

Shipping Services Files (SSF) Secure File Transmission Account Setup

Company Name:

This template is provided to document all of the materials and information needed for configuring secure file transmission for Shipping Services Files.

Shipping Services Files (SSF) Secure File Transmission Account Setup

Section A –Contact Information

This section requires 1 through 3 to be completed.

1. Enter Date Submitted:

2. Enter Company Contact Information:

a. Primary Business Contact:

Name:
Phone:
Email:

b. Primary Technical Contact:

Name:
Title:
Phone:
Email:

c. Primary Production Contact and/or Email Distribution Lists:
(Person(s) who should be notified if file transmissions fail.)

Name:
Title:
Phone:
Email:

Email Distribution List:

3. Select Customer Type: New Existing

a. Enter Mailer ID(s) :

b. Enter Login ID (i.e., mmc*, mme* or mmf*):

Shipping Services Files (SSF) Secure File Transmission Account Setup

Section B – Secure File Transmission Requirements

This section requires 1 through 2 to be completed.

1. Select applicable file transmission and average file sizes to configure:

For capacity planning and to make sure file transmissions are successful, based on transmission history, please provide responses to the following questions. If additional information is needed, your representative will contact you to discuss details of your file configuration.

- a. What type of file will be transmitted?
- b. What is the estimated size of the transmitted file?
- c. What is the transmission frequency of the file?

2. Check secure protocol type:

- AS2 Provisioning (Complete Section C)
- AS2 (Complete Section D)
- SFTP with PGP encryption (Complete Section E)

Section C – AS2 Provisioning Communication Requirements

This section requires 1 through 2 to be completed for AS2 Provisioning

1. Email address to send Provisioning Invitation:

2. OS Type (Note: Windows 8 is not supported):

- Windows 2008
- Windows 7
- Red Hat Enterprise Linux 5*
- SUSE Linux Enterprise Server 9, 10, and 11*

*with ability to run 32-bit executables

Shipping Services Files (SSF) Secure File Transmission Account Setup

Section D – AS2 Communication Requirements

This section requires 1 through 3 to be completed for AS2 configuration.

1. Is the setup using Connectship software?

No Yes (Software must be version 6.4 USPS update AC or version 6.5 USPS update F, or later)

2. Listed below are the default settings for sending to customers.

Specify required overrides needed and list new settings:

- a. Default Format Type: S/MIME Signed/Encrypted
 Override? List New Setting:
- b. Default Encryption Algorithm: AES 256
 Override? List New Setting:
- c. Default Signing Algorithm: SHA256 (LINUX)
 Override? List New Setting:
- d. Default Receipt Type: We request ASync MDNs (separate connection) when sending a payload to you.
 Override? List New Setting:
- e. Default Receipt/MDN Algorithm: Signed, SHA1
 Override? List New Setting:

2a. Customer AS2 Configuration for Production:

- a. Specify HTTP(s) or HTTP when sending to USPS. HTTP(s) HTTP
- b. Provide URL that USPS will send to:
- c. Provide port:
- d. Provide all of the I.P. address(s) of the URL:
- e. Provide all I.P addresses that connections could/will be FROM:
- f. Provide AS2 Identifier:

3. Customer AS2 Certificate exchange

- a. Email certificate to dts-com1@usps.gov prior to the working connectivity testing meeting.

Shipping Services Files (SSF) Secure File Transmission Account Setup

Section E – SFTP/PGP Communication Requirements

This section requires 1 through 2 to be completed for SFTP with PGP encryption configuration.

Note: If the customer requires that public key authentication be done instead of username and password, additional steps will be followed with that customer to set this up.

1. Check Customer's SFTP/PGP Configurations (*options can be both*):

Transmit and/or Pickup files using DTS Server:

- a. Provide all TCP/IP addresses of the customer's servers that will be connecting to USPS:
- b. Is the customer's file suffix .pgp?: Yes No
If no, provide suffix used:

Pull and/or Push files using Customer's Server (*options can be both*):

- a. Provide SFTP user ID and password on customer's SFTP server:
User ID: Note: Password will be exchanged verbally via phone.
- b. Provide default directory where USPS should push files to customer's SFTP server:
- c. Provide default directory where USPS should pull files from customer's SFTP server:
- d. Provide customer's TCP/IP address of their SFTP server and the port to use.
- e. Provide fully qualified domain name (sftp-server.acme.com) of their SFTP server, if used:
- f. Specify if firewall is in place that could possibly prevent USPS from connecting to customer's SFTP server or prevent them from connecting to USPS?:
 Yes No
- g. Are there password expiration or change requirements on the customer's server that DTS needs to be aware of?: Yes No
If yes, specify procedures for changing the password:
- h. Will DTS receive notifications from the customer's system prior to password expiration?: Yes No
- i. Is the customer's file suffix .pgp?: Yes No
If no, provide suffix used:

2. Customer PGP Key Exchange:

- a. Email pgp key to dts-com1@usps.gov prior to the working connectivity testing meeting.