CBSA ASFC

PROTECTION • SERVICE • INTEGRITY

PROTECTION • SERVICE • INTÉGRITÉ

Participants Requirements Document

Chapter 23

Single Window Initiative

Document Imaging Functionality

September 2017

Version 1.5

Canada Border Services Agency

Agence des services frontaliers du Canada

Canada

Revision History

Date Changes Made	Version	Changes Made	Changes Made By
Sep 8 2014	1.0	Initial draft version	SWI IT Solutions SWI Business IT Security IT Engineering B2B
November 21, 2014	1.1	Changes to the XSD, Query method, URN vs IID Key Restriction	SWI IT Solutions SWI Business IT Security IT Engineering B2B
February 1, 2015	1.2	Using ICM and CATE certificates instead of CRA PKI	IT Engineering
February 9, 2016	1.3	Updates to Querying the Image Status and Application Response sections	SWI Business
December, 2016	1.4	Web services security changes, clarification changes and updates to doc types accepted	IT Engineering/SWI Application IT/SWI Business
September 2017	1.5	• Added detail and clarity as per TCP questions and recommendations • Corrected case requirement for DIF Document type from upper to lower case. • Added detail on function of submitting multiple DIFs in one submission	SWI Business

TABLE OF CONTENTS

Introduction

This Participants Requirements Document (PRD) is meant to be read in conjunction with the Single Window Initiative (SWI) Integrated Import Declaration (IID) ECCRD. This PRD describes how to provide a digital attachment to the Government of Canada (GoC) and link it to an IID to satisfy Participating Government Agency (PGA) requirements that could not be incorporated directly into the IID.

Although all efforts were made to represent Participating Government Agency (PGA) information requirements using data fields within the IID itself, certain documents could not be *dematerialized* due to PGA legislative requirements that required presentation of paper documents and/or international agreements. In order for Canada to electronically validate a document, it generally must be the issuer of the document, which is not the case for some PGA documents. Examples of these include Phyto/Zoo-sanitary certificates, Veterinary certificates, Kimberley Process Diamond certificates, product labels and others.

Approximately 20% of the documents requested by PGAs could not be dematerialized at this time. In order to meet the SWI commitment to reduce paper, a new Document Imaging Functionality (DIF) was developed to provide a mechanism for trade to electronically represent, store and present these documents to the GoC.

The CBSA and PGAs continue to work with international organizations, such as the WCO and other United Nations committees (e.g., Electronic Transit eTIR, CITES) towards having international electronic certification (eCert) processes and procedures in place to support dematerialization of document efforts. As PGA legislative requirements are modernized and international efforts develop, the expectation is many of these documents that currently require DIF will be dematerialized within the IID.

This document provides the requirements for importers/brokers to construct systems that will allow them to electronically submit LPCO (Licence, Permit, Certificate or Other Documentation) images as opposed to presenting importation documentation in original paper format at the border. These LPCO images can be uploaded via a separate mechanism from IIDs and associated electronically to the IID.

This functionality, in many cases, will provide a flexible alternative to the current mechanisms of faxing, transporting and storing paper documents.

Business Process Overview

Images are documents required by Participating Government Agencies (PGAs) in the decision processing for admissibility and/or release of PGA regulated goods.

The general business process involving an IID and one image is:

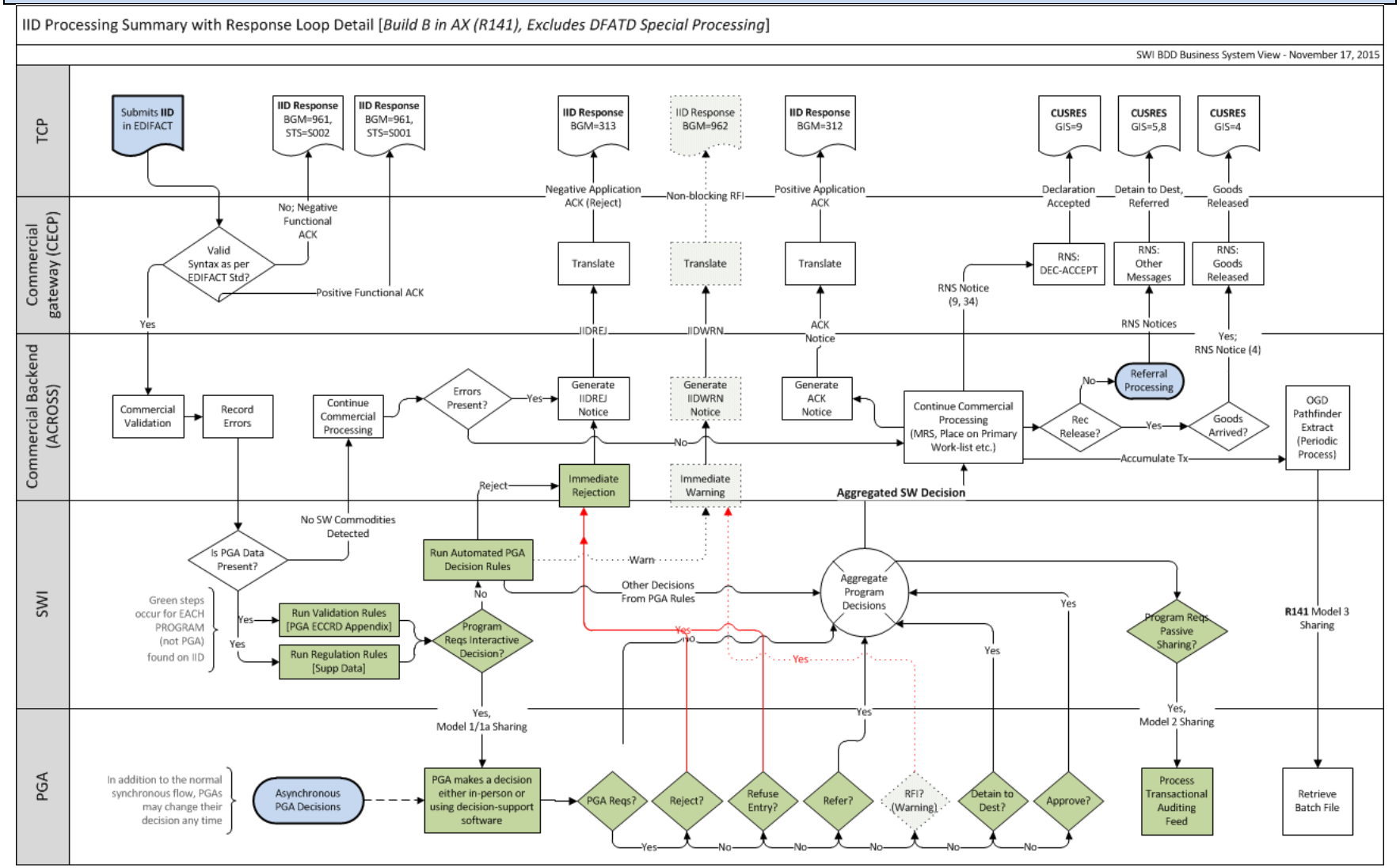
1. An original image is submitted to the CBSA using the connection and protocol described in this document.
    a. The metadata associated to the submitted image must contain a Unique Reference Number (URN) provided by the image submitter.
    b. Note that, although the format of a URN is the same as the format of an IID transaction number, a URN must not duplicate an existing release transaction number that is on file with the CBSA.
2. An IID is submitted containing a reference (the same URN associated to the image submitted in (1) above).
    a. For the EDIFACT IID, this would be contained in either the SG9.DOC.1366 element or the SG121.DOC.1366 element.
3. The CBSA provides both the IID and the associated image to the regulating PGAs and other internal CBSA groups for Admissibility/Release processing.

We recommend submitting the LPCO Images before the IID as some PGA requirements prefer having the images on file before the IID.

Please note that although the submitter must be CBSA authorized, there is no requirement for the submitter of an LPCO image to hold the same account security as the submitter of the associated IID.

It is incumbent upon Importers and Brokers to ensure that only authorized personnel transmit LPCO images to the CBSA.

IID and DIF Processing Summaries With Response Loop Detail



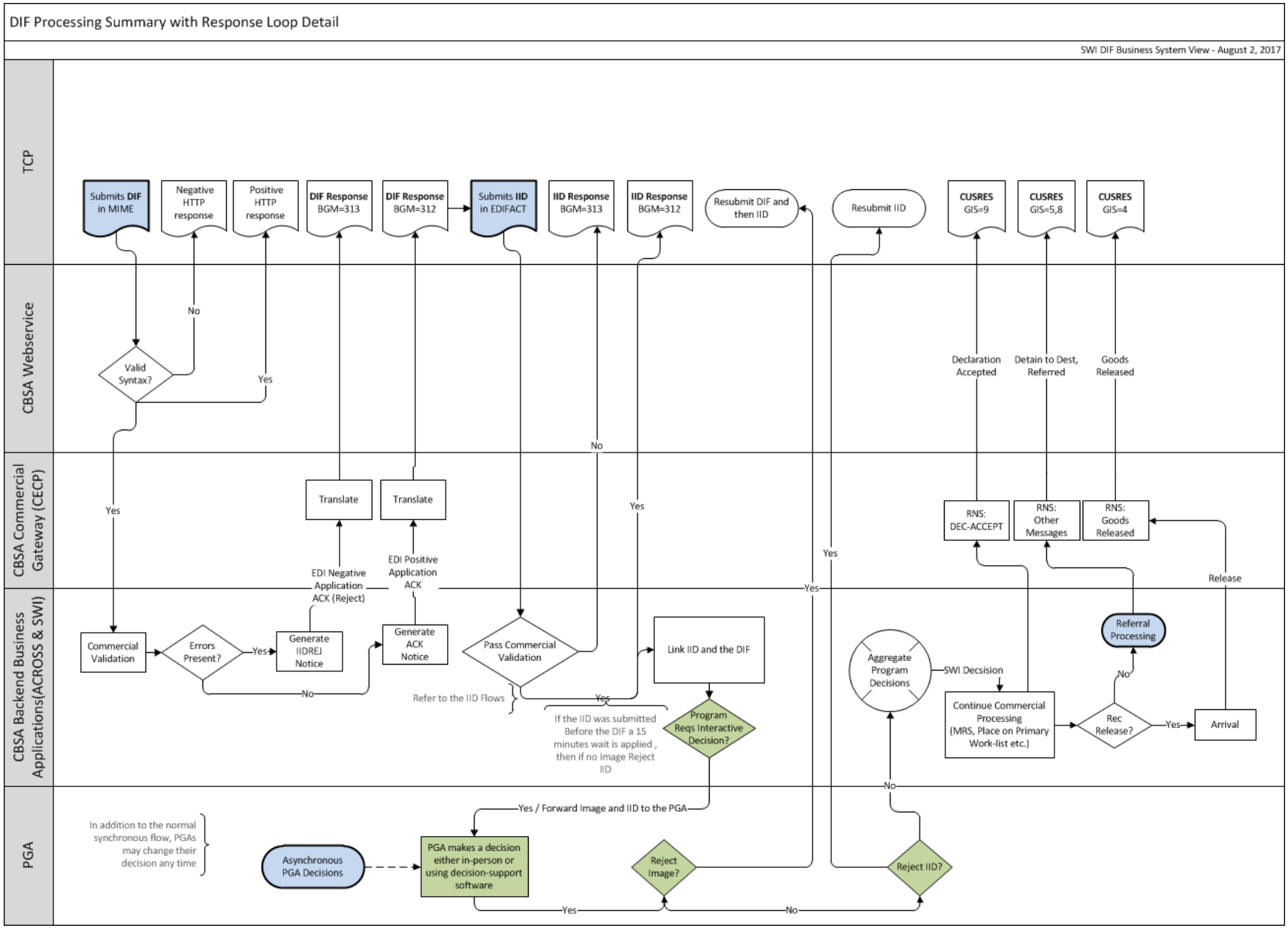

DIF Processing Summary with Response Loop Detail
SWI DIF Business System View - August 2, 2017
TCP
CBSA Webservice
CBSA Commercial Gateway (CECP)
CBSA Backend Business Applications(ACROSS & SWI)
PGA
Submits DIF in MIME
Negative HTTP response
Positive HTTP response
DIF Response BGM=313
DIF Response BGM=312
Submits IID in EDIFACT
IID Response BGM=313
IID Response BGM=312
Resubmit DIF and then IID
Resubmit IID
CUSRES GIS=9
CUSRES GIS=5,8
CUSRES GIS=4
No
Valid Syntax?
Yes
Declaration Accepted
Detain to Dest, Referred
Goods Released
Yes
Translate
Translate
No
Yes
RNS: DEC-ACCEPT
RNS: Other Messages
RNS: Goods Released
EDI Negative Application ACK (Reject)
EDI Positive Application ACK
Yes
Release
Commercial Validation
Errors Present?
Yes
Generate IIDREJ Notice
Generate ACK Notice
Pass Commercial Validation
Link IID and the DIF
Aggregate Program Decisions
SWI Decision
Referral Processing
No
No
Refer to the IID Flows
Yes
If the IID was submitted Before the DIF a 15 minutes wait is applied , then if no Image Reject IID
Program Reqs Interactive Decision?
Continue Commercial Processing (MRS, Place on Primary Work-list etc.)
Rec Release?
Yes
Arrival
Yes / Forward Image and IID to the PGA
No
In addition to the normal synchronous flow, PGAs may change their decision any time
Asynchronous PGA Decisions
PGA makes a decision either in-person or using decision-support software
Reject Image?
Reject IID?
Yes
No

Image Business Functions

Four business functions can be performed on images that are identical in concept to the four functions of an IID: Add, Cancel, Change and Amend. These are contained within the ***FunctionCode*** metadata element, and depending upon the state of the IID(s) linked to the image, may have some constraints applied. It is important to note that the state of the IID is based on the state of the associated Cargo, therefore if the cargo is not reported or arrived the IID is deemed to be pre-arrival, if the cargo is reported or arrived the IID is deemed to be post-arrival. The table below illustrates this best:

Referencing IID(s) State	Image Functions Allowed
Pre-arrival state of the IID	Associated DIFs can be Cancelled or Changed. New DIFs can be added
Post-arrival state of the IID	Associated DIFs can be Cancelled or Amended. New DIFs can be added
Post-release of the IID	Associated DIFs cannot be changed, Cancelled or Amended. Additional DIFs cannot be added.
Post Acquittal of the IID	Associated DIFs cannot be changed, Cancelled or Amended. Additional DIFs cannot be added.

This means that a business scenario like the following is supported:

1. An IID containing Health Canada (HC)-regulated goods is submitted with a reference to an existing LPCO image (e.g., medicine label) already on file.
    a. The IID submitter receives a positive ACK from the CBSA.
    b. CBSA retrieves the image and forwards both to HC for determination.
    c. HC receives the electronic release package and determines that the image is not clear enough.
2. The IID submitter receives a Reject from HC on the IID.
3. Pre or Post arrival release processing of the IID is stopped until a new valid image is sent by the Importer/Broker to CBSA.
    a. The image is updated using a Change or Amend image function (as defined in the chart above) to correct or update information associated to the LPCO rejected by HC.
    b. The updated LPCO image and/or metadata is forwarded to HC for another determination for any shipments that reference that URN.
    c. This may result in a message back to the importer/broker if the new image results in a reject again.
4. If all documents are accepted, normal Admissibility/Release processing resumes.

Linking Images to an IID

Two more factors that are considered when grouping images with an IID are *effective date* and *expiry date* associated with each image. In order for an image to be successfully linked to an IID it must:

- Have a URN referenced by that IID;
- Have an effective date less than or equal to the current date; and
- Have an expiry date greater than or equal to the current date.

Similar to the ***FunctionCode*** discussed above, the effective and expiry dates are provided **by the image submitter** in the metadata tags. This allows CBSA to confirm whether an image should be considered valid.

The image effective/expiry dates will be compared upon original submission of the IID (using the ***Estimated Time of Arrival*** quoted on the IID, that is, element DTM.2380 in the IID header). If the date when confirmed indicates the LPCO image is expired an IIDREJ will be sent to the sender of the IID. These dates will also be compared on an ongoing basis during the release process and if the goods reported on the IID release have still not arrived when an LPCO image expires, the submitter of the IID will be notified with an IIDREJ Notice on their IID. Note all notices go to the submitter of the IID; the submitter of the image(s) will **not** be notified.

Technical Process Overview

The LPCO web service is a RESTful web service hosted by CBSA that accepts HTTP posts of files in XML/XOP format.

The transmission of the file is secured using Transport Layer Security (TLS) and mutual authentication. Once the TLS stateful connection is established with the CBSA web server all communications over the connection are protected within an SSL tunnel. The client will be able to send HTTP posts to the server until the TLS session is terminated by either end.

At the successful completion of each HTTP post the web service will provide a return code indicating if it was accepted by the web service and a tracking number for Importer/Broker records.

In the event of an unsuccessful HTTP post the web service will also provide a return code indicating the class of error and if possible details on the error. In some cases a tracking number will be available for further troubleshooting with the CBSA help desk.

This helpdesk will also assist in the PKI registration process.

Help desk contact Information:

Technical Commercial Client Unit (TCCU)
Canada Border Services Agency
355 North River Road, Tower B, 6th Floor
Ottawa, Ontario
K1A 0L8
Telephone: 1-888-957-7224
Fax: (343) 291 5482
Email: tccu-ustcc@cbsa-asfc.gc.ca

Formatting of the message

To build the message an understanding is needed of the overall structure of the MIME (Multipurpose Internet Mail Extension) message, the XML metadata that is expected in the first body part of the message and how the xop:Include element refers to the documents being attached in the renaming body parts in the MIME message.

This section of the document is broken into three parts.

1. The first part describes the MIME structure needed to create a message that will be successfully received by CBSA and is called “Format of the XML/XOP message”.
2. The second part describes and is called “The Format of the XML in the first MIME body part”.
3. The third part has the rules around the types of documents allowed to be sent and attached to the remaining body part(s). It is called “the rules for the second body part(s)”.

Format of the XML/XOP message

The format of the message must conform to the WC3 XML-binary Optimized Packaging (XML/XOP) recommendation XOP10 from January 25th 2005. The MIME in the message must conform to RFC 2387 and RFC 2392.

The following is a breakdown of the MIME body parts and any specific rules that must be obeyed for the transaction to be processed successfully by the CBSA system. All unmentioned headers must still obey the internet RFC specifications mentioned above if used.

MIME header

This is a description of the values required in the MIME header.

Field	Notes
Message-Id: <*unique_message_id*>	A unique message identifier associated to each message transmission.
MIME-Version: 1.0	Required.
Content-Type: multipart/related; **boundary**="*boundary_separator*"; **type**="application/xop+xml"; **start**="<*content_id_xml_reference*>"; **start-info**="text/xml"	multipart/related is the only value acceptable for the **Content-Type** header. application/xop+xml is the only value acceptable for the **type** parameter. The **start** parameter must refer to the **Content-Id** value of the first Body part to follow. text/xml is the only value acceptable for the **start-info** parameter.
Line break	Required line break to signify the end of the body part.

MIME First Body Part (Meta-Data)

This part of the MIME must contain the XML LPCO meta-data with the XOP data elements referring to other body parts of the MIME message.

The XML must validate to the LPCO_Image_TCP.XSD schema definition. This formatting is described in the section called "Format of the XML in the first body part" found later in this document.

Field	Notes
--*boundary_separator*	Required.
Content-Type: application/xop+xml; charset=UTF-8; type="text/xml"	application/xop+xml is the only value acceptable for the Content-Type header. UTF-8 is the only value acceptable for the charset parameter. text/xml the only value acceptable for the type parameter.
Content-Transfer-Encoding: 8bit	8bit is the only value acceptable for the Content-Transfer-Encoding header.
Content-ID: <*content_id_xml_reference*>	This value must cross-reference with the start parameter of the Content-Type HTTP header.
Line Break.	Required line break.
XML_content	LPCOImages is the only acceptable XML root element for this body part. Note: XML must contain line breaks to satisfy the 8bit Content-Transfer-Encoding specification.
Line break	Required line break to signify the end of the body part.

MIME Second Body Part (Binary Attachment)

Field	Notes
--boundary_separator	Required.
Content-Type: application/octet-stream	application/octet-stream is the only value acceptable for the **Content-Type** header of this bodypart.
Content-Transfer-Encoding: binary	binary is the only value acceptable for the **Content-Transfer-Encoding** header of this bodypart.
Content-ID: <image_attachment_identifier>	The **Content-ID** value must cross-reference with an **<xop:include> href** attribute's URL of the first bodypart XML content. Note: do not include the cid URL prefix here.
	Required line break.
binary_data	The binary data must be transmitted as is with no encoding, line breaks nor escape sequences.
Line break	Required line break to signify the end of the body part.

MIME Trailer

This is required to indicate the end of the MIME structure.

Field	Notes
--boundary_separator--	Required. The two ”--“ at the end of the line signify the end of the MIME structure.

Complete Example of a XML/XOP message.

```
Message-ID: <58536309.1400077877380.JavaMail.ext001@WH1HCU16762>
Mime-Version: 1.0
Content-Type: multipart/related; start-info="text/xml"; type="application/xop+xml";
        start="<-963165769043289641.1400077877224@WH1HCU16762>";
        boundary="----=_Part_0_-338193320.1400077877317"

------=_Part_0_-338193320.1400077877317
Content-Type: application/xop+xml; type="text/xml"; charset=UTF-8
Content-Transfer-Encoding: 8bit
Content-ID: <-963165769043289641.1400077877224@WH1HCU16762>

<?xml version="1.0" encoding="UTF-8"?><LPCOImages xmlns:xop="http://www.w3.org/2004/08/xop/include"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="Images_R140_b2b.xsd">
        <B2BInfo Type="CECP1">
                <VanID>INET_CDX</VanID>
                <PartnerID>BCCCIG02</PartnerID>
                <PartnerQualifier/>
                <DocID>IIDT</DocID>
        </B2BInfo>
        <BN>12345RM00000001</BN>
        <MessageType>LPCO</MessageType>
        <Image>
                <ImageHeader>
                        <Identifier>12345123456789</Identifier>
                        <FunctionCode>09</FunctionCode>
                        <LPCOImageTypeCode>4004</LPCOImageTypeCode>
                        <LPCOReferenceNumber>Refnumber001</LPCOReferenceNumber>
                        <LPCOImageEffectiveDate>2014-04-21</LPCOImageEffectiveDate>
                        <LPCOImageExpiryDate>2014-07-30</LPCOImageExpiryDate>
                        <LPCOImageFormat>GIF</LPCOImageFormat>
                </ImageHeader>
        <xop:Include href="cid:-3112459487299887381.1400077877224@WH1HCU16762"/>
</Image>
</LPCOImages>
------=_Part_0_-338193320.1400077877317
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-ID: <-3112459487299887381.1400077877224@WH1HCU16762>
Content-Length: 545634

89a5è————————————————————————————————÷ Binary content that is inefficient to display in word. Õ3 Õf Õ™ ÕÌ Õÿ ÿ  ÿ3 ÿf ÿ™
ÿÌ ÿÿ3  3 33 f3 ™3 Ì3 ÿ3+ 3+33+f3+™3+Ì3+ÿ3U 3U33Uf3U™3UÌ3Uÿ3€ 3€33€f3€™3€
------=_Part_0_-338193320.1400077877317—
```

Here is an example of a file that would pass through the CBSA system. This file contains attachments with full binary content that we are unable to display in word correctly.

Test1.txt

First Body Part Format

The format of the XML in the first body part needs to conform to the attached LPCO_Image_TCP.xsd. A supporting XSD called xop-include.xsd is also needed and should be installed in the same directory as the LPCO_Image_TCP.xsd for most XML editors.

LPCO_Image_TCP.xsd


xop-include.xsd

The objective is to create an XML that looks similar to this.

```
<?xml version="1.0" encoding="UTF-8"?>
<LPCOImages xsi:noNamespaceSchemaLocation="LPCO_Image_TCP.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xop="http://www.w3.org/2004/08/xop/include">
	<B2BInfo Type="CECP1">
		<VanID>INET_CDX</VanID>
		<PartnerID>BCCCIG02</PartnerID>
		<PartnerQualifier/>
		<DocID>IIDT</DocID>
	</B2BInfo>
	<BN>12345RM00000001</BN>
	<MessageType>LPCO</MessageType>
	<Image>
		<ImageHeader>
			<Identifier>12345123456789</Identifier>
			<FunctionCode>09</FunctionCode>
			<LPCOImageTypeCode>4004</LPCOImageTypeCode>
			<LPCOReferenceNumber>Refnumber001</LPCOReferenceNumber>
			<LPCOImageEffectiveDate>2014-04-21</LPCOImageEffectiveDate>
			<LPCOImageExpiryDate>2014-07-30</LPCOImageExpiryDate>
			<LPCOImageFormat>GIF</LPCOImageFormat>
		</ImageHeader>
		<xop:Include href="cid:-3112459487299887381.1400077877224@WH1HCU16762"/>
	</Image>
</LPCOImages>
```

The values expected in each field are explained in the following table:

XML Field	Value
<?xml version="1.0" encoding="UTF-8"?> <LPCOImages xsi:noNamespaceSchemaLocation="LPCO_Image_TCP.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xop="http://www.w3.org/2004/08/xop/include">	Static value. Header of the XML.
B2BInfo Type="CECP1"	Static value. Used to identify partner information.
VanID (Mandatory)	Communication Method: • For the Customs Internet Gateway indicate INET_CDX • For a Direct Connect or a VANindicate the name of your Direct Connect/VAN.
PartnerID (Mandatory)	Enter your Mailbox ID
PartnerQualifier (Optional)	A partner qualifier is an identifier and the TCP will choose when to include the identifier, leave it blank or utilize a ZZZ. If the partner qualifier is included it will be included in the Notice sent to the TCP, if left blank nothing is returned in the Notice, if the ZZZ is included the ZZZ will be included in the TCP Notice.
DocID (Mandatory)	Enter IIDT for Test or IIDP for Production
/B2B_Info (Mandatory)	Static Value. End of partner information.
BN (Mandatory)	This needs to be a valid importer business number (BN), but does not have to correspond to any specific BN used on an IID referencing this image. It is suggested that brokers use a BN that is meaningful to their operations and IIDs that link to this image.
MessageType (Mandatory)	Static Value “LPCO”.
Image (Mandatory)	The image part of the XML can be repeated many times. The limit is that the total size of the XML/XOP message with attachments has to be less than 4 MB.
ImageHeader (Mandatory)	This tag contains the metadata for each picture being sent to the CBSA.
Identifier (Mandatory)	This is the Unique Reference Number (URN) identifying this image as described in SG9/SG121.DOC.1366 of the IID. It must be a unique 14-digit document reference that conforms to the same format as the transaction number, that is, the first 5 digits are the submitter's account security number, the next 8 digits are references to within the submitter's system, and the final digit is a check digit calculated as per the "Module 10" algorithm described in Appendix F of Customs Memorandum D17-1-10. It also cannot duplicate the transaction identifier of any release transaction (including IID) on file with the CBSA.
FunctionCode (Mandatory)	This is the "message function" of this image, which must be one of the following codes: • 01 Cancellation • 04 Change (pre-arrival change) • 09 Original • 05 Amend (post-arrival change)
LPCOImageTypeCode (Mandatory)	This is the LPCO Document Type Qualifier that corresponds to data element ‘SG9/SG121.DOC.1131’ on the IID map (For

<table>
<tr><td></td><td>a complete list of valid Codes please refer to Appendix G15 in the IID ECCRD.</td></tr>
<tr><td>LPCOReferenceNumber (Mandatory)</td><td>The unique identification number on this LPCO that distinguishes it from others of the same type should be provided here. This is often the “permit number” of the document, but may be referred to by different names depending upon the document and PGA requirements.

Please see PGA appendices for each LPCO to determine the exact identifier that should be provided, if applicable. Some LPCOs are product labels, or permit applications that have not yet been assigned a unique identifier because they have not been issued yet, and for these situations, this tag value should be omitted.

This is equivalent to the SG9/121.DOC.1004 data element on the IID.</td></tr>
<tr><td>LPCOImageEffectiveDate (Mandatory)</td><td>The date on which this permit becomes effective and can be linked to IIDs for the purposes of Admissibility/Release decisions on goods.

Note: For LPCOs that do not have an Effective Date, please enter the date of submission.</td></tr>
<tr><td>LPCOImageExpiryDate (Mandatory)</td><td>The date on which this permit becomes expired and will no longer be linked to IIDs for the purpose of Admissibility/Release decisions on goods.

Note: For LPCOs that do not have an Expiry Date, please enter the date as 9999-12-31.</td></tr>
<tr><td>LPCOImageFormat (Mandatory)</td><td>One of the following codes must be present to indicate how the attached binary file can be interpreted and displayed: NOTE IT IS MANDATORY THAT THE FORMAT CODE IS ENTERED IN LOWERCASE.

<table>
<tr><th>Accepted Image Format</th><th>Code</th></tr>
<tr><td>MS Word Legacy (97-2003) format</td><td>doc</td></tr>
<tr><td>MS Word XML format</td><td>docx</td></tr>
<tr><td>Graphics Interchange Format</td><td>gif</td></tr>
<tr><td>Joint Photographic Experts Group format</td><td>jpg</td></tr>
<tr><td>Portable Document Format</td><td>pdf</td></tr>
<tr><td>Portable Network Graphics format</td><td>png</td></tr>
<tr><td>Rich Text Format</td><td>rtf</td></tr>
<tr><td>Bitmap image file format</td><td>bmp</td></tr>
</table>
</td></tr>
<tr><td>/ImageHeader (Mandatory)</td><td>Static value.</td></tr>
<tr><td>xop:Include href="VALUE "/ (Mandatory)</td><td>This “VALUE” should refer to the value of the Content-ID: in the MIME body part the metadata is describing.</td></tr>
<tr><td>/Image> (Mandatory)</td><td>Static value.</td></tr>
<tr><td>/LPCOImages (Mandatory)</td><td>Static value.</td></tr>
</table>

Second Body Part Rules

The second body part can be repeated if multiple images are being sent and the image part of the XML is repeated.

The image must be in binary format. Please do not base64 encode this part of the MIME document or the transaction will fail.

The total size of the XML/XOP message needs to be less than 4MB or the transaction will fail. The document's total size should be monitored as binary attachments are added.

The body part should resemble the following and be properly terminated with the correct MIME boundary value:

```
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-ID: <-3112459487299887381.1400077877224@WH1HCU16762>
Content-Length: 545634

89a5è————————————————————————————————÷ Binary content that is inefficient to display in word. Õ3 Õf Õ™ ÕÌ Õÿ ÿ  ÿ3 ÿf ÿ™ ÿÌ ÿÿ3  3 33 f3 ™3 Ì3 ÿ3+ 3+33+f3+™3+Ì3+ÿ3U 3U33Uf3U™3UÌ3Uÿ3€ 3€33€f3€™3€
```

The xop:Include href="VALUE " in the XML from the first body part should correspond to the Content-ID: in this header.

The message structure of a DIF submission that includes two pictures referring to two different IIDs would resemble the following:

```
Message-ID: <58536309.1400077877380.JavaMail.ext001@WH1HCU16762>
Mime-Version: 1.0
Content-Type: multipart/related; start-info="text/xml"; type="application/xop+xml";
        start="<-963165769043289641.1400077877224@WH1HCU16762>";
        boundary="----=_Part_0_-338193320.1400077877317"

------=_Part_0_-338193320.1400077877317
Content-Type: application/xop+xml; type="text/xml"; charset=UTF-8
Content-Transfer-Encoding: 8bit
Content-ID: <-963165769043289641.1400077877224@WH1HCU16762>

<?xml version="1.0" encoding="UTF-8"?><LPCOImages xmlns:xop="http://www.w3.org/2004/08/xop/include"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="Images_R140_b2b.xsd">
        <B2BInfo Type="CECP1">
                <VanID>INET_CDX</VanID>
                <PartnerID>BCCCIG02</PartnerID>
                <PartnerQualifier/>
                <DocID>IIDT</DocID>
        </B2BInfo>
        <BN>12345RM00000001</BN>
        <MessageType>LPCO</MessageType>
        <Image>
                <ImageHeader>
                        <Identifier>12345123456789</Identifier>
```

```
                    <FunctionCode>09</FunctionCode>
                    <LPCOImageTypeCode>4004</LPCOImageTypeCode>
                    <LPCOReferenceNumber>Refnumber001</LPCOReferenceNumber>
                    <LPCOImageEffectiveDate>2014-04-21</LPCOImageEffectiveDate>
                    <LPCOImageExpiryDate>2014-07-30</LPCOImageExpiryDate>
                    <LPCOImageFormat>gif</LPCOImageFormat>
                </ImageHeader>
                <xop:Include href="pic1"/>
        </Image>
                <Image>
                <ImageHeader>
                    <Identifier>12345123456790</Identifier>
                    <FunctionCode>09</FunctionCode>
                    <LPCOImageTypeCode>4004</LPCOImageTypeCode>
                    <LPCOReferenceNumber>Refnumber001</LPCOReferenceNumber>
                    <LPCOImageEffectiveDate>2014-04-21</LPCOImageEffectiveDate>
                    <LPCOImageExpiryDate>2014-07-30</LPCOImageExpiryDate>
                    <LPCOImageFormat>doc</LPCOImageFormat>
                </ImageHeader>
                <xop:Include href="pic2"/>
        </Image>
</LPCOImages>
------=_Part_0_-338193320.1400077877317
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-ID: <pic1>
Content-Length: 545634

Binary file

------=_Part_0_-338193320.1400077877317
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-ID: <pic2>
Content-Length: 65428

Binary file

------=_Part_0_-338193320.1400077877317--
```

The types of documents that are valid are defined in the XSD but are repeated here for clarity:

doc, docx, gif, jpg, pdf, png, rtf, bmp

Interacting with the server

Posting a message to the web server

Once the TLS session is created multiple HTTP posts may be sent to the server at the following URLs:

- Client testing URL, Release TRaining Lab (RTR)
  - https://apps-to1.cbsa-asfc.gc.ca/b2bwssync/swi/tcp/v1/lpco
  - New releases will be deployed to RTR lab.
- Client testing URL, Production TRaining Lab (PTR)
  - https:// apps-wo.cbsa-asfc.gc.ca/b2bwssync/swi/tcp/v1/lpco
  - The application deployed to PTR lab is identical to Production.
- Production URL
  - https://apps.cbsa-asfc.gc.ca/b2bwssync/swi/tcp/v1/lpco

More information on how to do the HTTP post with TLS can be found in the security section of this document.

Response from the web server

The server will respond with a standard HTTP response code.

A successful post to the server will result in a HTTP response of 200 as well as a tracking number in the form of a UUID (Universally Unique Identifier). The UUID can be given to the helpdesk for further investigation. A successful response will look similar to this:

HTTP response = 200 OK

```
<b2b>
  <application>SwiApplication</application>
  <response>
    <uuid>80db27d9-0402-4955-9837-5403c80555df</uuid>
    <sentDateTime>2014-08-29T08:31:23.676-04:00</sentDateTime>
  </response>
</b2b>
```

A failed response will have an HTTP response code other than 200 (e.g., 401) as well as a tracking number in the form of a UUID and text indicating what the error is. The UUID can be given to the helpdesk for further investigation if needed.

HTTP response = 401

```
<b2b>
  <application>SwiApplication</application>
  <response>
    <uuid>7643e5c5-5d09-414d-a1b5-d23d0b610245</uuid>
    <sentDateTime>2014-08-29T09:38:02.937-04:00</sentDateTime>
    <error_code>401</error_code>
    <error_text><![CDATA[Unauthorized]]></error_text>
  </response>
</b2b>
```

Application Response

Upon submission of an image to the web service, any application response, positive or negative, will be generated from the CBSA commercial system through EDI and sent to the Transmitting Client. Thus, the web service return codes can be construed as the functional responses, and the application responses will be provided on the EDI channel.

These application responses will be formatted in EDIFACT 13A as per the IID responses described in the SWI IID ECCRD (Appendix C: IID EDIFACT Outbound MIG).

Sample Response Messages

DIF Positive Application Acknowledgement

This message indicates that the submitted image was validated by CBSA and no errors were found.

```
UNB+UNOC:3+X+X+130213:1553+X'
UNG+GOVCBR+IIDT+RECIPIENT:ZZZ+130213:1553+9999+UN+D:13A'
UNH+1234+GOVCBR:D:13A:UN'
BGM+312+12345XXXXXXXXXXX'
DTM+9:201707261447:203
RFF+AGO:XXXX
UNS+S
HYN+3
UNS+S
UNT+8+1234'
UNE+1+9999'
UNZ+1+X'
```

DIF Negative Application Acknowledgement

This message demonstrates how application errors will appear in a negative application acknowledgment reject against an Image submission. In this scenario, the date value provided in the XML metadata tag, "LPCOImageExpiryDate", is expired. As a result, error code **5E9** appears in the ERC line of the negative application response (SG17.ERC element 9321).

UNB+UNOC:3+X+X+130213:1553+X'
UNG+GOVCBR+IIDT+RECIPIENT:ZZZ+130213:1553+9999+UN+D:13A'
UNH+1234+GOVCBR:D:13A:UN'
BGM+313+12345XXXXXXXXXXX'
DTM+9:201707261335:203
RFF+AGO:XXXX
RCS+15+1::05
FTX+AAO+++
ERC+5E9
UNS+S
HYN+3
UNS+S
UNT+11+1234'
UNE+1+9999'
UNZ+1+X'

SWI Web Service Security

The CBSA has adopted a Public Key Infrastructure (PKI) to provide the security and integrity of the data transmitted. The web service uses mutual authentication and follows RFC 5246. The transactions are encrypted at the transport layer and the authentication is done using a PKI client certificate.

ICM (Internal Credential Management) and CATE (Client Application Testing Environment) are Credential Management systems created by SSC (Shared Services Canada) to support secure communications by businesses and individuals with the Government of Canada. Both of these systems are based upon the Entrust product suite, and as a consequence, participants will have to use Entrust Intelligence Security Provider (ESP) to acquire and manage the certificates.

CBSA is using both ICM and CATE as its Certification Authorities (CA) for issuing PKI Certificates to its business partners. ICM certificates are used for communication between **production** systems and CATE certificates are for communication between **test** systems. Please contact the TCCU to register and receive either (or both) certificates as desired.

The procedure to generate the PKI certificates can be found in that FTP site ftp://ftp.cbsa-asfc.gc.ca/pub/SWI

The generated certificates format is EPF (Entrust Profile File) which is Entrust proprietary format. The EPF file will include 2 certificates Digital Signature and Key Encipherment. The clients will be able to export the Digital Signature certificate to a standard x.509 format and use it for the client authentication.

NOTE: Issued certificates belong to the SSC and are to be used for CBSA business only.

Web Service Security Guidelines

SWI clients will use the following URL to send LPCO transactions to the test labs:

- https://apps-to1.cbsa-asfc.gc.ca/b2bwssync/swi/tcp/v1/lpco
- https:// apps-wo.cbsa-asfc.gc.ca/b2bwssync/swi/tcp/v1/lpco

For production, the following URL will be used:

- https:// apps.cbsa-asfc.gc.ca /b2bwssync/swi/tcp/v1/lpco

The following HTTP headers need to be set as follows:

- Content-type multipart/related
- accept text/html
- Expect 100-Continue

The LPCO web service follows RFC 5246 for Transport Layer Security (TLS) and mutual authentication, so two certificates are required: SSL Entrust certificates and PKI issued Identity certificate. The Entrust roots and certificate chains can be downloaded from http://www.entrust.net.

The following are the steps needed to perform a connection to the CBSA:

1. The client will load its identity certificate provided by ICM or CATE PKI.
2. The client will create an HTTPS connection using the Entrust root certificate for TLS handshaking (RFC 5246) and the PKI identity certificate for authentication. TLS v1.2 should be used to establish the secure connection.
3. Once the authentication is successful, the client will be able to send data using an HTTP Post command.
4. The client is required to authenticate only the first request. All subsequent requests should use the details contained within the SMSESSION cookie. Once this cookie expires, the client will have to re-authenticate.
5. If step 2 fails, the client will receive a 401 Unauthorized HTTP error.
6. CBSA supports the following CIPHERS:
   TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
   TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
   TLS_ECDHE_ECDSA_WITH_AES_128_CCM
   TLS_ECDHE_ECDSA_WITH_AES_256_CCM
   TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
   TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
   TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
   TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
   TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
   TLS_DHE_RSA_WITH_AES_128_CCM

TLS_DHE_RSA_WITH_AES_256_CCM
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_256_CCM
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA