TECHNICAL REFERENCE

Inforce Transactions
# Table of Contents

1 Overview ................................................................................................................................................ 3  
2 Roles and Responsibilities .................................................................................................................. 3  
  2.1 Participants .......................................................................................................................................... 3  
  2.2 DTCC Server ........................................................................................................................................ 4  
3 Communication Protocols ................................................................................................................... 5  
  3.1 SOAP –Messages ................................................................................................................................ 5  
  3.2 One-way SSL authentication ............................................................................................................... 6  
  3.3 Certificate Expiration Procedures for Receiving Participant .............................................................. 7  
4 General ACORD XML Message Types ................................................................................................ 8  
  4.1 Supported Message Types .................................................................................................................. 8  
5 SOAP Compliance .................................................................................................................................. 8  
6 General Protocols for All Messages .................................................................................................... 8  
  6.1 XML Parsing Policy .............................................................................................................................. 8  
  6.2 Message Resend Policy ....................................................................................................................... 8  
  6.3 Time Out Policy .................................................................................................................................. 8  
  6.4 Inforce Transactions with Attachments .............................................................................................. 9  
  6.5 XML Message Size with Attachments .............................................................................................. 9  
  6.6 Inforce Transactions Virus Scan with Attachments ......................................................................... 9  
  6.7 Web Service Requests ....................................................................................................................... 9  
    6.7.1 From Sender (Client) to DTCC (Server): .................................................................................. 9  
    6.7.2 From DTCC (Server) to Receiver (Client) : ............................................................................... 9  
    6.7.3 From Receiver (Client) to DTCC (Server): ............................................................................... 9  
  6.8 General Soap Envelope .................................................................................................................... 10  
    6.8.1 Soap-header ............................................................................................................................ 10  
    6.8.2 SOAP-Body ............................................................................................................................. 10  
7 Errors .................................................................................................................................................... 11  
  7.1 105 –107 Errors .................................................................................................................................. 11  
  7.1.1 Non Business Data Related Errors ......................................................................................... 11  
  7.1.2 Business Data Related Issues .................................................................................................. 13  
8 Appendix A: Schemas and Web Service Definition Language (WSDL) ........................................... 14  
9 Appendix B: Router Exchange Form / IP Address / URL’s .............................................................. 15  
10 Appendix C: Sample Messages ...................................................................................................... 15
1 Overview

Inforce Transactions is a DTCC Web Service that routes messages between distributors and insurance carriers using XML technologies. The messages in scope for this guide are ACORD TXLife 105 and ACORD TXLife 107 messages. Further detail of these messages can be found in the Inforce Transactions Customer Implementation Guide.

Inforce Transactions (IFT) messages are a combination of:

- XML message definitions and DTCC business rules (XML schemas)
- Rules for using these XML schemas
- Software service provided by various parties to use these schemas
- Connectivity between various parties, allowing the software services to communicate
- Definition of the roles, responsibilities, and security levels necessary to accomplish these goals.

The Inforce Transaction Technical Guide should be reviewed in conjunction with Inforce Transaction Implementation Guide and Inforce Transactions Connectivity Guide.

2 Roles and Responsibilities

There are several roles enacted by the parties using the DTCC Server, and each party may play more than one role as necessary to complete the business transaction. The Sender initiates a real-time web service request to the DTCC Server. The Sender is responsible for sending requests using the standardized XML message format provided by DTCC. The Recipient receives the request message originating at the sender and routed through the DTCC Server. The Recipient will see inbound XML messages from DTCC.

2.1 Participants

The Participants must provide a software service that connects to the DTCC Server. The sender acts as a Web Service client (HTTPS) to the DTCC Server, and DTCC Server acts as a Web Service End point (HTTPS) server to the sender. The sender’s software service can make one or more HTTPS Web Service calls to DTCC Service System; each message sent requires SOAP. The message, if applicable, will also include an attachment using MTOM. The response message from the Receiver will always be sent non-MTOM without attachment.

**Note to .NET operation system users:**

.NET users will need to make some modifications to support mixed encoding (mtom request, non-mtom response. We have found that .net requires same encoding for request and response. This implementation supports MTOM request and non-MTOM response (due to no attachments in response).
data and is intended to replace both MIME and DIME (DIME is a lightweight, binary message format that can be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct) Inforce Transactions. At the very beginning of web services people thought of sending text data with SOAP messages. But after some time people thought of sending binary files as a SOAP request or sending a sound clip as a web service request. So as a solution to these problems MTOM came into the act.


For more information, see JAX-WS 2.0 supports MTOM for SOAP 1.1

Using the HTTPS protocol, the sender makes a Web Service request to the Insurance DTCC Server and waits until Insurance Inforce Transactions makes the HTTPS Web Service response. In the case that the DTCC server(s) cannot respond; the sender’s software service must be able to handle various Web Service Faults (timeouts).

The receiver must provide a software service that receives Web Service requests from DTCC Server. The receiver acts as a Web Service endpoint server (using HTTPS) to the DTCC Server, and the DTCC Server acts as a Web Service (HTTPS) client to the Receiver. The receiver’s software service must support more than one concurrent Web Service request (HTTPS) from the DTCC Server.

Using the Web Services (HTTPS protocol), the DTCC Server makes a request to the receiver’s server and waits until the receiver’s server sends the Web Service response (HTTPS). Since the receiver’s server(s) may be unable to respond, the DTCC Server must therefore be able to handle various Web Service Faults. DTCC will timeout the message if not responded.

2.2 DTCC Server

The DTCC Server is a web service provided by DTCC which routes the XML-based interactive transaction messages from sender to recipient. The DTCC Server acts as a message transfer hub which can handle requests and responses from all participating counterparties. The DTCC Server provides a software service that connects to both sender and receiver.

In addition to providing the service, DTCC's role is to standardize communication formats, protocols, and security mechanisms allowing firms to interact with each other in real time. The Server provides for an open message standard architecture, allowing any number of firms to register for this service.
3 Communication Protocols

3.1 SOAP –Messages

For Sender Participant:
DTCC supports the following communication protocol to communicate with sender Participants.

- HTTPS: non-anonymous one way SSL using a digital certificate provided by DTCC, over the SMART network (.net) or participants may choose to go over the internet (.com)*.

*Only Inbound to DTCC can be sent via .com. Response back to Sender will be sent via SMART (.net)

***Please note: DTCC highly recommends using the more secure SMART network.

DTCC owns and manages all elements of the SMART, Securely Managed and Reliable Technology network - from its processing complex all the way through to the customer premises, including the hardware, software and even the relationships with multiple telecommunications carriers, to diversify connections and to ensure continuity of service. SMART uses Internet protocols over private networks to create a highly reliable web of connections. If any connection in the web fails for any reason, the network is "self-healing," and messages are automatically routed over alternate paths.

For more information on SMART connectivity, click on the link below to access the SMART Guide.


Copyright 2011 Depository Trust Clearing Corporation. All Rights Reserved.  Page 5
Version 1.0
The SOAP envelope message allows the sender to specify the receiver Participant ID for the message in the SOAP Header. DTCC will attempt to send the Web Service request to the appropriate user environment based on the information provided in the SOAP Header.

**B2B Authentication**

DTCC B2B systems require an inbound participant to set a specific value in the HTTP User-Agent request header. The User-Agent header’s value will contain the user’s account password. The password will be provided to the user by the DTCC Registration Support Group during the digital certificate download process.

The password value must be enclosed within specific delimiters, therefore, the format should be:

$DSD$password$DSD$

The sample code below shows how to set the User-Agent header:

```java
HttpURLConnection connection=(HttpURLConnection)new URL(url).openConnection();
connection.setRequestProperty("User-Agent","$DSD$"+password+"$DSD$" Spacer
```

**For Recipient Participant**

Inforce Transactions support the following communication protocol when DTCC sends a SOAP Request message to the receiver’s server and when the receiver returns a SOAP response to DTCC.

- HTTPS: One way SSL using trusted web server certificates signed by a third party trusted CA, over the SMART network (.net).

### 3.2 One-way SSL authentication

One-way SSL authentication enables the application operating as the SSL client to verify the identity of the application operating as the SSL server.

The SSL-client application is not verified by the SSL-server application.

**Figure 1** illustrates the certificate configuration for one-way SSL authentication between two applications:

**Figure 1. One-way SSL authentication, where DTCC is Client, Receiving Firm is Server**
Receivers must present a web server certificate signed by a trusted root CA to DTCC to complete the handshake on the outbound connectivity. **DTCC corporate policy does not allow for the presentation of a self-signed certificate.** DTCC allows both standard and extended validation certificates.

A list of Trusted Root CA’s that DTCC accepts can be found on Internet Explorer:
Internet Options -> Content -> Certificates -> Trusted Root CA
Or
In case of FireFox:
FireFox -> Options -> Advanced -> Encryption -> View Certificates -> Authorities

**Browser Test:**

Participants can verify the connection and their login credentials by doing a simple browser test by performing the following steps:
- Import the certificate provided by DTCC into a web browser (preferably IE)
- Open the web browser and connect to DTCC service by connecting to the URL provided by DTCC
- On prompt select the certificate imported. The DTCC web service will respond either with a SOAP message or a simple message about the web service.

### 3.3 Certificate Expiration Procedures for Receiving Participant

When a web server cert expires a firm must renew/purchase a new one to install on their server. Please purchase the certificate at least 4 weeks in advance of expiry and inform DTCC of the new certificate. This way DTCC can verify that the root certificate for the new certificate is in the DTCC keystore. This lead time will prevent unnecessary disruptions of service that may occur from missing setups.

Information provided to DTCC for verification of certificate should include:
1. Serial Number
2. Thumb Print
3. Intermediate and root chain of web server certificate
4 General ACORD XML Message Types

4.1 Supported Message Types

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Request</td>
<td>The Participant sends an XML message. DTCC validates the XML message and sends the message received to the recipient Participant.</td>
</tr>
<tr>
<td>Message Response</td>
<td>DTCC sends an XML message response to the sender Participant after validating the XML message. DTCC sends a status XML message to the sender Participant after receiving a status XML message from the receiver Participant.</td>
</tr>
<tr>
<td>Response Failure</td>
<td>DTCC sends a response failure XML message to the sender Participant if XML validation fails. DTCC sends a failure response XML message to the receiver Participant if validation fails.</td>
</tr>
</tbody>
</table>

Messages are transmitted using the SOAP messaging protocol and DTCC Insurance schemas which are based on ACORD XML standard format.

5 SOAP Compliance

DTCC developed the Web Services application using SOAP 1.1 technology with the Document Literal mode of messaging in compliance with and according to the WS-I Basic Profile.

6 General Protocols for All Messages

6.1 XML Parsing Policy

XML Schemas based on ACORD XML have been established for all message types. The Participants can choose to perform XML Schema validation according to their business needs.

DTCC Server performs DTCC XML Schema validation for all messages it receives without regard to origin from a sender or receiver. Insurance Inforce Transactions acts as a pass-through for Participants messages.

6.2 Message Resend Policy

The DTCC Server will automatically re-send requests on behalf of the sender up to 3 times. If a request does not successfully reach the receivers system, then the DTCC Server will respond to the sender with a connection failure response message. Receipt of a connection failure response message from the DTCC Server successfully terminates the protocol. The sender controls any resends by sending a separate request to the DTCC Server.

6.3 Time Out Policy

DTCC Inbound: 2 minutes for the completion of request and response.
DTCC Outbound: 5 minutes for the completion of request and response.

While messages have an average transmission time of six to eight seconds, according to our policy the maximum time for a message to transmit prior to being timed out is 15 minutes (based on 3 attempts of 5 minutes each).
6.4 **Inforce Transactions with Attachments**

DTCC expects Inforce Transactions request with Attachments using MTOM. Inline Attachments Transactions will not be allowed.

6.5 **XML Message Size with Attachments**

Standard practice is 6 meg per attachment up to 6 attachments per message for a maximum of 36 meg. A large XML file will cause resource constraints for all parties—the distributors, DTCC Server and the insurance carriers. The sender can control the size of the messages.

6.6 **Inforce Transactions Virus Scan with Attachments**

DTCC will not be scanning for viruses. DTCC will not be opening the Inforce Transactions. Standard procedures should have the receiver of the attachment scanning for viruses. If a virus is detected, the recipient can send an error code indicating virus detected.

6.7 **Web Service Requests**

6.7.1 **From Sender (Client) to DTCC (Server):**

- All requests from the distributor to the DTCC Server are sent using Web Service requests.
- The sender can send the XML message as followings:
  - DTCC Server supports XML type (xsd:anytype) to retrieve the message from the request.
  - DTCC Server responds to the Web Service request received. Refer the WSDL section in the document.

6.7.2 **From DTCC (Server) to Receiver (Client):**

- All requests from the DTCC Server to a receiver are sent using Web Service requests.
- The DTCC Server sends the XML message to the receiver using XML type (xsd:anytype). Refer the WSDL section in the document.
- DTCC is going to send an Insurance Inforce Transactions request using one-way SSL.

6.7.3 **From Receiver (Client) to DTCC (Server):**

- All responses back to the DTCC Server should be a SOAP Response (Non-MTOM).
  - Provided that the response passes the DTCC edit, DTCC will route the response back to Sender. If the response does not pass DTCC edit validations, DTCC will send resend Request (reject file) back to Receiver. No action with DTCC is expected by the Receiver from this request. The transaction is considered over after this action occurs.

6.8 **General Soap Envelope**

The SOAP <Envelope> is a simple schema composed of a single <Header> tag and the <Body> tag. The <Header> tag gives information about where to route the message, which has touched the message, and what type of message in enclosed in the envelope. The <Body> tag encapsulates any of the business messages.
The `<Header>` comprises routing information, which encapsulates a single `<MessageHeader>` and contains `<MessageName>`, `<AuthInfo>` and `<RouteInfo>` tags. These tags give the Insurance Inforce Transactions Server information about routing and all parties routing problem determination information.

If your application looks for SOAP Method Names (such as in .net), please note the following:

**SOAP Method Names:**
Stage2 Service Method Name: IWAServiceImpl
Stage2 Error Method Name: ErrorService
Stage3 Service Method Name: IWAServiceImpl

### 6.8.1 Soap-header

**Element Description**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MessageHeader&gt;</code></td>
<td>Root tag for the SOAP header elements.</td>
</tr>
<tr>
<td><code>&lt;MessageName&gt;</code></td>
<td>This is to give a description about the SOAP message. This is an optional field.</td>
</tr>
<tr>
<td><code>&lt;AuthInfo&gt;</code> (OPTIONAL)</td>
<td>This tag represents authentication information and contains User Name and Password information.</td>
</tr>
<tr>
<td><code>&lt;RouteInfo&gt;</code></td>
<td>This tag contains Routing information of the SOAP Request.</td>
</tr>
<tr>
<td><code>&lt;FromParticipant&gt;</code></td>
<td>Sender participant number if it is a request. Receiver participant number if it is an Inforce Transactions response.</td>
</tr>
<tr>
<td><code>&lt;ToParticipant&gt;</code></td>
<td>Receiver participant number if it is a request. Sender participant number if it is a response.</td>
</tr>
<tr>
<td><code>&lt;Sender&gt;</code></td>
<td>This is optional field gives the details of the company/person who is sending the request on behalf of Sender or Receiver.</td>
</tr>
<tr>
<td><code>&lt;RoutingTime&gt;</code></td>
<td>The message sending time from the sender/receiver.</td>
</tr>
</tbody>
</table>

### 6.8.2 SOAP-Body

The DTCC Server validates the elements of the `<Body>` tag as described in this and the preceding chapters. A SOAP-Body contains one TXlife message. The TXLife request contains one or more TXLifeRequest/TXLifeResponse messages. Please refer to the Data Dictionary for the full message architecture.
7 Errors

7.1 105–107 Errors

7.1.1 Non Business Data Related Errors

Errors that are not related to the TXLife xml payload will be sent as SOAPFaults.

7.1.1.1 <faultstring>
Error codes and error descriptions will both be sent in the <faultstring> text. This is being done to make the possible future update from soap 1.1 to soap 1.2 simpler. Soap 1.1 allows a user to create custom <faultcode> data, but soap 1.2 does not. Therefore at this time we will communicate error code and error description information in the <faultstring>. Eg: <faultstring>ERROR_CODE:ERROR_DESCRIPTION.

7.1.1.2 <faultcode>Server
This type of SOAPFault will be sent back to the distributor when an error has occurred at the DTCC server. If you receive one of these errors use the issue escalation procedures to notify DTCC.

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Server</faultcode>
      <faultstring>0006:DTCC Internal Error</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>

7.1.1.3 <faultcode>Client
This type of SOAPFault will be sent back to the distributor when an error has occurred at the DTCC server because of user input.

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Client</faultcode>
      <faultstring>0000:Invalid/Missing Client side Certificate/Password</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>

If you receive the error message above, make sure that the request is being sent to DTCC using the DTCC supplied digital certificate and password. If after ensuring that the correct security credentials are being used the issue remains, then proceed to use the issue escalation procedures to notify DTCC.
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Server</faultcode>
      <faultstring>0001:Invalid User Role</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>

If you receive the error message above, make sure that the request is being sent to DTCC using the DTCC supplied digital certificate and password. If after ensuring that the correct security credentials are being used the issue remains, then proceed to use the issue escalation procedures to notify DTCC.

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Client</faultcode>
      <faultstring>0002:MessageHeader tag is missing in SOAP-Header</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>

If you receive the error message above, make sure that the <MessageHeader> tag set in the soap header of the request is present.

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Client</faultcode>
      <faultstring>0003:Invalid From Participant Id or To Participant Id</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>

If you receive the error message above, make sure that the <FromParticipant> and <ToParticipant> tags in the <MessageHeader>tag contain the appropriate data.
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Client</faultcode>
      <faultstring>0004:Missing XML input</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>

If you receive the error message above, make sure that the <TXLife> element exists in the soap body.

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Client</faultcode>
      <faultstring>0005:XML input validation failed</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>

If you receive the error message above, make sure that the <TXLife> element in the soap body, is valid xml ( refer to the appropriate schema ).

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Server</faultcode>
      <faultstring>0006:DTCC Internal Error</faultstring>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>

If you receive the error message above, then an internal error has occurred. Proceed to contact DTCC.

7.1.2 Business Data Related Issues
These are errors which are related to the TXlife data set. These kinds of errors will be communicated using a regular xml response message ( the message will correspond to the appropriate response schema ). This is a sample response message:
7.1.3 Network Connectivity Issues

DTCC continuously monitors its network connections. There are probes that go out and periodically confirm the router is reachable. DTCC also receives traps indicating other issues with the link.

If a probe fails, DTCC Network Operations will open an incident, troubleshoot the problem, work with the participant/vendor, make sure their backup circuit is running and passing traffic, etc.

We do not allow customers to ping our hosts (Production or Test). DTCC does have addresses that we allow the participant to ping. Network engineers from participant and DTCC would need to discuss options.

8 Appendix A: Schemas and Web Service Definition Language (WSDL)

Download the Inforce Transactions WSDLs and Schemas (ZIP Archive, .zip) from the IPS Website.

This is the link to Record Layouts section where the WSDL and Schema are located.
http://www.dtcc.com/products/insurance/members/downloads/IFT_Schemas_1-0.zip

9 Appendix B: Router Exchange Form / IP Address / URL’s

The Router Exchange Form is filled out by participants prior to starting connectivity. This form is used to provide the proper ip address and ports needed for setup. It also provides the inbound and outbound urls needed to connect.

Inbound URL and IP Addresses (Sender to DTCC):

URLs:
Over the internet -> https://server.dtcc.com/inswsb2bpse/INSWS/services/IWAServiceImpl
Over SMART Network -> https://server.dtcc.net/inswsb2bpse/INSWS/services/IWAServiceImpl
Internal -> https://server.dtcc.org/inswsb2bpse/INSWS/services/IWAServiceImpl

IP Address (for both Production and Test): 207.45.47.43
Port: 443

Outbound URL and IP Addresses (DTCC to Receiver):
These are the IP addresses that a transmission from DTCC to the Receiver will be sent from:
Production: 207.45.47.38
Test: 207.45.47.39
Port: 443
URL for Outbound: Receiving firm must provide DTCC with the URL/endpoint that they wish the messages be directed to. There will be one URL for test and one URL for production. URL’s must be HTTPS.

10 Appendix C: Sample Messages

Sample messages are available at the IPS Website: under construction

Or click on:
Inforce Transactions XML Samples (ZIP Archive, .zip) – under construction

Note: The generated XML message could contain different data. These examples provided on our website are for illustration purposes. Please consult the schema for more information.
Change Log

<table>
<thead>
<tr>
<th>DATE</th>
<th>VERSION</th>
<th>CHANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/4/2011</td>
<td>v.01</td>
<td>First draft</td>
</tr>
<tr>
<td>09/08/2011</td>
<td>v.1.0</td>
<td>Final</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated 6.8 and added Section 7</td>
</tr>
</tbody>
</table>