Indiana SFTP Bulk Upload Guide

Alcohol, Cigarette and Other Tobacco Products

Electronic Taxpayer Service Center

Revised Jul. 2020

Indiana Department of Revenue

Table of Contents

Overview of Bulk Upload

The Indiana Department of Revenue (DOR) bulk upload facility provides taxpayers submitting files containing large numbers within a transaction a method to electronically submit a file to DOR. Bulk upload files are created by the sender and submitted to DOR for processing. The files are processed sequentially upon receipt. During high-volume processing, there may be a slight delay in processing as the files are worked in the order they are received. When the file processing has completed, an email is sent to the authorized representative on file with the results of the submission.

> ***Note:*** *If any records have invalid or incorrect formatted data, the entire return is rejected for those errors. If there are multiple returns in a file, each return can be accepted or rejected independently within the bulk file. The error message lists the returns that require corrective action. After corrections have been made,* ***only*** *the failed return(s) need resubmission.*

This SFTP bulk upload guide is specific to taxes related to Alcohol, Cigarette and Other Tobacco Products. For Withholding and Motor Vehicle Rental Tax, please use the guide specific to those tax types found at https://www.in.gov/dor/4035.htm.

Filing Bulk Returns through Secure SFTP

The following is an outline of the steps required to file bulk returns through the DOR secure SFTP site. The file layout of the specific return type being filed must be followed exactly as published.

Encryption for SFTP Submission

All files must be encrypted using PGP or GPG when sent to the DOR secure SFTP site. The steps in this process are as follows:

Step 1: Create your own public/private key pair using PGP/GPG.
Step 2: Request DOR's public key.
Step 3: Import the department's key into your encryption software for your use.
Step 4: Encrypt the data using only the department's public key.
Step 5: Upload the data to the secure SFTP site.

PGP/GPG encryption works between two parties each of which has a pair of encryption keys; one of which is public, the other being private. The data to be encrypted is encoded using the recipient's public key and signed by the sender's private key. The recipient checks the validity of the sender by checking the signature against the sender's public key. If that step passes, the data can be decrypted using the recipient's private key. In this way, the public key can be made public and there is no need for the private key to be sent to the recipient, thus improving security.

> ***NOTE:*** *If requested, acknowledgement files will be encrypted using the submitter's key and placed in the out SFTP folder for pickup by tax payer.*

PGP or GPG Software

Instructions on how to setup and use:

- PGP software is available in Appendix A
- GPG software is available in Appendix B

Certificate of Registration

If you do not have a Certificate of Registration, you must contact DOR to request the certificate. This certificate of registration contains your file naming convention, your SFTP site login name, and all necessary information to file electronically. Your secure SFTP site password will be emailed in a separate document. Along with the certificate, you also will be sent a link to download software to utilize to connect to the SFTP site. If you have software your company uses to connect to SFTP sites, it can be used in place of the software provided. To request a certificate of registration, you can send an email request to BulkFiler@dor.IN.gov.

Secure File Transfer

Files transmitted via the bulk upload process should be named using the convention shown on page 6. Errors in the naming convention will result in file rejection or delay. The file should be encrypted using PGP or GPG encryption. Please follow the guidelines in Appendix A, or Appendix B for encrypting a file.

The file, named according to specifications provided in your certificate of registration and encrypted using PGP or GPG, can now be uploaded to the SFTP site designated by the department. You can accomplish this programmatically or use SFTP software to connect to the site. You can download software to connect to the SFTP site at http://www.in.gov/iot/2767.htm. At this site select the Secure File Transfer (SFTP) option.

For further instructions on how to download a copy of SFTP, see Appendix A or Appendix B. If you already have software that supports SFTP, you may use your own software.

Acknowledgements

After uploading an encrypted file to the department's SFTP site, you will receive an email to notify you that your file has been processed with a detail of the results. The base filename will be the same as that of the file submitted to the SFTP site.

Within the acknowledgement, there will be a record of each return submitted in the uploaded file. The absence of any error messages or codes indicates the return processed successfully.

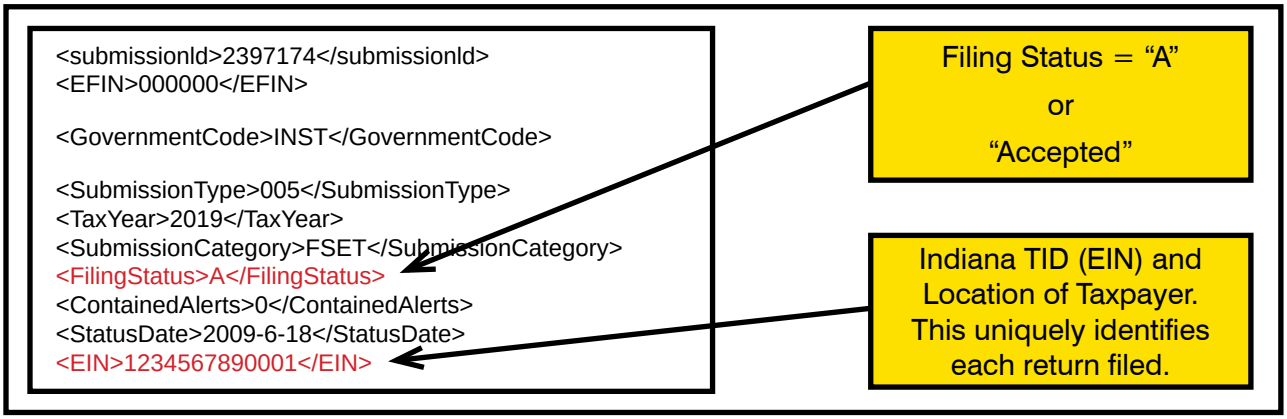
If you do not receive an acknowledgement within two hours, verify the following:

- File was named correctly. See your certificate of registration for proper file name.
- File was encrypted using the department's public key.

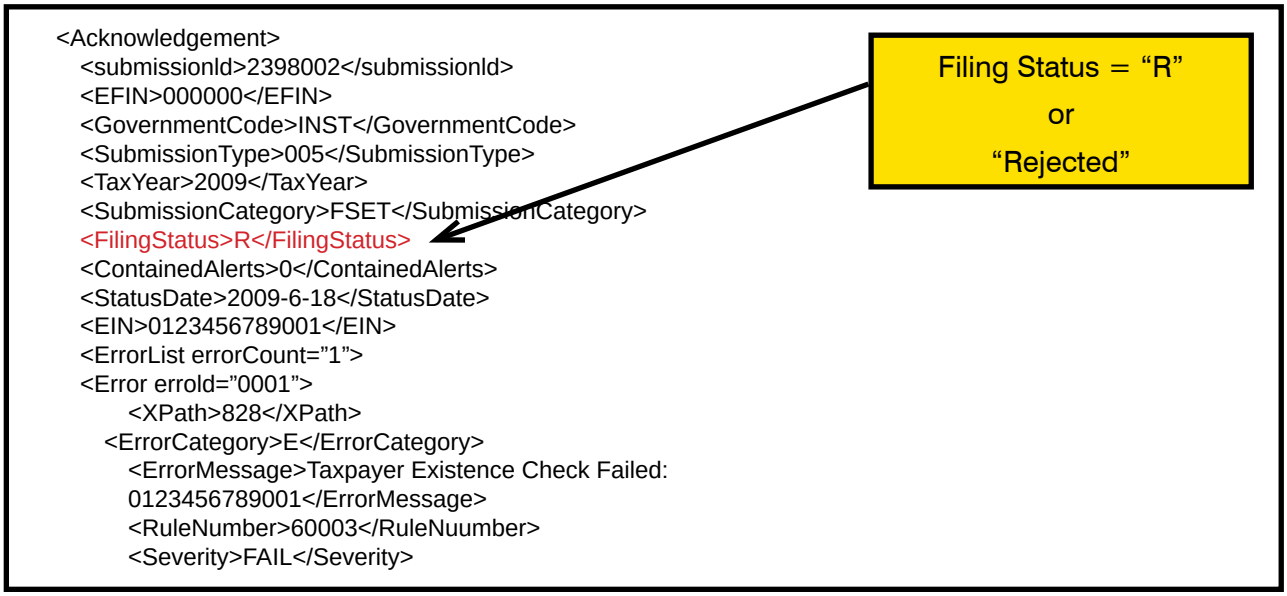
If these are correct, email the department (BulkFiler@dor.IN.gov) to verify DOR received the file.

> ***Note:*** *If you do not receive the acknowledgment file you cannot assume your file has been received and or accepted.*

The following example is a return with no errors. This indicates the return processed.



The following example shows a return that was rejected due to an invalid TID and location in the EIN element. When a return is submitted through the bulk upload process, the Indiana ID and location are verified against the DOR main database. If this TID and location do not match any active accounts in DOR's database, the return is rejected. This return should be corrected and resubmitted.



Test Files

To become certified to upload files to the DOR SFTP site, you must upload two consecutive different files with no errors. All the steps in uploading a production file also apply to test files. The only difference is in the filename. All test files submitted to the SFTP site must begin with the letter T, production files must begin with the letter P. Production files submitted by uncertified taxpayers to the DOR SFTP site will be rejected without any processing.

You can submit as many test files as needed. This is an automated process, so you do not need to contact the department when submitting test files.

After you have submitted two consecutive valid test files, you will need to email the department (BulkFiler@dor.IN.gov). DOR will review the files and let you know of any errors that need to be addressed. If there are no errors, DOR will then certify you to begin submitting production files for the submission type tested. If you do not contact the department prior to submitting your first production file, it will be rejected.

Contact Information

If you still have unanswered questions regarding the electronic filing of returns, please email them to Bulkfiler@dor.IN.gov.

File Naming Conventions

NOTE: *File names must be 21 characters in length, not including the file extensions. Incorrectly named files will not be processed or acknowledged.*

NOTE: *Duplicate filenames in a calendar year will be rejected.*

Position	Number of Characters	Values
1	1	File Type Indicator Valid Indicators: P = Production T = Test
2-11	10	Submitter Identifier as assigned through DOR's registration process. Left Zero padded.
12-14	3	Tax Form Code 560 = ALC-DWS 561 = ALC-FW 562 = ALC-M 563 = ALC-PS 564 = ALC-W 570 = OTP-PACT 571 = OTP-CT19 572 = OTP-M 580 = CIG-PT 581 = CIG-CT19 582 = CIG-M 583 = CIG-TS
15	1	File format that is used to represent the data in the file. This is the file format that was certified. 1 = XML 2 = ASCII
16-21	6	Sequence Number incremented from 000001 for each transmission of the specified Tax Form Code made by the Submitter in a given tax year.
22-25	4	Extension depending on the file format. File format extensions 1 = .xml 2 = .txt
26-26	4	File Extension after encryption .pgp .gpg

Examples:

Before Encryption:

File name of production file (P), submitter identifier 12345678, tax type WH-1 (005), file type - xml (1), sequence 7, P00123456780051000007.xml

After Encryption:

P00123456780051000007.xml.gpg

Quick Reference

Registration Steps

Step 1: Request a certificate of registration. This provides the filename as well as the SFTP login name and password. To request a certificate of registration, you can send an email request to BulkFiler@dor.IN.gov. Visit www.in.gov/dor/4035.htm#registration for more information.

Step 2: Get instructions on how to download and install the PGP or GPG software by referring to Appendix A for PGP or Appendix B for GPG.

Step 3: Download and install the SFTP software from http://www.in.gov/iot/2767.htm. Follow the instructions in Appendix C.

Step 4: Successfully upload two consecutive test files that result in no errors.

Step 5: Contact the department after two valid test files have been submitted.

Steps Repeated Each Return Cycle

Step 1: Create a file containing the returns to be submitted. The file must be in accordance with the specifications. The filename must be in accordance with the certificate of registration.

Step 2: Encrypt the file using the DOR public key. The filename should be the same as that in the previous Step 2 with the additional suffix of .PGP or .GPG. Failure to encrypt the file being submitted could result in your company being decertified to submit bulk returns.

Step 3: Connect to the DOR secure SFTP site using your software or the software downloaded from https://extranet.in.gov/sftp/base. Follow the instructions in Appendix C.

Step 4: Copy the file to the attached SFTP site.

Step 5: You should receive an email with the acknowledgement XML attached. If requested an encrypted acknowledgement file can be picked up on the SFTP site.

Step 6: Fix and resubmit any returns that did not process due to errors.

> ***Note:*** *Resubmit only the returns that failed. Do not resubmit the entire file.*

APPENDIX A – PGP setup and use

Introduction

PGP (pretty good privacy) is a software package used for encryption of files and emails. PGP is now owned by Symantec and is available for a license fee. PGP is downloadable and available for purchase at https://www.symantec.com/products/information-protection/encryption/command-line.

All of the commands in this document were executed in a Command (DOS) window. These commands can also be executed in a Powershell Window. All commands are shown in Courier font. Answers to prompts are highlighted in **bold red** as in the example below:

```
C:\>pgp --gen-key “Your key Name” --key-type “RSA” --encryption-bits 2048 --pass
phrase “Your passphrase” --signing-bits 2048
Your key Name:generate key (2078:non-standard user ID)
Acquiring entropy from system state....done Generating key Your key Name
progress.....******* ........................******* done
0x7CC44594:generate key (0:key successfully generated)
Acquiring entropy from system state....done Generating subkey
progress.....................................................................
.****** **
.....................................................................................
....******* done
0xEF5C71EE:generate key (0:subkey successfully generated)
```

In order to use encryption, a key is required. Keys are composed of a private and a public part. When you encrypt a file for submission to the Indiana Department of Revenue (DOR), you use the public part of the key; when decrypting you use the private part. Below is the command to generate a key.

Conventions used in this tutorial:

- Commands are shown in Courier New type in black.
- Answers to prompted are shown in **bold red** type.
- Substitutions are shown in **bold blue** type.

A transcript for each of the commands below can be found in **Appendix I.**

Install PGP

Purchase the software and download the software from https://www.symantec.com/products/informationprotection/encryption/command-line and follow the installation instructions.

Generate a key

Generating keys is an interactive process.

****Note that you need to remember the passphrase for your key!** Execute the following command

```
C:\>pgp --gen-key “your key name” --key-type “RSA” --encryption-bits 2048 --passphrase
“your passphrase for this key” --signing-bits 2048
```

Once your key is generated, execute the command below to list the keys in your keyring.

```
C:\>pgp --list-keys
```

Export a key

The DOR will email your acknowledgement file by default. If you wish to have your acknowledgment file placed on the DOR server for your retrieval it will be encrypted. If this is your choice, you must export the public part in order to provide it to DOR so your acknowledgement file can be encrypted.

Key names are likely to have spaces and other special characters in the name. The double quotes (") around the name of the key ensure that it is treated properly by PGP and by Windows.

To export the public part of a key, execute the command below, substituting an output file name for **Acme.asc** and your key name for **"Acme LLC (DOR files)"**.

```
C:\>pgp --export "Acme LLC (DOR files)" --output "Acme.asc"
```

Import key

Since you will be encrypting data and sending to DOR, you will need to import the DOR public key to use for encryption.

If you are encrypting, you are using a public key which is what DOR provides. The example below assumes that the DOR public key is stored in a file called "Indiana Department of Revenue ERF.asc" and is in the directory where you are executing the GPG command. Note the use of double quotes (")around the key name below. Execute this command to import a key.

```
C:\>pgp --import "Indiana Department of Revenue ERF.asc"
```

Encrypt a file

Below find the command to encrypt a file, remembering to substitute an appropriate output file name for "file_to_encrypt.txt.gpg" and the name of your file to be encrypted for "file_to_encrypt.txt". Use the key public key provided by DOR that you imported earlier.

```
C:\>pgp --recipient "Indiana Department of Revenue ERF <RAtkison@dor.in.gov>" --output
"file_to_encrypt.txt.gpg" --encrypt "file_to_encrypt.txt"
```

Decrypt a file

To decrypt the file, use the private part of the key you generated earlier. Remember to substitute your key name for "Acme LLC (DOR files)" and the name of the output of the decryption for file_to_decrypt.txt and the name of the file to decrypt for file_to_decrypt.txt.gpg. Note that you will need the passphrase for this step.

```
C:\>gpg -u "Acme LLC (DOR files)" --output file_to_decrypt.txt --decrypt file_to_decrypt.
txt.gpg
```

APPENDIX B – GPG setup and use

Introduction

PGP (pretty good privacy) is a software package used for encryption of files and emails. PGP is now owned by Symantec and is available for a license fee. GPG is the free version of PGP and is downloadable at https://www.gpg4win.org/

All of the commands in this document were executed in a Command (DOS) window. These commands can also be executed in a Powershell Window. All commands are shown in Courier font. Answers to prompts are highlighted in **bold red** as in the example below:

```
PS C:\> gpg --gen-key
gpg (GnuPG) 2.0.26; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it. There is NO
WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
(1)     RSA and RSA (default)
(2)     DSA and Elgamal    (3) DSA (sign only)
   (4) RSA (sign only) Your selection? 1
```

In order to use encryption, a key is required. Keys are composed of a private and a public part. When you encrypt a file for submission to the Indiana Department of Revenue (DOR), you use the public part of the key; when decrypting you use the private part. Below is the command to generate a key.

Conventions used in this tutorial:

- Commands are shown in Courier New type in black.
- Answers to prompted are shown in **bold red** type.
- Substitutions are shown in **bold blue** type.

A transcript for each of the commands below can be found in Appendix J.

Install GPG

Download the software from https://www.gpg4win.org/ and follow the installation instructions.

Generate a key

Generating keys is an interactive process.

****Note that you need to remember the passphrase for your key!** Execute the following command

```
PS C:\>gpg --gen-key

The gen-key command will prompt you for the following values. Kind of key
- 1) RSA and RSA (default)
Your selection? 1
Keysize – 2048
What keysize do you want? (2048) 2048
Key expiration – 0 = key does not expire
Key is valid for? (0) 0
```

Key Name – Choose a name for your key (below find an example)

```
Real name: Acme LLC
Email address:

Comment: DOR files
You selected this USER-ID:
    "Acme LLC (DOR files)"
Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

Choose a passphrase. Passphrases are different from passwords in that they can include spaces and can be very long. **DO NOT FORGET YOUR PASSPHRASE AND KEEP IT SECURE.**

The passphrase prompt is a Window.

Once your key is generated, execute the command below to list the keys in your keyring.

```
C:\>gpg --list-keys
```

Export a key

The DOR will email your acknowledgement file by default. If you wish to have your acknowledgment file placed on the DOR server for your retrieval it will be encrypted. If this is your choice, you must export the public part in order to provide it to DOR so your acknowledgement file can be encrypted.

Key names are likely to have spaces and other special characters in the name. The double quotes (") around the name of the key ensure that it is treated properly by GPG and by Windows.

To export the public part of a key, execute the command below, substituting an output file name for **Acme.asc** and you key name for **"Acme LLC (DOR files)"**.

```
C:\>gpg --armor --output Acme.asc --export "Acme LLC (DOR files)"
```

Import and sign key

Since you will be encrypting data and sending it to us, you will need to import the DOR public key to use for encryption.

If you are encrypting, you are using a public key which is what DOR provides. The example below assumes that the DOR public key is stored in a file called “Indiana Department of Revenue ERF.asc” and is in the directory where you are executing the GPG command. Note the use of double quotes (“)around the key name below. Execute this command to import a key.

```
C:\>gpg --import "Indiana Department of Revenue ERF.asc"
```

Once the key is imported, you will want to sign the key. This is not a requirement but if you do not sign this key you will be prompted each time you encrypt a file to verify the key before encrypting. This step will prevent the prompt each time you encrypt a file. Remember to substitute your key name for **“Acme LLC (DOR files)”** in the example below.

```
C:\>gpg -u "Acme LLC (DOR files)" --sign-key "Indiana Department of Revenue ERF
<RAtkison@dor.in.gov>"
```

Encrypt a file

Below find the command to encrypt a file, remembering to substitute an appropriate output file name for **“file_to_encrypt.txt.gpg”** and the name of your file to be encrypted for **“file_to_encrypt.txt”**. Use the public key provided by DOR that you imported earlier.

```
C:\>gpg --recipient "Indiana Department of Revenue ERF <RAtkison@dor.in.gov>" --output
"file_to_encrypt.txt.gpg" --encrypt "file_to_encrypt.txt"
```

Decrypt a file

To decrypt the file, use the private part of the key you generated earlier. Remember to substitute your key name for **“Acme LLC (DOR files)”** and the name of the output of the decryption for **file_to_decrypt.txt** and the name of the file to decrypt for **file_to_decrypt.txt.gpg**. Note that you will need the passphrase for this step.

```
C:\>gpg -u "Acme LLC (DOR files)" --output file_to_decrypt.txt --decrypt file_to_decrypt.
txt.gpg
```

APPENDIX C - SFTP Client Installation and Setup Instructions (WinSCP)

The following instructions will guide you through the process on how to install and set up the software to send the department your files.

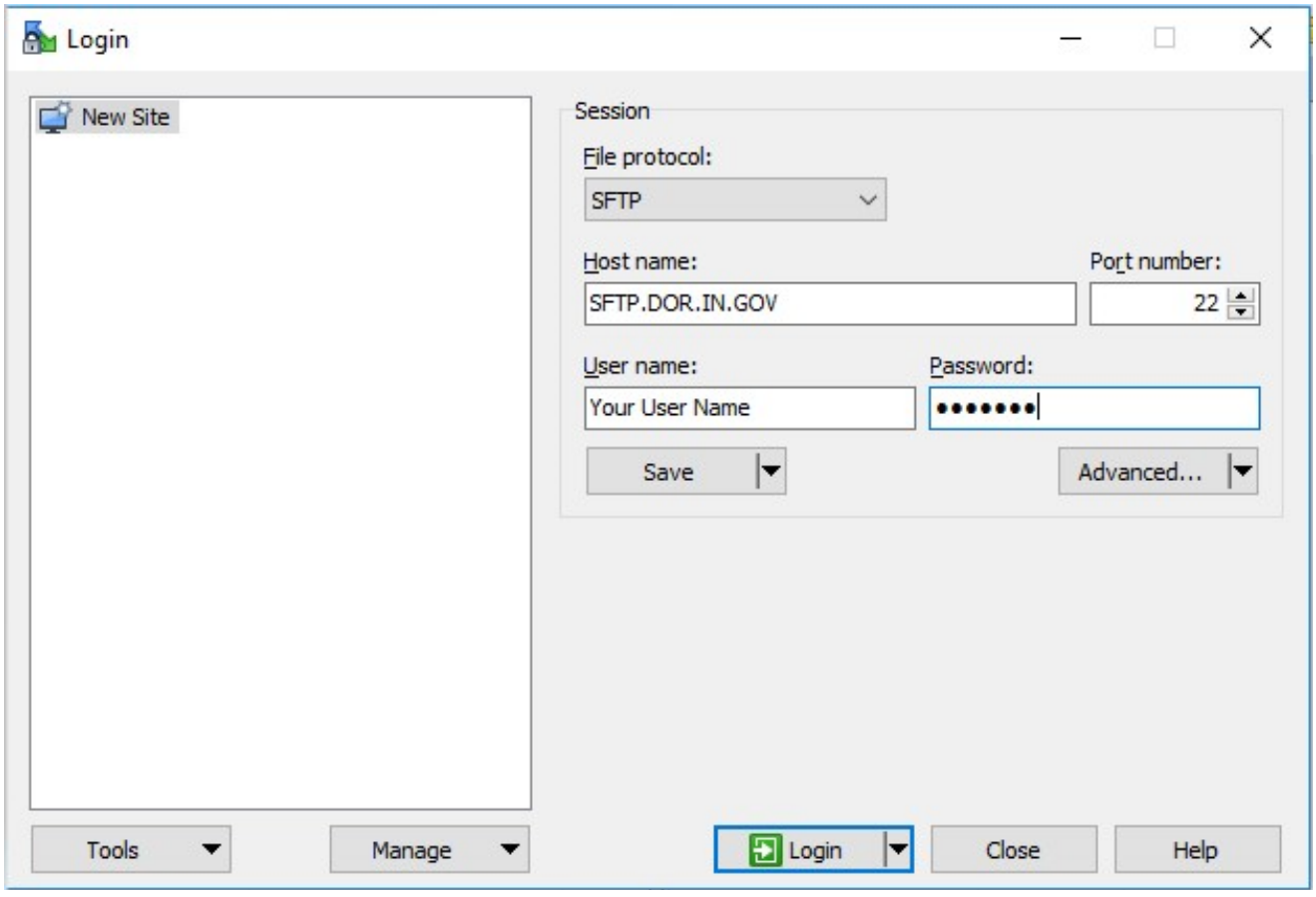
- Go to http://www.in.gov/iot/2767.htm
- Click Secure File Transfer (SFTP).
- Click GUI(Winscp376setup.exe).
- After installing, run WinSCP by double-clicking the desktop icon.

Setting Up and Saving a Secure SFTP Session (OPTIONAL)

- Select SFTP for the File Protocol
- Populate Host Name with: SFTP.DOR.IN.GOV
- Populate Port number with 22
- Populate User name with user name supplied by DOR department
- Populate Password with password supplied by DOR department

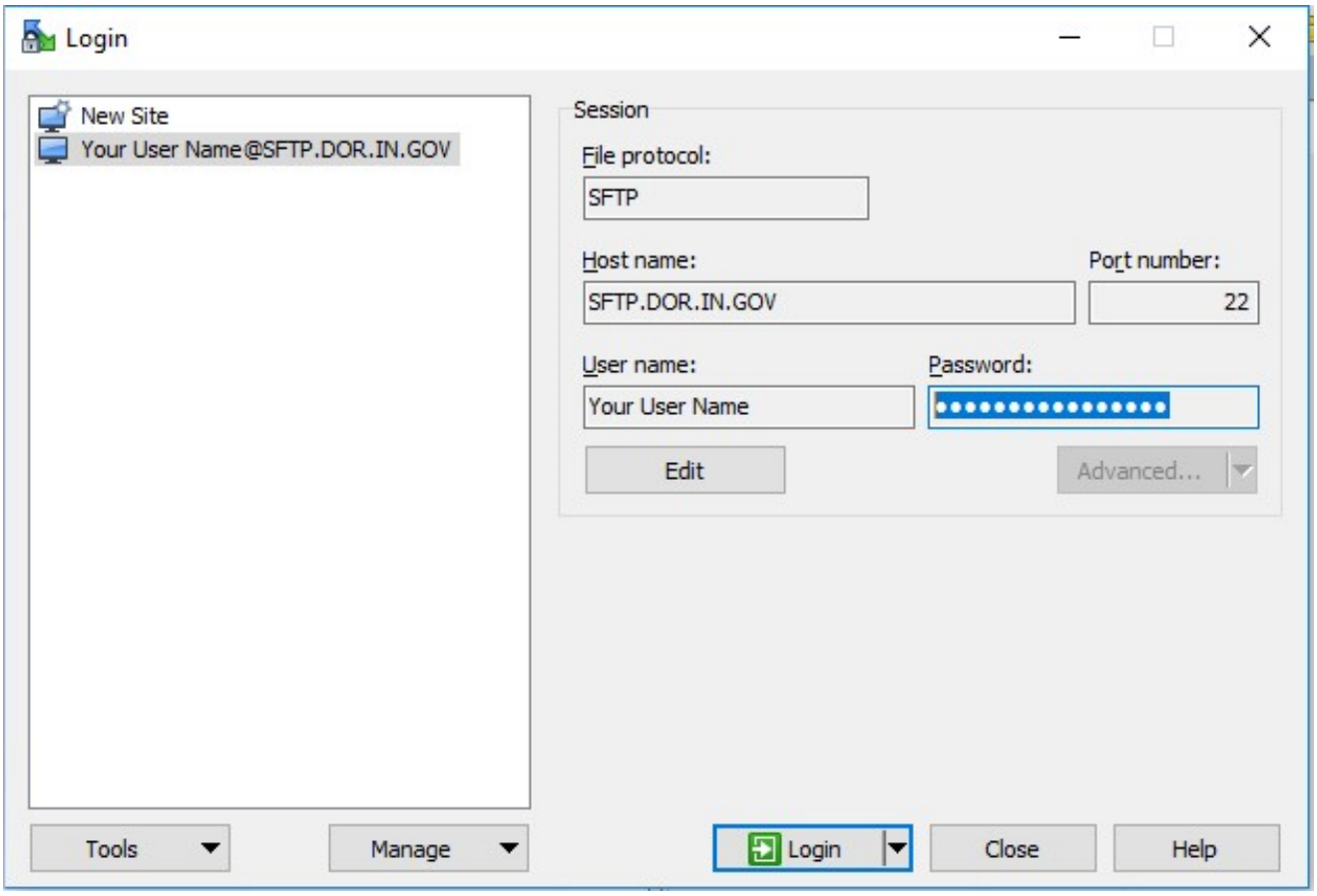
NOTE: *Due to the complexity of the password, it is easier to cut and paste the password into the password field.*

- Click the Save button, supply a site name and folder location (you may wish to save the password)



APPENDIX D – Using WinSCP to Send a File

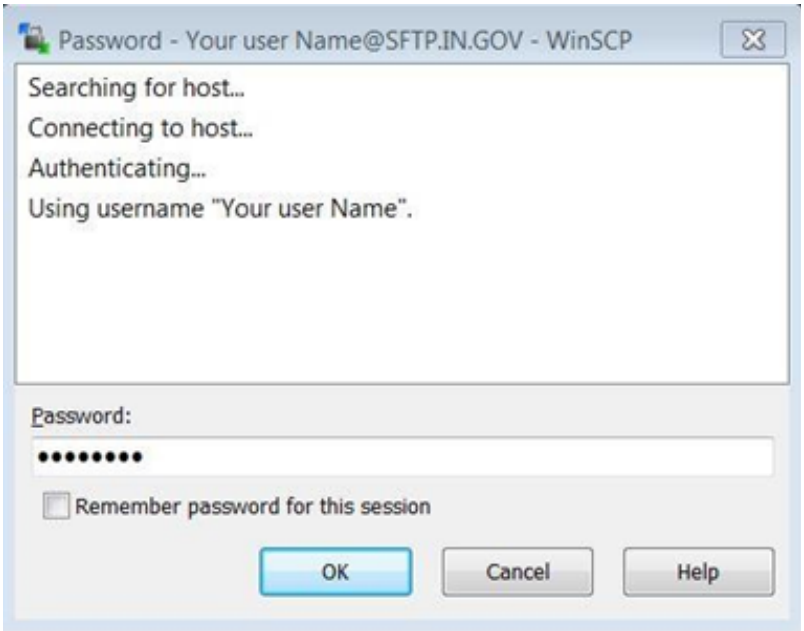
- Double-click the WinSCP icon on your desktop:
- If you previously saved a stored session, click on the name you saved (Your User Name@SFTP.DOR.IN.GOV) and click Login.



- Enter your password (if not saved) and click OK
- This window will open, if you do not want to see this screen each time you login click the "Never show this banner again" check box.

- If you did not provide a password on the login screen you will get this window where you will be prompted to enter your password.

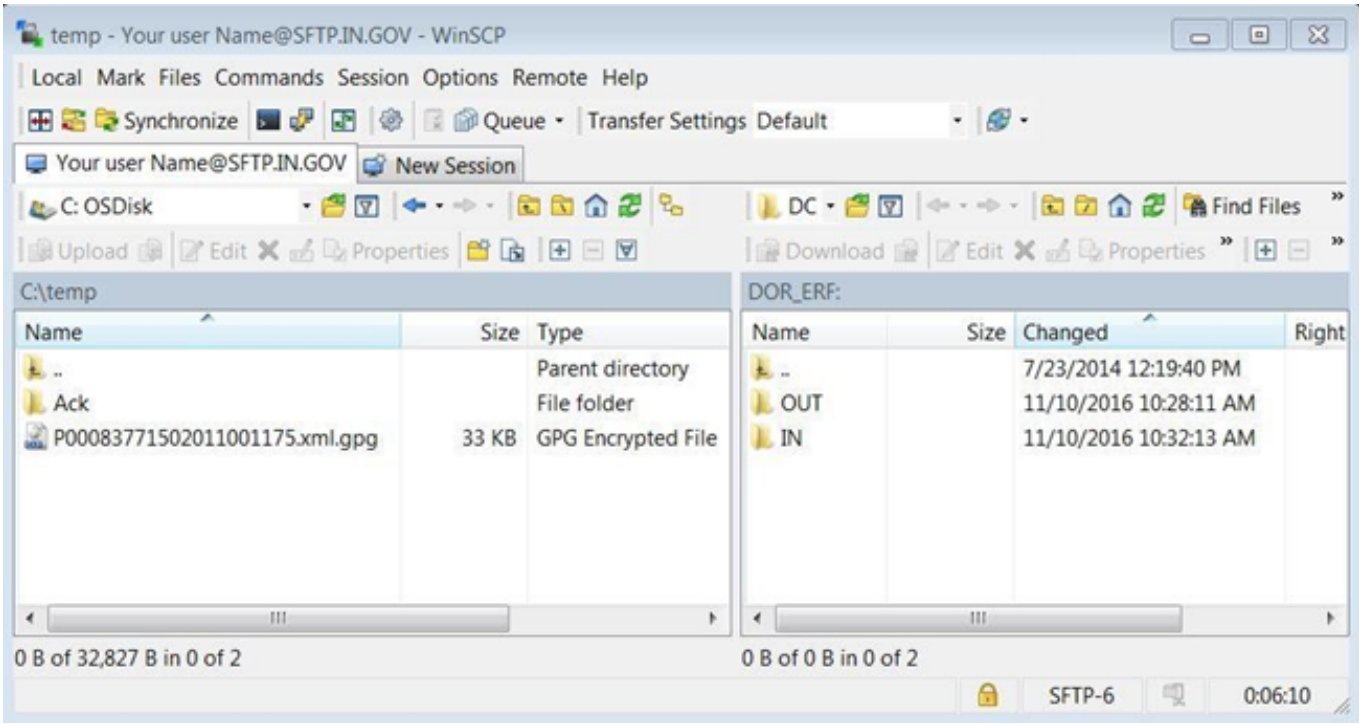
NOTE: *Due to the complexity of the password, it is easier to cut and paste the password into the password field.*



- Accept the host keys and Authorized User Policy. Click Continue.

- Bulk Filing

- The program window will display and split the local directory and the remote directory as two side-by-side panes.



- Using the left pane, go to the location where you created your secure PGP/GPG Zip file. Click and drag that file from the left pane and drop it into the IN folder in the right pane. Repeat as desired. When you are done, click the X in the upper-right corner to close this screen.

APPENDIX E – Common Errors

Submission Errors

Error	Trigger
I did not receive an acknowledgement email.	File was not named correctly. Files not adhering to the naming convention will NOT be acknowledged or processed. If you do NOT receive an acknowledgement email, contact the department before resending any files.
“File not Found” error.	File was not encrypted using the department key.
“Duplication filename this calendar year” error.	Each file submission must have a unique filename within a calendar year.
Uncertified submitter.	The department has not certified your company to submit production files. Please contact the department to resolve this issue.
I do not know the passphrase for PGP.	The passphrase is the passphrase you entered when creating your private key. The department does not know and will not ask for your passphrase. If you do not remember your passphrase, you can delete your private key and create a new one.
I can’t log into the SFTP server.	If you unsuccessfully attempt to login to sftp.dor.in.gov, your ID or IP address could be blocked. Please send an email to BulkFiler@dor.IN.gov and include your ID and IP address. It usually takes 2-3 days to unlock your ID or IP address.
Indiana Department of Revenue key is disabled.	Bring up Symantec Encryption Desktop by clicking your start icon in Windows and clicking All Programs>Symantec Encryption>Symantic Encryption Desktop. Then click the view tab at the top. Then click PGP Keys. Find Indiana Department of Revenue ERF and right click it. Then select Enable. This should enable you to use the key.

File Errors

Error	Trigger
Errors in acknowledgements	The three most common file errors are: 1. Special characters in text fields - i.e. comma (,) period (.) semi-colon (;) colon (:) ampersand (&) apostrophe (‘) number (#) 2. Putting decimals into fields that require whole numbers 3. Space at end of text field

Encrypted Acknowledgements

After sending DOR your file, you have the choice to get your acknowledgement encrypted. If you want your acknowledgement to be encrypted, send an email to BulkFiler@dor.IN.gov with an attachment that is your public key file. DOR will use this to encrypt your acknowledgement. You will need to use your private key to decrypt the acknowledgement upon receipt. You will also be able to pick up an encrypted copy of your acknowledgement in the Outbox using WinSCP.

APPENDIX F – Common Acronyms

Acronym	Desscription
ALC	Alcohol
CIG	Cigarettes
DOR	Indiana Department of Revenue
OTP	Other Tobacco Products
PGP	Pretty Good Privacy (encryption technology)
SFTP	Secure File Transfer Protocol

APPENDIX G – INtax Supported Form Types

Tax Type	INtax Supported Forms
Gasoline Use Tax	GT-103, GT-103DR
Fuel Tax (Motor Fuel and Special Fuel)	MF-360, SF-401, SF-900
Type II Gaming	TTG-103
Aviation Fuel Tax	AVF-150

APPENDIX H – Acknowledgment Error Messages / Resolutions

Error Number	Message	Resolution
01000	General File Level Error	This error is triggered when a file in an unrecognized format is received. For example a PDF file.
01002	Duplicate Employer TID	A file submission may not contain multiple returns with the TID and Location. This will cause the entire file to reject. To resolve this issue you may combine the returns into one return or upload multiple files.
01005	ReadFIleData General Error	
01006	ReadFileData XML Error	
01008	RF Record Not Found	
01010	Duplicate File	This filename has already been received this calendar year.
01011	Payment Exception	This submitter is not certified to attach payments.
10001	Decryption Failed	This error is triggered when DOR is unable to decrypt a file. This could be due to the absence of the proper keys in the DOR master key ring or the encryption by the wrong key. In the event of this error, the file should be encrypted and resent. When this error occurs, no returns contained in the file were processed.
60002	Empty or Invalid Data Record	
60003	Taxpayer Existence Check Error	Each return has a state ID (TID) and location. The TID is 10 digits and the location is always 3 digits. This ID number is verified in the DOR main database to insure the taxpayer is registered to file tax returns in Indiana for the tax type being uploaded. If the process does not find the TID and Location, the individual return will fail. You should then ascertain the correct ID and refile that one failed return.
60005	Uncertified Submitter	All bulk upload submitters must be certified to upload returns to the SFTP site. If a submission is received and the submitter is not certified by the department, the file will be rejected. To resolve this issue please follow the process described in the Bulk Upload Guide.
60015	Schema not active	Schema not active
60016	Schema not found	Schema not found
60017	Invalid schema info	Invalid schema info
60018	Invalid Tax Form Code for channel	Invalid Tax Form Code for channel
60019	Intake Queue Write Failure	Intake Queue Write Failure
60020	Invalid employer record (txt file)	Invalid employer record (txt file)
60021	Invalid TaxID in the RS Record	Invalid TaxID in the RS Record
60022	Invalid County Code in W2 data	Invalid County Code in W2 data
60027	Invalid Submission	Invalid Submission
65000	General XML Error	
65001	XML NameSpace Missing	
65002	XML Validation Error	
65003	XML Deserialization Error	The XML could not be deserialized

APPENDIX I – Transcripts of PGP command execution

Generate a key

```
C:\>pgp --gen-key "Acme LLC (DOR files)" --key-type "RSA" --encryption-bits 2048
--passphrase "your passphrase for this key" --signing-bits 2048
Acme LLC (DOR files):generate key (2078:non-standard user ID)
Acquiring entropy from system state....done
Generating key Acme LLC (DOR files) progress.........................*******
.........................******* done
0xD15FB61E:generate key (0:key successfully generated)
Acquiring entropy from system state....done
Generating subkey
progress.............................................................*******
.........................******* done
0x14EF2D32:generate key (0:subkey successfully generated)

C:\>pgp --list-keys
 Alg  Type Size/Type Flags   Key ID     User ID
----- ---- --------- ------- ---------- -------
*RSA4 pair 2048/2048 [VI---] 0xD15FB61E Acme LLC (DOR files)
1 key found

C:\>
```

List keys

```
C:\>pgp --list-keys
 Alg  Type Size/Type Flags   Key ID     User ID
----- ---- --------- ------- ---------- -------
*RSA4 pair 2048/2048 [VI---] 0xD15FB61E Acme LLC (DOR files)
1 key found

C:\>
```

Export a key

```
C:\Users\JBond\Documents\DOR\erf\samples>pgp --export "Acme LLC (DOR files)" --output
"Acme.asc"
0xD15FB61E:export key (0:key exported to Acme.asc)

C:\Users\JBond\Documents\DOR\erf\samples>dir Acme.asc
Volume in drive C is OSDisk
Volume Serial Number is D0C7-13C7

Directory of C:\Users\JBond\Documents\DOR\erf\samples
10/17/2016  11:11 AM             2,220 Acme.asc
               1 File(s)          2,220 bytes
               0 Dir(s)  365,066,407,936 bytes free
C:\Users\JBond\Documents\DOR\erf\samples>
```

Import a key

```
C:\Users\JBond\Documents\DOR\erf\samples>pgp --list-keys
 Alg  Type Size/Type Flags   Key ID     User ID
----- ---- --------- ------- ---------- -------
*RSA4 pair 2048/2048 [VI---] 0xD15FB61E Acme LLC (DOR files)
1 key found
C:\Users\JBond\Documents\DOR\erf\samples>
C:\Users\JBond\Documents\DOR\erf\samples>pgp --import “Indiana Department of Revenue
ERF.asc”
Indiana Department of Revenue ERF.asc:import key (0:key imported as 0xDC88DED2 Indiana
Department of Revenue ERF <RAtkison@dor.in.gov>)

C:\Users\JBond\Documents\DOR\erf\samples>
C:\Users\JBond\Documents\DOR\erf\samples>
pgp --list-keys
Alg  Type Size/Type Flags   Key ID     User ID
----- ---- --------- ------- ---------- -------
RSA4 pub 2048/2048 [-----] 0xDC88DED2 Indiana Department of Revenue ERF <RAtkison@dor.
in.gov>
*RSA4 pair 2048/2048 [VI---] 0xD15FB61E Acme LLC (DOR files)
2 keys found

C:\Users\JBond\Documents\DOR\erf\samples>
```

Encrypt a file

```
C:\Users\JBond\Documents\DOR\erf\samples>dir file_to_encrypt.txt
 Volume in drive C is OSDisk
 Volume Serial Number is D0C7-13C7

 Directory of C:\Users\JBond\Documents\DOR\erf\samples

10/17/2016  11:14 AM                 0 file_to_encrypt.txt
               1 File(s)              0 bytes
               0 Dir(s)  365,066,395,648 bytes free

C:\Users\JBond\Documents\DOR\erf\samples>

C:\Users\JBond\Documents\DOR\erf\samples>pgp --recipient “Indiana Department of
Revenue ERF
<RAtkison@dor.in.gov>” --output “file_to_encrypt.txt.pgp” --encrypt “file_to_encrypt.
txt”
0xDC88DED2:encrypt (3064:key invalid) file_to_encrypt.txt:encrypt (0:output file file_to_
encrypt.txt.pgp)
C:\Users\JBond\Documents\DOR\erf\samples>dir file_to_encrypt.*
 Volume in drive C is OSDisk
 Volume Serial Number is D0C7-13C7

 Directory of C:\Users\JBond\Documents\DOR\erf\samples

10/17/2016  11:14 AM                 0 file_to_encrypt.txt
10/17/2016  11:15 AM               355 file_to_encrypt.txt.pgp
               2 File(s)            355 bytes
               0 Dir(s)  365,065,060,352 bytes free

C:\Users\JBond\Documents\DOR\erf\samples>
```

Decrypt a file

```
C:\Users\JBond\Documents\DOR\erf\samples>dir file_to_decrypt.txt.pgp
 Volume in drive C is OSDisk
 Volume Serial Number is D0C7-13C7

 Directory of C:\Users\JBond\Documents\DOR\erf\samples

10/17/2016  12:38 PM               355 file_to_decrypt.txt.pgp
               1 File(s)            355 bytes
               0 Dir(s)  365,060,759,552 bytes free

C:\Users\JBond\Documents\DOR\erf\samples>pgp -u "Acme LLC (DOR files)" –output file_to_
decrypt.txt -decrypt file_to_decrypt.txt.pgp --passphrase "your passphrase for this
key" file_to_decrypt.txt.pgp:decrypt (0:output file file_to_decrypt.txt)

C:\Users\JBond\Documents\DOR\erf\samples>dir file_to_decrypt.txt*
 Volume in drive C is OSDisk
 Volume Serial Number is D0C7-13C7

 Directory of C:\Users\JBond\Documents\DOR\erf\samples

10/17/2016  01:22 PM                 0 file_to_decrypt.txt
10/17/2016  12:38 PM               355 file_to_decrypt.txt.pgp
               2 File(s)            355 bytes
               0 Dir(s)  365,060,763,648 bytes free

C:\Users\JBond\Documents\DOR\erf\samples>
```

APPENDIX J – Transcripts of GPG command execution

Generate a key

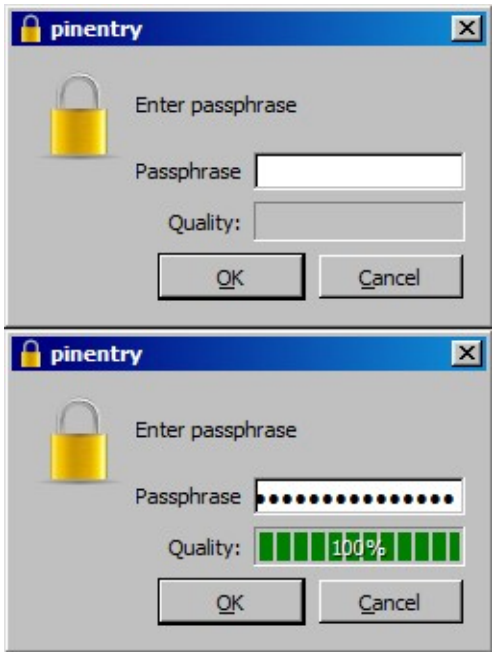
```
PS C:\> gpg --gen-key gpg (GnuPG) 2.0.26; Copyright (C) 2013 Free Software Foundation,
Inc.
This is free software: you are free to change and redistribute it. There is NO
WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
(1)     RSA and RSA (default)
(2)     DSA and Elgamal    (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.
```

```
Real name: Acme LLC
Email address:
Comment: DOR files
You selected this USER-ID:
    "Acme LLC (DOR files)"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O You need a Passphrase to protect
your secret key.
```




```
DOR needs to generate a lot of random bytes. It is a good idea to perform some other
action (type on the keyboard, move the mouse, utilize the disks) during the prime
generation; this gives the random number generator a better chance to gain enough
entropy. DOR needs to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the disks) during
the prime generation; this gives the random number generator a better chance to gain
enough entropy.
gpg: key 9508D9BE marked as ultimately trusted public and secret key created and
signed.
 gpg: checking the trustdb gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust
model gpg: depth: 0  valid:   9  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 9u gpg:
depth: 1  valid:   1  signed:   0  trust: 1-, 0q, 0n, 0m, 0f, 0u pub   2048R/26F74212
2016-09-19
      Key fingerprint = 86DE 3FD1 EC58 992D 8266  BFEE 68FF CD6C 26F7 4212 uid
[ultimate] Acme LLC (DOR files) sub   2048R/D6E5BE8F 2016-09-19

C:\>gpg --list-keys
C:/Users/JBond/AppData/Roaming/gnupg/pubring.gpg
------------------------------------------------
pub   2048R/26F74212 2016-09-19 uid
[ultimate] Acme LLC (DOR files) sub
2048R/D6E5BE8F 2016-09-19

C:\>
```

List keys

```
C:\>gpg --list-keys
C:/Users/JBond/AppData/Roaming/gnupg/pubring.gpg
------------------------------------------------
pub   2048R/26F74212 2016-09-19 uid
[ultimate] Acme LLC (DOR files) sub
2048R/D6E5BE8F 2016-09-19

C:\>
```

Export a key

```
C:\>gpg --armor --output Acme.asc --export "Acme LLC (DOR files)"
C:\>dir Acme.asc
 Volume in drive C is OSDisk
 Volume Serial Number is D0C7-13C7

 Directory of C:\

09/19/2016  09:42 AM             1,716 Acme.asc
               1 File(s)          1,716 bytes
               0 Dir(s)  367,325,331,456 bytes free

C:\>
```

Import a key

```
C:\>gpg --import "Indiana Department of Revenue ERF.asc"
gpg: key DC88DED2: public key "Indiana Department of Revenue ERF <RAtkison@dor.
in.gov>" imported gpg: Total number processed: 1 gpg:               imported: 1  (RSA:
1)
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model gpg: depth: 0  valid:
9  signed:   1  trust: 0-, 0q, 0n, 0m, 0f, 9u gpg: depth: 1  valid:   1  signed:   0
trust: 1-, 0q, 0n, 0m, 0f, 0u
C:\>gpg --list-keys
C:/Users/JBond/AppData/Roaming/gnupg/pubring.gpg ------------------------------------
----------- pub   2048R/DC88DED2 2008-10-24 uid       [ unknown] Indiana Department of
Revenue ERF <RAtkison@dor.in.gov> sub   2048R/CE38E5A6 2008-10-24

C:\>
```

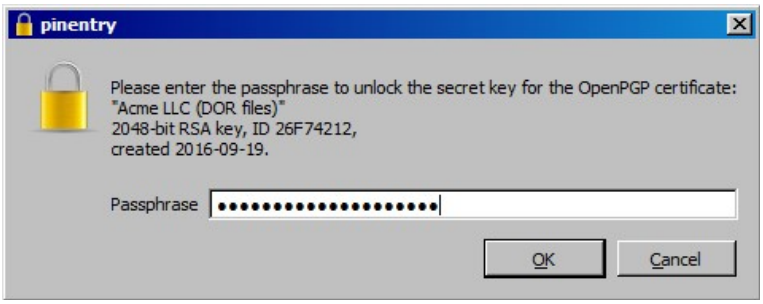
Sign the imported key

```
C:\>gpg -u "Acme LLC (DOR files)" --sign-key "Indiana Department of Revenue ERF
<RAtkison@dor.in.gov>"
 pub  2048R/DC88DED2  created: 2008-10-24  expires: never       usage: SC
trust: unknown       validity: unknown sub  2048R/CE38E5A6  created: 2008-10-
24  expires: never       usage: E [ unknown] (1). Indiana Department of Revenue ERF
<RAtkison@dor.in.gov>
  pub  2048R/DC88DED2  created: 2008-10-24  expires: never       usage: SC
trust: unknown       validity: unknown
 Primary key fingerprint: 9782 BBA7 F6A4 33CD 7A95  3B30 7A32 1AC0 DC88 DED2
     Indiana Department of Revenue ERF <RAtkison@dor.in.gov>

Are you sure that you want to sign this key with your key "Acme LLC (DOR files)"
(26F74212)

Really sign? (y/N) y
You need a passphrase to unlock the secret key for user: "Acme LLC (DOR files)"
2048-bit RSA key, ID 26F74212, created 2016-09-19

C:>
```



Encrypt a file

```
C:\>dir file_to_encrypt.*
 Volume in drive C is OSDisk
 Volume Serial Number is D0C7-13C7

  Directory of C:\

12/02/2014  04:16 PM                49 file_to_encrypt.txt
               1 File(s)             49 bytes
               0 Dir(s)  367,343,636,480 bytes free

C:\>gpg --recipient “Indiana Department of Revenue ERF <RAtkison@dor.in.gov>” --output
“file_to_encrypt.txt.pgp” --encrypt “file_to_encrypt.txt” gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model gpg: depth: 0  valid:
9  signed:   2  trust: 0-, 0q, 0n, 0m, 0f, 9u gpg: depth: 1  valid:   2  signed:   0
trust: 2-, 0q, 0n, 0m, 0f, 0u
C:\>dir file_to_encrypt.*
 Volume in drive C is OSDisk
 Volume Serial Number is D0C7-13C7

 Directory of C:\

12/02/2014  04:16 PM                49 file_to_encrypt.txt
09/19/2016  10:33 AM               399 file_to_encrypt.txt.pgp
               2 File(s)            448 bytes
               0 Dir(s)  367,341,506,560 bytes free C:\>
```

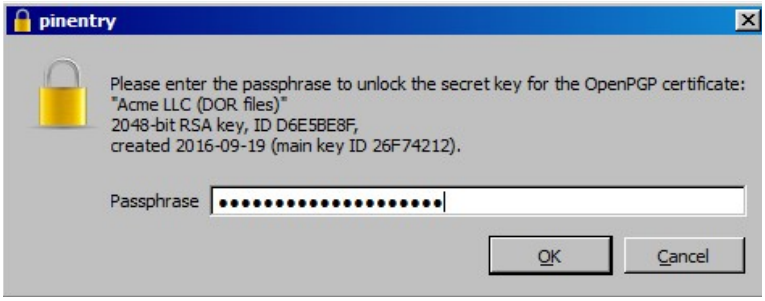
Decrypt a file

```
C:\>dir file_to_decrypt.*
 Volume in drive C is OSDisk
 Volume Serial Number is D0C7-13C7

 Directory of C:\

09/19/2016  10:58 AM               416 file_to_decrypt.txt.gpg
               1 File(s)            416 bytes
               0 Dir(s)  367,338,627,072 bytes free

C:\>gpg -u “Acme LLC (DOR files)” --output file_to_decrypt.txt --decrypt file_to_decrypt.
txt.gpg
You need a passphrase to unlock the secret key for user: “Acme LLC (DOR files)”
2048-bit RSA key, ID D6E5BE8F, created 2016-09-19 (main key ID 26F74212)
 gpg: encrypted with 2048-bit RSA key, ID D6E5BE8F, created 2016-09-19      “Acme LLC
(DOR files)”
```




```
C:\>dir file_to_decrypt.*
 Volume in drive C is OSDisk
 Volume Serial Number is D0C7-13C7

 Directory of C:\

09/19/2016  11:00 AM                73 file_to_decrypt.txt
09/19/2016  10:58 AM               416 file_to_decrypt.txt.gpg
               2 File(s)            489 bytes
               0 Dir(s)  367,337,385,984 bytes free

C:\>
```