

## USPS Data Transfer Services

<b>Secure Protocol Options</b>			
<b>Communications Method</b>	<b>Communications Products</b>	<b>Transport/ Protocol</b>	<b>Encryption/ Key Management</b>
<p><b>EDI/INT AS2 (preferred solution)</b> The "Internet Engineering Task Force Working Group for Electronic Data Interchange – Internet Integration" is an open standards group that defines how to move standard EDI data over the Internet (charter and standards available at <a href="http://www.ietf.org/html.charters/ediint-charter.html">http://www.ietf.org/html.charters/ediint-charter.html</a>). The USPS is equipped to leverage these existing standards to connect with remote business partners. This option requires that the Business Partner also use an EDIINT capable software product.</p>	<p>There are more than 20 interoperable EDIINT certified software products currently available; for further information consult The Drummond Group. <a href="http://www.drummondgroup.com">www.drummondgroup.com</a> Product currently utilized by USPS is Gateway Interchange supporting AS.2 communications.</p>	<p><b>AS2: S/MIME over HTTP(S)</b> Server ports may be placed outside of the canonical 80/443 set for technical or architectural reasons.</p>	<p>Transaction data is generally signed, with the keys provided in X.509v3 certificates. The Secure Hash Algorithm (SHA1) is used to provide an integrity check against tampering. Body encryption is performed with AES 256 bit encryption. Receipts or acknowledgements may be signed and are generally sent and expected for both the transport and application layers to provide non-repudiation of receipt.</p>
<p><b>SFTP/PGP</b> USPS provides an SFTP solution to allow direct transmissions of files to USPS and for delivery of files to business partner SFTP servers. USPS also provides a solution for business partners that do not have SFTP server to use SFTP to PUT/deposit and GET/pick-up files.</p> <p>While SSH secures the authentication and transport of files, USPS still requests that all files transmitted are PGP encrypted so that data at rest is still protected and data integrity can be assured.</p> <p>This option requires that the Business Partner also use SFTP and PGP capable software products.</p>	<p><b>SFTP</b> is part of the SSH suite. More information may be found at: <a href="http://en.wikipedia.org/wiki/SSH">http://en.wikipedia.org/wiki/SSH</a></p> <p>Users may implement the full SSH suite or use programs which implement SFTP. A list of products, both commercial and open source, may be requested from USPS.</p> <p>PGP and GPG are implementations of a popular encryption package.</p> <p><b>PGP</b> PGP Corporation <a href="http://www.pgp.com">www.pgp.com</a> <b>GnuPG</b> Freeware <a href="http://www.gnu.org">www.gnu.org</a></p>	<p><b>SSH</b> is used as a secure, encrypted transport layer for SFTP over port 22.</p>	<p>SSH automatically negotiates a secure encrypted link per RFC 4253 which handles encryption, compression and integrity verification automatically.</p> <p>Our standard SFTP implementation also requires payload encryption: Current USPS PGP public key is RSA algorithm and 2048 bit key length. For partner keys. Supported body encryption algorithms include 128 bit IDEA and 128 bit Triple-DES</p>
<p><b>Provisioning using EDIINT AS2</b> Because the setup and maintenance of AS2 software can be costly, USPS can provide a preconfigured software package, called Gateway Interchange or Activator, which you download and install on your server. The software uses the AS2 protocol over HTTPS to transfer files securely with USPS. With this software, you have the option of using the Securewebmailbox configuration which ensures that all file transfers are initiated on the partner's end (USPS does not connect to your server directly). USPS and Axway provide all support and updates to the software. For more information on AS2, see the detailed description under our preferred solution section.</p>	<p>Gateway Interchange Activator client, limited license version. (see USPS Provisioning Services Prerequisites Guide for supported OS versions for this client)</p>	<p><b>AS2: S/MIME over HTTP(S)</b> Server ports may be placed outside of the canonical 80/443 set for technical or architectural reasons.</p>	<p>Transaction data is generally signed, with the keys provided in X.509v3 certificates. The Secure Hash Algorithm (SHA1) is used to provide an integrity check against tampering. Body encryption is performed with AES 256 bit encryption. Receipts or acknowledgements may be signed and are generally sent and expected for both the transport and application.</p>