

Report to the Uniform Code Council (UCC)

AS2 Conformance Validation

Final Status

Test Round AS2-2Q02

August 27, 2002

Report to the Uniform Code Council (UCC)

AS2 Conformance Validation

Final Status

Test Round AS2-2Q02

Prepared By:

DRUMMOND GROUP, INC.

www.drummondgroup.com

Test Participants







DRUMMOND GROUP, Inc. is pleased to announce that the following participants in the AS2 Conformance Validation & Interoperability Test 2Q02 have completed all requirements and passed tests (*see Final Test Results*) between each product demonstrating interoperability and conformance to the AS2 document. Minor exceptions to full interoperability are noted below.


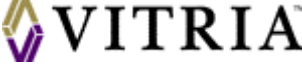

To fully understand what completing the test means in the use of the products in production, please read this document carefully.

Workarounds were necessary in some cases and we continue to find immaturity in the interoperability between PKI toolkits. Both of these issues are documented below (*see Interoperability Caveats*).

Sincerely,

Rik Drummond
CEO Drummond Group Inc.

 <p>bTrade, Inc. Transaction Delivery Networks http://www.btrade.com Product Name: TDAccess, TDPeer, TDNgine, TDBrowser using EDIINT engine, vs. 3.0</p>	 <p>Cleo Communications http://www.cleo.com Product Name: Cleo LexiCom, vs. 2.0</p>
 <p>Hewlett Packard http://www.hp.com/hps Product Name: Compaq ASx Transport Service (CATS), vs. 3</p>	 <p>Cyclone Commerce http://www.cyclonecommerce.com Product Name: Cyclone Interchange/Activator, vs. 4.2</p>
 <p>Cyclone Commerce http://www.cyclonecommerce.com Product Name: Cyclone Interchange/Activator, vs. 4.1.3</p>	 <p>Global eXchange Services http://www.gxs.com/gxs/products/product/enterprise Product Name: Enterprise System™, vs. 7.5</p>
 <p>InterTrade Systems Corporation Intelligent Commerce http://www.intertrade.com Product Name: TradeLinks, vs. 2.5</p>	 <p>IPNet Solutions, Inc. http://www.ipnetsolutions.com Product Name: IPNet eBizness™ Transact, vs. 3.6</p>
 <p>IPNet Solutions, Inc. http://www.ipnetsolutions.com Product Name: IPNet BizManager™, vs. 2</p>	 <p>iSoft http://www.isoft.com Product Name: iSoft Peer-to-Peer Agent, vs. 3.1</p>
 <p>Sterling Commerce http://www.sterlingcommerce.com * Product Name: Sterling Integrator, vs. 2.0</p>	 <p>Sterling Commerce http://www.sterlingcommerce.com * Product Name: Sterling Information Broker, vs. 3.5</p>

 <p>TIBCO The Power of Now™</p> <p>http://www.tibco.com Product Name: TIBCO BusinessConnect™ AS2 Transport, vs. 1.0.0</p>	 <p>VITRIA Vitria</p> <p>http://www.vitria.com Product Name: BusinessWare B2Bi Server, vs. 1.4</p>
 <p>webMethods webMethods</p> <p>http://www.webmethods.com Product Name: webMethods Integration Platform, vs. 4.6</p>	

Please note that for the remainder of the document, the following names will be used for the products that were tested:

TDAccess, TDPeer, TDNgine, TDBrowser using EDIINT engine, vs. 3.0 will be referred to as bTrade.

Cleo LexiCom, vs. 2.0 will be referred to as Cleo.

Compaq ASx Transport Service (CATS), vs. 3 will be referred to as Compaq.

Cyclone Interchange/Activator, vs. 4.2 will be referred to as Cyclone I.

Cyclone Interchange/Activator, vs. 4.1.3 will be referred to as Cyclone II.

TradeLinks, vs. 2.5 will be referred to as InterTrade.

IPNet eBizness Transact, vs. 3.6 will be referred to as IPNet I.

IPNet BizManager, vs. 2 will be referred to as IPNet II.

ISoft Peer-to-Peer Agent, vs. 3.1 will be referred to as iSoft.

Sterling Integrator, vs. 2.0 will be referred to as Sterling I.

Sterling Information Broker, vs. 3.5 will be referred to as Sterling II.

TIBCO BusinessConnect AS2 Transport, vs. 1.0.0 will be referred to as Tibco.

BusinessWare B2Bi Server, vs. 1.4 will be referred to as Vitria.

webMethods Integration Platform, vs. 4.6 will be referred to as webMethods.

*

© 2002 Sterling Commerce, Inc.

All rights reserved. Sterling Commerce and the Sterling Commerce logo are trademarks of Sterling Commerce, Inc. or its affiliated companies.

Abstract

This is the third round of 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 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 discover and correct 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 and XML data. This test is focused primarily on EDI transactions. The data is mostly X12 or EDIFACT but also includes an XML file. 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 Notification reports) both unsigned and digitally signed MDNs, including non-Repudiation of Receipt (NRR) hashing. As an addendum, some purposely-erroneous data is also exchanged to test the reaction of each system under error conditions.

New to this test round is the addition of compression. While not a requirement of AS2, compression has become a highly demanded addition for AS2 systems. As a result, it has been included in the J tests in the third Test-Group.

This test suite is not just focused on determining who can pass the tests, although that is the end result, but on encouraging and promoting interoperability between the participating vendors. By slowly building upon previous tests, proving conformance to the standards, working with other vendors to ensure interoperable features and allowing participants to correct or debug their code during the process, the end result is an entire community of AS2 interoperable products.

As this paper reports, all the vendors passed the final test (a subset of the entire test suite encompassing the most complex test, which also test simpler tests). However, there were some exceptions that should be noted. The H.3 Test involving asynchronous MDNs via email (SMTP) was made

optional to the participants. GXS elected not to participate in the H.3 Test. Also regarding the H.3 Test, Vitria elected to receive asynchronous SMTP MDN requests but elected not to request asynchronous SMTP MDNs themselves. All other vendors fully participated in this test.

Also, since Cyclone II is an existing AS2 product (AS2 version 1.0) and does not support compression, it did not participate in any of the J Tests involving compression testing.

The entire test was conducted over a twenty-two week period, the First test-step (debug) was completed in seventeen weeks. The Second test-step (Dry-Run) then took three weeks. Because of corrections in the AS2 specification midway through the debug testing, a second Dry-Run was added to prepare participants for the final test. The Third test-step (Final-Run) was conducted over the following two weeks.

Test Additions

There are two notable additions to this round of interoperability testing. One is the addition of compression testing, and the second is use of a modified standard of AS2 headers and their implementations. Since both of these additions affect the interoperability stance of the vendors and backwards compatibility, they are specifically addressed in the sections below.

AS2 Version Header

Within this round of AS2 interoperability testing, it was decided to add an AS2 Version Header to help with both backwards compatibility and potential future AS2 additions. Products in this round on interoperability testing added this header with the value of *1.1*. The version header will indicate the addition of AS2 functionality. The *1.1* version in these current AS2 products indicates the sending system supports all of the AS2 basic functionality of the current draft and compression as it is defined in the EDIINT Compression Draft specification. Future rounds of AS2 testing may use a different version if additional functionality has been added. The presence of this header does not hinder interoperability with older versions of AS2.

Compression

Because of repeated requests from supply-chains, compression was added to this round of interoperability testing. For more information on the compression procedure used in these tests, refer to the IETF draft, "Compressed Data for EDIINT", by T. Harding ([draft-ietf-ediint-compression-01.txt](#)).

For all new products or new versions of existing products in this test round, compression was added and tested. This included all products except for the Cyclone Interchange vs. 4.1.2, which is an older AS2 product that does not support compression. To differentiate between versions of AS2 that support compression and those that do not, new product-versions added an AS2 Version Header with a version of *1.1* to their products. For more information on the version, refer to the latest version of the AS2 draft.

AS2 System Identifiers

Because of confusion with vendors on acceptable names for the AS2-To and AS2-From headers, the naming convention for these headers was modified. AS2 1.1 products implemented these changes. Refer to the latest version of the AS2 draft for more information. Some issues with interoperability arose in the testing of these system identifiers (*see [Interoperability Caveats](#)*).

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 (4th Quarter 2000)

Test Round AS2-2Q01 (2nd Quarter 2001)

Test Round AS2-2Q02 (11 March 2002)

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 J.

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.4, F.3, G.5)

Test-Step-3 (Final Conformance Validation)

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

Test Round AS2-xQ0X (Date TBD)

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

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

Test-Steps

Test-Step-1 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-Groups

Test-Group-1 is composed of Tests A through D. 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 and *Test-Group-3* consists of completing Tests E.1 through E.4 and Tests F through J, respectively, 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.

Conformance Validation

UCC *Conformance 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 J 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. The three primary impediments to interoperability are Firewalls, Proxy Servers and Certificate Configurations. The former two must be configured locally to allow access to and from the Internet. Certificates should conform to X.509 standards and any system should ignore extensions not understood. However, since most vendor products incorporate security toolkits, it is not entirely within the control of the AS2 software vendors to support all possible certificate fields or extensions. For this reason, certificates should be kept as simple as possible, with one field or Set per Sequence (*see description below*). Creativity is not encouraged when building certs.

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

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)

Data Types

Testing consisted of transporting a variety of test data types, EDI-X12, EDIFACT and XML of a variety of sizes. The following MIME Content-Types were used:

```
Content-Type: application/EDI-X12
Content-Type: application/EDIFACT
Content-Type: application/XML
Content-Type: application/PKCS7-signature
Content-Type: application/PKCS7-mime
Content-Type: message/disposition-notification
Content-Type: multipart/signed
Content-Type: multipart/report
```

File Size

In a few instances between trading partners, the file size of the large file, 10MB, created a problem with the infrastructure used by some trading partners. Because of corporate timeout limits that were imposed upon the trading partners, the 10MB file could not be processed before the connection was timed-out due to firewall restrictions. To solve this, the

file size was reduced. A 1MB EDI file was used on the G.5 test, and a 8MB EDI file was used in the J.6 test. This change should not be thought of as a hindrance to AS2 interoperability.

Folded Headers

Problems were encountered 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 so the software tested includes workarounds for this problem. They have indicated this may be corrected in a future release.

Several of the participants are planning MVS (mainframe) implementations that 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 indicating the ongoing immaturity of interoperability between PKI software. 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 that 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 a variety of public certificate authorities. Some individual participants generated their own certificates (those whose systems had this capability -- not required). Certificates were tested as common certs while some participants chose to use separate certs for signing and encrypting. Certificates were created with a variety of fields filled in, with and without *urls*, and with/without a trusted root (self-signed certificates). While there is no way to test all possible certificate scenarios, a wide variety of situations were used.

AS2 System Identifier

Within this round of AS2 interoperability testing, it was decided to modify the requirements for naming convention of the AS2 System Identifiers that are passed within the AS2-To and AS2-From header fields. These requirements have been updated in the AS2 specification draft. However, it was discovered during testing that some vendors required the EDI address in their payloads to be the same as the AS2 System Identifiers. Other vendors had expectations that these system identifiers match the naming convention used by X12 and EDIFACT standards. Agreement on system identifiers was made between trading partners to insure interoperability and the tests proceed accordingly. However, full compliance to the AS2 standard for naming the AS2-To and AS2-From fields was not achieved during this test round. For specifics in the handling of AS2 System Identifiers, individual vendors should be consulted on their handling of this naming convention.

Asynchronous MDNs

The intention of the asynchronous MDN is to allow a response for an AS2 request to be sent immediately with the MDN sent later after the processing of the request has been accomplished. During this round of testing, it was determined that some vendors do not respond immediately with an HTTP response but instead hold open the connection while the MDN is created. In some cases, the MDN is sent back before the HTTP response. While this did not prevent participants from being interoperable, it is not in compliance with the spirit of asynchronous MDNs.

Final Test Results

Completed

STATUS	A	C	F.3	G.1	G.2	G.3
A <i>bTrade</i>	bcdefghijklmno BCDEFGHIJKLMNO	bcdefghijklmno BCDEFGHIJKLMNO	bcdefghijklmno BCDEFGHIJKLMNO	bcdefghijklmno BCDEFGHIJKLMNO	bcdefghijklmno BCDEFGHIJKLMNO	bcdefghijklmno BCDEFGHIJKLMNO
B <i>Cleo</i>	acdefghijklmno ACDEFGHIJKLMNO	acdefghijklmno ACDEFGHIJKLMNO	acdefghijklmno ACDEFGHIJKLMNO	acdefghijklmno ACDEFGHIJKLMNO	acdefghijklmno ACDEFGHIJKLMNO	acdefghijklmno ACDEFGHIJKLMNO
C <i>Compaq</i>	abdefghijklmno ABDEFGHIJKLMNO	abdefghijklmno ABDEFGHIJKLMNO	abdefghijklmno ABDEFGHIJKLMNO	abdefghijklmno ABDEFGHIJKLMNO	abdefghijklmno ABDEFGHIJKLMNO	abdefghijklmno ABDEFGHIJKLMNO
D <i>Cyclone I</i>	abcefgghijklmno ABCEFGHIJKLMNO	abcefgghijklmno ABCEFGHIJKLMNO	abcefgghijklmno ABCEFGHIJKLMNO	abcefgghijklmno ABCEFGHIJKLMNO	abcefgghijklmno ABCEFGHIJKLMNO	abcefgghijklmno ABCEFGHIJKLMNO
E <i>Cyclone II</i>	abcdfghijklmno ABCDFGHIJKLMNO	abcdfghijklmno ABCDFGHIJKLMNO	abcdfghijklmno ABCDFGHIJKLMNO	abcdfghijklmno ABCDFGHIJKLMNO	abcdfghijklmno ABCDFGHIJKLMNO	abcdfghijklmno ABCDFGHIJKLMNO
F <i>GXS</i>	abcdeghijklmno ABCDEGHIJKLMNO	abcdeghijklmno ABCDEGHIJKLMNO	abcdeghijklmno ABCDEGHIJKLMNO	abcdeghijklmno ABCDEGHIJKLMNO	abcdeghijklmno ABCDEGHIJKLMNO	abcdeghijklmno ABCDEGHIJKLMNO
G <i>InterTrade</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO
H <i>IPNet I</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO
I <i>IPNet II</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO
J <i>iSoft</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO
K <i>Sterling I</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO
L <i>Sterling II</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO
M <i>Tibco</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO
N <i>Vitria</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO
O <i>webMethods</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO

STATUS	G.5	H.1	H.2	H.3
A <i>bTrade</i>	bcdefghijklmno BCDEFGHIJKLMNO	bcdefghijklmno BCDEFGHIJKLMNO	bcdefghijklmno BCDEFGHIJKLMNO	bcde ghijklm o BCDE GHIJKLMNO
B <i>Cleo</i>	acdefghijklmno ACDEFGHIJKLMNO	acdefghijklmno ACDEFGHIJKLMNO	acdefghijklmno ACDEFGHIJKLMNO	acde ghijklm o ACDE GHIJKLMNO
C <i>Compaq</i>	abdefghijklmno ABDEFGHIJKLMNO	abdefghijklmno ABDEFGHIJKLMNO	abdefghijklmno ABDEFGHIJKLMNO	abde ghijklm o ABDE GHIJKLMNO
D <i>Cyclone I</i>	abcefgghijklmno ABCEFGHIJKLMNO	abcefgghijklmno ABCEFGHIJKLMNO	abcefgghijklmno ABCEFGHIJKLMNO	abce ghijklm o ABCE GHIJKLMNO
E <i>Cyclone II</i>	abcdfghijklmno ABCDFGHIJKLMNO	abcdfghijklmno ABCDFGHIJKLMNO	abcdfghijklmno ABCDFGHIJKLMNO	abcd ghijklm o ABCD GHIJKLMNO
F <i>GXS</i>	abcdeghijklmno ABCDEGHIJKLMNO	abcdeghijklmno ABCDEGHIJKLMNO	abcdeghijklmno ABCDEGHIJKLMNO	N/A
G <i>InterTrade</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcde hijklm o ABCDE HIJKLMNO
H <i>IPNet I</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcde gijklm o ABCDE GIJKLMNO
I <i>IPNet II</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcde ghijklm o ABCDE GHJKLMNO
J <i>iSoft</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcde ghiklm o ABCDE GHIKLMNO
K <i>Sterling I</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcde ghijlm o ABCDE GHILMNO
L <i>Sterling II</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcde ghijkm o ABCDE GHIJKMNO
M <i>Tibco</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcde ghijkl o ABCDE GHIJKLNO
N <i>Vitria</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcde ghijklmno
O <i>webMethods</i>	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcdefghijklmno ABCDEFHIJKLMNO	abcde ghijklm ABCDE GHIJKLMN

STATUS	J.3	J.4	J.6	STATUS
A <i>bTrade</i>	bcd fghijklmno BCD FGHIJKLMNO	bcd fghijklmno BCD FGHIJKLMNO	bcd fghijklmno BCD FGHIJKLMNO	DONE
B <i>Cleo</i>	acd fghijklmno ACD FGHIJKLMNO	acd fghijklmno ACD FGHIJKLMNO	acd fghijklmno ACD FGHIJKLMNO	DONE
C <i>Compaq</i>	abd fghijklmno ABD FGHIJKLMNO	abd fghijklmno ABD FGHIJKLMNO	abd fghijklmno ABD FGHIJKLMNO	DONE
D <i>Cyclone I</i>	abc fghijklmno ABC FGHIJKLMNO	abc fghijklmno ABC FGHIJKLMNO	abc fghijklmno ABC FGHIJKLMNO	DONE
E <i>Cyclone II</i>	N/A	N/A	N/A	DONE
F <i>GXS</i>	abcd ghijklmno ABCD GHIJKLMNO	abcd ghijklmno ABCD GHIJKLMNO	abcd ghijklmno ABCD GHIJKLMNO	DONE
G <i>InterTrade</i>	abcd fhijklmno ABCD FHIJKLMNO	abcd fhijklmno ABCD FHIJKLMNO	abcd fhijklmno ABCD FHIJKLMNO	DONE
H <i>IPNet I</i>	abcd fgijklmno ABCD FGijklmno	abcd fgijklmno ABCD FGijklmno	abcd fgijklmno ABCD FGijklmno	DONE
I <i>IPNet II</i>	abcd fghjklmno ABCD FGHjklmno	abcd fghjklmno ABCD FGHjklmno	abcd fghjklmno ABCD FGHjklmno	DONE
J <i>iSoft</i>	abcd fghiklmno ABCD FGHiklmno	abcd fghiklmno ABCD FGHiklmno	abcd fghiklmno ABCD FGHiklmno	DONE
K <i>Sterling I</i>	abcd fghijlmno ABCD FGHijlmno	abcd fghijlmno ABCD FGHijlmno	abcd fghijlmno ABCD FGHijlmno	DONE
L <i>Sterling II</i>	abcd fghijkmno ABCD FGHijkmno	abcd fghijkmno ABCD FGHijkmno	abcd fghijkmno ABCD FGHijkmno	DONE
M <i>Tibco</i>	abcd fghijklno ABCD FGHijklno	abcd fghijklno ABCD FGHijklno	abcd fghijklno ABCD FGHijklno	DONE
N <i>Vitria</i>	abcd fghijklmo ABCD FGHijklmo	abcd fghijklmo ABCD FGHijklmo	abcd fghijklmo ABCD FGHijklmo	DONE
O <i>webMethods</i>	abcd fghijklmn ABCD FGHijklmn	abcd fghijklmn ABCD FGHijklmn	abcd fghijklmn ABCD FGHijklmn	DONE

Note: Caps mean sent, Lower case mean received

Uppercase indicates successful send. Lower case indicates successful receive. For example, if bTrade has a *B* under Test A this indicates a successful send to Cleo on Test A. If bTrade has a *b* under Test A, this indicates a successful receive from Cleo on Test A. All participants submit a cumulative status sheet after each set of tests and the results are summarized on the table above.

Test results were gathered directly from the participants. Only success was reported. Since each Test involved a full duplex (both directions i.e. a send and a reply) for each participant and each participant captured and reported receiving and responding to each test, all tests were reported in duplicate. If a participant believed they sent data and received receipts correctly, that result must be correlated with the corresponding report from the participant at the receiving end of that transaction. In this way, we gather full interoperability testing results from all participants and to all participants (full matrix). This gives a positive interoperability result on each test data and for each testing scenario.

While not every possible situation may be tested, a large portion of the expected real-world scenarios is represented.

About DRUMMOND GROUP, INC.

The Drummond Group Inc. works with software vendors, vertical industry and the standards community to drive adoption for standards by facilitating vertical industry pilots, interoperability conformance testing and building competitive supply chain strategies. Founded in 1990, the vendor-neutral group represents best-of-breed in the industry on linking horizontal infrastructure technologies, standards and interoperability issues with the needs of vertical industry such as retail, grocery, healthcare, transportation, government and automotive.

For further information, please contact Beth Morrow at 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.

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 would 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 C: XML Interchange in a RFC1767 Bodypart

Test Description: This test expands on Test B by adding an XML file to the MIME envelope.

Test Setup:

Data Used: The XML data from Test-Data #6 (XML file).

Expected Results: The contents of the MIME message and XML file are the same for the original and received copies.

Test F: Receipt Request /Unsigned Receipt Returned

Test Description: The initiator creates a normal exchange as in Test B. 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>
- F.1 Signed	Unsigned
- F.2 Encrypted	Unsigned
- F.3 Signed/ Encrypted	Unsigned

Test Setup: Use Test B 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
- 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: F.3 *EDIFACT*

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

Test G: Receipt Request /Signed Receipt Returned

Test Description: The initiator creates a normal exchange as in Test B. 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 G.

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/HTTP	Signed
- G.2 Signed/ HTTPS	Signed
- G.3 Encrypted	Signed
- G.4 Signed/Encrypted	Signed
- G.5 Signed/Encrypted Large File	Signed

Test Setup: Use Test B 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:

G.1	EDIFACT
G.2	EDI-X12
G.3	EDI-X12
G.5	1MB EDI

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.

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:

- 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

Test H: Asynchronous Receipt Request /Signed Receipt Returned

Test Description: The initiator creates a normal exchange as in Test B. This test is the same as the signed MDN in test H with the addition of the asynchronous option. The presence of the Receipt-Delivery-Option indicates that an Asynchronous Receipt has been requested.

Note: This test is several tests using different URLs for the signed asynchronous messages.

<u>Originator</u>	<u>Type</u>	<u>Sample Return URL</u>
- H.1 HTTP	Encrypted	http://www.company.com/ediua
- H.2 HTTPS	Signed	https://www.company.com/ediua
- H.3 MAILTO	Signed/Encrypted	mailto:ediua-user@company.com

Test Setup: Use Test B 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
 Receipt-Delivery-Option: *return-url*

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
- 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:
- 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)

Data Used: *Same as tests G.1-G.3*

Expected Results: The Asynchronous (HTTP Status code of 200 returned and session terminated – MDN send initiated later) return of a signed-MDN to the "EDI gateway's address" (the address in the "Receipt-Delivery-Option:" 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.

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: Q2hlY2sgSW50XwdyaXRlQ, <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:

- 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
- Whenever a receipt-delivery-options header exists, the return value found in this header supercedes any value in the Disposition-Notification header
- A MDN MUST NOT request a MDN

Test J: Compressed Data File Transfer

Test Description: The initiator creates a normal exchange as in Test B. The file is then compressed and sent. For more information, see "Compressed Data for EDIINT", by T. Harding ([draft-ietf-ediint-compression-01.txt](#)).

Originator

- J.1 Compressed Data
- J.2 Compressed Data
- J.3 Signed & Compressed Data
- J.4 Compressed & Encrypted Data
- J.5 Encrypted & Signed & Compressed Data
- J.6 Encrypted & Signed & Compressed Data (Large File)

Recipient returns a MDN

- No MDN
- Signed MDN
- Signed MDN
- Signed MDN
- Signed MDN
- Signed MDN

Test Setup: Use Test B as the basic data.

Data Used:

J.3	EDI-X12
J.4	EDIFACT
J.6	8MB EDI

Expected Results: The test data, after decryption/decompression, has not changed in transit. The signature, if appropriate, is still valid.

For MDNs: The return of a Signed-MDN to the "EDI gateway 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 "AAAAAAAAAA" has <"authentication-failed" | "decryption-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:

- 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
- Disposition: automatic-action/MDN-sent-automatically; processed/error: authentication-failed
- Disposition: automatic-action/MDN-sent-automatically; processed/error: integrity-check-failed
- Disposition: automatic-action/MDN-sent-automatically; processed/error: decryption-failed
- Disposition: automatic-action/MDN-sent-automatically; processed/error: decompression-failed

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

