



Pantellos Document Services

HTTPS Delivery Service Protocol



HTTPS Delivery Service Overview

Part of the Pantellos Document Services Architecture, the HTTPS Delivery Service allows trading partners to exchange transaction documents with the Pantellos Marketplace using simple HTTP Post operations over an SSL-secured Internet connection. The initial release of HTTPS Delivery Services will support xCBL documents. When used in conjunction with Pantellos xCBL Versioning Services, xCBL 2.0, 2.2 and 3.0 are supported. The HTTPS Delivery Service has been designed to be flexible and to support additional document standards and xCBL versions in the future.

The HTTPS Delivery Service can only be used for posting asynchronous documents. This specifically excludes synchronous xCBL Request-Response pairs such as OrderStatus, PriceCheck and AvailabilityCheck. Also, the HTTPS Delivery Service does not support attachments. However, all of the transaction services available within the Pantellos Marketplace are available for documents delivered with the post delivery service protocol.

This document describes the protocol required to use the HTTPS Delivery Service.

For additional information, please contact Ben Keating: ben.keating@pantellos.com

Protocol Specification

This specification uses the Hypertext Transfer Protocol HTTP/1.1 over TCP/IP for transmitting documents using the HTTP POST method. Refer to the World Wide Web Consortium website at <http://www.w3c.org/Protocols/> for the HTTP/1.1 standard.

Responses

Responses with a status code of 200 or 202 would mean a successful completion of a post. For errors, a status code in the 400 range would be the equivalent of a client (sender) error, while a status code in the 500 range would mean a server (recipient) error. See RFC 2616 on <http://www.w3c.org/Protocols/> for further explanations on HTTP status codes.

HTTP Header Fields

The following table lists both required and optional headers used in the protocol.

Field	Description	Required (Y/N)
content-length	Length of message as defined by the HTTP 1.1 Standard	Y
content-type	Must be text/xml	Y
authorization:Basic	This is of the form userid:password which must be base-64 encoded (Refer to RFC 2617 for more information on Basic vs. Digest)	Y
x-sender	Senders MarketSite Participant ID	Y
x-receiver	Receiver's MarketSite Participant ID	Y
x-schema	The schema of the document – for example: xCBL , CXML, EDI	Y
x-version	This is the version of the schema. For example, if the schema is xCBL then the version must be one of 20 , 22 or 30 . If the schema is EDI then the version must be 4010	Y
x-docType	The name of the document type within the schema. This must conform to both the schema and version. For example, if the schema is xCBL and the version is 30, valid docTypes would include Order , OrderResponse, ChangeOrder, Invoice, etc.	Y
x-specVersion	The version of the Pantellos HTTP Post specification. Currently must be set to 1.0	Y
x-messageld	The message identifier assigned by the trading partner	N
x-correlationId	The correlation ID that will identify all response documents to the originator	N
x-marketplace-url	The URL of the Marketplace	N