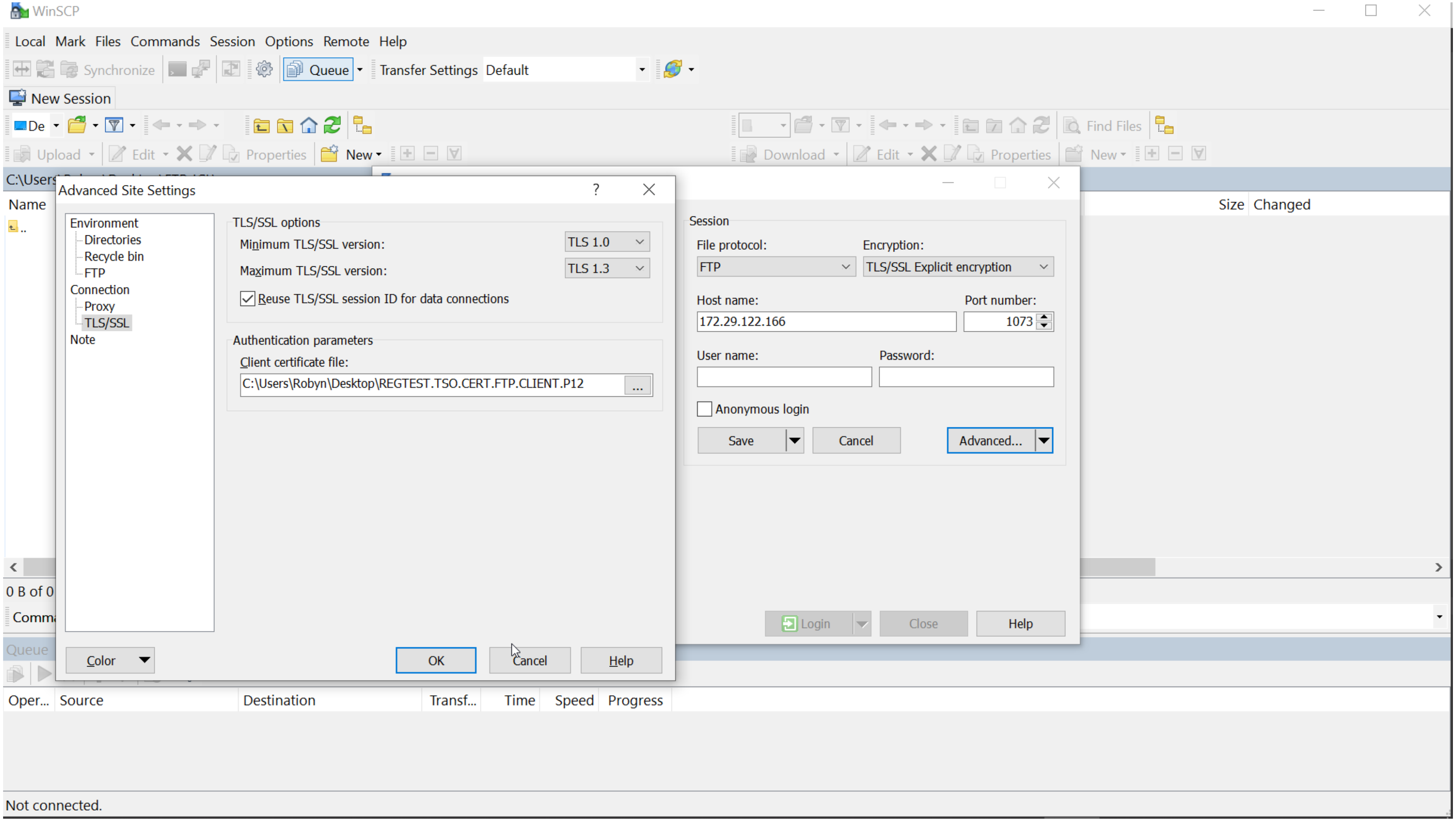
FTPS Client

- Verify the certificate is signed by proper CA, the private key has been generated and the private key password works

```
RACDCERT CHECKCERT(‘REGTEST.TSO.CERT.FTP.CLIENT.P12') PASSWORD(‘PVTKEYPW’)

Certificate 1:
Digital certificate information for user REGTEST:

  Label: REGTEST 3rd party FTP cert
  Certificate ID: 2QfZxcfjxeLj2cXH48Xi40DzmYRAl4GZo6hAxuPXQIOFmaNA
  Status: TRUST
  Start Date: 2021/01/12 07:48:08
  End Date:   2022/01/12 07:48:09
  Serial Number:
       >0176F6DA91E0<
  Issuer's Name:
       >CN=RSH SimpleAuthority TEST CA.OU=TEST.O=TESTRSH.C=US<

  Subject's Name:
       >CN=Robyn Test Cert - REGTEST.O=RSH Consulting Inc.SP=MA.C=US<

  Signing Algorithm: sha256RSA
  Key Usage: HANDSHAKE
  Key Type: RSA
  Key Size: 2048
  Private Key: YES
  Ring Associations:
  *** No rings associated ***
```

FTPS Client Connection – Configuration

- Binary download P12 file to the FTP client machine and configure client



Advanced Site Settings – TLS/SSL

TLS/SSL options

Minimum TLS/SSL version: TLS 1.0

Maximum TLS/SSL version: TLS 1.3

☑ Reuse TLS/SSL session ID for data connections

Authentication parameters

Client certificate file: C:\Users\Robyn\Desktop\REGTEST.TSO.CERT.FTP.CLIENT.P12

Session

File protocol: FTP

Encryption: TLS/SSL Explicit encryption

Host name: 172.29.122.166

Port number: 1073

User name:

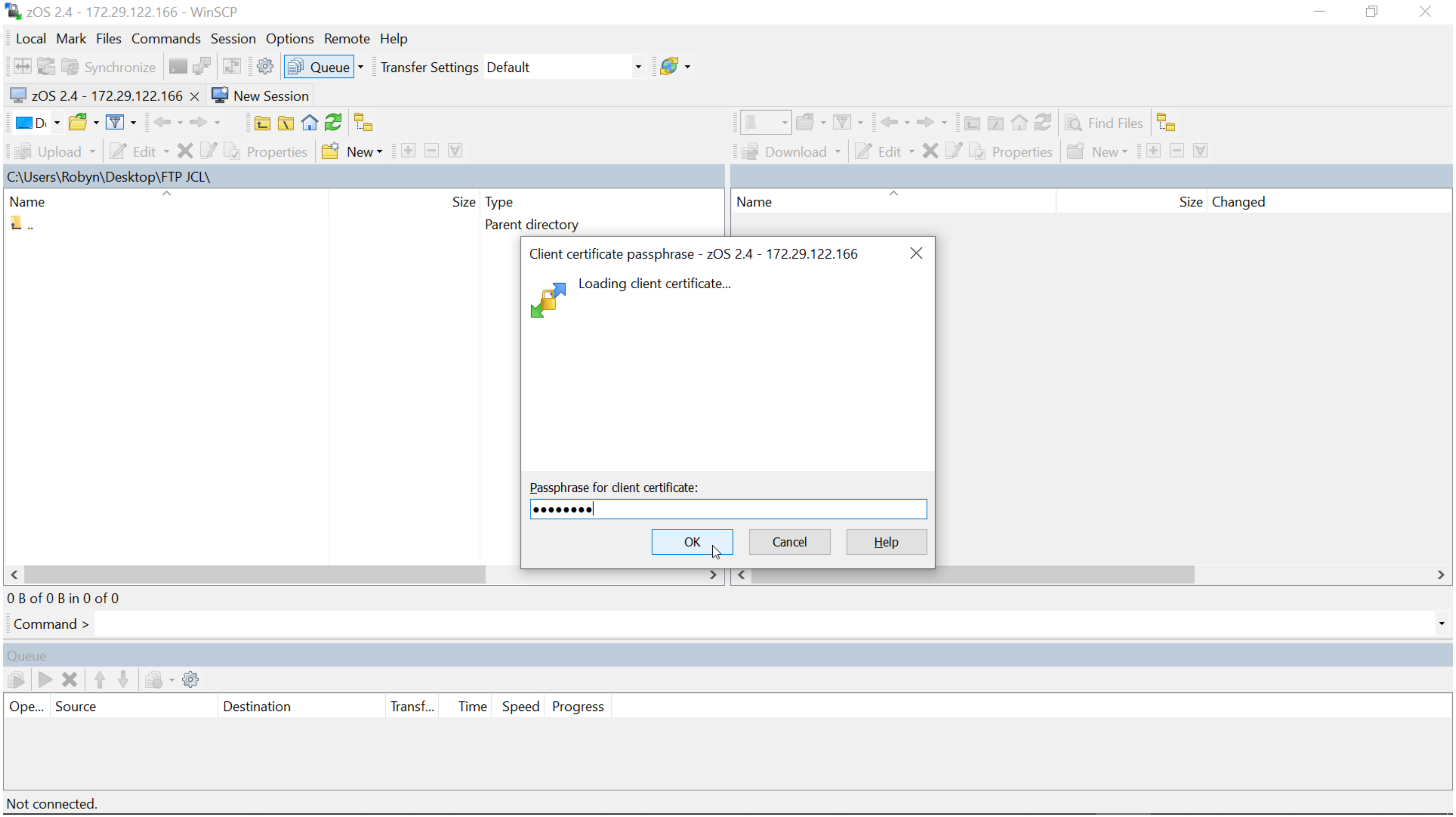
Password:

□ Anonymous login

Not connected.

FTPS Client Connection – Connecting

- The private key passphrase is required, not the 37 character RACF passphrase



zOS 2.4 - 172.29.122.166 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize
Queue
Transfer Settings Default
zOS 2.4 - 172.29.122.166
New Session
Find Files
Upload
Edit
Properties
New
Download
Edit
Properties
New

C:\Users\Robyn\Desktop\FTP JCL\

Name	Size	Type
..		Parent directory

Name	Size	Changed

Client certificate passphrase - zOS 2.4 - 172.29.122.166

Loading client certificate...

Passphrase for client certificate: ••••••••

0 B of 0 B in 0 of 0

Command >

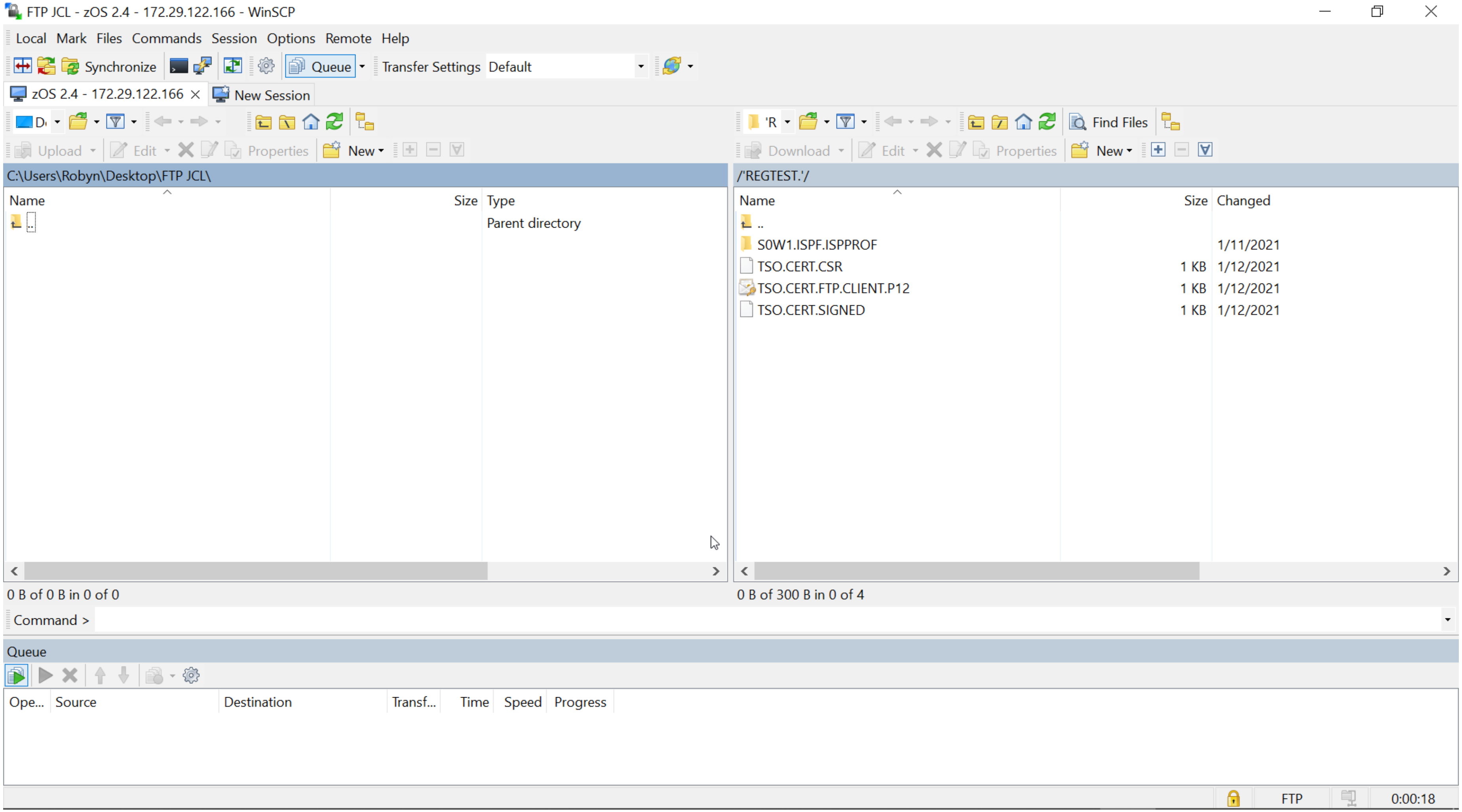
Queue

Ope...	Source	Destination	Transf...	Time	Speed	Progress

Not connected.

FTPS Client Connection – Connected!

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



FTP JCL - zOS 2.4 - 172.29.122.166 - WinSCP

C:\Users\Robyn\Desktop\FTP JCL\

Name	Size	Type
..		Parent directory

/'REGTEST.'/

Name	Size	Changed
..		
S0W1.ISPF.ISPPROF		1/11/2021
TSO.CERT.CSR	1 KB	1/12/2021
TSO.CERT.FTP.CLIENT.P12	1 KB	1/12/2021
TSO.CERT.SIGNED	1 KB	1/12/2021

0 B of 0 B in 0 of 0

0 B of 300 B in 0 of 4

Command >

Queue

Ope...	Source	Destination	Transf...	Time	Speed	Progress

FTP 0:00:18

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 from the JES SPOOL
  - See RSH RACF tips article “FTP and JES” from April 2010 Volume 4, Issue 2.
    https://www.rshconsulting.com/racftips/RSH_Consulting__RACF_Tips__April_2010.pdf
- 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.
- JES is a challenge for WINSCP
  - WINSCP looks for file names and file types
  - Can not determine names and file types from JES
- JES is easy for Windows FTP client, so that is what we will use

FTP-JES Interface

```
C:\Users\Robyn\Desktop\JCL>ftp 172.29.122.166
Connected to 172.29.122.166.
220-FTP 18:59:49 on 2021-01-12.
220 Connection will close if idle for more than 5 minutes.
501 command OPTS aborted -- no options supported for UTF8
User (172.29.122.166:(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. The library with the exit must be APF authorized. The library containing FTCHKCMD must be PROGRAM profile protected, if the PROGRAM class 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=TCPIP.LOADLIB.USEREXIT,DISP=SHR
```

FTP-JES Interface Blocking

```
C:\Users\Robyn\Desktop\JCL>ftp 172.29.122.166
Connected to 172.29.122.166.
220-FTP 19:08:56 on 2020-01-12.
220 Connection will close if idle for more than 5 minutes.
501 command OPTS aborted -- no options supported for UTF8
User (172.29.122.166:(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!