

Final Report
AS2 Interoperability Test
First Quarter 2006 (1Q06)



April 7, 2006

Prepared & Facilitated by:
Drummond Group Inc.
www.drummondgroup.com

Table of Contents

Cover Letter	3
Disclaimer	4
Test Participants	5
Definitions	8
Interoperability Test Summary	9
Interoperability Test Results.....	10
Interoperability Test History.....	11
Interoperability Issues	12
Interoperability Issues Resolved or Affirmed This Round.....	12
Interoperability Issues Resolved or Affirmed from previous Test Rounds	13
Test Requirements	16
Trading Partner Requirements	16
Technical Requirements	16
S/MIME encryption and digital signatures.....	17
Compression	17
Synchronous and Asynchronous Receipts	17
Transports.....	17
Payloads.....	17
Error Reporting.....	18
Optional Test	18
Multiple Attachment Testing.....	18
Test Case Summary.....	19
Test Data.....	20
Required Test Cases Detail	21
Test Case: A.....	21
Test Case: B.....	21
Test Case: C.....	22
Test Case: D.....	22
Test Case: E.....	23
Test Case: F.....	23
Test Case: G	24
Test Case: H.....	24
Test Case: I	25
Test Case: J.....	25
Test Case: K.1.....	26
Test Case: K.2.....	26
Test Case: K.3.....	27
Optional Test Case Detail.....	28
M.1 XML and PDF Attachments	28
M.2 XML and TIF Attachments	28
Assigned AS2 and EDI Identifiers	29
Overview of the DGI Interoperability Compliance Process®.....	30
DGI In-the-Queue Test Round.....	30
DGI Interoperability Test Round	30
InSitu™ Test System.....	31
About Drummond Group Inc.	32

Cover Letter

DRUMMOND GROUP Inc. (DGI) is pleased to announce that the following participants in the AS2-1Q06 Interoperability Test Round have completed all requirements and passed tests (see Interoperability Test Summary below) between each product demonstrating interoperability and conformance. Final tests were run Mar. 27-31, 2006.

This tenth round of AS2 interoperability testing had one optional test -- multiple attachments. This was the second fully automated AS2 interoperability test. DGI InSitu™ automation was integrated into all of the participating products. InSitu™ enhancements, once again, further reduced the testing effort for participants and increased the ease of executing test cases and analyzing their results. The next round of AS2 interoperability testing will continue to require new participants to be automated so that AS2 interoperability testing remains fully automated.

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

Sincerely,





Rik Drummond
CEO,
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>Axway-Cyclone</p> <p>http://www.axway.com</p> <p>Product Name: XFB Gateway 6.9 for XIP 3.1</p>	 <p>Axway-Cyclone</p> <p>http://www.cyclonecommerce.com</p> <p>Product Name: Cyclone Interchange/Activator/Central version v5.4 for XIP 3.1</p>
 <p>Boomi Software</p> <p>http://www.boomi.com</p> <p>Product Name: Boomi AS2 Transport v3.3</p>	 <p>Bridgewater</p> <p>http://www.bridgewater.com</p> <p>Product Name: AS2Bridge 3.1</p>
 <p>Cleo Communications</p> <p>http://www.cleo.com</p> <p>Product Name: VersaLex™ v3.0 tested in VLTrader™ v3.0</p>	 <p>Compinia GmbH & Co. Kg</p> <p>http://www.compinia.com/</p> <p>Product Name: ComAS2 v1.0</p>
 <p>Covast</p> <p>http://www.covast.com</p> <p>Product Name: Covast AS2 Adapter v4.3</p>	 <p>Electronic Data Systems</p> <p>http://www.eds.com</p> <p>Product Name: EDS*ELIT AS2 Connector v3.0</p>

 <p>EXTOL International</p> <p>The Complete B2B Application www.extol.com</p> <p>http://www.extol.com</p> <p>Product Name: EXTOL Secure Engine V5R2 tested in EXTOL Secure V5R2.3</p>	 <p>GXS</p> <p>http://www.gxs.com</p> <p>Product Name: AS2 Engine v3.9</p>
 <p>IBM</p> <p>http://www.ibm.com</p> <p>Product Name: IBM WebSphere Partner Gateway – Express v6.0</p>	 <p>IBM</p> <p>http://www.ibm.com</p> <p>Product Name: IBM WebSphere Partner Gateway v6.0</p>
 <p>iSoft Corporation</p> <p>http://www.isoft.com</p> <p>Product Name: Commerce Suite Server v3.4</p>	 <p>iWay Software Inc. Accelerating Business Integration</p> <p>http://www.iwaysoftware.com</p> <p>Product Name: iWay Adapter for AS2 v5.5 SP5</p>
 <p>n software InSoftware</p> <p>http://www.nsoftware.com</p> <p>Product Name: IP*Works! EDI / AS2 v7.2</p>	 <p>nuBRIDGES nuBridges LLC</p> <p>http://www.nubridges.com</p> <p>Product Name: truExchange EDI-INT v3.2</p>

 <p>SAA Consultants Ltd.</p> <p>http://www.saaconsultants.com</p> <p>Product Name: REIMS B2B Frameworks Module V5Re</p>	 <p>SEEBURGER AG</p> <p>http://www.seeburger.com</p> <p>Product Name: SEEBURGER EDI-INT AS2 Adapter v6.2.2 tested in SEEBURGER Business Integration Server Release 5.5.1</p>
 <p>Sterling Commerce</p> <p>http://www.sterlingcommerce.com</p> <p>Product Name: Sterling Information Broker v3.8</p>	 <p>Sterling Commerce</p> <p>http://www.sterlingcommerce.com</p> <p>Product Name: Gentran Integration Suite/ Sterling Integrator v4.1</p>
 <p>Sterling Commerce</p> <p>http://www.sterlingcommerce.com</p> <p>Product Name: Connect: Enterprise for UNIX v2.4</p>	 <p>TIBCO Software Inc.</p> <p>http://www.tibco.com</p> <p>Product Name: TIBCO BusinessConnect™ AS2 Transport v5.1.0 tested in TIBCO BusinessConnect™ v5.1</p>
 <p>Transentric LLC</p> <p>http://www.transentric.com</p> <p>Product Name: Transentric Agilink Connector AS2 v3.0</p>	 <p>Tumbleweed Communications</p> <p>http://www.tumbleweed.com</p> <p>Product Name: Tumbleweed AS2 Engine v2.0.1 tested in SecureTransport Server v4.5.1</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

This is the tenth round of interoperability testing for IETF AS2 standard which is documented in: ***RFC 4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)***. AS2 (Applicability Statement 2) is the specification standard by which vendor applications communicate EDI (EDIFACT or X12), binary, or XML data securely over the Internet. AS2 is published through the [IETF EDIINT Work Group](#).

The purpose of the test is to provide a venue for vendors to test and correct their software systems in a non-competitive 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 AS2 in terms of security and receipts. Digital signatures, encryption, HTTP/HTTPS transports, unsigned and signed receipts, synchronous and asynchronous receipts, and data compression are all tested. Test data payloads simulating traditional POs and UCCnet messages were used with document formats of X12, EDIFACT and XML. Products were also tested with erroneous AS2 messages to verify they could properly recognize message errors and return the appropriate MDNs.

As in previous Interoperability test rounds, this test round continued conformance checking of error values within MDNs. 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 identify and resolving the problem.

The test round repeated the optional multiple attachment testing which was introduced in the eighth interoperability test round. Along with completing the required test case, four products completed the optional multiple attachment testing.

Interoperability Test Results

The successful sending and receiving of all Test Case messages by all the products-with-version with each other is the Test Criteria for determining successful interoperability of all products with each other. Each test case describes the format and payload of a test message; a description of the test cases used in this test round is found in the “Test Case Summary” section of this Final Report.

The Interoperability Test Round was completed in seven weeks. During the first six weeks, the testing was focused on finding interoperability errors and correcting them. During Mar 27-31, 2006, code changes were not allowed.

During this final week, 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 both through InSitu and by the participants themselves and demonstrated by supplying the messages sent and received.

The following participants also took part in and successfully completed Multiple Attachments Optional testing for this round.

- Cleo Communications
- GXS
- iSoft Corporation
- /nSoftware

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.

Interoperability Test History

This is the tenth AS2 Interoperability Test administered by DGI.

AS2 1Q06 Interoperability Test – Feb-Mar 2006

Previous tests included the following:

AS2 3Q05 Interoperability Test – September-October 2005
AS2 1Q05 Interoperability Test – February-April 2005
AS2 3Q04 Interoperability Test – August-September 2004
AS2 1Q04 Interoperability Test – February-March 2004
AS2 3Q03 Interoperability Test – July-September 2003
AS2 1Q03 Interoperability Test – January-February 2003
AS2 2Q02 Interoperability Test – March-August 2002
AS2 2Q01 Interoperability Test – May-August 2001
AS2 4Q00 Interoperability Test – October-December 2000

Interoperability Issues

During the course of previous interoperability tests, several interoperability issues were discovered or questioned and then resolved through the debugging stage of the test. All products from this test comply with these resolved issues. These issues are listed below to assist in resolving any supply-chain trading problem which may occur between products-with-version from this test and AS2 products-with-version from outside the test, including backward versions of these test products.

Interoperability Issues Resolved or Affirmed This Round

1. Certificates and security toolkit related errors continued to be observed in this test round. Certificates using unusual fields or extensions could create problems within supply-chains. Not all possible certificate fields or extensions were tested against every AS2 product's toolkit, and potential issues could still exist due to certain certificate fields and extensions.

For example, there was an issue with a participant SSL certificate was not properly formatted (for DER encoding). It caused another participant to reject it during the SSL handshake. The participant's certificate had an explicit default value in the version identifier. The certificate had a 0 in this field, when it should be version 1 (everyone else's certificates had version 1).

2. Also, it was discovered that security toolkit versions are not always interoperable from version to version, and this Interop revealed and helped resolve these incompatibility in the security toolkits. However, security toolkits were not exhaustively tested for interoperability.

A list of the public-key certificates used by the participants in this and previous test round may be found on the DGI website at:

<http://www.drummondgroup.com/html-v2/standards.html>

3. The AS2 specification requires that human-readable portion of MDN must contain "Final-Recipient". Please see <http://www.ietf.org/rfc/rfc4130.txt> section 7.4.2. A participant was not sending "Final-Recipient" however it was required.
4. A participant was sending "folded headers" in the MDN's and this caused an error because at least one other participant did not process "folded headers". In previous Interop's, it was a consensus item to not fold the headers.

Example:

Content-Type: multipart/report; report-type=disposition-notification;
boundary="----=_Part_1139974138134"

5. An AS2 server was attempting to connect to port 80 instead of 443 when the URL was provided without a port, for example:
`https://hostname/` The correct port to connect to should be 443, (the default port for SSL when port is not specified). The default port for non-ssl is port 80. Please see: <http://rfc.net/rfc2616.html>
6. MDN conformance testing revealed that one participant's MDN disposition text says, "Disposition: automatic-action/MDN-sent-automatically; processed". It should have returned error text "processed/error: authentication-failed" or "processed/error: integrity-check-failed".

Interoperability Issues Resolved or Affirmed from previous Test Rounds

1. Some products could not accept certain characters or certain strings of AS2 identifiers. Two specific issues were: 1) having a space (" ") at the third location, e.g. "AS 2", and 2) identifiers containing a comma (","). While these conflicts were very rare and not associated with every participant, supply-chain implementers of these products should avoid identifiers with this syntax and discuss with their AS2 vendor any potential AS2 Identifier issues.
2. Trailing long white spaces (LWS) at the end of HTTP headers is not permitted. Leading LWS is allowed within HTTP (RFC2616) but not clear if trailing LWS is or is not.
3. The value "RSA-SHA1" was used by some participants for the MIC algorithm of the digital signature. It is a valid value and should be considered equal to that of the more common "SHA1" value. "RSA-SHA1" is a legacy value from an earlier S/MIME implementation.
4. Field names in MDNs, such as Original-Message-ID, are case-insensitive. According to RFC2298, section 3.1.1, "field names are case-insensitive, so the names of notification fields may be spelled in any combination of upper and lower case letters." As well, it is permissible to have a white space character (" ") before the message-id value of the Original-Message-ID field in the MDN. Thus, the two examples below are considered identical:
 - a. Original-Message-ID:<123foo@example>
 - b. Original-Message-ID: <123foo@example>

5. The Message-ID header is not required in MDNs.
6. Chunked encoding for HTTP 1.1 requests and responses is acceptable for AS2. Rules for implementing, supporting and understanding chunked encoding can be found in the HTTP 1.1 standard, RFC2616.
7. Some products require valid EDI/XML documents on inbound messages and will generate MDNs with errors if they are invalid. This includes both valid formatting and/or recognized identifiers.
8. Certificate serial numbers must not be negative, per RFC3280. While some AS2 systems accept negative serial numbers, other systems cannot accept negative values.
9. Certificates are uniquely identified through their Issuer name and their serial number. As with negative serial numbers, certain AS2 systems will reject duplicate certificates, but others can accept them.
10. Some products utilizing the open source OpenSSL experienced problems in SSL transactions. The cause was due to the sending of empty fragments in the transaction which caused some trading partner products to corrupt the inbound document. The solution was to modify configuration flags within OpenSSL.
11. HTTP Content-length header is not necessarily required on MDN. The HTTP standard specifies the use and requirement of this header, and the AS2 draft is being updated to refer back to the HTTP standard for the use of content-length.
12. MIME Folded headers continue to cause problems with several products due to their associated web server. Folded headers were not used during the test and should be avoided in actual implementation.
13. The use of quotation marks on AS2 System Identifiers should not be used for atomic names. Also, the use of quotation marks on AS2 System Identifiers must be consistent for both the payload messages as well as for the MDNs. That is, if quotation marks are used in the payload message, they also must be present in MDNs.
14. A 204 (No content) HTTP response would be acceptable in an HTTP response of an async MDN request. This should be accepted (assuming the response has no body). From the latest version (13) of the AS2 draft, section 7.6, notice the comment of the response being "in the 200 range." HTTP RFC2616 states that if a 204 is returned, there is to be no message body and the message is terminated by the first empty line after the header fields. So, the 204 will work as long as there are only HTTP headers in the response.

15. If certificates use the country attribute, the country attribute may only contain two characters. For example, "C=USA" is invalid and instead should be listed as "C=US".
16. Encrypted messages can contain multiple RecipientInfo structures within the CMS data, including one describing the originator. Refer to RFC 2630 Section 6 for more details.
17. Consensus was reached that AS2 messages with EDI payloads should identify the content-type either as application/EDI-X12 or application/EDIFACT and NOT application/EDI-CONSENT.
18. The Message-ID is not required in Asynch MDN's because the AS2 standard states it SHOULD be contained, that is, it is not required. Asynch MDN's should not be rejected if MDN's do not contain Message-ID because it is not required. It is recommended that it be present. Please refer to the meanings of SHOULD and MUST.

Test Requirements

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

Trading Partner Requirements

All participants were required to establish trading partner relationships with each other. Each participant provided their security certificates (including TLS server certs) 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 certs for S/MIME and SSL while others used one certificate for all forms of security.

Participants were responsible for configuring themselves in InSitu™ which included their certificates and providing both their HTTP and HTTP/S URLs. Participants then configured their firewalls to allow all participants access to their product-with-version.

DGI provided the AS2 identifiers and EDI identifiers used in the test. The AS2 identifiers covered a wide range of possible values.

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 AS2 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 ***RFC 4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)*** found at <http://www.ietf.org/rfc/rfc4130.txt?number=4130>

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 AS2 draft document, compression is part of AS2 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.

Synchronous and Asynchronous Receipts

Along with digital signatures, receipts provide authentication of transaction. Synchronous receipts provide information on the reception and handling of the message over the same transport. Asynchronous receipts are sent to the originator of the transaction over a new transport. Synchronous and asynchronous receipts on both HTTP and HTTP/S transports were tested. Request for signed receipts were made over synchronous and asynchronous 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 (None-Repudiation of Receipt).

Transports

Both HTTP and HTTP/S transports were used for this test. Both HTTP version 1.0 and version 1.1 servers were involved in this test. For HTTP/S, only server side authentication was tested. Asynchronous receipts were returned over both HTTP and HTTP/S transports. For this test, asynchronous MDNs over SMTP were not tested.

Payloads

X12, EDIFACT and XML payloads were used in the test cases. Two test cases used X12 payloads of 2MB and 50MB, respectively. The payload data used in testing were traditional POs and UCCnet sample messages. 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.

Optional Test

The multiple attachment optional test introduced in the eighth test round was conducted again in this tenth test round. Any participant could have participated in this test but since it was optional, not all elected to receive certification for this optional test.

Multiple Attachment Testing

AS2 transmissions generally contain only a single EDI or XML payload document, and this is what has been solely tested within past DGI interoperability tests. However, some transactions require multiple documents to communicate all relevant information. Multiple attachments allows for two or more documents to be sent in a single AS2 message.

These documents can be of formats other than EDI or XML, such as PDF and TIF image files. Based on an open standard (<http://www.ietf.org/internet-drafts/draft-meadors-multiple-attachments-ediint-02.txt>), multiple attachment testing provides for the same security used in single payload AS2 transmission.

Test Case Summary

The following summarizes the test cases each participant was required to send and received with each other.

Test Case	Msg Payload	Msg Transport	Msg Security	Compression	MDN Transport	MDN Security
A	Data #1	HTTP	Signed/Encrypted	No	Sync	Unsigned
B	Data #2	HTTP	Signed/Encrypted	No	Sync	Signed
C	Data #3	HTTP	Signed/Encrypted	No	Async/HTTPs	Signed
D	Data #4	HTTP	Encrypted	Yes	Sync	Signed
E	Data #5	HTTP	Encrypted	No	Sync	Signed
F	Data #6	HTTP	Signed	No	Sync	Signed
G	Data #7	HTTPs	Signed	Yes	Sync	Signed
H	Data #8	HTTPs	Signed	No	Async/HTTP	Signed
I	Data #9	HTTPs	Signed	No	Async/HTTPs	Signed
J	Data #10	HTTP	Signed/Encrypted	Yes	Async/HTTP	Signed

Test cases K1-K3 are error scenario test cases.

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

All test cases were conducted via InSitu™ and InSitu-enabled participant AS2 products.

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 PO with an apostrophe (!) for segment terminator. Size is 12kB.
- Test Data #2. X12 PO with line feed (0x0a) for segment terminator. Size is 3kB.
- Test Data #3. UCCnet XML file. Size is 9kB.
- Test Data #4. XML PO. Size is 36kB.
- Test Data #5. EDIFACT Purchase Order (PO) with standard apostrophe (") for segment terminator. Size is 6kB.
- Test Data #6. EDIFACT Purchase Order (PO) with standard apostrophe (") for segment terminator. Size is 10kB.
- Test Data #7. EDIFACT Purchase Order (PO) with standard apostrophe (") for segment terminator. Size is 15kB.
- Test Data #8. EDIFACT Purchase Order (PO) with standard apostrophe (") for segment terminator. Size is 2kB.
- Test Data #9. Large X12 file. Size is 2MB.
- Test Data #10. Very large X12 file. Size is 50MB.

Required Test Cases Detail

Test Case: A

Test Description	The initiator creates a signed, encrypted exchange over HTTP with a request for a synchronous, unsigned MDN.
Message Payload	Test Data # 1
Message Transport	HTTP
Message Security	Signature, Encryption
Message Compression	No
MDN Transport	Synchronous
MDN Security	No Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Test Case: B

Test Description	The initiator creates a signed, encrypted exchange over HTTP with a request for a synchronous, signed MDN.
Message Payload	Test Data # 2
Message Transport	HTTP
Message Security	Signature, Encryption
Message Compression	No
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Test Case: C

Test Description	The initiator creates a signed, encrypted exchange over HTTP with a request for an asynchronous, signed MDN.
Message Payload	Test Data # 3
Message Transport	HTTP
Message Security	Signed, Encryption
Message Compression	No
MDN Transport	Asynchronous/HTTPs
MDN Security	Signature
Expected Results	The payload is successfully transferred, the initial HTTP connection is closed with a 200 OK, and then an MDN with a disposition value of "processed" is returned over a new HTTPs connection.

Test Case: D

Test Description	The initiator creates an encrypted, compressed exchange over HTTP with a request for a synchronous, signed MDN.
Message Payload	Test Data # 4
Message Transport	HTTP
Message Security	Encryption
Message Compression	Yes
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Test Case: E

Test Description	The initiator creates an encrypted exchange over HTTP with a request for a synchronous, signed MDN.
Message Payload	Test Data # 5
Message Transport	HTTP
Message Security	Encryption
Message Compression	No
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Test Case: F

Test Description	The initiator creates a signed exchange over HTTP with a request for a synchronous, signed MDN.
Message Payload	Test Data # 6
Message Transport	HTTP
Message Security	Signature
Message Compression	No
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Test Case: G

Test Description	The initiator creates a signed, compressed exchange over HTTPs with a request for a synchronous, signed MDN.
Message Payload	Test Data # 7
Message Transport	HTTPs
Message Security	Signature
Message Compression	Yes
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Test Case: H

Test Description	The initiator creates a signed exchange over HTTPs with a request for an asynchronous, signed MDN over HTTP.
Message Payload	Test Data # 8
Message Transport	HTTPs
Message Security	Signature
Message Compression	No
MDN Transport	Asynchronous/HTTP
MDN Security	Signature
Expected Results	The payload is successfully transferred, the initial HTTPs connection is closed with a 200 OK, and then an MDN with a disposition value of "processed" is returned over a new HTTP connection.

Test Case: I

Test Description	The initiator creates a signed exchange over HTTPs with a request for an asynchronous, signed MDN.
Message Payload	Test Data # 9
Message Transport	HTTPs
Message Security	Signature
Message Compression	No
MDN Transport	Asynchronous/HTTPs
MDN Security	Signature
Expected Results	The payload is successfully transferred, the initial HTTPs connection is closed with a 200 OK, and then an MDN with a disposition value of "processed" is returned over a new HTTPs connection.

Test Case: J

Test Description	The initiator creates a signed, encrypted, compressed exchange over HTTP with a request for an asynchronous, signed MDN.
Message Payload	Test Data # 10
Message Transport	HTTP
Message Security	Signed, Encryption
Message Compression	Yes
MDN Transport	Asynchronous/HTTP
MDN Security	Signature
Expected Results	The payload is successfully transferred, the initial HTTP connection is closed with a 200 OK, and then an MDN with a disposition value of "processed" is returned over a new HTTP connection.

Test Case: K.1

Test Description	The DGI test administrator sends a corrupted signed message to the participant. The data signed over is altered after the digital signature is created and applied. The recipient should not be able to match the digital signature with the payload. The participant must return a MDN with the disposition value correctly identifying the error.
Message Payload	Test Data # 1
Message Transport	HTTP
Message Security	Signed
Message Compression	No
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The MDN is returned with a disposition type, modifier and extension of either “processed/error: authentication-failed” or “processed/error: integrity-check-failed”.

Test Case: K.2

Test Description	The DGI test administrator sends a improperly encrypted message to the participant. The payload data is encrypted using a different certificate than that of the recipient. As a result, the recipient should not be able to decrypt the encrypted MIME body part. The participant must return a MDN with the disposition value correctly identifying the decryption error.
Message Payload	Test Data # 1
Message Transport	HTTP
Message Security	Encryption
Message Compression	No
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The MDN is returned with a disposition type, modifier and extension of “processed/error: decryption-failed”.

Test Case: K.3

Test Description	The DGI test administrator sends a corrupted compressed message to the participant. The compressed data structure is altered. The recipient should not be able to decompress the compressed MIME body part. The participant must return a MDN with the disposition value correctly identifying the error.
Message Payload	Test Data # 1
Message Transport	HTTP
Message Security	None
Message Compression	Yes
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The MDN is returned with a disposition type, modifier and extension of either “processed/error: decompression-failed” or “unexpected-processing-error”.

Optional Test Case Detail

The Optional Test Case Overview describes the multiple attachment test cases which some participants executed.

M.1 XML and PDF Attachments

M.1 Description

The originator creates a Multipart-Related MIME structure with a type parameter of "application/xml". The two attachments are ma_test_data_1.xml (root body part) and ma_test_data_2.pdf attachments. The Multipart-Related structure is signed and sent requesting a signed MDN.

M.1 Test Configuration

Transport: HTTP

Security: Signature

Compression: No

MDN Transport: Synchronous, signed

Attachments: ma_test_data_1.xml (root) and ma_test_data_2.pdf

M.1 Expected Results

The recipient is able to extract the two attachments and return an MDN with the expected MIC calculation in the signed MDN.

M.2 XML and TIF Attachments

M.2 Description

The originator creates a Multipart-Related MIME structure with a type parameter of "application/xml". The two attachments are ma_test_data_3.xml (root body part) which uses the "application/xml" media type and ma_test_data_4.tif which uses the "image/tiff" media type. The Multipart-Related structure is signed and encrypted sent requesting a signed MDN.

M.2 Test Configuration

Transport: HTTP

Security: Signature, Encrypted

Compression: No

MDN Transport: Synchronous, signed

Attachments: ma_test_data_3.xml (root) and ma_test_data_4.tif

M.2 Expected Results

The recipient is able to extract the two attachments and return an MDN with the expected MIC calculation in the signed MDN.

Assigned AS2 and EDI Identifiers

A variety of AS2 and EDI identifiers were used by the products of this test. The AS2 identifiers contained spaces, colons, dashes and other printable characters along with alphanumeric characters to ensure products could handle a variety of AS2 identifiers.

Company	AS2 Identifier	EDI Identifier
Axway	axway	ZZaxway
Boomi	boomi	ZZboomi
Bridgeware	Bridge_!_ware	ZZbridge
Cleo	CLEO	ZZcleo
Compinia	Compinia(as2)	ZZcompinia
Covast	Covast!	Zzcovast
Cyclone	Cyclone One	ZZcyclone1
EDS	EDS *Elit	ZZeds
Extol	Extol;AS2	ZZextol
GXS	GXS Interop	ZZgxs
IBM	IBM_1	ZZibm1
IBM	2nd IBM	ZZibm2
iSoft	iSoft [test]	ZZisoft
iWay	(iway)	ZZiway
/nSoftware	n/Software	ZZnsoftware
nuBridges	nuBridges	ZZnubridges
SAA Consultants	SAA	ZZsaa
Seeburger	Seeburger	ZZseeburger
Sterling	Sterling_1	ZZsterling1
Sterling	SterComm-2	ZZsterling2
Sterling	SC_No. 3	ZZsterling3
Tibco	www.tibco.com	ZZtibco
Transentric	Transentric	ZZtransentric
Tumbleweed	Tumbleweed	ZZtumbleweed

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 AS2 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 website as "In the Queue," but they will not be given product Interoperability Status on the 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 AS2 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 website. Interoperability Test Rounds are periodically repeated to verify that as product names, versions or releases change, the products remain interoperable.

InSitu™ Test System

DGI has created a system for the automation of interoperability testing called InSitu™. InSitu is an innovative technology developed for conducting automated interoperability testing that allows multiple products to coordinate the sending and receiving of test cases without human intervention. Manpower requirements for coordinating testing have been eliminated, allowing participants to focus on debugging their code-base.

InSitu-enabled products are tested together under the direction of the InSitu Server and the test administrator. InSitu is used only for the automation of the sending, receiving and reporting of test cases evaluation, and does not change the requirements of the test case or how the test instance result is interpreted. All products-with-version implemented InSitu into their systems to enable automated testing.

About Drummond Group Inc.

Drummond Group Inc. (DGI) is an independent, privately held company that works with software vendors, vertical industries and the standards community to drive adoption for standards by conducting interoperability and conformance testing, publishing related strategic research and developing vertical industry strategies. Founded in 1999, DGI represents best-of-breed in the industry on linking horizontal infrastructure technologies, standards and interoperability issues with the needs of vertical industries such as retail, grocery, health care, transportation, government and automotive. For more information, please visit www.drummondgroup.com or email: info@drummondgroup.com.