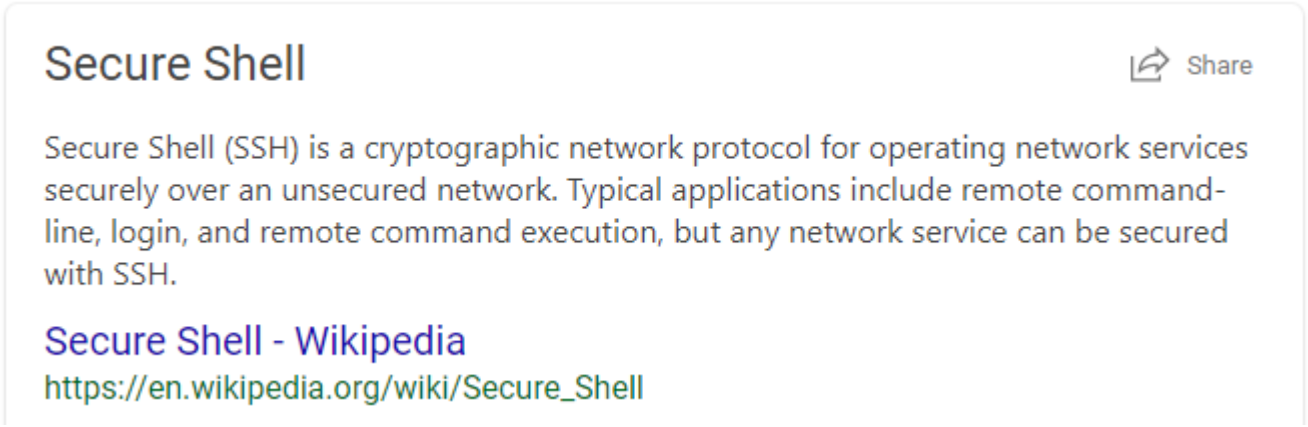
To FTP or SFTP

That is the Question

(Ed Jaffe)

What is SFTP?

- SFTP is the secure file transfer protocol that comes with SSH
- What is SSH?



- SSH is available for every modern computing platform
  - At PSI we use SSH on z/OS, Windows 10, Mac OS, and Linux
  - We use SFTP on all of those platforms as well
- Most implementations use OpenSSH (UNIX-based code)
  - https://www.openssh.com/

Other Secure File Transfer Protocols

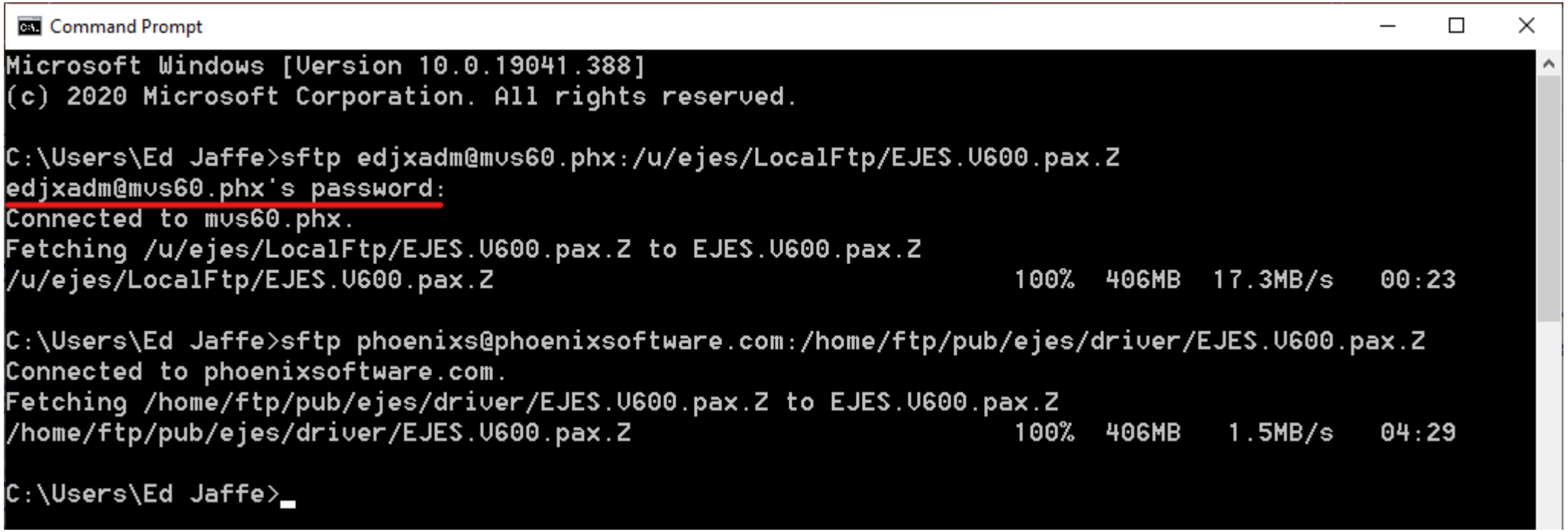
- FTPS
  - Ordinary FTP with encrypted data
  - Complex to set up on z/OS
    - Set up digital certificates in your External Security Manager (usually RACF, ACF2, or Top Secret)
    - Update your TCP/IP and FTP profile to use AT-TLS
    - Set up AT-TLS policy using IBM Configuration Assistant for z/OS Communication Server
    - Configure and set up Policy Agent on z/OS (PAGENT)
- HTTPS
  - Sadly, there is no cURL in the base of z/OS UNIX ☹
  - Available only in dedicated or Java applications (e.g., RECEIVE ORDER)

SSH Authentication

- Generally, only two authentication protocols supported:
  - Password prompt
  - Public/private key pair (RSA or DSA)
- SSH is engineered so that script execution always prompts interactively
- When you use a public/private key pair no password prompt is needed. This is generally how we configure our in-house systems.
  - ssh-keygen command generates the key pairs for a user
  - You take your public key and add it to the authorized_keys file owned by the user on the remote system to which you wish to connect.
  - This works well, but it is a manual process that requires access to both systems to get it set up.

Sample SFTP Downloads With and Without a Password

- The same file is downloaded from two different servers:
  - The first server requires a password.
  - The second server is pre-configured with my public key stored it the remote user's authorized_keys file. No password is needed.



Performing Those Same Downloads in A Batch Job

- Password required.

```
****** ******************************** Top of Data ********************************
000001 //SFTPJOB   JOB 1,JAFFE,CLASS=A,MSGCLASS=T,NOTIFY=&SYSUID
000002 //*
000003 //GETFILE   EXEC PGM=BPXBATCH,REGION=64M
000004 //STDOUT    DD SYSOUT=*
000005 //STDERR    DD SYSOUT=*
000006 //STDPARM   DD *
000007 SH sftp edjxadm@mvs60.phx:/u/ejes/LocalFtp/EJES.V600.pax.Z
000008 //
****** ***************************** Bottom of Data ******************************
```

```
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----›
FOTS1346 Permission denied, please try again..
FOTS1346 Permission denied, please try again..
FOTS1373 edjxadm@mvs60.phx: Permission denied (publickey,password)..
FOTS0841 Connection closed.
****************************** Bottom of Data ******************************
```

- Public/private key pair used. Password not required.

```
****** ******************************** Top of Data ********************************
000001 //SFTPJOB   JOB 1,JAFFE,CLASS=A,MSGCLASS=T,NOTIFY=&SYSUID
000002 //*
000003 //GETFILE   EXEC PGM=BPXBATCH,REGION=64M
000004 //STDOUT    DD SYSOUT=*
000005 //STDERR    DD SYSOUT=*
000006 //STDPARM   DD *
000007 SH sftp phoenixs@phoenixsoftware.com:/home/ftp/pub/ejes/driver/EJES.V600.pax.Z
000008 //
=COLS> ----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----8
****** ***************************** Bottom of Data ******************************
```

```
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----›
Fetching /home/ftp/pub/ejes/driver/EJES.V600.pax.Z to EJES.V600.pax.Z
Connected to phoenixsoftware.com.
****************************** Bottom of Data ******************************
```

Making SFTP in Batch Work for Other Servers

- It would seem not only prudent but also a requirement to use public/private key authentication for batch use of SFTP. Of course, this is practical for transfers between trusted servers only.
- But, suppose you wish to use batch job SFTP to transfer files to/from a server for which you are unable to edit the remote user's authorized_keys file?
  - This could be useful for ad-hoc batch file transfers to/from any modern server for which you have login credentials, especially if anonymous SFTP is supported.
- The answer lies in a little-known feature intended to allow a GUI password window to be displayed on the GNOME desktop which the operator accesses using an X Windows (aka X11 or X) server.
  - SSH_ASKPASS environment variable identifies a password script
  - DISPLAY environment variable contains the word "DISPLAY"

A Practical Example (Securely Transfer a File to IBM's Site)

```
****** ***************************** Top of Data ******************************
000001 //FTP2MVS  JOB 1,JAFFE,CLASS=A,MSGCLASS=T,NOTIFY=&SYSUID
000002 //*
000003 //  EXPORT SYMLIST=(*)
000004 //  SET CASENUM='1234567'
000005 //  SET CASEDATE='200820'
000006 //  SET CASEDESC='HSMDEATH'
000007 //  SET TRSFHLQ='EDJXADM'
000008 //  SET FTYPE='DUMP'
000009 //  SET WORKPATH='/local/smpnts'
000010 //  SET XFERUID='anonymous'
000011 //  SET XFERPWD='edjaffe@phoenixsoftware.com'
000012 //*
000013 //SFTP      EXEC PGM=BPXBATCH
000014 //STDENV    DD *,SYMBOLS=JCLONLY
000015 SSH_ASKPASS=&WORKPATH./sftp.pw.sh
000016 DISPLAY=DISPLAY
000017 //STDPARM   DD *,SYMBOLS=EXECSYS
000018 SH cd &WORKPATH.;
000019 cp -Bv
000020 "//'&TRSFHLQ..T&CASENUM..D&CASEDATE..&CASEDESC..&FTYPE..TRS'"
000021 trsfile;
000022 echo "echo '&XFERPWD.'" > sftp.pw.sh;
000023 chmod 700 sftp.pw.sh;
000024 echo "cd /toibm/mvs" > sftp.cmds;
000025 echo "put trsfile
000026 TS00&CASENUM..D&CASEDATE..&CASEDESC..&FTYPE..TRS" >> sftp.cmds;
000027 chmod 600 sftp.cmds;
000028 /bin/sftp -oBatchMode=no -oStrictHostKeyChecking=no -oPort=22
000029 -b &WORKPATH./sftp.cmds
000030 &XFERUID.@sftp.ecurep.ibm.com;
000031 rm sftp.pw.sh;
000032 rm sftp.cmds
000033 //STDOUT    DD SYSOUT=*
000034 //STDERR    DD SYSOUT=*
000035 //
****** ***************************** Bottom of Data ***************************
```

A Practical Example (Securely Transfer a File to IBM's Site)

- The script copies a traditional MVS data set to my home directory
- The script initiates *anonymous* sftp (password = email address)
  - You can also use a transferid and password assigned to you by IBM
  - For now, that is optional. You generate them in IBM's support portal.
- SFTP uploads the file to IBM's Customer Data Repository (ECuRep)

```
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----
EDJXADM.T3915225.D200716.ARC1BKUP.DUMP.TRS -> trsfile: binary
sftp> cd /toibm/mvs
sftp> put trsfile
Uploading trsfile to /toibm/mvs/IS003915225.D200716.ARC1BKUP.DUMP.TRS
Welcome to the IBM Enhanced Customer Data Repository (ECuRep).
.
Before using this service refer to the terms of use for exchanging diagnostic.
data with IBM (see https://ibm.com/support/docview.wss?uid=ibm10739407)!.
.
For Documentation and FAQ please see the ECuRep homepage.
https://ibm.com/support/docview.wss?uid=ibm10739631.
.
   LOGIN.
     user      : [transferid].
     password  : [password_of_transferid].
    - or -.
     user      : [anonymous].
     password  : [your_email_address].
.
Please report questions to: contact@ecurep.ibm.com.
Connection closed after 15 minutes idle.
Connected to sftp.ecurep.ibm.com.
********************************************************************** Bottom of Data
```

Acknowledgements Knowing and Unknowing

- Robert Hering (IBM Germany)
- Kurt Quackenbush (IBM)