

**FLORIDA DEPARTMENT OF FINANCIAL SERVICES
DIVISION OF WORKERS' COMPENSATION**

**Secure Socket Layer (SSL) / File Transfer Protocol (FTP)
Instructions for POC EDI and Claims EDI**

EDI trading partners shall use the following instructions as a guide for establishing a Secure Socket Layer/File Transfer Protocol (SSL/FTP) account with the Florida Division of Workers' Compensation if sending the following data via the SSL/FTP method of transmission:

- Proof of Coverage (POC) EDI transactions required in Rule 69L-56, F.A.C.,
- Voluntary Claims EDI transactions allowed in Rule 69L-56, F.A.C.

Selecting and Installing a SSL/FTP Client Software Program:

These instructions are tailored using *WS-FTP Pro, version 9.0*, client software program on a Microsoft Windows platform. If the EDI trading partner selects a different SSL/FTP client software program, the SSL/FTP program selected must utilize one of the following certificate negotiation methods for establishing an SSL connection with the Division's SSL/FTP server: AUTH SSL, AUTH TLS-P, AUTH TLS, AUTH TLS-C. **For a complete listing of SSL/FTP Programs that run on a variety of platforms, refer to the following web site:**

http://www.ford-hutchinson.com/~fh-1-pfh/ftps-ext_col.html

Requesting a Signed Certificate from the Division:

The SSL/FTP transmission vehicle utilizes signed digital certificates with 128-bit encryption technology and complies with security requirements set out in the Health Insurance Portability and Accountability Act (HIPAA). Before sending POC EDI and Claims EDI data to the Division via SSL/FTP, the trading partner shall create and email a "Certificate Signing Request" to the Division at poc.edi@fldfs.com.

Note: If the trading partner is sending both POC and Claims EDI data to the Division, the trading partner shall create and send only one Certificate Signing Request file. The Division will authenticate and sign the Certificate Signing Request file and return (email) a Signed Certificate (.crt) file to be used by the trading partner in connecting to the Division's SSL/FTP server. If the trading partner is also sending medical data to the Division via SSL/FTP, a separate SSL/FTP account must be established for medical transmissions. However, the same SSL Signed Certificate may be used for medical, POC and Claims. Eventually, the two accounts may be merged, but at present will be maintained as separate accounts by the Division. The client software program (e.g., WS-FTP Pro) will also use the same certificate for both SSL/FTP accounts.

The following steps (using the example WS-FTP Pro Client Software Program) need only be performed once by the trading partner to generate an encryption Private Key (.key) file, a Self-Signed Digital Certificate (.crt) file, and a Certificate Signing Request (.csr) file:

1. Run WS-FTP Pro and close the "Site Manager" dialog box that pops up for connecting to profiles.
2. Select the "Options" button at the bottom of the screen and click on the tree-view item "Client Certificates" under the "SSL" branch.

**FLORIDA DEPARTMENT OF FINANCIAL SERVICES
DIVISION OF WORKERS' COMPENSATION**

**Secure Socket Layer (SSL) / File Transfer Protocol (FTP)
Instructions for POC EDI and Claims EDI**

3. Click on the "Create" button to start the process of creating a new certificate request.
4. In the "Certificate Name" field, enter your Division-assigned six-character **Trading Partner ID** (FTP userid). Note: If not known, contact the Division to obtain your Trading Partner ID.
5. For the "Expiration Date" field, enter a date that is 20 years into the future.
6. For the "**Pass Phrase**" field, make up a password or pass phrase (multiple words separated by spaces). Do not lose the Pass Phrase or provide to anyone outside your organization, as it is your "private" encryption key. The Pass Phrase does not have to be the same as your "**FTP account password**" (i.e., your SSL/FTP server login password, which should be a minimum of 10 and maximum of 15 alpha-numeric characters).
7. Re-type the "Pass Phrase" in the "Confirm Pass Phrase" field.
8. Click the "Next" button to proceed to the next window.
9. Enter the "City" and two-letter abbreviation for your "State" in the requested fields. Enter "US" in the "Country" field. Click on the "Next" button.
10. For the "Common Name" field, enter the URL of your company's web site. If your company does not have a web site, enter your own name in this field (First Name plus Last Name).
11. Enter your email address in the "Email" field (required).
12. For the "Organization" field, enter your company's name.
13. For the "Unit" field, enter the name of your department within your company. If you do not have a department name, enter "EDI" for the unit name. Click the "Next" button.
14. Click on the "Finish" button. You will receive a confirmation pop-up message if it was successful. Click on the "OK" button of the pop-up confirmation message to close this window.



15. This will create three files in the "C:\Documents and Settings\your_computer_login_ID\Application Data\IpSwitch\WS_FTP\SSL\Certs" directory, Self-Signed Certificate file (.crt), Private Key File (.key), and a Certificate Signing Request File (.csr).
16. You will now be returned to the list of the Client Certificates, where you should see your new FTP userid certificate listed.
17. Click OK, and then exit the WS-FTP Pro program.
18. Using your email software, attach the Certificate Signing Request (.csr) file to an email message and send it to the SSL/FTP account manager at poc.edi@fldfs.com.
19. Upon receiving the Certificate Signing Request (.csr) file from the trading partner, the Division's SSL/FTP account manager will authenticate your company's identity, digitally sign your certificate request, and email you a Signed Certificate file (.crt) for you to use in connecting to the Division's SSL/FTP server. The filename for the returned signed certificate file will have the same name as the .csr file sent to the division, but with "_Signed" added to the filename. For example, if a Certificate Signing Request File called "ABCINS.csr" is sent, then an "ABCINS_Signed.crt" Signed Certificate file will be returned by the Division.

**FLORIDA DEPARTMENT OF FINANCIAL SERVICES
DIVISION OF WORKERS' COMPENSATION**

**Secure Socket Layer (SSL) / File Transfer Protocol (FTP)
Instructions for POC EDI and Claims EDI**

At this point, the Division has activated the EDI trading partner's SSL/FTP account.

Receiving and Configuring the Signed Certificate from the Division:

Upon receipt of the Division's email containing the Signed Certificate (.crt) file, the EDI trading partner shall save the file, and, using the following steps in the example WS-FTP Pro Client Software as a guide, configure the selected SSL/FTP Software Program to use the Signed Certificate for secure file transfers:

1. From the email, save the attached Signed Certificate File (.crt) to the "C:\Program Files\ipSwitch\WS_FTP Pro" directory. This can be accomplished in most email programs by right clicking on the attachment icon and selecting "Save As," then navigating to the desired directory. **NOTE:** On occasion, due to email virus protection, the Division may have to send the signed certificate with a .txt filename extension added to the end of the filename (e.g., ABCINS.crt.txt). If this is the case, trim off the .txt as you are saving the file to make it a .crt filename extension (e.g., ABCINS.crt).
2. Run WS-FTP Pro, and close the Site Manager dialog box that pops up connecting to profiles.
3. Click the "Options" button at the top of the screen, and click on the tree-view item "Client Certificates" under the "SSL" branch.
4. Click on the "Import" button.
5. Click on the "Browse" button in the lower right corner, and navigate to the "C:\Program Files\ipSwitch\WS_FTP Pro" directory to select the signed certificate file (e.g., ABCINS_Signed.crt), and click the "Open" button after selecting it. This will place the signed certificate filename into the "Public Key File" box. **NOTE:** This may be a little confusing, because it is actually a certificate you are selecting at this prompt. Rest assured, you do want to select your signed certificate for this step (not the key file).
6. Click on the "Next" button to proceed to the next window.
7. To select the "Private Key File", click on the "Browse" button, and navigate to the C:\Documents and Settings\Your Username\Application Data\Ipswitch\WS_FTP\SSL\Certs directory, and select your 6 character "userid.key" file (e.g., ABCINS.key), and then click the "Open" button.
8. Click the "Next" button to proceed to the next window.
9. Enter your pass phrase in the "Password" field.
10. Click the "Next" button to proceed to the next window.
11. For the "Certificate Name", enter your 6-character Trading Partner ID (FTP userid) followed by an underscore "_" and the word "Signed". For example: ABCINS_Signed
12. Click the "Next" button to proceed to the next window.
13. Click "Finish" to finish importing the Signed SSL Certificate.
14. Click "OK" close the Settings window.
15. Exit WS FTP Pro.

**FLORIDA DEPARTMENT OF FINANCIAL SERVICES
DIVISION OF WORKERS' COMPENSATION**

**Secure Socket Layer (SSL) / File Transfer Protocol (FTP)
Instructions for POC EDI and Claims EDI**

Creating a New Connection Profile to Connect to the Division of Workers' Compensation SSL/FTP Site:

Using the following steps in the example WS-FTP Pro Client Software as a guide, the EDI trading partner shall configure the SSL/FTP software with the Division's SSL/FTP Site address, and specifically configure the connection profile to use SSL encryption for the connection and data channels:

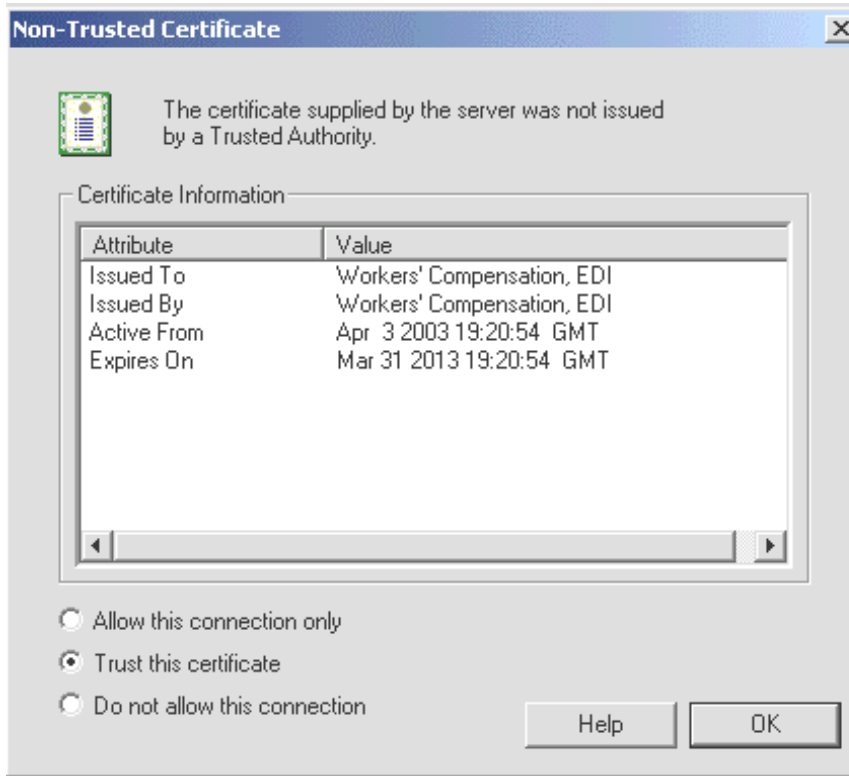
1. Run WS-FTP Pro.
2. Click on the "Create Site" button on the "Site Manager" dialog box that comes up.
3. A "Wizard" type user interface for creating the connection will appear.
4. Enter a name to give the connection, such as "FL WC SSL FTP Site".
5. Click "Next".
6. Enter sslftp.fldfs.com in the "Host Name or IP Address" field.
7. Click "Next".
8. Enter the userid (six-character Trading Partner ID), and the assigned FTP account password.
9. Click "Next".
10. Select Connection Type "FTP/SSL (AUTH SSL)".
11. Click "Next".
12. Un-check the "Connect to the Site" checkbox.
13. Click "Finish". You will be returned to the connection dialog box.
14. Make sure the new connection profile is still selected and click on the "Edit" button.
15. Click on the "SSL" tree branch on the left side of the "Site Options" window.
16. Select your new signed Client Certificate in the dropdown box (e.g., ABCINS_Signed).
17. Check the box that reads "Use only 128 bit SSL for Secure Connections".
18. Click "OK" to accept the changes to the connection profile.

Connecting to the Division of Workers' Compensation SSL/FTP Site:

When connecting to the Division's SSL/FTP server for the first time, the following confirmation message will appear:

**FLORIDA DEPARTMENT OF FINANCIAL SERVICES
DIVISION OF WORKERS' COMPENSATION**

**Secure Socket Layer (SSL) / File Transfer Protocol (FTP)
Instructions for POC EDI and Claims EDI**



Select the “Trust this Certificate” option and click OK. This represents that the Self-Signed Certificate is accepted (accepting the Division’s identity). The Division is performing identity verifications before signing any certificates.

Upon connection, the following three sub-directories will be listed: incoming, outgoing, and badfiles. The subdirectories are to be used for the following purpose:

The trading partner shall use the **incoming** directory to place all incoming data files sent to the Division.

Important: DO NOT ZIP any files before transmitting them. The SSL/FTP connection is a 128-bit secured, encrypted channel, and the files do not need to be zipped.

The Division will place acknowledgement files and reports (including the Claims EDI Report Card, and Rejected Records Not Successfully Resubmitted Report) in the **outgoing** directory and will send an email notification to the trading partner when files are placed in this directory for retrieval by the trading partner. The trading partner shall delete the file(s) from the outgoing directory after retrieval.

If the Division’s system detects that an incoming file cannot be processed (i.e. – defective, empty, bad filename, etc.), the Division will send an email notification to the trading partner identifying the problem and place the file into the **badfiles** directory for further action by the trading partner. The trading partner shall delete the file from this directory after resolving the problem.

**FLORIDA DEPARTMENT OF FINANCIAL SERVICES
DIVISION OF WORKERS' COMPENSATION**

**Secure Socket Layer (SSL) / File Transfer Protocol (FTP)
Instructions for POC EDI and Claims EDI**

File Naming Formats:

The following file naming conventions shall be used for uploading files to the Division:

FTP naming convention: **Suserid148-CCYYMMDD-HHMMSSz.TXT**
 SuseridA49-CCYYMMDD-HHMMSSz.TXT
 SuseridPOC-CCYYMMDD-HHMMSSz.TXT

- The first letter in the filename is fixed and shall be "S"; "userid" represents the Division-assigned six character Trading partner ID. "148", "A49", and "POC" refer to the electronic formats in which the data are sent.
- The **CCYYMMDD** represents the date the transmission was sent, the **HHMMSS** should reflect the hour, minutes, and seconds, and "z" represents whether the file is being sent as test ("T") or production ("P"), followed by **.TXT**.

Test Instructions: The EDI trading partner shall send to the Division a test transfer file to ensure the file is submitted in the correct format. To test EDI DWC-1 submissions, the trading partner shall send both 148 and A49 test files. For all test files, the trading partner shall place a "T" at the end of the base part of the filename to indicate that the transmission is a Test file. For example:

Suserid148-20010910-093011T.TXT
SuseridA49-20010910-093512T.TXT
SuseridPOC-20011231-100013T.TXT

After the Division has received and processed the initial test transmission using SSL/FTP and confirmed the trading partner's ability to receive and process acknowledgements (AK1 transaction), the trading partner shall continue to send transmissions using the "T" Test/Production Indicator until approved for production status. After the trading partner has been approved by the Division to send POC EDI or Claims EDI data in production status, the trading partner shall change the Test/Production Indicator to "P".

The file naming convention for the Acknowledgement transaction (AK1) for Claims and Proof of Coverage EDI is:

CLMAK1-userid-CCYYMMDD-HHMMSSz.TXT

POCAK1-userid-CCYYMMDD-HHMMSSz.TXT

userid = 6-character Trading Partner ID
z = T/P Indicator (test/production)

Note: The date and time on the AK1 filename corresponds to the date and time (including seconds) that the file was created and does not correspond to any original incoming file sent by the trading partner.

**FLORIDA DEPARTMENT OF FINANCIAL SERVICES
DIVISION OF WORKERS' COMPENSATION**

**Secure Socket Layer (SSL) / File Transfer Protocol (FTP)
Instructions for POC EDI and Claims EDI**

Important: The trading partner shall transfer files in **binary mode**. Transmitting the file in ASCII mode may disrupt the line termination within the file, causing the file to be unreadable by the Division's system.

The trading partner shall send the data file in plain ASCII text file format (inside an encrypted ZIP file) with fixed record length, a carriage return (Hex 0D), and line feed character (Hex 0A) at the end of each record.

Programming notes:

The WS-FTP Pro software has a very powerful scripting language that allows automation of the connection and file transfers, should there be a need to automate.