TECHNICAL REFERENCE

InForce Transactions (IFT) Web Services

Last Updated: December 2017

Table of Contents

1 Overview

InForce Transactions (IFT) is a DTCC Web Service that routes messages between distributors and insurance carriers using XML technologies. There are several messages in scope for this guide that support the life cycle of an insurance contract. The IFT Web Services comprise of the following ACORD TXLife messages:

- Arrangements (107)
- Death Notification (810)
- Financial Withdrawals (105)
- Fund Transfers (102)
- Policy Administration (113)
- Policy Administration Inquiry (115)
- Values Inquiry (212)

Further detail of these messages can be found in the InForce Web Services Implementation Guide.

InForce Transactions (IFT) messages are a combination of:

- XML message definitions (XML Schemas) and DTCC business rules
- 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 IFT Web Service Implementation Guide and IFT Web Services Connectivity Guide available on our I&RS website:

http://www.dtcc.com/wealth-management-services/insurance-and-retirement-services

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. The recipient initiates a real-time web services response to the DTCC server. The recipient is responsible for sending response messages using the DTCC

implementation of the standard XML message format. The sender will receive the response message routed through the DTCC server.

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).

Using the HTTPS protocol, the sender makes a Web Service request to the Insurance DTCC Server and waits until Insurance Inforce Web 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.

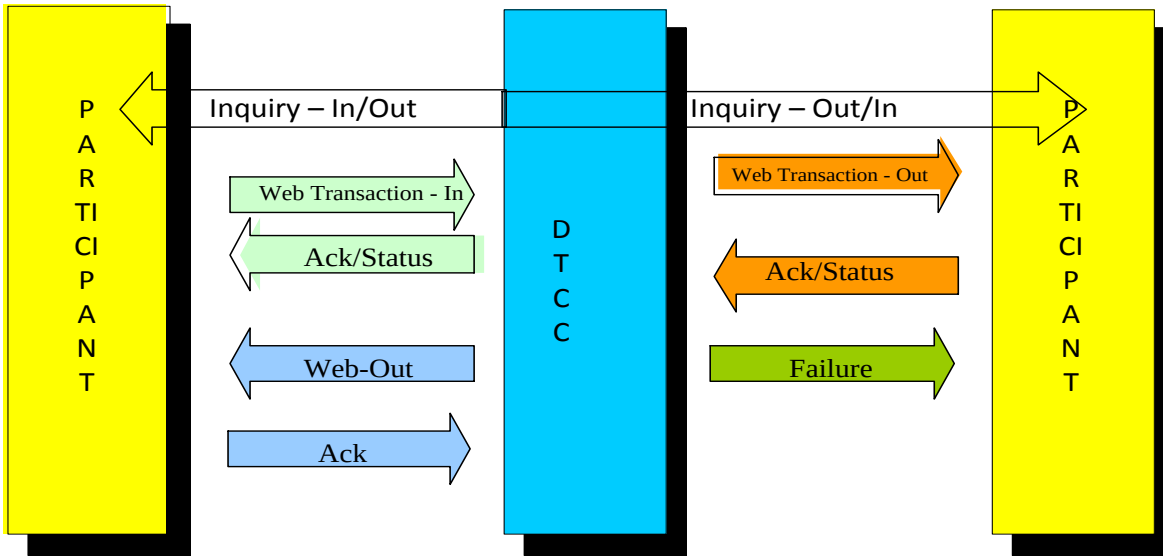
Using the Web Services (HTTPS protocol), the DTCC Server makes a request to the receiver's server and waits until the receiver's server sends the Web Service response (HTTPS). Since the receiver's server(s) may be unable to respond, the DTCC Server must therefore be able to handle various Web Service 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.

DTCC supports both Synchronous and Asynchronous process. For Values and Policy Administration Inquiry messages between the message sender and DTCC, DTCC utilizes the Synchronous process whereas each party is required to wait for a response. Whereas, for all other transactions including all message transactions between DTCC and the recipient, DTCC uses the Asynchronous process.



3 Communication Protocols

3.1 Communication Certificate Overview

There are 3 available uses of digital certificates with IFT web services processing. They are described as follows:

1 – Certificate presented from the I&RS client (BD or Service Provider) to DTCC upon submission (inbound to DTCC) of a web services request messages. This certificate is provided to the I&RS client from the DTCC Portal by downloading this certificate to their local workstation or server which transmits the web services request messages to DTCC.

Who is responsible for managing this certificate expiration: DTCC's Registration Support Group (RSG) along with the Customer Registration Support (CRS) system.
When this certificate is about to expire (30 days in advance of expiration), the CRS system will notify the client (via email) whom downloaded the certificate of their upcoming certificate expiration. CRS will continue to notify this client weekly, until the clients renews their certificate or the certificate expires.

The AC (Access Coordinator) at clients' company can reissue the certificate using DTCC CRS portal.

2 – Certificate presented from the I&RS client (Carrier or Service Provider) to DTCC upon submission (outbound from DTCC) of a web services request messages. This certificate is purchased by the I&RS client from a 'trusted authority' (eg: GeoTrust). The I&RS client will notify DTCC by emailing InsuranceSupport@dtcc.com and your I&RS relationship manager of their renewed certificate to make sure this certificate's root is present and recognized in I&RS's Keystore table. This certificate supports the 1 way authentication. Client has to present the entire chain during handshake since DTCC only maintains the root certificates.

Who is responsible for managing this certificate expiration: The I&RS client who purchased the certificate is responsible to manage and renew prior to the certificate's expiration date. When this certificate is about to expire (at least 30 days in advance of expiration), the client should prepare to purchase and renew their expiring certificate and alert DTCC.

3 – Certificate presented from the DTCC to the I&RS client (BD, Carrier or Service Provider) upon submission (outbound from DTCC) of web services request or response messages. The certificate is provided by DTCC to the I&RS client to support 2 way or mutual authentication.

The I&RS client should whitelist this certificate to recognize when DTCC presents the certificate. DTCC requires mutual authentication when a client is communicating with DTCC over the internet protocol. It is optional for the SMART communication protocol.

Who is responsible for managing certificate expiration: DTCC supports the management of this certificate. When this certificate is about to expire (at least 30 days in advance of expiration). DTCC will notify the client of the upcoming certificate expiration and will present the renewed certificate information to the impacted client(s).

3.2 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/BT Radiance network (.net) or participants may choose to go over the internet (.com)*.**

*****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 to access the SMART Guide.

Clients using single request and response messages (synchronous) can use BT Radiance. This technology has no fixed DNS, won't be useful for asynchronous messaging

Clients can use Internet (.com) on the inbound to DTCC with the certificate provided by DTCC and by providing the user id and password in WSSE elements of SOAP message. If clients choose to use Internet (.com) on the outbound from DTCC, they must implement 2-way SSL.

Note: DTCC suggests using TLS version TLSv1.1 and above for the transport layer. Highly recommends using TLSv1.2

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 populating user id and password in the WSSE headers of SOAP message (refer the Authentication section). The password will be provided to the user by the DTCC Registration Support Group during the digital certificate download process. Client AC (Access Coordinator) at clients' company has ability to create user ids, reset passwords and issue certificates for their internal users using DTCC CRS portal.

Passwords expire every 90 days and clients need to track their own expiration.

Clients can reset their password by either:
- reset the password from the DTCC Web Portal. Use the revised password with your webservice transmissions.
- submit the XML request message to electronically reset your password. Upon receiving a successful XML response message result, use the revised password with your web service transmissions.

Refer to the zip file under the InForce Web Transactions (IFW) section on the I&RS website's Record Layout landing page.

Authentication

DTCC B2B systems require an inbound participant to set a specific value in the SOAP header along with the DTCC provided certificate. The <wsse:Security> tag in the SOAP Header will contain the user's account name and password(clear text). The password will be provided to the user by the DTCC Registration Support Group during the digital certificate download process or by the Access Coordinator at clients' company.

The sample code below shows how to set the SOAP header:

```
<wsse:Security  soapenv:actor=http://schemas.xmlsoap.org/soap/actor/next>
    <wsse:UsernameToken>
        <wsse:Username>someusername</wsse:Username>
        <wsse:Password Type=http://docs.oasis-open.org/wss/2004/01/oasis-
        200401-wss-username-token-profile-
        1.0#PasswordText>yourpasswordhere</wsse:Password>
    </wsse:UsernameToken>
</wsse:Security>
```

For Recipient Participant

Inforce Transactions support the following communication protocols 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 over SMART using trusted web server certificates signed by a third party trusted CA, over the SMART network (.net).**

- **2-way SSL over internet.**

Note: DTCC won't allow self-signed certificates

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. Root chain of web server certificate

4 General ACORD XML Message Types

4.1 Supported Message Types

DTCC supports following ACORD messages: 102, 105, 107, 212, 113, 115 and 810

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 should perform XML Schema validation according to the DTCC basic Schema rules.

It is highly recommended, during pre-production testing phases, clients test and validate their XML messages against the DTCC basic schema before transmitting the message to DTCC for processing. This is recommended for a higher level of assurance the message will pass DTCC validation.

DTCC Server performs DTCC XML Schema validation for all messages it receives without regard to origin from a sender or receiver

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.

6.2 Supported white listed allowable Characters

0-9 (number)	A-Z (Capital Letters)
a-z (lower letters)	* (asterisk)
_ (space)	@ (at symbol)
# (pound sign/number sign)	. (period, dot)
, (comma)	‘ (single quote)
_ (underscore)	/ (forward slash)
~ (estimate sign)	\ (backwards slash)

(hyphen)	% (percentage)
$ (dollar sign)	! (exclamation point)
((open parenthesis)	) (close parenthesis)
& (amersand sign)	" (single quote)
+ (plus sign)	: (colon)
; (semicolon)	® (trademark symbol)

Note: Refer the schema for validation restrictions

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). However for the Values Inquiry 212 and Policy Administration Inquiry DTCC will attempt to connect 1 time and after 60 seconds will then return a timeout response to the sender.

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 usage suggests maximum size is 6 megabytes per attachment up to 6 attachments per message for a maximum of 36 megabytes.

6.6 InForce Transactions Virus Scan with Attachments

DTCC will not be scanning attachment documentation for viruses contained within XML messages.. 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.

• DTCC Server responds to the Web Service request received. Refer the WSDL section in this 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.
- DTCC is going to send an Insurance Inforce Transactions request using one-way SSL or 2 way SSL (mutual authentication) depending on the client setup.

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 envelope. The <Body> tag encapsulatesthe ACORD message based on the DTCC schema rules.

The <Header> comprises routing information, which encapsulates a single < MessageHeader> and contains <MessageName> and <RouteInfo> tags. These tags give the DTCC Inforce Transactions Server information about routing and all parties involved with the message. Please see Soap Header section in this document for processing and business rules.

If your application looks for Web Service Endpoint Names (such as in .net), please note the following:

WEB SERVICE ENDPOINT NAMES:
Stage2 Service Method Name: IWAServiceImpl
Stage2 Error Method Name: IWAServiceImpl
Stage3 Service Method Name: IWAServiceImpl

SOAP ACTIONS:

- processWithdrawal
- processWithdrawalCancel
- processArrangement
- processArrangementCancel
- processValueInquiry21208
- processValueInquiry
- processFundTransfer
- processFundTransferCancel
- processPolicyAdministration

- processPolicyAdministrationCancel
- processPolicyAdministrationInquiry
- processDeathNotification
- processValueInquiry21208Resend (Carrier wsdl only)
- processValueInquiryResend (Carrier wsdl only)
- processFundTransferResend (Carrier wsdl only)
- processFundTransferCancelResend (Carrier wsdl only)
- processPolicyAdministrationInquiryResend (Carrier wsdl only)
- processPolicyAdministrationResend (Carrier wsdl only)
- processDeathNotificationResend (Carrier wsdl only)

6.8.1 Soap-header

Element Description

Note: The <FromParticipant> and <ToParticipant> elements are validated by DTCC**.** These elements are also validated against the <DTCCMemberCode> included in the SOAP message body.

Element	Description
<MessageHeader>	Root tag for the SOAP header elements.
<MessageName>	This is to give a description about the SOAP message. This is an optional field.
<RouteInfo>	This tag contains Routing information of the SOAP Request.
<FromParticipant>	Sender participant number if it is a request. Receiver participant number if it is an Inforce Transactions response.
<ToParticipant>	Receiver participant number if it is a request. Sender participant number if it is a response.
<Sender>	This is optional field gives the details of the company/person who is sending the request on behalf of Sender or Receiver.
<RoutingTime>	The message sending time from the sender/receiver.
<wsse:Security>	This is for user authentication

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

may only contain one TXLifeRequest/TXLifeResponse message. Please refer to the Data Dictionary for the full message architecture and the DTCC Schema file(s).

7 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. Below are examples of certain error types.

This list is not all inclusive and may not be indicative of current implemented error conditions.

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.

```
<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 and 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 and 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.

Conditions

1. The FromParticipant tag is missing from the soap header
2. The FromParticipant tag is blank in the soap header
3. The FromParticipant tag contains a value which does not exist in DTCC Participant Table
4. The FromParticipant tag does not match the broker Party's DTCCMemberCode field

5. The ToParticipant tag is missing from the soap header
6. The ToParticipant tag is blank in the soap header
7. The ToParticipant tag contains a value which does not exist in DTCC Participant Table
8. The ToParticipant tag does not match the carrier Party's DTCCMemberCode field

Condition #	Response
1	SOAP fault exception message 0006: FromParticipant tag is missing/invalid in the soap header
2	SOAP fault exception message 0006: FromParticipant tag is missing/invalid in the soap header
3	SOAP fault exception message 0003: FromParticipant tag is missing/invalid in the soap header
4	TXLifeResponse – The FromParticipant tag does not match the broker Party's DTCCMemberCode field
5	SOAP fault exception message 0006:The ToParticipant tag is missing/invalid in the soap header
6	SOAP fault exception message 0006: The ToParticipant tag is missing/invalid in the soap header
7	SOAP fault exception message 0003: The ToParticipant tag is missing/invalid in the soap header
8	TXLifeResponse – The ToParticipant tag does not match the carrier Party's DTCCMemberCode field

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 (he message will correspond to the appropriate response schema). This is a sample response message:

```
<TXLife xmlns="http://ACORD.org/Standards/Life/2"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://ACORD.org/Standards/Life/2 C:\Temp\Schemas1.5\AR_RES.xsd">
    <TXLifeResponse >
        <TransRefGUID>0</TransRefGUID>
        <TransType tc="107">String</TransType>
        <TransExeDate>1967-08-13</TransExeDate>
        <TransExeTime>14:20:00.0Z</TransExeTime>
        <CorrelationGUID>String</CorrelationGUID>
        <TransResult>
```

```
                    <ResultCode tc="5">Failure</ResultCode>
                    <ResultInfo>
                        <ResultInfoCode tc="200">Error Description</ResultInfoCode>
                        <ResultInfoSysMessageCode/>
                    </ResultInfo>
                </TransResult>
            </TXLifeResponse>
</TXLife>
```

7.1.3 Network Connectivity Issues

DTCC continuously monitors its network. 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. Please contact your Relationship Manager if you need more information.

8 FAQs

Below are few FAQs by Sender and Receiver.

8.1 Sender FAQs

`Client supplied invalid authentication information`
Client: • Check the *certificate* expiry date • Check the password in the WSSE headers of SOAP message • Validate *User ID* by logging into *PSE (https://portalu.dtcc.com)* or *Production (https://portal.dtcc.com)* portal depending on the environment • If the above steps do not work, email DTCC support (insurancesupport@dtcc.com) with *User ID* and *transaction timestamp.*

`Received 200 – validation errors`

Client:

- Check *Messaging Dashboard* for error message.
- Validate message sent against schema.
- If the above steps don't solve the issue, reach out to DTCC support (insurancesupport@dtcc.com) with TransRefGUID and Date and time of transaction.

`Receiving null response from DTCC`
Client: • Check *Messaging Dashboard* for error message. • Check for SOAP-FAULT (Error stream). • If the above steps don't solve the issue, reach out to DTCC support (insurancesupport@dtcc.com) with TransRefGUID and Date and time of transaction.

`Connectivity issues - ClosedChannelException`
Client: • Check *Messaging Dashboard* for error message. • Verify the URL. • If the above steps don't solve the issue, reach out to DTCC support (insurancesupport@dtcc.com) with TransRefGUID and Date and time of transaction.

8.1 Receiver FAQs

`DTCC is rejecting responses sent`
Client: • Check *Messaging Dashboard* for error message. • Check whether receiver received *Resend* message from *DTCC* with errors. • If the above steps don't solve the issue, reach out to DTCC support (insurancesupport@dtcc.com) with TransRefGUID and Date and time of transaction.

`Connectivity issues - ClosedChannelException`
Client: • Check *Messaging Dashboard* for error message. • Verify the URL. • If the above steps don't solve the issue, reach out to DTCC support (insurancesupport@dtcc.com) with TransRefGUID and Date and time of transaction.

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

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

http://www.dtcc.com/wealth-management-services/insurance-and-retirement-services

10 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. Please contact insurancesupport@dtcc.com for the most recent version of the Router Exchange Form.

11 Appendix C: Sample Messages

Sample messages are available at the IPS Website as a separate zip file.

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

Change Log

DATE	VERSION	CHANGE
5/4/2011	v.01	First draft
09/08/2011	v.1.0	Final Updated 6.8 and added Section 7
09/25/2013	V2.0	Removed AuthInfo under 6.8.1, Added wsse:Security under 6.8.1
10/02/2013	V3.0	Added Data Power under 3.1, added web service endpoint names and soap actions under 6.8, Removed URL's and IP's from section 9 and added support e-mail address.
09/03/2015	V4.0	Added reference to new IFT messages (113, 115 and 810)
December 2017	V5.0	Updates to various sections in the document to adjust and make current.