

**Final Report**

**AS3 Interoperability Test**

**First Quarter 2011 (1Q11)**



**March 2, 2011**

Prepared & Facilitated by:  
Drummond Group Inc.  
[www.drummondgroup.com](http://www.drummondgroup.com)

## Table of Contents

Cover Letter .....	4
Disclaimer .....	5
Test Participants .....	6
Definitions .....	7
Interoperability Test Summary .....	8
VLM Optional Test Participants .....	9
Interoperability Test History .....	10
Interoperability Issues Affirmed and Resolved .....	11
AS3-1Q11 Test Results .....	11
AS3-1Q10 Test Results .....	11
AS3-1Q09 Test Results .....	12
Issues Resolved .....	12
Very Large Message Test .....	14
AS3-1Q08 Test Results .....	15
Issues Resolved .....	15
Very Large Message Test .....	18
AS3-1Q07 Test Results .....	18
AS3 Version and EDIINIT-Features Header .....	18
Base64 Content-Transfer Encoding .....	19
FTP Servers .....	19
Folded Headers .....	19
Very Large Message Experimental Test AS3-1Q07 .....	19
AS3 Test Data .....	20
AS3-2Q06 Test Results .....	20
Very Large Message Experimental Test .....	20
Connection Timeouts: .....	21
Firewall Timeouts: .....	21
Processing Errors: .....	21
Test Requirements .....	22
Interoperability Test Execution .....	22
Technical Requirements .....	23
S/MIME encryption and digital signatures .....	23
Compression .....	24
Asynchronous Receipts (or MDNs) .....	24
Transports .....	24
Payloads .....	24
Error Reporting .....	24
Appendix A: Test Case Summary .....	25
Test Data .....	26
Appendix B: AS3 and EDI Identifiers .....	27
Host Identifiers .....	27
Remote Identifiers .....	27
Appendix C: AS3 Choreographies .....	28
Server Choreography Superset .....	28
Company Name: Axway .....	29
Secure Server Logon .....	29
Non-secure Server Logon .....	29
Document Upload .....	29
Document Download .....	30
MDN Upload .....	30

MDN Download .....	30
Comments.....	30
Company Name: Cleo.....	31
Secure Server Logon .....	31
Non-secure Server Logon .....	31
Document Upload .....	31
Document Download .....	31
MDN Upload .....	31
MDN Download .....	31
Company Name: IBM.....	32
Secure Server Logon .....	32
Non-secure Server Logon .....	32
Document/MDN Upload .....	32
Document/MDN Download.....	32
Comments.....	32
Company Name: GXS.....	33
Secure Server Logon .....	33
Non-secure Server Logon .....	33
Document Upload .....	33
Document Download .....	34
MDN Upload .....	34
MDN Download .....	34
Comments.....	34
Company Name: Sterling .....	35
Secure Server Logon .....	35
Non-secure Server Logon .....	35
Document Upload .....	35
Document Download .....	35
MDN Upload .....	35
MDN Download .....	36
Other Actions.....	36
Overview of the DGI Interoperability Compliance Process®.....	37
DGI In-the-Queue Test Round.....	37
DGI Interoperability Test Round .....	37
About Drummond Group Inc.....	38

## Cover Letter

DRUMMOND GROUP Inc. (DGI) is pleased to announce that the following participants in the AS3-1Q11 Interoperability Test Round have completed all requirements and passed tests (see Interoperability Test Summary below) between each product demonstrating interoperability and conformance. The setup, connectivity and debugging testing were conducted from Jan 10 to Feb 11. The Final Certification run was conducted during the week of Feb 14 – Feb 18, 2011.

This AS3 interoperability testing had one optional test – very large message (VLM) with a payload of 500 MB and 1 GB as in previous AS3 Interop tests.

To fully understand what completing the test means in the use of the products-with-version in production, please read this document carefully.





Sincerely,

Aaron Gomez  
Principal, Standards Certification and Testing  
Drummond Group Inc.

## **Disclaimer**

Drummond Group Inc. (DGI) conducts interoperability and conformance testing in a neutral test environment for various companies and organizations ("Participant"). At the end of the testing process, DGI may list the name of the Participant in the final test report along with an indication that the Participant passed the test. The fact that the name of the Participant appears in the final report is not an endorsement of the Participant or its products or services, and DGI therefore makes no warranties, either express or implied, regarding any facet of the business conducted by the Participant.

## Test Participants

 <p><b>Axway</b></p> <p><a href="http://www.axway.com">http://www.axway.com</a></p> <p><b>Product Name: Axway B2Bi 1.5/Axway Interchange 5.10/Axway Activator 5.10</b></p>	 <p><b>Cleo Communications</b></p> <p><a href="http://www.cleo.com">http://www.cleo.com</a></p> <p><b>Product Name: VersaLex™ v4.3 tested in VLTrader™ v4.3</b></p>
 <p><b>GXS</b></p> <p><a href="http://www.gxs.com">http://www.gxs.com</a></p> <p><b>Product Name: BizManager 3.3</b></p>	 <p><b>IBM</b></p> <p><a href="http://www.ibm.com/">http://www.ibm.com/</a></p> <p><b>Product Name: IBM WebSphere Partner Gateway V6.2.1</b></p>
 <p><b>Sterling Commerce, an IBM Company</b></p> <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: IBM Sterling B2B Integrator v5.0 with Standards Library v6.2</b></p>	 <p><b>Sterling Commerce, an IBM Company</b></p> <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: IBM Sterling B2B Integrator v5.1 with Standards Library v7.0</b></p>

## Definitions

**Interoperability** – A product is deemed interoperable with all other products in the Interoperability Test Round if and only if it demonstrates in a full-matrix manner the pair wise exchange of data covering the *Test Criteria* between all products in the Interoperability Test Round. A product is either totally interoperable or it is not interoperable. Waivers or exceptions are not given in demonstrating interoperability for the *Test Criteria* unless the entire *Product Test Group* and DGI agree.

**Interoperable products** – Group of products, from the *Product Test Group*, which successfully completed the *Test Criteria*, in a full-matrix manner with every other *Product Test Group* participant in an Interoperability Test Round without any errors in the final test Phase. Interoperable products receive a Drummond Certified™ Seal.

**Product Test Group** – A group of products involved in an interoperability or conformant Test Round.

**Product, product-with-version, or product-with-version-with-release** – are interchangeable and are defined for the purpose of a Test Round as a product name, followed by a product version, followed by a single digit release. The assumption is that version and release syntax is as: “VV.Rx...x,” where VV is the version numeral designator, R is the single digit release numeral designator and x is the sub-release multiple digit numeral designator. DGI assumes that any digits of less significance than the R place do not indicate code changes on the product-with-version-with-release tested in the Test Round. A vendor must list a product as product name, followed by version digits followed by a decimal point followed by a single release designator digit before the Test Round is complete.

**Test Case** – The test criteria is a set of individual test cases, often 10 to 50 which the product test group exchange among themselves to verify conformance and interoperability.

**Test Criteria** – A set of individual tests, based on one or more standard specifications, that is used to verify that a product is conformant to the specification(s) or that a set of Product-with-version’s are interoperable under the *Test Criteria*.

## Interoperability Test Summary

AS3 (Applicability Statement 3) is the specification standard (RFC 4823, <http://www.ietf.org/rfc/rfc4823.txt>) by which vendor applications communicate EDI (EDIFACT or X12), binary and XML data securely over the Internet via FTP. AS3 is published through the IETF EDIINT Work Group.

The purpose of this interoperability test is to provide a venue for vendors to test and correct their software systems in a noncompetitive environment. To accomplish this, each product-with version both sends and receives specific messages with the Product Test Group. In both sending and receiving, products-with versions verify the message structure and security requirements are correct, the intended payload was transferred intact, and the receipt for the message was correctly delivered verifying the transaction was successful.

The test cases cover the full scope of AS3 in terms of security and receipts. Digital signatures, encryption, FTP/FTPS transports, unsigned and signed receipts, and data compression, and Very Large Messages are all tested. Test data payloads were used with document formats of X12, EDIFACT and XML.

As in previous Interoperability test rounds, this test round continued conformance checking of error values within MDN's. Participants were purposefully sent corrupted signed, encrypted and compressed messages and were required to respond with an appropriate MDN error value. In situations where trading partner profiles and certificates are improperly loaded or network firewall problems exist, proper MDN error values can greatly assist a trading partner in identifying and resolving the problem.

The Interoperability Test Round was completed in five weeks. During these weeks, the testing was focused on finding and correcting interoperability errors. During the Final Run, code changes and debug settings were not allowed and a final full-matrix test was performed.

During this final testing, all products-with-version tested with each other without error demonstrating full-matrix interoperability. This final version of code as denoted by each product-with-version version listed in the "Test Participants" section of this Final Report are deemed Drummond Certified™ and interoperable with each other (as a group) as they all sent and received each required test case successfully. Results were reported by the participants themselves and demonstrated by supplying the messages sent and received.

No warranty of product interoperability is implied over and above the publishing of the results of the Test Round as completed by all vendors during the specified time period of testing.

## VLM Optional Test Participants

The following products participated in the optional Very Large Message testing. The testing gradually built up to two large payloads of 500 MB and 1 GB. Participants demonstrated that they could exchange the payloads which was compressed, encrypted and signed.

Company	Product Name	Optional tests
<a href="#">Axway</a>	Axway B2Bi 1.5/Axway Interchange 5.10/Axway Activator 5.10	VLM-500MB, VLM-1G
<a href="#">Cleo Communications Inc.</a>	VersaLex™ v4.3 tested in VLTrader™ v4.3	VLM-500MB, VLM-1G
<a href="#">GXS</a>	BizManager 3.3	VLM-500MB, VLM-1G
<a href="#">IBM</a>	IBM WebSphere Partner Gateway V6.2.1	VLM-500MB, VLM-1G
<a href="#">Sterling Commerce, an IBM Company</a>	IBM Sterling B2B Integrator v5.0 with Standards Library v6.2	VLM-500MB, VLM-1G
<a href="#">Sterling Commerce, an IBM Company</a>	IBM Sterling B2B Integrator v5.1 with Standards Library v7.0	VLM-500MB, VLM-1G

## **Interoperability Test History**

This is the eighth AS3 Interoperability Test administered by DGI.

AS3 1Q11 Interoperability Test – Jan-Feb 2011

Previous tests included the following:

AS3 1Q10 Interoperability Test – Jan-Feb 2010

AS3 1Q09 Interoperability Test – Jan-Feb 2009

AS3 1Q08 Interoperability Test – Jan-Feb 2008

AS3 1Q07 Interoperability Test – Feb-Mar 2007

AS3 2Q06 Interoperability Test – April-June 2006

AS3 2Q05 Interoperability Test – May-July 2005

AS3 4Q04 Interoperability Test – October-December 2004

## **Interoperability Issues Affirmed and Resolved**

### **AS3-1Q11 Test Results**

During the course of testing, issues resolved in this test round were not related to AS3 server's themselves, but revolved around establishing connectivity, setting up the correct choreography and troubleshooting firewall settings or certificates, similar to previous AS3 Interop rounds.

Additionally, one participant resolved outbound AS3 messages that were not being sent and staying in a pending state for both TLS and non-TLS messages. This same participant also had to make code changes to their FTP server, to return the appropriate response when the user logged into the FTP server which they used for testing.

### **AS3-1Q10 Test Results**

During the course of testing, issues resolved in this test round were not related to AS3 server's themselves, but revolved around establishing connectivity, setting up the correct choreography and troubleshooting firewall settings or certificates, similar to previous AS3 Interop rounds.

For instance, two participants were having problems performing a "PUT" on another's AS3 server over SSL. The issue was resolved by removing the CCC mode and not to do a "PORT" command (and to do only PASV) and also to do an explicit connection. Hence that AS3 server's choreography change by removing the "PORT" AND "CCC" from their choreography .

VLM testing was also conducted in this AS3 Interop as in the previous Interop. No issues were reported.

## AS3-1Q09 Test Results

During the course of testing, interoperability issues did arise and were resolved. Some issues resolved in this test round were not related to AS3 server's themselves, but revolved around establishing connectivity and required troubleshooting firewall settings or certificates, similar to previous AS3 Interop rounds.

### Issues Resolved

The following issues were resolved during the debug phase of testing.

1. Participants resolved Choreography issues by observing the rules for uploading and downloading per each products Choreography as given in the appendix in this document.
2. The majority of the connectivity issues had to do with certificates and using the correct upload/download directories, that is following the choreography
3. Participant was generating filenames with very long filenames.

For example:

```
T1234_as3_test_data_TC_A.edi123177322331583000D60177594023644  
0000000000000636
```

The resulting error:

Error: Parameter -ftp\_command(-ftpc) too long (char), size must be 80.

Participant resolved by removing the extra numeric characters following the extension.

4. At least two participants do not set the "Content transfer Encoding as Binary" when sending the signed/compressed payload. When no Content-Transfer-Encoding is provided, one receiving participant could not verify signature because they thought Content-Transfer-Encoding was required. Participant fixed by not looking for Content-Transfer-Encoding and default to "binary". All other receiving participants were already defaulting to "binary" and not requiring Content-Transfer-Encoding.

- Participant could not decompress other participants messages which as compressed with “deflate” from ZLIB.
- Participant added “filename preservation” and their Content-Type then had an optional field, “name”, for example:

Content-Type: application/EDI-X12; name="file.out"

One receiving participant was trying to use the name parameter but anything after the colon should be considered comments per the specifications and should be ignored. Receiving participant solved by ignoring anything after the colon.

- Participant was using non-SSL URL when the test case requested SSL.

For example:

Receipt-Delivery-Option: <ftp://abc/inbound>

Participant resolved and added in the correct SSL url.

- Participant was using an invalid SSL certificate:

DumpASN on the certificate turned up the following twice:

```
231 30 17: SEQUENCE {
233 06 3: OBJECT IDENTIFIER commonName (2 5 4 3)
238 13 10: PrintableString 'nuExCS_SSL'
: Error: PrintableString contains illegal character(s).
```

That offending values were contained in the Issued To and the Issued By fields. Participant re-issued the certificate without underscores.

- Due to a certificate issue, participant reported that for test case B where other participant is the originator or recipient, the following error was being generated:

```
> AUTH TLS
234 AUTH TLS OK. TLS enabled and waiting for negotiation.
> PBSZ 0
```

]

After the SSL certificate was updated, this issue was resolved

10. Participant was not using secure port and caused PROT commands to fail.
11. Participant was not correlating the MDN to the original message properly.
12. Participant was not signing MDN's as requested.

## **Very Large Message Test**

In this round, participants exchanged a 200 MB< 500 MB and 1 GB payload (very large message – VLM). Testing went very smooth as participants had previously certified VLM messages in previous AS3 Interops.

The 200 MB test was used mostly to help participants debug their products with a “smaller” payload. Testing focused on 500 MB and 1 GB payloads. Participants demonstrated successful transfer and processing without any issues being reported.

The VLM dictated that sender compress, encrypt and sign the payload while the recipient had to demonstrate successfully receiving and processing the payload by uncompressing, decrypting and verifying the signature.

VLM testing was also automated.

## AS3-1Q08 Test Results

During the course of testing, interoperability issues did arise and were resolved. Some issues resolved in this test round were not related to AS3 server's themselves, but revolved around establishing connectivity and required troubleshooting firewall settings or certificates, similar to previous AS3 Interop rounds.

### Issues Resolved

The following issues were resolved during the debug phase of testing.

- One participant was returning the internal IP address on PASV calls. Some participants required the public IP address. Resolved by moving the FTP server to DMZ.
- One participant required EDI identifiers within the EDI. For all other participants the payload is agnostic (or can be configured to be agnostic) and do not need or verify the EDI identifiers within the EDI payloads. The EDI test payloads were properly setup for this participant.
- One participant had issues with decompressing messages with all participants.
- For Test Case "E" the message is SMIME (signed/encrypted). The content type header that you can see (i.e., human readable) is at the CMS layer (the outer layer of the SMIME message), and its content type is application/pkcs7-mime.

The content type header from one participant was fine:

**Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m**

The CMS object of a good example message contains a valid MIME message content type as:

**Content-Type: multipart/signed; micalg=sha1;  
protocol="application/pkcs7-signature"; boundary="----  
=\_Part\_0\_12984448.1200363068560"**

However, for this same participant, they were generating a “bad” message because the CMS object contained an invalid MIME message content type as (missing micalg and protocol):

**Content-Type: multipart/signed; boundary="----  
=\_Part\_5\_1395020582.1200068882859"**

That is an invalid content type as stated in RFC3851, section 3.4.3.2:

Step 5. The MIME entity of the application/pkcs7-signature is inserted into the second part of the multipart/signed entity.

The multipart/signed Content type has two required parameters: the protocol parameter and the micalg parameter.

The protocol parameter MUST be "application/pkcs7-signature". Note that quotation marks are required around the protocol parameter because MIME requires that the "/" character in the parameter value MUST be quoted.

The micalg parameter allows for one-pass processing when the signature is being verified. The value of the micalg parameter is dependent on the message digest algorithm(s) used in the calculation of the Message Integrity Check.

- One participant was not generating the correct MIC and thus MDN's were failing with all participants. This occurred for test cases H and I.
- One participant was not properly verifying the signature of messages from all other participants.
- One participant was not responding to the ftp session quit command with the appropriate response code.
- One participant could not verify the signature of a message because the signedAttributes of the signature is set to null. However, this is an optional field and not required.

Example Message Received:

#### **Received Content From Sender Participant**

```
PKCS7 SignedData:  
  version: 1  
  digestAlgorithms (1):  
    digestAlgorithms[0]: SHA  
  encapsulatedContentInfo:  
PKCS7 EncapsulatedContentInfo:
```

```
contentType: 1.2.840.113549.1.7.1
content: null
certificates (0): null
certificate revocation lists (0): null
signers (1):
signer[0]: PKCS7 SignerInfo:
version: 1
PKCS7 SignerIdentifier:
  issuer: C=US,
  EMAILADDRESS=sender@testparticipant.com, CN=Tester, OU=QA,
  O="Test Participant"
  serialNumber: 11111111
  digestAlgorithm: SHA
  signatureAlgorithm: RSA
  signedAttributes: null
  digestEncryptionAlgorithmId: SHA
  signature:
```

Please see: <http://www.ietf.org/rfc/rfc2630.txt>

### 5.3 SignerInfo Type

Per-signer information is represented in the type SignerInfo:

```
SignerInfo ::= SEQUENCE {
  version CMSVersion,
  sid SignerIdentifier,
  digestAlgorithm DigestAlgorithmIdentifier,
  signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature SignatureValue,
  unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL }

SignerIdentifier ::= CHOICE {
  issuerAndSerialNumber IssuerAndSerialNumber,
  subjectKeyIdentifier [0] SubjectKeyIdentifier }

SignedAttributes ::= SET SIZE (1..MAX) OF Attribute
UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute

Attribute ::= SEQUENCE {
  attrType OBJECT IDENTIFIER,
  attrValues SET OF AttributeValue }

AttributeValue ::= ANY

SignatureValue ::= OCTET STRING
```

## **Very Large Message Test**

In this round, participants exchanged a 500 MB and 1 GB payload (very large message – VLM). Testing went very smooth as participants had previously experimented with VLM messages in previous AS3 Interops.

A 100 MB and 200 MB were also used to help participants debug their products with “smaller” payloads, however, it quickly became apparent that these payloads were easily being transferred and processed. Testing then focused on 500 MB and 1 GB payloads, and finally on the 1 GB payload. Participants demonstrated successful transfer and processing without any issues being reported.

VLM testing came after the debug phase and this contributed to the smooth testing of VLM. Participants also setup their servers with greater memory than usual as would normally be configured in production environments.

The VLM dictated that sender compress, encrypt and sign the payload while the recipient had to demonstrate successfully receiving and processing the payload by uncompressing, decrypting and verifying the signature.

## **AS3-1Q07 Test Results**

During the course of testing, interoperability issues did arise and were resolved. Some issues resolved in this test round were not related to AS3 server’s themselves, but revolved around establishing connectivity and required troubleshooting firewall settings or certificates, similar to previous AS3 Interop rounds.

### **AS3 Version and EDIINT-Features Header**

One participant was rejecting AS3 messages because they contained EDIINT-Features Header and AS3 Version = 1.2. The EDIINT-Features Header is an ASn (AS1, AS2, AS3) tag which communicates features that the ASn application supports, for instance, CEM and MA.

It is mainly used in AS2 however, for some companies, the tag generation code is common between ASn products and thus the tag appears in all ASn products. No features have been certified under AS3 however one participant included EDIINT-Features with MA and another with CEM.

It was decided that AS3 messages should NOT be rejected because of the inclusion of EDIINT-Features header. Additionally, inclusion of the EDIINT-Features Header requires the use of AS3 version 1.2, and AS3 messages should not be rejected because AS3 Version is not equal to 1.1

## **Base64 Content-Transfer Encoding**

The AS3 specification is contradictory on whether base64 (or other encoding methods) is allowed, however, AS3 participants have for years supported base64 encoding, and at least one offers a configurable option to send base64 encoded messages. Although it is not necessary to base64 encode AS3 messages, consensus was arrived at that it is not illegal. One participant initially did not support AS3 messages that were base64 encoded, however this support was added during the course of AS3 Interop testing.

## **FTP Servers**

The majority of AS3 products are developed with FTP servers developed in-house. Some AS3 products used within this test chose 3rd party FTP server to use in their testing. The 3rd party FTP servers are not listed in this report because they are not the direct focus of this test. However, by publishing the server choreographies in Appendix C, implementers of these products can determine or configure their FTP server to properly interact with any of the AS3 products in this test. Implementers should contact the product vendors about specifics of their FTP server capability and recommendations.

## **Folded Headers**

One participant was rejecting AS3 messages that had Folded Headers however Folded Headers are allowed in AS3 message exchanges. This participant included support for folded headers.

## **Very Large Message Experimental Test AS3-1Q07**

In this round, as in the previous round, participants exchanged a 500MB payload during the Very Large Message (VLM) test. This test demonstrated similar type of results as in the previous AS3 2Q06 Interop rounds. Participants expressed interest in continuing testing however due to schedule conflicts and the open issues from this and the previous Interop round, this test case was not promoted to a required test case as had been anticipated in the previous AS3 Interop round. It remained as an experimental test for AS3 1Q08.

Additionally, in this test round, it was reported by one participant that they inspect the VLM content. The Participants AS3 product runs on UNIX platform and a CRLF in the VLM binary data was causing problems; that is, a Windows payload to UNIX platform was causing Interop issues.

Most participants had issues sending to and from another participant due to firewall issues. IT did not feel it was firewall but there was not enough time to resolve.

One participant commented that executing the VLM was time-consuming taking approximately 3 hrs. The participant possibly needed to optimize his OS or machine. However, most participants were able to complete the VLM testing in 50 minutes.

Participants expressed a strong desire to have it included in future AS3 rounds, and based on testing done in the last Interop round and this one, it is now clear that 2-4 weeks of additional time are needed in the schedule to allow participants ample time to completely debug their applications for VLM exchanges. Participants were encouraged to work toward ensuring that 500 MB can be exchanged seamlessly internally before participation in the next AS3 Interop round scheduled for sometime in early 2008.

## **AS3 Test Data**

AS3 Test data centers on exchanging EDI or XML documents. No binary payloads are part of the required test cases (i.e., .pdf, .tif, .doc, etc.). The Very Large Payload was a binary data file, not EDI. Future AS3 rounds may consider adding required test cases using test data of varying sizes and of different formats.

## **AS3-2Q06 Test Results**

### **Very Large Message Experimental Test**

During this AS3 Interop an experimental test was conducted to ascertain the readiness of the participant products to exchange a Very Large Message (VLM). The type of the payload for this test was selected to be a binary file of about 500 MB in size. All participants participated in the testing and each participant acted as both host and client during the exchange of the VLM. Since it was an experimental test non-successful exchanges did not affect certification results.

The test required that the VLM binary file be encrypted, compressed, and signed then transferred over a non-SSL connection. The AS3 specification implies that the content-type for binary files be application/EDI-CONSENT, however, all participants agreed that application/octet-stream was acceptable and would be used.

The transfer time was typically in the range of 1.5 hours.

In general, all participants were able to exchange the VLM with a few exceptions. The types of issues encountered during this testing are described below.

### **Connection Timeouts:**

At least one product was timing out due to the fact that a connection to the host was first established, then the actual packaging of the VLM was started. Since the processing time (encrypting, compressing and signing the VLM) varied from 2 minutes to 10-12 minutes, the connection to the host would time out. This was resolved by increasing the timeout parameters on the client side.

### **Firewall Timeouts:**

A couple of participant's firewalls timed out and had to be re-configured to allow for the transfer to occur.

### **Processing Errors:**

One participant's product currently encodes the VLM in one large OCTET string while all others chunked their encoding in smaller manageable OCTET strings. This impacted one participant's product which was not able to un-package the VLM when it was received due to the memory requirements needed to handle the payload processing. If the VLM would have been increased to 1GB, or 2GB, or larger, it is unknown if other participant products would have experienced similar processing errors of the VLM encoded as one large OCTET string.

## Test Requirements

In order to complete the test, each participant was required to meet the trading partner and technical requirements of the test.

### Interoperability Test Execution

Interoperability is determined by each product-with-version successfully sending and receiving each test case with each other. Each test case describes the security format and payload of the message. The message must be sent as described with the expected results to be considered successful. The successful sending and receiving of these messages by all the participants are the Test Criteria for the interoperability test. A description of the test cases used in this test round is found in the Appendix.

Each participant executed each test case of the Test Criteria as both the originator and the recipient of the test case with the other participants. Each product demonstrated the ability to interact with each others AS3 server and server choreographies.

Each participant was required to provide an FTP server, digital certificates and basic trading partner information. While every AS3 product had FTP client capabilities, some did not have an embedded FTP server but were designed for working with a generic FTP server. Those participants who did not have an embedded FTP server selected a 3rd party server of their choosing to use in testing.

Also, each participant provided their digital security certificates (including SSL server certificates) to the other participants for storage in their trusted store. Each certificate conformed to the X.509 standards but varied with respect to the fields used in the certificates. Some participants generated their own self-signed certificates (those whose systems had this capability – not required) and other acquired them from well-known third party Certificate Authorities. Some participants chose to use separate certificates for S/MIME and SSL while others used one certificate for all forms of security.

All participants were required to establish trading partner relationships with each other. Participants were responsible for distributing both their FTP URLs and logins and configuring their firewalls to allow all participants access to their product-with-version. DGI provided the AS3 identifiers and EDI identifiers used in the test.

## **AS3 Server Choreographies**

The term “choreography” within AS3 Interoperability testing refers to the actions between a client and server and the FTP commands which enable these actions to occur. The primary actions are server logon (secure and un-secure), document upload, document download, MDN upload and MDN download. Refer to the appendix for a template describing the choreography of each AS3 server used in this test.

The choreography comes from the requirements of the server, and each AS3 product/FTP client must be flexible to support the different needs of the servers. Each participant must state its desired choreography for the server it provides for testing. The choreography will list the FTP commands in their necessary order with a brief description, if necessary, of options in using the actions and commands, such as if documents and MDNs are uploaded and download in the same fashion. The Product Test Group also defined a Superset Choreography which defines the base FTP commands needed to support environments (client/server) which the Test Criteria was performed.

The choreography describes the means for delivering, retrieving and deleting AS3 messages. It includes information on how an upload is communicated to the server as finished and available for a trading partner download, for example renaming the extension from .tmp. As well, it states if the party downloading the message must send the DEL command to clean up the file or if the message is removed through other means within the server.

By publishing and testing their expected choreography, participants can be assured that they can interoperate using either their server or the FTP server of trading partner participant.

## **Technical Requirements**

In order to be part of the certified interoperable products-with-versions, each participant must both successfully send and receive all tests cases with the other participants. These tests cases, which can be found in the Appendix, cover the basis of the AS3 standard. The test cases demonstrate the products-with-versions can cover the technical requirements listed in the sections below. For additional technical information concerning these sections, refer to the IETF document, "FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet," by T. Harding and R. Scott ([AS3 RFC 4823](#)).

## **S/MIME encryption and digital signatures**

S/MIME encryption and digital signatures provide confidentiality and content-integrity of the data being transported. Key length in the security certificates was between 512 bits and 2048 bits. Triple DES (3DES) was the encryption algorithm used, and other algorithms, such as RC2 or DES,

were not tested. SHA-1 hashing was used in creating the digital signatures, but the MD5 was not used.

## **Compression**

While not a part of the AS3 draft document, compression is part of AS3 interoperability testing. Compression is highly useful in transporting large EDI/EC payloads. During this interoperability test, payloads for test cases with compression demonstrated significant reduction in file sizes. For a document which is signed and compressed, compression may be applied to the document itself (compressed and then signed) or to the document and signature (document signed and then compressed). Products must accept either compression option, but may choose to send using only one of the compression options.

## **Asynchronous Receipts (or MDNs)**

Along with digital signatures, receipts provide authentication of transaction. Asynchronous receipts are sent to the originator of the transaction over a new transport. Asynchronous receipts on both FTP and FTP/S transports were tested. Request for signed receipts were made during the original transactions. When a request for a signed receipt is made, the “Received-content-MIC” MUST always be returned to the requester. The “Received-content-MIC” presents the receipts in the form of NRR (Non-Repudiation of Receipt). Non-repudiation of receipt is a “legal event” that occurs when the originator of the message request a signed receipt to unequivocally verify the recipient received the message

## **Transports**

Both FTP and FTP/S transports were used for this test. The FTP RFC can be found at <http://www.ietf.org/rfc/rfc0959.txt>, and the FTP/S RFC is located at <http://www.ietf.org/rfc/rfc4217.txt>

## **Payloads**

X12, EDIFACT and XML payloads were used in the test cases. Two test cases used X12 payloads of 2MB and 50MB, respectively. A description of the payload files used can be found in the Appendix.

## **Error Reporting**

Products were sent erroneous signed, encrypted and compressed messages and required to return MDNs with the appropriate error message.

## Appendix A: Test Case Summary

The following summarizes the test cases each participant was required to send and received with each other. Each participant acted as both originator and recipient with every other participant trading partner for each of the test cases below

Test Case	Msg Payload	Msg Transport	Msg Security	Compression	MDN Requested	MDN Security
A	Data #1	FTP	None	No	No	N/A
B	Data #2	FTP/S	None	No	Yes	Unsigned
C	Data #3	FTP	Signed	No	Yes	Signed
D	Data #4	FTP	Signed	Yes	Yes	Signed
E	Data #5	FTP	Signed/Encrypted	No	Yes	Signed
F	Data #6	FTP/S	None	Yes	Yes	Unsigned
G	Data #7	FTP	Encrypted	No	Yes	Signed
H	Data #8	FTP	Encrypted	Yes	Yes	Signed
I	Data #9	FTP	Signed/Encrypted	Yes	Yes	Signed
J	Data #3	FTP/S	Signed	No	Yes	Signed
VLM.1	Data #10	FTP	None	Yes	Yes	Unsigned
VLM.2	Data #11	FTP/S	Signed/Encrypted	Yes	Yes	Signed
VLM.3	Data #12	FTP/S	Signed/Encrypted	Yes	Yes	Signed

Test cases K1-K3 are error scenario test cases.

K.1	Data #1	FTP	Signed	No	Sync	Signed
K.2	Data #1	FTP	Encrypted	No	Sync	Signed
K.3	Data #1	FTP	None	Yes	Sync	Signed

Test cases K1-K3 are error scenario test cases and were conducted with the DGI test administrator and the participant. Each participant had to process corrupted signed, encrypted and compressed messages and return the appropriate MDN to DGI.

**K.1 Signature Failure.** Participant must recognize the invalid digital signature and return an MDN with the disposition value of *"processed/error; authentication-failed"* or *"processed/error: integrity-check-failed"*.

**K.2 Encryption Failure.** Participant must recognize an alternate trading partner's encrypted data and return an MDN with the disposition value of *"processed/error; decryption-failed"*.

**K.3 Compression Failure.** Participant must recognize the invalid compressed data and return an MDN with the disposition value of *"processed/error; decompression-failed"* or *"processed/ error: unexpected-processing-error"*.

## Test Data

The test data described below was used as payloads in the test cases of the interoperability test round. This test data was distributed to the participants prior to the test.

Test Data #1: X12	Size: 11 KB
Test Data #2: EDIFACT	Size: 1.1 KB
Test Data #3: XML	Size: 8 KB
Test Data #4: X12	Size: 2 MB
Test Data #5: X12	Size: 2 KB
Test Data #6: XML	Size: 36 KB
Test Data #7: EDIFACT	Size: 9 KB
Test Data #8: EDIFACT	Size: 1.1 KB
Test Data #9: X12	Size: 50 MB
Test Data #10: X12	Size: 200 MB
Test Data #11: X12	Size: 500 MB
Test Data #12: X12	Size: 1000 MB (1 GB)

## Appendix B: AS3 and EDI Identifiers

The following list shows the AS3 and EDI identifiers that were used by the products during this test.

### Host Identifiers

Company	AS3 Identifier	EDI Qualifier	EDI Identifier
Axway	axway1	ZZ	axway1
Cleo	Cleo	ZZ	cleo
GXS	gxs	ZZ	gxs
IBM	IBM_1	ZZ	ibm1
Sterling, and IBM Company	sterling2	ZZ	sterling2
Sterling, and IBM Company	sterling4	ZZ	sterling4

### Remote Identifiers

Company	AS3 Identifier	EDI Qualifier	EDI Identifier
Axway	axway1	ZZ	axway1
Cleo	Cleo	ZZ	cleo
GXS	gxs	ZZ	gxs
IBM	IBM_1	ZZ	ibm1
Sterling, and IBM Company	sterling2	ZZ	sterling2
Sterling, and IBM Company	sterling4	ZZ	sterling4

## Appendix C: AS3 Choreographies

### Server Choreography Superset

#### I. Log on

If Secure

"AUTH TLS"

Either

"PBSZ 0"

"PROT P"

"USER <username>"

"PASS <password>"

Or

"USER <username>"

"PASS <password>"

"PBSZ 0"

"PROT P"

Else Not Secure

"USER <username>"

"PASS <password>"

#### II. Set Data Channel Requirements

Binary data type is required in AS3.

"TYPE I"

Passive mode is required in DGI interoperability testing.

"PASV"

#### III. Choose Directory

Optionally choose a directory.

"CWD <directory>"

#### IV. Upload File

If using a designated filename, upload file by:

"STOR <filename>"

Else use an undesignated filename, upload file by:

"STOU"

Optionally rename file.

"RNFR <original filename>"

"RNTO <new filename>"

#### V. Download File

Retrieve directory list of files

"NLST"

Download file

"RETR <filename>"

Optionally delete the file

"DELE <filename>"

#### VI. Log Off

Log off server

"QUIT"

**NOTE:** Set Data Channel Requirements, Choose Directory, Upload File and Download File steps may be repeated or performed in different order if necessary. Steps which begin with "Optionally" are optional. Steps involving "If" and "Else" and "Either" and "Or" are choices and only one of these steps is required. All other steps are required.

## Company Name: Axway

### Secure Server Logon

Command

AUTH TLS (or AUTH SSL)

PBSZ 0

PROT P

USER <username>

PASS <password>

### Non-secure Server Logon

Commands

USER <username>

PASS <password>

### Document Upload

Commands

TYPE I

STRU F

MODE S

CWD inbound

PASV/PORT

STOR <filename>

QUIT

## Document Download

Commands

TYPE I

STRU F

MODE S

CWD <to(user)>

## The <user> is defined as your company name.

Ex: CWD tocleo

PASV/PORT

NLST

RETR

DELE

QUIT

## MDN Upload

Commands

Same as Document upload.

## MDN Download

Commands

Same as Document download.

## Comments

"When sending files to Axway, your user id will place you in your root directory. You will see a sub-directory, inbound. Axway will be polling the inbound directory for files transferred to it from a trading partner.

## Company Name: Cleo

### Secure Server Logon

Commands

AUTH TLS (or AUTH SSL)

PBSZ 0

PROT P

USER <username>

PASS <password>

### Non-secure Server Logon

Commands

USER username

PASS password

### Document Upload

Commands

CWD inbox

PASV or PORT x,x,x,x,x,x

STOR filename

QUIT

### Document Download

Commands

CWD outbox/payload

PASV or PORT x,x,x,x,x,x

NLST

PASV or PORT x,x,x,x,x,x

RETR filename1

DELE filename1

PASV or PORT x,x,x,x,x,x

RETR filenameN

DELE filenameN

QUIT

### MDN Upload

Same as Document upload.

### MDN Download

Commands

CWD outbox/mdn

PASV or PORT x,x,x,x,x,x

NLST

PASV or PORT x,x,x,x,x,x

RETR filename1

DELE filename1

PASV or PORT x,x,x,x,x,x

RETR filenameN

DELE filenameN

QUIT

## Company Name: IBM

### Secure Server Logon

Commands

"AUTH TLS"

"PBSZ 0"

"PROT P"

"USER <username>"

PASS <password>"

### Non-secure Server Logon

Commands

USER username

PASS password

### Document/MDN Upload

Commands

TYPE I

CWD inbox

STOR filename

**RNFR <filename>**

**RNTO <filename>**

QUIT

### Document/MDN Download

Commands

CWD outbox

PASSV/PORT

NLST

RETR

DELE

QUIT

### Comments

The commands in **red** are not necessarily to be used.

## **Company Name: GXS**

### **Secure Server Logon**

Commands

AUTH TLS (or AUTH SSL)

PBSZ 0

PROT P

USER <username>

PASS <password>

At this point the following firewall friendly CMD can optionally be issued.

### **Non-secure Server Logon**

Commands

USER <username>

PASS <password>

### **Document Upload**

Commands

CWD inbound

PASV x,x,x,x,x,x

STOR tmpfilename

RNFR tmpfilename

RNTO filename

QUIT

## Document Download

Commands

CWD outbound

PASV x,x,x,x,x,x

NLST

PASV x,x,x,x,x,x

RETR filename1

DELE filename1

....

PASV x,x,x,x,x,x

RETR filenameN

DELE filenameN

QUIT

## MDN Upload

Commands

Same as Document upload.

## MDN Download

Commands

Same as Document download.

## Comments

The FTP server does not delete incomplete files if an error is encountered during an upload because it provides support for REST (restart).

Associated with each of the logins is an "inbound" and an "outbound" directory established for each vendor.

If GXS is acting as the host, GXS will be placing outbound AS3 files to each vendor in their "outbound" directory. Resulting MDNs should be put into the "inbound" directory. Any inbound AS3 files to GXS (still acting as host) should be placed in the "inbound" directory as well.

If GXS is acting as the client, please return any MDNs to the "inbound" directory.

## Company Name: Sterling

### Secure Server Logon

AUTH TLS  
PBSZ 0  
PROT P  
USER <username>  
PASS <password>

### Non-secure Server Logon

USER <username>  
PASS <password>

### Document Upload

TYPE I  
PASV  
CWD Incoming  
STOR <filename>  
QUIT

### Document Download

TYPE I  
PASV  
CWD Outgoing  
NLST  
RETR <filename>  
QUIT

### MDN Upload

TYPE I  
PASV  
CWD Incoming  
STOR <filename>  
QUIT

## MDN Download

TYPE I

PASV

CWD Outgoing

NLST

RETR <filename>

QUIT

## Other Actions

**Comments:** Please DO NOT delete any files after downloading from the Outgoing directory

## Overview of the DGI Interoperability Compliance Process®

Interoperability of B2B products for the Internet is essential for the long-term acceptance and growth of electronic commerce. To foster interoperability, DGI facilitates interoperability and conformance tests. This section contains a description of the test process involved with creating and listing interoperable products.

### DGI In-the-Queue Test Round

In-the-Queue Test Rounds are designed to allow participants—with products new to DGI interoperability testing, or previously certified products that have made significant product changes or undergone version changes, or missed the most recent test round—to both test and debug their products with the DGI Test Server.

The DGI Test Server is a collection of products-with-version from the previous Interoperability Test Round. These products were provided by the vendors on a voluntary basis. The DGI Test Server allows products new to the interoperability process to be debugged in a quicker manner by testing with proven products-with-version.

Through the In-the-Queue Test Rounds, participants will see their products-with-version become conformant to the AS3 standard and interoperable with the DGI Test Server products. Products which successfully complete In the Queue Test Rounds are considered compliant to the respective standard and will be listed on the [www.drummondgroup.com](http://www.drummondgroup.com) website as "In the Queue," but they will not be given product Interoperability Status on the [www.drummondgroup.com](http://www.drummondgroup.com) website.

Successful test completion also qualifies that particular product to participate in the next DGI Interoperability Test round, but does NOT guarantee successful completion of the full Interoperability Test Round. DGI makes no warrants or guarantees that products passing In the Queue Test Rounds will pass the Interoperability Tests.

### DGI Interoperability Test Round

Products-with-version from the previous AS3 Interoperability Test Round and products-with-version from the In-the-Queue tests come together in a vendor-neutral and non-competitive environment to test with each other in order to become interoperable with each other. In an Interoperability Test Round, each product-with-version must successfully test with each other in order to be certified as interoperable.

The DGI Interoperability Test Round verifies conformance to a standard and then verifies that members of the Product Test Group are interoperable among themselves. Interoperability is an all or nothing within the Product Test Group over the Test Criteria. A product is either interoperable with all other products in the Test Group or not.

Products-with-version which demonstrate complete interoperability among the passing members of the Product Test Group are given a Drummond Certified™ Seal and are listed with Interoperability Status on the [www.drummondgroup.com](http://www.drummondgroup.com) website. Interoperability Test Rounds are periodically repeated to verify that as product names, versions or releases change, the products remain interoperable.

## About Drummond Group Inc.

[Drummond Group Inc.](http://www.drummondgroup.com) (DGI) is the trusted interoperability [test lab](#) offering global testing services through the product life cycle. Auditing, QA, conformance testing, custom software test lab services, and [consulting](#) are offered in addition to interoperability testing. Founded in 1999, DGI has tested over a thousand international software products used in vertical industries such as automotive, consumer product goods, healthcare, energy, financial services, government, petroleum, pharmaceutical and retail. For more information, please visit [www.drummondgroup.com](http://www.drummondgroup.com) or email: [info2@drummondgroup.com](mailto:info2@drummondgroup.com)