

Certification Final Report
AS1 Interoperability Test
Second Quarter 2008 (2Q08)

June 23, 2008

Prepared & Administered by:
DRUMMOND GROUP INC.
www.drummondgroup.com

Table of Contents

Cover Letter	3
Disclaimer	4
Test Participants	5
Definitions	6
Interoperability Test Summary	7
Interoperability Test History	8
Test Case Summary	9
Core Basic Tests	9
Error Test Cases	9
Interoperability Test Results	10
Interoperability Issues	11
Issues Encountered or Consensus Items From Current Test Round	11
Interoperability Issues Resolved or Consensus Items Affirmed from Previous Test Rounds ...	11
Corrupt messages may not supply a receipt	11
Final-Recipient contains the sender's identifier	11
EDI Identifier Headers	12
Mail Server	12
Testing Requirements	14
Trading Partner Requirements	14
Technical Requirements	14
S/MIME encryption and digital signatures	14
Compression	15
Receipts	15
Payloads	15
Error Reporting	15
Test Data	16
Test Case Criteria	17
Test Case: A	17
Test Case: B	17
Test Case: C	18
Test Case: D	18
Test Case: E	19
Test Case: F	19
Test Case: G	20
Test Case: H	20
Test Case: I.1	21
Test Case: I.2	22
Test Case: I.3	22
Overview of the DGI Interoperability Compliance Process®	23
DGI In-the-Queue Test Round	23
DGI Interoperability Test Round	24
About Drummond Group Inc.	25

Cover Letter

DRUMMOND GROUP Inc. is pleased to announce that the following participants in the Drummond Certified™ AS1 Interoperability & Conformance Validation Test 2Q08 (AS1-2Q08) have completed all requirements and passed tests (see Interoperability Test Summary below) between each product demonstrating interoperability and conformance. Final certifying testing was executed in two days, May 29th to May 30th, 2008. 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</p> <p>http://www.axway.com</p> <p>Product Name: Synchrony Gateway v6.11</p>	 <p>Axway</p> <p>http://www.axway.com</p> <p>Product Name: Synchrony Gateway Interchange v5.6/Synchrony Endpoint Activator v5.6</p>
 <p>Inovis</p> <p>http://www.inovis.com</p> <p>Product Name: BizManager v3.1</p>	 <p>nuBridges, Inc.</p> <p>http://www.nubridges.com</p> <p>Product Name: nuBridges Exchange i 3.2</p>
 <p>nuBridges, Inc.</p> <p>http://www.nubridges.com</p> <p>Product Name: nuBridges Exchange C.S. 3.4</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 sixth round of interoperability testing for IETF AS1 standard which is documented in: ***RFC 3335 – MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet, Applicability Statement #1 (AS1)***. AS1 describes how to exchange EDI (X12, UN/EDIFACT, EDI for Administration, Commerce and Transport), XML, or other business data over the SMTP Transport, or email. AS1 RFC 3335 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 AS1 in terms of security and receipts. Digital signatures, encryption, unsigned and signed receipts, and compression are all tested. Products were also tested with erroneous AS1 messages to verify they could properly recognized message errors and return the appropriate MDNs. *Compression* is not a part of RFC 3335, but it was used in the interoperability test cases. Compression utilizes the capability to express a message with a large payload in a reduced size to leverage rapid delivery of the message. The “Test Requirements” section goes into further detail how compression was used and maybe used within the AS1 message structure.

Test data payloads simulating traditional POs and eBusiness messages used with document formats of X12, EDIFACT, and XML to verify payload data were not altered from one endpoint to the other. Please note that EDI/XML translation and mapping or any other payload processing feature was not tested as it lies completely out of scope of the AS1 specification.

The Interoperability Test Round was executed in two weeks, and the Certification Run was executed in two days, May 29th to May 30th, 2008, where code changes and debug settings were not allowed.

Interoperability Test History

This is the sixth AS1 Interoperability Test administered by DGI.

AS1 2Q08 Interoperability Test: May-June 2008

Previous tests included the following:

AS1 1Q07 Interoperability Test

AS1 2Q06 Interoperability Test

AS1 2Q05 Interoperability Test

AS1 2Q04 Interoperability Test

AS1 2Q03 Interoperability Test

AS1 1Q02 Interoperability Test

Test Case Summary

The following summarizes the test cases each participant was required to send and received with each other. Test case specifics can be found in the [Test Criteria](#) section.

Core Basic Tests

Test Case	Msg Payload	Msg Security	Compression	MDN Security
A Test	Data #1	Signed	No	Unsigned
B Test	Data #2	Signed	No	Signed
C Test	Data #3	Encrypted	No	Signed
D Test	Data #4	Signed/Encrypted	No	Signed
E Test	Data #5	None	Yes	Unsigned
F Test	Data #6	Signed	Yes	Signed
G Test	Data #7	Encrypted	Yes	Signed
H Test	Data #8	Signed/Encrypted	Yes	Signed

Error Test Cases

I.1-I.3 test cases are designed to check the conformance of MDN error responses. They are conformance tests in which the participants are tested against a DGI MDN error tool. DGI test administrator sends an erroneous digitally signed, an encrypted message, and an erroneous compressed message for I.1, I.2 and I.3, respectively. The participant is expected to recognize the error and return the proper error response in the MDN.

Error Test Case I.1 – I.3

Test Case	Msg Payload	Msg Security	Compression	MDN Security
I.1	Data #1	Signed	No	Signed
I.2	Data #1	Encrypted	No	Signed
I.3	Data #1	None	Yes	Signed

Interoperability Test Results

Interoperability is determined by each product-with-version successfully sending and receiving each test case with each other. Each test case describes the format, security, 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 “Test Criteria” section of the Final Report.

On the final two days (May 29 thru May 30, 2008), all products-with-version listed in this test report successfully sent and received each test case 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). Results were reported by the participants 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.

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 products-with-version from outside the test, including backward versions of these test products.

Issues Encountered or Consensus Items from Current Test Round

No new consensus items were made for this test round. Previous consensus items continued to be reference points during this interoperability test round.

During testing, it was observed that one mail server used in testing, Google's Gmail, was inserting a valid DKIM-Signature header with lengths of over 512 bytes. While valid, mail headers of this length are uncommon, and one participant had to make a product adjustment during debug testing to accommodate the length. Implementers of older versions of AS1 products should check to confirm their product is able to support mail headers of this length.

Interoperability Issues Resolved or Consensus Items Affirmed from Previous Test Rounds

Corrupt messages may not supply a receipt

One participant was not able to return the MDN of a corrupt message (compressed) without a code change. Systems could refuse to return the MDN if a corrupt message was received.

Final-Recipient contains the sender's identifier

Final-Recipient MUST contain the mailbox address of the recipient (from the From header of the MDN). Some AS1 Systems could fail on the back-end if the mailbox address is not defined within the trading partner relationship. If the Original-Recipient field is absent, the Final-Recipient field may be the only information available to identify the MDN with the message recipient.

EDI Identifier Headers

During the test cycle, participants identified AS2 headers appearing in an AS1 message. The Test Group made a conclusive decision to inspect and fail the test if AS2/AS3 header(s) appear in a message. If a message met the test criteria and did not contain any AS2/AS3 headers, the test was marked as passed; otherwise failed. All messages meet the test criteria in the Final Run, therefore demonstrating complete interoperability.

Mail Server

In order to provide protection to their networks, company mail servers are often very restrictive of the messages that are received. Combined with anti-virus software, which is often loaded on these servers, the email messages processed by the mail servers are often altered or even blocked. This can pose a serious problem with AS1 messages because this alteration can corrupt the security applied to the transaction.

The test participants had to ensure their mail servers and networks would not alter their AS1 messages in a way that created a test case failure. This required making modifications to the design of their product, a configuration change to their mail server or rerouting their email through a different mail server altogether. Since mail servers are not under the control of these AS1 products-with-version, users of the products from this test should consult with their network administrator or the customer support of their AS1 vendor in determining if their mail server could be affected by the issues listed below.

Some email servers alter the headers within an AS1 MDN which can create digital signature authentication failures. Participants resolved this issue through various modifications of configuration settings on their mail servers.

- A problem was observed due to AS1 messages which had individual lines over 1,000 characters (including terminating carriage return-line feed). Many mail servers do not support file lines of this length. AS1 products were modified so that lines of this length would not occur.
- The message-id header for one participant was modified due to a mail server. This affected the association of the returning MDN and resolved by selecting a different mail server.
- A problem was observed where the mail server was not properly reporting the email file size when downloading the AS1 message. As a result, the

message was not fully retrieved and thus not fully processed. The resolution was the selection of a different email server which did not have this bug.

Testing Requirements

In order to be part of the product test group, each participant was required to meet certain trading partner requirements and technical requirements.

Trading Partner Requirements

All participants were required to establish trading partner relationships with each other. Each participant provided their trading identifiers and security 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. Participants generated their own self-signed certificates. Some participants chose to use separate certificates for digital signing and encryption while others used one certificate for all forms of security.

Participants were responsible for distributing their Trading Partner Identifiers unique to their mail environments.

Identifiers were compliant according to RFC 2822 lexical naming standards.

Technical Requirements

In order to be part of the certified interoperable products-with-version, each participant must both successfully send and receive all tests cases with the other participants. These test cases, which can be found in the “Test Case Summary”, cover the basis of the AS1 standard. The test cases demonstrate the products-with-version fulfilled the technical requirements listed in the sections below. For additional technical information concerning these sections, refer to **RFC 3335 – MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet, Applicability Statement 1 (AS1)** found at (<http://www.ietf.org/rfc/rfc3335.txt?number=3335>).

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; MD5 was optional.

Compression

While not a part of the RFC 3335, compression is part of AS1 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.

The compression draft can be found at <http://www.ietf.org/internet-drafts/draft-ietf-ediint-compression-06.txt>.

Receipts

Along with digital signatures, receipts provide authentication of transaction. The presence of the header field "Disposition-Notification-To: *email-address*" in the message indicates a request for an MDN in the response. The nature of the underline transport dictates that the MDN is returned asynchronously. All participants were responsible for retrieving receipts from the *email-address* specified in the origin message. When a request for a signed receipt is made, the "Received-content-MIC" MUST always be returned to the requester. The "Received-content-MIC" ALLOWS for NRR (Non-Repudiation of Receipt) because the Original-Message-ID and a digital signature MUST be present. 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.

Payloads

X12, EDIFACT, and XML payloads were used in the test cases. One test case used an X12 payload of 11MB which compression was applied. The payload data used in testing were traditional POs and 1SYNC sample messages. A description of the payload files used can be found in the "Test Data" description.

Error Reporting

Products were sent erroneous signed, encrypted, and compressed messages and required to return MDNs with the appropriate error message. These tests reveal the necessity to detect message failures which directs the originator to handle the transaction according to its business desires.

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 was only used to verify successful endpoint-to-endpoint transfer and not used in any payload processing or mapping.

1. Test Data #1 (test_data_1.edi). X12 PO with an apostrophe (!) for segment terminator. Size is 12kB.
2. Test Data #2 (test_data_2.edi). X12 PO with carriage return (0x0d 0x0a) for segment terminator. Size is 3kB
3. Test Data #3 (test_data_3.xml). XML file. Size is 9kB
4. Test Data #4 (test_data_4.xml). XML PO. Size is 36kB.
5. Test Data #5 (test_data_5.edi). EDIFACT Purchase Order (PO) with standard apostrophe (") for segment terminator. Size is 6kB.
6. Test Data #6 (test_data_6.edi). EDIFACT Purchase Order (PO) with standard apostrophe (") for segment terminator. Size is 10kB.
7. Test Data #7 (test_data_7.edi). EDIFACT Purchase Order (PO) with standard apostrophe (") for segment terminator. Size is 15kB.
8. Test Data #8 (test_data_8.edi). Very large X12 file. Size is 11MB.

Test Case Criteria

This section describes the test case criteria.

Test Case: A

Test Description	The originator will send a message with different designators on the RFC1767 MIME. This test case focuses on sending a signed message requesting an unsigned receipt.
Message Payload	Test Data # 1
Message Transport	SMTP
Message Security	Signed
Message Compression	No
MDN Security	No Signature
Expected Results	The payload is successfully transferred according to the security settings. An unsigned MDN with a disposition value of "processed" is returned.

Test Case: B

Test Description	The originator will send a message with different designators on the RFC1767 MIME. This test case focuses on sending a signed message requesting a signed receipt.
Message Payload	Test Data # 2
Message Transport	SMTP
Message Security	Signature
Message Compression	No
MDN Security	Signature
Expected Results	The payload is successfully transferred according to the security settings. A signed MDN with a disposition value of "processed" is returned.

Test Case: C

Test Description	The originator will send a message with different designators on the RFC2376 MIME. This test case focuses on sending an encrypted message requesting a signed receipt.
Message Payload	Test Data # 3
Message Transport	SMTP
Message Security	Encryption
Message Compression	No
MDN Security	Signature
Expected Results	The payload is successfully transferred according to the security settings. A signed MDN with a disposition value of "processed" is returned.

Test Case: D

Test Description	The originator will send a message with different designators on the RFC2376 MIME. This test case focuses on sending a signed-encrypted message requesting a signed receipt.
Message Payload	Test Data # 4
Message Transport	SMTP
Message Security	Signed-Encryption
Message Compression	No
MDN Security	Signature
Expected Results	The payload is successfully transferred according to the security settings. A signed MDN with a disposition value of "processed" is returned.

Test Case: E

Test Description	The originator will send a message with different designators on the RFC1767 MIME. The message will be compressed without security requesting unsigned MDN. Compressed payload will adhere to the draft: draft-ietf-ediint-compression-06.
Message Payload	Test Data # 5
Message Transport	SMTP
Message Security	None
Message Compression	Yes
MDN Security	No Signature
Expected Results	The payload is successfully transferred and decompressed according to the security settings. An unsigned MDN with a disposition value of "processed" is returned.

Test Case: F

Test Description	The originator will send a signed compressed message with different designators on the RFC1767 MIME. The message will be compressed before or after the security (signed) is applied and requesting a signed MDN. Compressed payload will adhere to the draft: draft-ietf-ediint-compression-06
Message Payload	Test Data # 6
Message Transport	SMTP
Message Security	Signature
Message Compression	Yes
MDN Security	Signature
Expected Results	The payload is successfully transferred and decompressed according to the security settings. A signed MDN with a disposition value of "processed" is returned.

Test Case: G

Test Description	The originator will send a encrypted compressed message with different designators on the RFC1767 MIME. The message will be compressed before or after the security (encrypted) is applied and requesting a signed MDN. Compressed payload will adhere to the draft: draft-ietf-ediint-compression-06
Message Payload	Test Data # 7
Message Transport	SMTP
Message Security	Encrypted
Message Compression	Yes
MDN Security	Signature
Expected Results	The payload is successfully transferred and decompressed according to the security settings. A signed MDN with a disposition value of "processed" is returned.

Test Case: H

Test Description	The originator will send a signed-encrypted compressed message with different designators on the RFC1767 MIME. The message will be compressed before or after the security (signed-encrypted) is applied and requesting a signed MDN. Compressed payload will adhere to the draft: draft-ietf-ediint-compression-06
Message Payload	Test Data # 8
Message Transport	SMTP
Message Security	Signature-Encrypted
Message Compression	Yes
MDN Security	Signature
Expected Results	The payload is successfully transferred and decompressed according to the security settings. A signed MDN with a disposition value of "processed" is returned.

Test Case: I.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	SMTP
Message Security	Signed
Message Compression	No
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: I.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	SMTP
Message Security	Encryption
Message Compression	No
MDN Security	Signature
Expected Results	The MDN is returned with a disposition type, modifier and extension of “processed/error: decryption-failed”.

Test Case: I.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	SMTP
Message Security	None
Message Compression	Yes
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”.

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 AS1 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 AS1 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.

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