

## ***REPORT TO THE UNIFORM CODE COUNCIL (UCC)***

---

***AS2 Conformance Validation***

***Final Status***

***Test Round AS2-4Q00***

***December 12, 2000***

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

## Abstract

AS2 (Applicability Statement 2) is the draft specification standard (RFC Standards Track) by which vendor applications communicate EDI (EDIFACT or X.12) data over the Internet. AS2 is an expansion of the AS1 specification (which specifies EDI data transmission over SMTP) to provide for EDI data transmission over HTTP.

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, the systems are put through a series of three Test-Steps, each containing three Test-Groups (or some subset thereof). The Test-Groups are designed to test and discover weaknesses with vendor systems and to build upon previous tests until full compliance is realized. The first Test-Group is composed of exchanging Security Certificates (*certs*) and basic EDI data. Since this test is focused on EDI transactions, the data is exclusively X.12 or EDIFACT. The data ranges from small data files to very large (50MB) files. Once it has been established that participants can transfer data successfully, the participants are then asked (in the second Test-Group) to pass the data securely in all combinations of digitally signing and encrypting the data. Finally (in the third Test-Group), the signed/encrypted data is passed with requests for receipts or MDNs (Message Disposition Notifications) in all combinations of digitally signing and encrypting the MDN. As an addendum, some purposely erroneous data was also exchanged to test the reaction of each system under error conditions.

This test is not just focused on determining who can pass the test, although that is the end result, but on encouraging and promoting interoperability between the participating vendors. By slowly building the interoperability features and allowing vendors to correct, or debug their code during the process, the end result is an entire suite of interoperable products. As this paper reports, all the vendors<sup>1</sup> passed the final test (a subset of the entire test structure encompassing the hardest tests along with a sampling of the easier ones).

The entire test was conducted over a eight-week period, the first step (debug) was completed in five weeks. A one week break then ensued to give participants time to recompile code (remove debug features) and reinstall. The second step (Dry-Run) then took one week – to prepare participants for the final test. The final test was conducted the following week.

---

<sup>1</sup> Two additional vendors began the test but dropped out early in the process. Those vendor's names or products are not mentioned in this paper.

## The Conformance Test

### *What is the AS2 Compliance Validation Test?*

The process for each **Test Round** has three, interrelated Test-Steps. Each **Test-Step** is composed of three Test-Groups (or some subset of these). Each **Test-Group** has a series of **Tests**.

#### **Test Round AS2-4Q00 (4<sup>th</sup> Quarter 2000)**

##### ***Test-Step-1 (Debug Step)***

Complete all tests from each Test-Group to allow Code Check & Debug. There are three Test-Groups comprising tests A through L.

##### ***Test-Step-2 (Dry Run)***

Software installed from scratch following “written” install procedure as it appears in the Product-with-version Installation Manual.

Run some subset of the tests (at least one test from each Test-Group – e.g. Tests A, E, F.3, J)

##### ***Test-Step-3 (Final Compliance Validation)***

Final Verification and official compliance test. One or Two Day Event (no product fixes or code debug activities will be allowed). Successful test completion demonstrates Interoperability to UCC/DGI satisfaction.

#### **Test Round AS2-xQ01 (Date TBD)**

There will be other rounds of testing annually (or semi-annually as required). Continued UCC sanctioned AS2 Interoperability **Compliance Validation** will require each Product-with-Version to participate in future Testing Rounds to retain their compliance rating.

#### **Test Round AS2-xQ02 (Date TBD)**

Each subsequent Test-Round is composed of the same three Test-Steps as described above.

### *Test-Steps*

**Test-Step-1 (Debug)** is designed to help companies implement interoperable products by conducting a series of product verification tests. (Test-Step-1 testing is composed of three Test-Groups. Test-Group-1 is MIME-only tests, Test-Group-2 is S/MIME tests and Test-Group-3 is Signed-Receipt tests.) In Test-Step-1, product developers learn and adjust their products as they go. Test-Step-1 testing is conducted periodically –

usually at least once a year or when three or more new products become available to establish a new Test-Group.

**Test-Step-2** (Dry-Run) is to make sure the participants are ready for the final test.

**Test-Step-3** (Final) is the AS2 Compliance Validation.

## *Test-Groups*

**Test-Group-1** is composed of Tests A through E. Once a company has completed Test-Group-1, their product-with-version is deemed interoperable with those of their Test-Group-1 Test-Group. Test-Group-1 must be completed before advancing to Test-Group-2.

**Test-Group-2** consists of completing Tests F.1 through F.4 (test data transfers without MDN -- signed and encrypted tests) and

**Test-Group-3** consists of Tests G through L (test data transfers with MDN) with all other products that have previously been verified. Again, this must be completed to UCC/DGI's satisfaction. Once this has been accomplished, UCC will verify the product as *AS2 Conformance Validated*. If the code of a previously tested product is changed, the product-with-version must go back through Test-Group-2 & Test-Group-3 testing to ensure interoperability with all the other products.

After a product has completed Test-Group-2 & Test-Group-3 testing in a manner that is satisfactory to UCC, the product-with-version must be commercialized and released within 90 days of completion of Test-Step-3. If the product-with-version is not released within 90 days, *Conformance Validation* will be withdrawn and the product-with-version will be required to complete Test-Group-2 & Test-Group-3 testing again.

## *Compliance Validation*

UCC *Compliance Validation* of a product-with-version will be issued when the following have been completed to UCC/DGI's satisfaction: the product-with-version has passed Test-Steps-3 as defined in this document. This means that each product must exchange information as described in Tests A through L between all products-with-version that have previously passed Test-Step-3 tests.

## **Test Specifics**

To see the text of each of the final tests, please refer to the [Appendix](#).

## **Interoperability Caveats**

### *Testing Conditions*

Interoperability is highly dependant upon test conditions and specifications. Altering or exceeding the conditions under which the test is performed may significantly alter the interoperability results.

Although higher levels of security are available, it was deemed sufficient and prudent to perform the tests using the following certificate data:

### **Client Certificates**

- 128/1024 bit encryption
- Triple DES
- SHA1 (preferred) or MD5

### **Server Certificates**

- SSL port 443 (unless otherwise specified)
- Server Side Authentication only
- No Basic Authentication (not necessary although supported in most cases)

### *File Size*

Although very large file size was tested (50MB) this scenario did not go through rigorous, full matrix testing (all participants to all other participants). Each participant demonstrated the ability to send and receive files of this size to at least two other participants. Very large file encryption/decryption/signing can be very bandwidth and processor intensive. Due to time constraints and test platform limitations, the maximum file size for encryption/decryption/signing and MDN testing was limited to 10MB. Files larger than this were deemed to be a test of the test environment rather than of the software.

Some participants did attempt to perform 50MB encrypted/signed transfers and problems were found with timeouts and synchronous MDN deliveries (sender might timeout while waiting for the MDN to be delivered). This was found to be a limitation on the standard and some work-around was needed. Some participants performed this side test successfully.

### *Folded Headers*

There have been problems detected when sending folded headers (headers continued on multiple lines) to systems on Microsoft Internet Information Server (IIS). Microsoft does not currently have any plans to correct this problem in the current version of IIS. They have indicated this may be corrected in a future release.

Several of the participants are planning MVS (mainframe) implementations which will require the use of folded headers (line lengths need to be

shorter than 76 characters). This will prevent interoperability between these mainframe implementations and systems running on IIS.

As a work-around, all participants removed folded headers for products in this test.

### Certificate Header Field Population








Some systems have experienced difficulties with some certificates -- specifically those built with multiple attributes. A certificate contains a series of **Sequences**. Each **Sequence** may contain a series of **Sets**. While all toolkits retain the Sequence order in security operations, some may reorder Sets within a given Sequence. While this is not specifically incorrect, it may cause problems interoperating with toolkits which expect the order to be respected.

The work-around for this problem is to put only one **Set** per **Sequence**. The RSA toolkit allows this using the New-Line-Flag option.

### Certificate Types

Certificate exchange/installation is typically the most difficult type of problem encountered during installation in the *real-world*. We tested certificates as thoroughly as possible. Certificates were generated multiple times (per participant) by Verisign, Entrust and some individual participants (those whose systems had this capability -- not required). Certificates were created with a variety of fields filled in, with and without *urls*, and with/without a trusted root (self-signed certificates). Many problems were encountered and corrected. The only problem unsolved was the single Sequence/multiple attribute problem (documented above).

### Test Participants

 <b>Trade.com</b> <small>Deploying e-Business Networks</small> <b>bTrade</b> Product Name: EDIINT for Secure Access 2000 Version: 1.38	 <b>Compaq Computer</b> Product Name: Compaq ASx Transport Service (CATS) Version: 2.0
 <b>Cyclone Commerce</b> Product Name: Cyclone Interchange Version: 3.1	 <b>IPNet Solutions</b> Product Name: eBizness Secure Messaging Component (part of eBizness Transact v3.3)
 <b>Netfish Technologies</b> Product Name: XDI Suite Version: 4.2	 <b>Sterling Commerce</b> Product Name: E-Marketplace Enabling Services Version: 3.3
 <b>webMethods, Inc.</b> Product Name: webMethods B2B Version: 3.6	

### Test Results

## AS2 - EDI Interoperability Testing Status Report - Final

Receive: lower case  
Send UPPERCASE

Only success is shown below

Test	A	F.4	G.3	H.1	H.2	H.3	H.4	Status
	12/11/00	12/11/00	12/11/00	12/11/00	12/11/00	12/11/00	12/11/00	
A bTrade	bcdegi BCDEGI	bcdegi BCDEGI	bcdegi BCDEGI	bcdegi BCDEGI	bcdegi BCDEGI	bcdegi BCDEGI	bcdegi BCDEGI	Done 12/12/00
B Compaq	acdegi ACDEGI	acdegi ACDEGI	acdegi ACDEGI	acdegi ACDEGI	acdegi ACDEGI	acdegi ACDEGI	acdegi ACDEGI	Done 12/12/00
C Cyclone Commerce	abdegi ABDEGI	abdegi ABDEGI	abdegi ABDEGI	abdegi ABDEGI	abdegi ABDEGI	abdegi ABDEGI	abdegi ABDEGI	Done 12/11/00
D IPNet Solutions	abcegi ABCEGI	abcegi ABCEGI	abcegi ABCEGI	abcegi ABCEGI	abcegi ABCEGI	abcegi ABCEGI	abcegi ABCEGI	Done 12/12/00
E Netfish	abcdgi ABCDGI	abcdgi ABCDGI	abcdgi ABCDGI	abcdgi ABCDGI	abcdgi ABCDGI	abcdgi ABCDGI	abcdgi ABCDGI	Done 12/11/00
G Sterling Commerce	abcdei ABCDEI	abcdei ABCDEI	abcdei ABCDEI	abcdei ABCDEI	abcdei ABCDEI	abcdei ABCDEI	abcdei ABCDEI	Done 12/12/00
I Web Methods	abcdeg ABCDEG	abcdeg ABCDEG	abcdeg ABCDEG	abcdeg ABCDEG	abcdeg ABCDEG	abcdeg ABCDEG	abcdeg ABCDEG	Done 12/12/00

Note: Missing rows F and H represent participants who dropped out of the testing at an early stage.

Uppercase indicates successful send. (e.g. if bTrade has a “d” under test A this indicates a successful send to IPNet. Lower case indicates successful receive. All participants submit a cumulative status sheet after each test (see below) and the results are summarized on the table above.

### AS2 - EDI Interoperability Testing Status Report - Final Round

S = Sent v = verified by receiver Example: Sm/Rm = Sent/MDN / Received/MDN

R = Received, p = processed OK and sent back verification, m = sent back appropriate MDN

for: **Compaq**  
as of: **Dec 12, 2000 , 7:30AM (CST)**  
E = Error detected - fix and resend, b= bounced

Test	A	F.4	G.3	H.1	H.2	H.3	H.4	Status
bTrade	S/R	Sv/Rv	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	DONE
Compaq	*	*	*	*	*	*	*	
Cyclone Commerce	S/R	Sv/Rv	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	DONE
IPNet Solutions	S/R	Sv/Rv	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	DONE
Netfish	S/R	Sv/Rv	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	DONE
Sterling Commerce	S/R	Sv/Rv	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	DONE
Web Methods	S/R	Sv/Rv	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	Sm/Rm	DONE

\*Note: This is a sample report sheet for Compaq, i.e. no data in the Compaq row.

## **About DRUMMOND GROUP, INC.**

The Drummond Group, Inc. . ([www.drummondgroup.com](http://www.drummondgroup.com)) provides B2B strategy, research analysis, and industry pilot facilitation. Founded by Rik Drummond, a recognized leader in eBusiness and international standards organizations, the group represents best-of-breed in the industry on horizontal infrastructure technologies and standards which support B2B commerce. Key areas include XML, Internet EDI, PKI, EAI, architecture, integration, interoperability and B2B business models. Drummond Group offers an integrated vendor neutral approach that concentrates on the intersection of technology, business processes, and culture of an organization to build strategy that reduces risk, lowers cost, and fosters e-Business. For further information, please contact Beth Morrow at [Beth@drummondgroup.com](mailto:Beth@drummondgroup.com)

## Appendix

### *Test A Certificate Exchange*

Test Description: Exchange of certificates by eMail in "certificate-only PKCS#7 in S/MIME" between all test members. This means that S/MIME certificate-only messages are to be enclosed in application/PKCS#7-MIME. MIME headers.

Originator

- A.1 With URL
- A.2 Without URL
- A.3 Self Certified
- A.4 Certification Authority Certified

Recipient

- Interpret URL
- Does not require URL
- Interprets Certificate correctly
- Interprets Certificate correctly

Test Setup: The URL, which matches the source URL EDI translator address SHOULD be carried in the certificate. However, the receiver SHOULD NOT expect that the certificate will contain a URL. The complete certification chain MUST be included in all certificates. All certificate verifications MUST "chain to root". In the case of a self signed certificate the certificate is signed by itself. Note the sender may send one or more combinations of the test above. The receiver should be able to interpret A.1/A.3, A.1/A.4, A.2/A.3 and A.2/A.4 combinations. Additionally, the certificate hash should match the hash recomputed by the receiver.

Data Used: N/A

### *Test F.4: Signed then Encrypted – Included Certificate*

**Test Description:** The data from Test D is signed per the draft\_ietf\_edint\_as2\_07.txt specification and encrypted for confidentiality. For this test, the Certificate SHOULD be included. All participants should be able to receive data with, or without, an included Certificate.

**Test Setup:** 1024-bit key length for signature, triple DES for encryption, and SHA1 or MD5 message digest.

**Data Used:** Test B or similar data.

**Expected Results:** The decrypted data is the same as that sent, the signature is appropriate, and the message digest is correct.

*Test G: Receipt Request /Unsigned Receipt Returned*

**Test Description:** The initiator creates a normal exchange as in Tests <B | E>. The presence of the header field “MDN-request-header” (“Disposition-Notification-To:” *url*) in the message indicates to the receiving system that an unsigned Message Disposition Notice (MDN) is expected to be received by the exchange initiator.

**Note:** This is several tests using different combinations of signed and encrypted messages.

<u>Originator</u>	<u>Recipient returns a MDN</u>
- G.1 Signed	Unsigned
- G.2 Encrypted	Unsigned
- G.3 Signed/ Encrypted	Unsigned

**Test Setup:** Use Tests < B | E > as the basic data with the presence of the “Disposition-Notification-To:” to indicate the request of a receipt (unsigned-receipt). A MDN request SHOULD never be ignored between EDI – UA’s that support these recommendations.

Originator: MDN-request-header = “Disposition-Notification-To:” initiator’s EDI gateway address.

Recipient: Normal EDI processing set.

*The message originator processing may include:*

Turn on “MDN expected” for this transaction

Set time-based counter for expecting an MDN

Reconcile received MDN and sent messages for the fields: Reporting-UA:, Original-Recipient:, Final-Recipient:, Original-Message-ID:, and Disposition:

Identify lost or delayed messages based on no MDN

Determine whether automated process can occur based on MDN message content

*The original message receiver processing should include:*

Turn on “Send MDN”

Verify the MDN format

Set time-based counter for returning an MDN

Return MDN with appropriate status (disposition)

**Data Used:** *TBD at the time of the test.*

*Continued...*

**Expected Results:** The return of a MDN to the “EDI gateway address” (the address in the “Disposition-Notification-To:” *url*) with the following contents:

- MDN Bodypart 1:

The message sent on YYYY MMM DD at HH:MM:SS (EDT) -0400 to <*url*> with subject “AAAAAAAAAAAA” has <” been processed” | “been processed with warning” | “been processed with error” | “failed”>. This is not a guarantee that the EDI message has been completely processed or understood by the receiving translator.

*Note:* This section may be any type of text, the above is an example only.

- MDN Bodypart 2:

Return one of the following for the disposition field:

Disposition: automatic-action/MDN-sent-automatically; processed

Disposition: automatic-action/MDN-sent-automatically; processed/ error

Disposition: automatic-action/MDN-sent-automatically; processed/ warning

Disposition: automatic-action/MDN-sent-automatically; failed

**Notes:**

- Original-Recipient and Final-Recipient could be different
- The value in Original-Message-ID should match the original Message-ID header value
- Disposition: Each testing agent should return a different disposition status code to the initiator

- MDN Bodypart3:

This bodypart SHOULD be blank or missing for HTTP.

*Test H: Receipt Request /Signed Receipt Returned*

**Test Description:** The initiator creates a normal exchange as in Tests < B | E >. The presence of the header field “MDN-request-header” (“Disposition-Notification-To:” *url*) in the RFC822 message headers indicates to the receiving system that a Signed-Message Disposition Notice (MDN) is expected to be received by the exchange initiator. Both of these must be present for Test H.

**Note:** This is several tests using different combinations of signed and encrypted messages.

<u>Originator</u>	<u>Recipient returns a MDN</u>
- H.1 Signed/HTTP	Signed
- H.2 Signed/ HTTPS	Signed
- H.3 Encrypted	Signed
- H.4 Signed/Encrypted	Signed

**Test Setup:** Use Tests < B | E > as the basic data with the presence of the  
Disposition-Notification-To: *url*  
Disposition-notification-options: signed-receipt-protocol=optional,pkcs7-signature;  
signed-receipt-micalg=optional, sha1, md5  
to indicate the request for a signed-receipt. A MDN request should never be ignored between EDI-UA’s that support these recommendations.

*The message originator processing may include:*

- Turn on “Signed-MDN expected” for this transaction
- Set time-based counter for expecting a Signed-MDN
- Reconcile received MDN and sent messages for the fields: Reporting-UA:,  
Original-Recipient:, Final-Recipient:, Original-Message-ID:, Disposition:,  
Signed-receipt-disposition:, and Received-content-MIC:
- Identify lost or delayed messages based on no MDN
- Determine whether automated process can occur based on MDN message content

*The original message receiver processing should include:*

- Turn on “Send signed-MDN”
- Verify the request format and the signature
- Set time-based counter for returning an MDN
- Return Signed-MDN with appropriate status (disposition codes)

Recipient: Normal EDI processing set.

**Data Used:** *TBD at the time of the test.*

*Continued...*

**Expected Results:** The return of a signed-MDN to the “EDI gateway’s address” (the address in the “Disposition-Notification-To:” string) with the following contents:

- MDN Bodypart 1:

The message sent on YYYY MMM DD at HH:MM:SS (EDT) -0400 to <url> with subject “AAAAAAAAAAAA” has <” been processed” | “been processed with warning” | “been processed with error” | “failed”>. This is not a guarantee that the EDI message has been completely processed or understood by the receiving translator.

This is not a guarantee that the EDI message has been completely processed or understood by the receiving translator.

*Note: This section may be any type of text; the above is an example only.*

- MDN Bodypart 2:

Return one of the following for the disposition field:

- Received-content-MIC: Q2hlY2sgSW50XwdyaXRIQ, <SHA1 | MD5>  
Disposition: automatic-action/MDN-sent-automatically; processed
- Disposition: automatic-action/MDN-sent-automatically; processed
- Disposition: automatic-action/MDN-sent-automatically; processed/error
- Disposition: automatic-action/MDN-sent-automatically; processed/warning
- Disposition: automatic-action/MDN-sent-automatically; failed

If the above error condition is blank or omitted there is assumed to be no error.

**Notes:**

- For testing purposes Original-Recipient and Final-Recipient should be the same.
- The value in Original-Message-ID should match the original Message-ID header value. Each tester should pick a different value for the test.
- Signed-receipt-disposition: Each tester should pick a different value for the test
- The Received-content-MIC: should match the MIC of the original message in Base64 content transfer type encoding
- Received-content-MIC: The test default is Base64 transfer encoding
- The identity of the signature of the entire signed-MDN may not match the From: field of the message

- MDN Bodypart3:

This bodypart SHOULD be blank or missing for HTTP.