

## AS2 Interoperability Test

GSRN: (8018) 08622830000000597

## Final Report

First Quarter 2005 (1Q05)

April 18, 2005

Sponsored by  
Uniform Code Council, Inc. (UCC)  
[www.uc-council.org](http://www.uc-council.org)

Prepared & Facilitated By:  
DRUMMOND GROUP INC.  
[www.drummondgroup.com](http://www.drummondgroup.com)

## Table of Contents

Cover Letter .....	4
Disclaimer .....	5
Test Participants .....	6
Test History.....	9
Definitions .....	10
Interoperability Test Summary .....	11
Overview of Interoperability Testing Process .....	13
DGI In the Queue Test Round .....	13
DGI Interoperability Test Round .....	13
InSitu™ Test System.....	14
Test Requirements .....	15
Trading Partner Requirements .....	15
Technical Requirements .....	15
S/MIME encryption and digital signatures.....	15
Compression .....	16
Synchronous and Asynchronous Receipts .....	16
Transports.....	16
Payloads.....	16
Error Reporting.....	17
Optional Tests .....	18
CEM Testing.....	18
Multiple Attachment Testing.....	18
Final Test Results.....	19
Interoperability Caveats .....	20
Certificates and Security Toolkits .....	20
AS2 Identifiers.....	20
Interoperability Issues Resolved or Affirmed This Round.....	20
Interoperability Issues Resolved or Affirmed from previous Test Rounds .....	21
Appendix .....	24
Test Data.....	24
Required Test Case Overview.....	25
Test Case: A .....	26
Test Case: B .....	26
Test Case: C.....	27
Test Case: D.....	27
Test Case: E .....	28
Test Case: F .....	28
Test Case: G.....	29
Test Case: H.....	29
Test Case: I.....	30
Test Case: J.....	30
Test Case: K.1.....	31
Test Case: K.2.....	31
Test Case: K.3.....	32
Optional Test Case Overview .....	33
L.1 Certificate Exchange Messaging .....	33
L.2 AS2 Messages with Certificate Set B.....	33
M.1 XML and PDF Attachments .....	34
M.2 XML and TIF Attachments .....	34
Assigned AS2 Identifiers.....	35

About Drummond Group Inc. .... 36

## **Cover Letter**

DRUMMOND GROUP Inc. (DGI) is pleased to announce that the following participants in the AS2-1Q05 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 March 31 - April 6, 2005.

This eighth round of AS2 testing added two optional tests, certificate exchange messaging and multiple attachments, to the test scope. These tests provide further functionality and flexibility for the users of AS2. Also, the use of the DGI InSitu™ automation was implemented within nearly 75% of participating products-with-version, drastically reducing the testing effort for those participants. The next round of AS2 interoperability testing will have all participants 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

 <a href="http://www.boomi.com">http://www.boomi.com</a> <b>Product Name: Boomi AS2 Transport v3.2.0</b>	<b>Boomi Inc.</b>	 <a href="http://www.bridgeware.com">http://www.bridgeware.com</a> <b>Product Name: AS/2 Bridge v2.4</b>	<b>Bridgeware</b>
 <a href="http://www.cecid.hku.hk">http://www.cecid.hku.hk</a> <b>Product Name: Hermes Messaging Gateway v2.0</b>	<b>CECID (Center for E-Commerce Infrastructure Development)</b>	 <a href="http://www.templarsoftware.com">http://www.templarsoftware.com</a> <b>Product Name: Templar Engine v5.5</b>	<b>Classified Information, Inc.</b>
 <a href="http://www.cleo.com">http://www.cleo.com</a> <b>Product Name: VersaLex v2.3 tested in Lexicom v2.3</b>	<b>Cleo Communications</b>	 <a href="http://www.clickcommerce.com">http://www.clickcommerce.com</a> <b>Product Name: EDIINT Engine Version 7.1 tested in bTrade TDAccess v2.4</b>	<b>Click Commerce, Inc.</b>
 <a href="http://www.covast.com">http://www.covast.com</a> <b>Product Name: Covast AS2 Adapter v4.1</b>	<b>Covast</b>	 <a href="http://www.cyclonecommerce.com">http://www.cyclonecommerce.com</a> <b>Product Name: Cyclone Interchange/Activator/Central v5.3</b>	<b>Cyclone Commerce</b>
 <a href="http://www.cyclonecommerce.com">http://www.cyclonecommerce.com</a> <b>Product Name: Cyclone Interchange/Activator v4.2</b>	<b>Cyclone Commerce</b>	 <a href="http://www.edicom.es/">http://www.edicom.es/</a> <b>Product Name: Edicom AS2 Server v1.5</b>	<b>EDICOM</b>

 <a href="http://www.eds.com">http://www.eds.com</a> <b>Product Name: EDS*ELIT AS2 Connector v2.4</b>	<b>Electronic Data Systems</b>	 <a href="http://www.extol.com">http://www.extol.com</a> <b>Product Name: EXTOL Secure Engine V52 tested in EXTOL Secure V5R2.1</b>	<b>EXTOL International</b>
 <a href="http://www.gxs.com">http://www.gxs.com</a> <b>Product Name: AS2 Engine v3.6</b>	<b>Global eXchange Services, Inc.</b>	 <a href="http://www.illicom.com">http://www.illicom.com</a> <b>Product Name: ASX ONE v1.3</b>	<b>ILLICOM</b>
 <a href="http://www.inovis.com">http://www.inovis.com</a> <b>Product Name: BizManager v3.0</b>	<b>Inovis, Inc.</b>	 <a href="http://www.intercommit.nl">http://www.intercommit.nl</a> <b>Product Name: Go-direct Express v2.0/Go-direct Pro v2.0/Go-direct ISP v2.0</b>	<b>InterCommIT</b>
 <a href="http://www.isoft.com">http://www.isoft.com</a> <b>Product Name: Commerce Suite Server v3.2</b>	<b>iSoft Corporation</b>	 <a href="http://www.isoft.com">http://www.isoft.com</a> <b>Product Name: Commerce Suite Server v3.4</b>	<b>iSoft Corporation</b>
 <a href="http://www.iwaysoftware.com">http://www.iwaysoftware.com</a> <b>Product Name: iWayAdapter for AS2 v5.5 SP3</b>	<b>iWay Software</b>	 <a href="http://www.nsoftware.com">http://www.nsoftware.com</a> <b>Product Name: IP*Works! EDI/AS2 v6.5</b>	<b>/n software inc.</b>
 <a href="http://www.nubridges.com/">http://www.nubridges.com/</a> <b>Product Name: truExchange EDI-INT v3.2</b>	<b>nuBridges, LLC</b>	 <a href="http://www.oracle.com">http://www.oracle.com</a> <b>Product Name: Oracle Application Server 10g v10.1.2</b>	<b>Oracle Corporation</b>

 <p><a href="http://www.saaconsultants.com">http://www.saaconsultants.com</a></p> <p><b>Product Name: REIMS B2B Frameworks Module V5Re</b></p>	<p>SAA Consultants Ltd.</p>	 <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: Gentran Integration Suite/Sterling Integrator v4.0</b></p>	<p>Sterling Commerce</p>
 <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: Connect:Enterprise for UNIX v2.2</b></p>	<p>Sterling Commerce</p>	 <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: Connect:Enterprise for UNIX v2.3</b></p>	<p>Sterling Commerce</p>
 <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: Sterling Information Broker v3.7</b></p>	<p>Sterling Commerce</p>	 <p><a href="http://www.tibco.com">http://www.tibco.com</a></p> <p><b>Product Name: TIBCO BusinessConnect™ AS2 Transport v2.0.2</b></p>	<p>TIBCO Software Inc.</p>
 <p><a href="http://www.transentric.com">http://www.transentric.com</a></p> <p><b>Product Name: Transentric Agilink Connector AS2 v3.0</b></p>	<p>Transentric LLC</p>		



## Test History

This is the eighth AS2 Interoperability Test administered by DGI.

AS2 1Q05 Interoperability Test – February-April 2005.

GSRN: [\(8018\) 086228300000000597](#)

Previous tests included the following:

AS2 3Q04 Interoperability Test – August-September 2004.

GSRN: [\(8018\) 086228300000000429](#)

AS2 1Q04 Interoperability Test – February-March 2004.

GSRN: [\(8018\) 086228300000000245](#)

AS2 3Q03 Interoperability Test – July-September 2003.

GSRN: [\(8018\) 086228300000000085](#)

AS2 1Q03 Interoperability Test – January-February 2003.

GSRN: [\(8018\) 862283000000000015](#)

AS2 2Q02 Interoperability Test – March-August 2002.

GSRN: [\(8018\) 862283000000000043](#)

AS2 2Q01 Interoperability Test – May-August 2000

AS2 4Q00 Interoperability Test – October-December 2000

Note: The first two AS2 interoperability tests were done by Drummond Group Inc. prior to the creation of the eBusinessReady® seal.

## 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* – is that group of products, from the *Product Test Group*, which successfully completed the *Test Criteria*, in a full duplex manner with every other *Product Test Group* participant in an Interoperability Test Round without any errors in the final test Phase.

*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.

*Sealed* – a product is sealed when it is issued the eBusinessReady® ([www.ebusinessready.org](http://www.ebusinessready.org)) seal of interoperability for successfully completing an Interoperability test round.

*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 are 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 eighth round of interoperability testing for IETF AS2. AS2 (Applicability Statement 2) is the draft specification standard (RFC Standards Track) 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.

A new addition to this test round were two optional tests: certificate exchange messaging (CEM) and multiple attachments. These features build upon the core functionality of AS2 to provide valuable benefits to the end-user. Along with completing the required test case, the products from Cleo Communications, Electronic Data Systems, Inovis, Inc. and /n software completed the CEM testing, and the products from Cleo Communications, Electronic Data Systems, Global eXchange Services, Inc., Inovis, Inc. and /n software completed the multiple attachment testing.

The Interoperability Test Round was completed in ten weeks. During the first nine weeks, the testing was focused on finding and correcting interoperability errors. During March 31 - April 6, 2005, code changes and debug settings were not allowed. During this final week, the products-with-version tested with each other without error demonstrating interoperability. This final version of code from each product-with-version has been deemed interoperable.

All products-with-versions listed in the previous section (“Test Participants”) were successful in the testing without exception and were interoperable over all the Test Criteria.

## Overview of Interoperability Testing 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](http://www.drummondgroup.com) website as "In the Queue," but they will not be given product Interoperability Status on either the [www.drummondgroup.com](http://www.drummondgroup.com) or [www.ebusinessready.org](http://www.ebusinessready.org) websites.

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 Seal from the eBusinessReady® program and listed on the [www.eBusinessReady.org](http://www.eBusinessReady.org) website. The seal contains a specific GSRN number that ties each of those products together. Those products that receive the same GSRN number are deemed interoperable. However, interoperability Test Rounds must be periodically repeated to verify that as product names, versions or releases change, the product remains 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. Once fully implemented within a Product Test Group, manpower requirements for coordinating testing, aside from normal product debug needs, should be nearly non-existent.

Within an interoperability test, InSitu-enabled products are tested together under the direction of the InSitu Server and the test administrator. InSitu is only for the automation of the sending, receiving and evaluation of test cases and does not change the requirements of the test case or how the test instance result is interpreted. When testing with non-InSitu-enabled products, InSitu-enabled products had to test in the traditional manual fashion.

For this test, nearly a three-fourths of the products-with-version implemented InSitu into their systems for the automation of testing. The round of AS2 interoperability testing will have all participants using InSitu automation.

## Test Requirements

In order to complete the test, each participant was required to meet the trading partner requirements 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 SSL 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 distributing both their HTTP and HTTP/S URLs and configuring 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 used 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 the IETF draft, "HTTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet," by D. Moberg and R. Drummond ([AS2 Draft](#)).

### **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 Tests

Two sets of optional tests were introduced into this test round. These two tests were referred to as Certificate Exchange Messaging or CEM testing and multiple attachment testing. Any participant could participate in either of the tests but as they were optional they were not required to receive certification.

### CEM Testing

CEM testing is based on a new open standard (<http://www.ietf.org/internet-drafts/draft-meadors-certificate-exchange-01.txt>) which allows for the exchanging of digital certificates among active trading partners without interruption to the current trading relationship. As certificates near expiration or their security become compromised, trading partner need a means to effectively introduce new certificates into the trading relationship without downtime to their systems or their business transactions. CEM provides a secure, seamless and automated means of introducing new certificates into a trading partner relationship. Cleo, EDS, Inovis and nSoftware participated in and successfully completed CEM optional testing for this round.

### 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-00.txt>), multiple attachment testing provides for the same security used in single payload AS2 transmission. Cleo, EDS, GXS, Inovis and nSoftware participated in and successfully completed multiple attachment testing for this round.

## Final 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 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.

Between March 31 - April 6, 2005, all products-with-version listed in this test report successfully sent and received each test case with each other. Results of the test cases were reported by the participants themselves and demonstrated by supplying the messages transmitted and product logs. It is the products-with-version from these dates which are sealed as eBusinessReady interoperable.

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 Caveats**

While all the products-with-version successfully tested with each other, there are some caveats to consider in interpreting these results and using the products from this test.

## **Certificates and Security Toolkits**

Certificates and security toolkit related errors observed from this test round were reduced from previous test rounds. However, certificates with 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. A list of the public-key certificates used by the participants in the test round may be found on the DGI website at: <http://www.drummondgroup.com/html-v2/standards.html>

## **AS2 Identifiers**

A variety of AS2 identifiers were used by the products of this test. These identifiers contained spaces, colons, dashes and other printable characters along with alphanumeric characters. A list of the assigned AS2 identifiers can be found in the Appendix.

However, there were some products which could not accept certain characters or certain strings of AS2 identifiers. Two issues observed in this round include having a space (" ") at the third location, e.g. "AS 2" and 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.

## **Interoperability Issues Resolved or Affirmed This Round**

During the course of this interoperability tests, two 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 here 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.

- A consensus item from a previous test was that quotation marks around parameter values within MIME headers should not be used unless it is stipulated by the standard. After examining latest version of MIME and IETF standards, this decision was removed and products must follow syntax guidelines for accepting quotation marks per the rules of the underlining standards.
- 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.

## **Interoperability Issues Resolved or Affirmed from previous Test Rounds**

- 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.
- 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:
  - Original-Message-ID:<123foo@example>
  - Original-Message-ID: <123foo@example>
- The Message-ID header is not required in MDNs.
- 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.
- 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.
- Certificate serial numbers must not be negative, per RFC3280. While some AS2 systems are accepting of

negative serial numbers, other systems cannot accept negative values.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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".

- 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.

## Appendix

### 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 Case Overview

The Required Test Case Overview describes the test cases each participant sent 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 #3	HTTP	Encrypted	Yes	Sync	Signed
E	Data #2	HTTP	Encrypted	No	Sync	Signed
F	Data #2	HTTP	Signed	No	Sync	Signed
G	Data #3	HTTPs	Signed	Yes	Sync	Signed
H	Data #1	HTTPs	Signed	No	Async/HTTP	Signed
I	Data #4	HTTPs	Signed	No	Async/HTTPs	Signed
J	Data #5	HTTP	Signed/Encrypted	Yes	Async/HTTP	Signed

Test cases K1-K3 are error scenario test cases and were conducted with the DGI test administrator and the participant.

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

## Test Case: A

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

## Test Case: B

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

## Test Case: C

<b>Test Description</b>	The initiator creates a signed, encrypted exchange over HTTP with a request for an asynchronous, signed MDN.
<b>Message Payload</b>	Test Data # 3
<b>Message Transport</b>	HTTP
<b>Message Security</b>	Signed, Encryption
<b>Message Compression</b>	No
<b>MDN Transport</b>	Asynchronous/HTTPs
<b>MDN Security</b>	Signature
<b>Expected Results</b>	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

<b>Test Description</b>	The initiator creates an encrypted, compressed exchange over HTTP with a request for a synchronous, signed MDN.
<b>Message Payload</b>	Test Data # 3
<b>Message Transport</b>	HTTP
<b>Message Security</b>	Encryption
<b>Message Compression</b>	Yes
<b>MDN Transport</b>	Synchronous
<b>MDN Security</b>	Signature
<b>Expected Results</b>	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

## Test Case: E

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

## Test Case: F

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

## Test Case: G

<b>Test Description</b>	The initiator creates a signed, compressed exchange over HTTPs with a request for a synchronous, signed MDN.
<b>Message Payload</b>	Test Data # 3
<b>Message Transport</b>	HTTPs
<b>Message Security</b>	Signature
<b>Message Compression</b>	Yes
<b>MDN Transport</b>	Synchronous
<b>MDN Security</b>	Signature
<b>Expected Results</b>	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

## Test Case: H

<b>Test Description</b>	The initiator creates a signed exchange over HTTPs with a request for an asynchronous, signed MDN over HTTP.
<b>Message Payload</b>	Test Data # 1
<b>Message Transport</b>	HTTPs
<b>Message Security</b>	Signature
<b>Message Compression</b>	No
<b>MDN Transport</b>	Asynchronous/HTTP
<b>MDN Security</b>	Signature
<b>Expected Results</b>	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

<b>Test Description</b>	The initiator creates a signed exchange over HTTPs with a request for an asynchronous, signed MDN.
<b>Message Payload</b>	Test Data # 4
<b>Message Transport</b>	HTTPs
<b>Message Security</b>	Signature
<b>Message Compression</b>	No
<b>MDN Transport</b>	Asynchronous/HTTPs
<b>MDN Security</b>	Signature
<b>Expected Results</b>	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

<b>Test Description</b>	The initiator creates a signed, encrypted, compressed exchange over HTTP with a request for an asynchronous, signed MDN.
<b>Message Payload</b>	Test Data # 5
<b>Message Transport</b>	HTTP
<b>Message Security</b>	Signed, Encryption
<b>Message Compression</b>	Yes
<b>MDN Transport</b>	Asynchronous/HTTP
<b>MDN Security</b>	Signature
<b>Expected Results</b>	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**

<b>Test Description</b>	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.
<b>Message Payload</b>	Test Data # 1
<b>Message Transport</b>	HTTP
<b>Message Security</b>	Signed
<b>Message Compression</b>	No
<b>MDN Transport</b>	Synchronous
<b>MDN Security</b>	Signature
<b>Expected Results</b>	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**

<b>Test Description</b>	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.
<b>Message Payload</b>	Test Data # 1
<b>Message Transport</b>	HTTP
<b>Message Security</b>	Encryption
<b>Message Compression</b>	No
<b>MDN Transport</b>	Synchronous
<b>MDN Security</b>	Signature
<b>Expected Results</b>	The MDN is returned with a disposition type, modifier and extension of “processed/error: decryption-failed”.

**Test Case: K.3**

<b>Test Description</b>	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.
<b>Message Payload</b>	Test Data # 1
<b>Message Transport</b>	HTTP
<b>Message Security</b>	None
<b>Message Compression</b>	Yes
<b>MDN Transport</b>	Synchronous
<b>MDN Security</b>	Signature
<b>Expected Results</b>	The MDN is returned with a disposition type, modifier and extension of either “processed/error: decompression-failed” or “unexpected-processing-error”.



## Optional Test Case Overview

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

### L.1 Certificate Exchange Messaging

#### L.1 Description

Both the participant and their trading partner load new certificate set (Set B) through CEM messages.

#### L.1 Test Configuration

##### Certificate Exchange Message Request

**Transport:** HTTP

**Security:** Signature

**Compression:** No

**MDN Transport:** Synchronous, signed

#### L.1 Expected Results

CEM Response messages are received with CertStatus values of "Accepted" for each certificate in Certificate Set B.

### L.2 AS2 Messages with Certificate Set B

#### L.2 Description

With Certificate Set B now loaded for both the participant and their trading partner, both participant and trading partner send two messages, Message A and Message B, to each other for a total of four messages. Message A is signed over HTTPS, and Message B is encrypted over HTTP. Both request a signed MDN. Goal is to verify Certificate Set B have been properly configured.

#### L.2 Test Configuration

##### Message A

**Payload:** Test Data # 1 (X12)

**Transport:** HTTPS

**Security:** Signature, Encryption

**Compression:** No

**MDN Transport:** Synchronous, signed

#### L.2 Expected Results

All MDNs are returned with a disposition value of "processed".

## 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

#### Certificate Exchange Message Request

**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

#### Certificate Exchange Message Request

**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 Identifiers

ZZboomi  
Bridge-ware  
CeCid & AS2  
CLEO  
48661000038  
Covast!  
Cyclone One  
Cyc. #2  
EDlcom-AS2  
EDS \*Elit  
Extol;AS2  
GXS Interop  
InterCommIT  
illicom@example.org  
Inovis (InSitu)  
iSoft [test]  
iSoft-2  
iWay::AS2  
n/Software  
nuBridges  
Oracle+AS2  
SAA  
Sterling\_1  
SterComm-2  
SC\_No. 3  
Sterling Five  
01-02488901-510  
[www.tibco.com](http://www.tibco.com)  
Transentric

## **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](http://www.drummondgroup.com) or email: [info@drummondgroup.com](mailto:info@drummondgroup.com).