

**Final Report**  
**AS2 Interoperability Test**  
**First Quarter 2007 (1Q07)**



**May 7, 2007**

Prepared & Facilitated by:  
Drummond Group Inc.  
[www.drummondgroup.com](http://www.drummondgroup.com)

## Table of Contents

|  |    |
|--|----|
| Cover Letter .....   | 4  |
| Disclaimer .....   | 5  |
| Test Participants .....  | 6  |
| Interoperability Test Summary .....  | 9  |
| Interoperability Test Results - Required Test Cases .....                    | 10 |
| Optional Test Cases .....  | 11 |
| Certificate Exchange Messaging .....   | 11 |
| Multiple Attachment Testing .....  | 11 |
| Filename Preservation .....  | 11 |
| Filename Preservation for MA .....   | 12 |
| Interoperability Test Results - Optional Test Cases .....                    | 13 |
| Optional Test - CEM .....  | 13 |
| Optional Test - MA .....   | 13 |
| Optional Test - Filename Preservation .....                                  | 14 |
| Optional Test - Filename Preservation for MA .....                           | 14 |
| Interoperability Test History .....  | 15 |
| Definitions .....  | 16 |
| Interoperability Issues .....  | 17 |
| Interoperability Issues Resolved or Affirmed AS2-1Q07 .....                  | 17 |
| Interoperability Issues Resolved or Affirmed AS2-3Q06 .....                  | 18 |
| Interoperability Issues Resolved or Affirmed AS2-1Q06 .....                  | 19 |
| Interoperability Issues Resolved or Affirmed from previous Test Rounds ..... | 20 |
| Test Requirements .....  | 23 |
| Trading Partner Requirements .....   | 23 |
| Technical Requirements .....   | 23 |
| S/MIME encryption and digital signatures .....                               | 23 |
| Compression .....  | 23 |
| Synchronous and Asynchronous Receipts .....                                  | 24 |
| Transports .....   | 24 |
| Payloads .....   | 24 |
| Error Reporting .....  | 24 |
| Required Test Cases .....  | 25 |
| Test Data for Required Test Cases .....                                      | 26 |
| Required Test Cases - Detail .....   | 27 |
| Required Test Case A: .....  | 27 |
| Required Test Case B: .....  | 27 |
| Required Test Case C: .....  | 28 |
| Required Test Case D: .....  | 28 |
| Required Test Case E: .....  | 29 |
| Required Test Case F: .....  | 29 |
| Required Test Case G: .....  | 30 |
| Required Test Case H: .....  | 30 |
| Required Test Case I: .....  | 31 |
| Required Test Case J: .....  | 31 |
| Required Test Case K.1: .....  | 32 |
| Required Test Case K.2: .....  | 32 |
| Required Test Case K.3: .....  | 33 |

|   |    |
|---|----|
| Optional Test - Multiple Attachments.....   | 34 |
| Optional Test Cases - Detail .....  | 34 |
| Test Case M.1: XML and PDF Attachments.....   | 34 |
| Test Case M.2: XML and TIF Attachments.....   | 34 |
| Optional Test - Certificate Exchange Messaging.....                                   | 35 |
| Overview .....  | 35 |
| Test Goal and Setup .....   | 35 |
| Test Certificates .....   | 35 |
| Test Cases Detail.....  | 37 |
| Test Case N: Handling of Multiple Signature Certificates among Trading Partners.....  | 37 |
| Test Case O: Handling of Multiple Encryption Certificates among Trading Partners..... | 38 |
| Test Case P: Handling of Multiple TLS Certificates among Trading Partners.....        | 39 |
| Test Case Q: Sending Multiple Certificates in a CEM Request.....                      | 40 |
| Test Case R: Sending One Certificate for Multiple Usages .....                        | 41 |
| Assigned AS2 and EDI Identifiers .....  | 42 |
| Overview of the DGI Interoperability Compliance Process®.....                         | 43 |
| DGI In-the-Queue Test Round.....  | 43 |
| DGI Interoperability Test Round .....   | 44 |
| InSitu™ Test System.....  | 44 |
| About Drummond Group Inc. ....  | 45 |

## Cover Letter

DRUMMOND GROUP Inc. (DGI) is pleased to announce that the following participants in the AS2-1Q07 Interoperability Test Round have completed all requirements and passed all required test cases (see Interoperability Test Summary below) between each product - demonstrating interoperability and conformance. Final tests were run April 23 – April 26, 2007.

This twelfth round of AS2 interoperability testing continued to offer two important optional tests – Multiple Attachments (MA) and Certificate Exchange Messaging (CEM). In addition, the Filename Preservation optional profile was offered for the first time, with thirteen companies participating.

This was the fourth fully automated AS2 interoperability test. DGI's InSitu™, a patented test automation tool, continues to receive excellent feedback from participants.

The next round of AS2 interoperability testing will continue to add new AS2 optional test cases including AS2 Reliability.

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") on open technical standards. At the end of the testing process, DGI may list the name of the Participant in the final test report along with an indication that the Participant passed the test. The fact that the name of the Participant appears in the final report is not an endorsement of the Participant or its products or services, and DGI therefore makes no warranties, either express or implied, regarding any facet of the business conducted by the Participant.

## Test Participants

|   |  |
|---|--|
|  <p><b>Axway</b></p> <p><a href="http://www.axway.com">http://www.axway.com</a></p> <p><b>Product Name: Synchrony Gateway v6.9</b></p>                                       |  <p><b>Axway</b></p> <p><a href="http://www.axway.com">http://www.axway.com</a></p> <p><b>Product Name: Synchrony Gateway Interchange v5.5 / Synchrony EndPoint Activator v5.5</b></p> |
|  <p><b>Boomi Software</b></p> <p><a href="http://www.boomi.com">http://www.boomi.com</a></p> <p><b>Product Name: Boomi AS2 Transport v3.3.0</b></p>                          |  <p><b>BridgeGate International</b></p> <p><a href="http://www.BridgeGateIntl.com">http://www.BridgeGateIntl.com</a></p> <p><b>Product Name: BridgeGateAS2 v4.0</b></p>                |
|  <p><b>Bridgeware</b></p> <p><a href="http://www.bridgeware.com">http://www.bridgeware.com</a></p> <p><b>Product Name: AS2Bridge v4.2</b></p>                              |  <p><b>Cleo Communications</b></p> <p><a href="http://www.cleo.com">http://www.cleo.com</a></p> <p><b>Product Name: VersaLex™ v3.4 tested in VLTrader™ v3.4</b></p>                  |
|  <p><b>Click Commerce, Inc.</b></p> <p><a href="http://www.clickcommerce.com/">http://www.clickcommerce.com/</a></p> <p><b>Product Name: TDAccess/TDNgine v2.7.2.1</b></p> |  <p><b>The Descartes Systems Group Inc.</b></p> <p><a href="http://www.descartes.com/">http://www.descartes.com/</a></p> <p><b>Product Name: Descartes GLN AS2 v2.1</b></p>           |

|  |   |
|--|---|
|  <p><b>EDS</b></p> <p><a href="http://www.eds.com">http://www.eds.com</a></p> <p><b>Product Name: EDS*ELIT AS2 Connector v3.2</b></p>                             |  <p><b>EXTOL</b><br/>International, Inc.</p> <p><a href="http://www.extol.com">http://www.extol.com</a></p> <p><b>Product Name: EXTOL International / EXTOL Secure Engine v5.2 tested in EXTOL Secure Exchange v5.3</b></p> |
|  <p><b>GXS</b></p> <p><a href="http://www.gxs.com">http://www.gxs.com</a></p> <p><b>Product Name: AS2 Engine v4.1</b></p>   |  <p><b>IBM</b></p> <p><a href="http://www.ibm.com">http://www.ibm.com</a></p> <p><b>Product Name: IBM WebSphere Partner Gateway – Express v6.0</b></p>   |
|  <p><b>IBM</b></p> <p><a href="http://www.ibm.com">http://www.ibm.com</a></p> <p><b>Product Name: IBM WebSphere Partner Gateway v6.1</b></p>                    |  <p><b>Inovis</b></p> <p><a href="http://www.inovis.com/">http://www.inovis.com/</a></p> <p><b>Product Name: BizManager v3.1</b></p>  |
|  <p><b>nuBridges, Inc.</b></p> <p><a href="http://www.nubridges.com">http://www.nubridges.com</a></p> <p><b>Product Name: nuBridges Commerce Suite v3.4</b></p> |  <p><b>nuBridges, Inc.</b></p> <p><a href="http://www.nubridges.com">http://www.nubridges.com</a></p> <p><b>Product Name: nuBridges EDI-INT v3.2</b></p>  |

|   |  |
|---|--|
|  <p><b>n software</b> /n software inc.</p> <p><a href="http://www.nsoftware.com/">http://www.nsoftware.com/</a></p> <p><b>Product Name: IP*Works! EDI/AS2 v8.0</b></p>   |  <p><b>SEEBURGER</b> SEEBURGER AG<br/>BUSINESS INTEGRATION</p> <p><a href="http://www.seeburger.de/">http://www.seeburger.de/</a></p> <p><b>Product Name: SEEBURGER EDI-INT AS2 Adapter v6.2.3 tested in SEEBURGER Business Integration Server Release 6.2.3</b></p> |
|  <p><b>sterling commerce</b> Sterling Commerce</p> <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: Sterling Information Broker v3.9</b></p>   |  <p><b>sterling commerce</b> Sterling Commerce</p> <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: Connect:Enterprise UNIX v2.4</b></p>   |
|  <p><b>sterling commerce</b> Sterling Commerce</p> <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: Gentrان Integration Suite/ Multi-Enterprise Financial Gateway v4.2</b></p>         |  <p><b>sterling commerce</b> Sterling Commerce</p> <p><a href="http://www.sterlingcommerce.com">http://www.sterlingcommerce.com</a></p> <p><b>Product Name: Gentrان Integration Suite/ Multi-Enterprise Financial Gateway v5.0</b></p>                             |
|  <p><b>TIBCO</b> TIBCO Software Inc.<br/>The Power of Now®</p> <p><a href="http://www.tibco.com">http://www.tibco.com</a></p> <p><b>Product Name: TIBCO BusinessConnect™ AS2 Transport v5.2.0 as tested in TIBCO BusinessConnect™ v5.2</b></p> |  <p><b>Tumbleweed</b> Tumbleweed Communications Corp.<br/>Messaging. Secure and Simple.</p> <p><a href="http://www.tumbleweed.com">http://www.tumbleweed.com</a></p> <p><b>Product Name: Tumbleweed SecureTransport v4.6.1</b></p>                                 |

## Interoperability Test Summary

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

The purpose of the test is to provide a venue for vendors to test and correct their software systems in a non-competitive environment. To accomplish this, each product-with-version both sends and receives specific messages with the Product Test Group. In both sending and receiving, products-with-versions verify the message structure and security requirements are correct, the intended payload was transferred intact, and the receipt for the message was correctly delivered verifying the transaction was successful.

The test cases cover the full scope of AS2 in terms of security and receipts. Digital signatures, encryption, HTTP/HTTPS transports, unsigned and signed receipts, synchronous and asynchronous receipts, and data compression are all tested. Test data payloads simulating traditional POs and UCCnet messages were used with document formats of X12, EDIFACT and XML.

Products were also tested with erroneous AS2 messages to verify they could properly recognize message errors and return conforming error values within MDNs. That is, Participants were purposefully sent corrupted signed, encrypted and compressed messages and were required to respond with an appropriate MDN error value. In situations where trading partner profiles and certificates are improperly loaded or network firewall problems exist, proper MDN error values can greatly assist a trading partner in identify and resolving the problem.

The test round repeated the optional Multiple Attachment (MA) testing which was introduced in the eighth interoperability test round. Along with completing the required test case, seven products completed the optional MA testing.

The optional Certificate Exchange Messaging (CEM) continued to be tested in this test round. It originally was tested in AS2-1Q05, in the prior round AS2-3Q06, and now for the third time in AS2-1Q07. Along with completing the required test case, four products completed the optional CEM testing in this test round.

Two new profiles, "Filename Preservation" and "MA with Filename Preservation", were added. Both focus on preserving the Filename associated with the payloads sent and received during AS2 message exchanges. Filename Preservation is especially important for the banking industry but its implementation is generic so it may be used by any industry.

## Interoperability Test Results - Required Test Cases

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

The Interoperability Test Round (including Optional Tests) was completed in seven weeks. During the first six weeks, the testing was focused on finding interoperability errors and correcting them. Code changes were not allowed during final week of testing which occurred during April 23 – April 26, 2007.

During all weeks of testing, including the final week, all products-with-version tested with each other in a full-matrix fashion. During the final week, all products executed all required test cases in a full-matrix fashion without error demonstrating full-matrix interoperability.

This final version of code as denoted by each product-with-version version listed in the “Test Participants” section of this Final Report are deemed Drummond Certified™ and interoperable with each other (as a group) as they all sent and received each required test case successfully. Results were reported both through InSitu and by the participants themselves and demonstrated by supplying the messages sent and received.

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.

Also, please note that products certified in this AS2-1Q07 Drummond Certified list have achieved interoperability with other products-with-version listed within this specific test round. No warranties are made for interoperability between products from two different test rounds (including optional test cases).

## Optional Test Cases

Any participant could have participated in these tests but since they were optional, not all elected to receive certification for this optional test.

The AS2-Version header for AS2 products supporting these features is 1.2, and each product includes the additional AS2 header EDIINT-Features (documented in IETF standard <http://www.ietf.org/internet-drafts/draft-meadors-ediint-features-header-02.txt>).

The EDIINT-Features feature name (or value) is "multiple-attachments". The EDIINT-Features header name (or value) is "CEM" For instance, and application supporting both of these features, would include the following headers in AS2 messages:

AS2-Version: 1.2

EDIINT-Features: CEM, multiple-attachments

## Certificate Exchange Messaging

Certificate Exchange Messaging is an IETF I-D for the automation of exchanging digital certificates within EDI-INT applications, primarily AS2. If you have a trading partner relationship established but one or more certificates is set to expire, CEM allows you to securely exchange the digital certificates, load them, and switch over without the massive effort of coordinating the manual switching of certificates between trading partners. We have tested CEM in one previous AS2 Interop as an optional feature and have re-introduced it in this Interop. It is based on an IETF open standard, <http://www.ietf.org/internet-drafts/draft-meadors-certificate-exchange-06.txt>, CEM provides for a secure and automated way of updating certificates which are due to expire.

## 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 IETF open standard <http://www.ietf.org/internet-drafts/draft-meadors-multiple-attachments-ediint-03.txt>, multiple attachment testing provides for the same security used in single payload AS2 transmission.

## Filename Preservation

Based on an IETF open standard <http://www.ietf.org/internet-drafts/draft-harding-filename-preservation-00.txt>, Filename Preservation is a method for preserving the filename associated with a payload as provided in the Content-Disposition MIME header [RFC 2183].

The companies and products that took part in and successfully completed Filename Preservation demonstrated the capability of providing a filename and in preserving that filename upon receiving it. That is, the filename provided was preserved in both directions.

When acting as Senders, participating companies and products were certified that they communicated the filename of the business document during packaging and transport of the EDIINT MIME message to its trading partner.

When acting as Recipients, participating companies, demonstrated that they were able to retrieve the filename of the MIME wrapped business document.

### **Filename Preservation for MA**

As mentioned under Filename Preservation above, the Content-Disposition header was added to the MIME bodyPart that encapsulates the business document. If the EDIINT MIME message contains multiple attachments then each individual MIME bodyPart that encapsulates an attachment had its own Content-Disposition header describing the filename of the attachment.

The test scenarios were similar to the Filename Preservation test indicated above, except that the test cases were repeated with multiple attachments.

## Interoperability Test Results - Optional Test Cases

Those companies listed under each optional test completed the corresponding Optional Test Case with each other, in a full-matrix fashion. That is, each participant acted as both recipient and originator.

Also, please note that products certified in this AS2-1Q07 Drummond Certified list have achieved interoperability with other products-with-version listed within this specific test round. No warranties are made for interoperability between products from two different test rounds (including optional test cases).

### Optional Test - CEM

The following companies and products also took part in and successfully completed Certificate Exchange Messaging (CEM) Optional testing for this round.

| Company                          | Product  |
|----------------------------------|--|
| Axway                            | Synchrony Gateway Interchange v5.5 / Synchrony EndPoint Activator v5.5 |
| Cleo Communications              | VersaLex™ v3.4 tested in VLTrader™ v3.4                                |
| The Descartes Systems Group Inc. | Descartes GLN AS2 v2.1   |
| Inovis                           | BizManager v3.1  |

### Optional Test - MA

The following companies and products took part in and successfully completed Multiple Attachments (MA) Optional testing for this round.

| Company                          | Product  |
|----------------------------------|--|
| Cleo Communications              | VersaLex™ v3.4 tested in VLTrader™ v3.4  |
| The Descartes Systems Group Inc. | Descartes GLN AS2 v2.1   |
| GXS                              | AS2 Engine v4.1  |
| Inovis                           | BizManager v3.1  |
| /n software inc.                 | IP*Works! EDI/AS2 v8.0   |
| nuBridges, Inc.                  | nuBridges Commerce Suite v3.4  |
| SEEBURGER AG                     | SEEBURGER EDI-INT AS2 Adapter v6.2.3 tested in SEEBURGER Business Integration Server Release 6.2.3 |

## Optional Test - Filename Preservation

The following companies and products also took part in and successfully completed Filename Preservation both Inbound and Outbound messages. The filename provided is preserved in both directions.

| Company                          | Product  |
|----------------------------------|--|
| Axway                            | Synchrony Gateway Interchange v5.5 / Synchrony EndPoint Activator v5.5                             |
| Axway                            | Synchrony Gateway v6.9   |
| Cleo Communications              | VersaLex™ v3.4 tested in VLTrader™ v3.4  |
| Click Commerce, Inc.             | TDAccess/TDNgine v2.7.2.1  |
| The Descartes Systems Group Inc. | Descartes GLN AS2 v2.1   |
| EDS                              | EDS*ELIT AS2 Connector v3.2  |
| IBM                              | IBM WebSphere Partner Gateway v6.1   |
| Inovis                           | BizManager v3.1  |
| /n software inc.                 | IP*Works! EDI/AS2 v8.0   |
| nuBridges, Inc.                  | nuBridges EDI-INT v3.2   |
| nuBridges, Inc.                  | nuBridges Commerce Suite v3.4  |
| SEEBURGER AG                     | SEEBURGER EDI-INT AS2 Adapter v6.2.3 tested in SEEBURGER Business Integration Server Release 6.2.3 |
| TIBCO Software Inc.              | TIBCO BusinessConnect™ AS2 Transport v5.2.0 as tested in TIBCO BusinessConnect™ v5.2               |

## Optional Test - Filename Preservation for MA

The following companies and products also took part in and successfully completed Filename Preservation for both Inbound and Outbound MA messages as well. The filename provided is preserved in both directions.

| Company                          | Product  |
|----------------------------------|--|
| Cleo Communications              | VersaLex™ v3.4 tested in VLTrader™ v3.4  |
| The Descartes Systems Group Inc. | Descartes GLN AS2 v2.1   |
| Inovis                           | BizManager v3.1  |
| /n software inc.                 | IP*Works! EDI/AS2 v8.0   |
| SEEBURGER AG                     | SEEBURGER EDI-INT AS2 Adapter v6.2.3 tested in SEEBURGER Business Integration Server Release 6.2.3 |

## **Interoperability Test History**

This is the twelfth Interoperability Test administered by DGI.

AS2 1Q07 Interoperability Test – Feb-Apr 2007

Previous tests included the following:

|  |      |
|--|------|
| AS2 3Q06 Interoperability Test – Sept-Oct          | 2006 |
| AS2 1Q06 Interoperability Test – Feb-Mar           | 2006 |
| AS2 3Q05 Interoperability Test – September-October | 2005 |
| AS2 1Q05 Interoperability Test – February-April    | 2005 |
| AS2 3Q04 Interoperability Test – August-September  | 2004 |
| AS2 1Q04 Interoperability Test – February-March    | 2004 |
| AS2 3Q03 Interoperability Test – July-September    | 2003 |
| AS2 1Q03 Interoperability Test – January-February  | 2003 |
| AS2 2Q02 Interoperability Test – March-August      | 2002 |
| AS2 2Q01 Interoperability Test – May-August        | 2001 |
| AS2 4Q00 Interoperability Test – October-December  | 2000 |

## Definitions

**Interoperability** – A product is deemed interoperable with all other products in the Interoperability Test Round if and only if it demonstrates in a full-matrix manner the pair wise exchange of data covering the *Test Criteria* between all products in the Interoperability Test Round. A product is either totally interoperable or it is not interoperable. Waivers or exceptions are not given in demonstrating interoperability for the *Test Criteria* unless the entire *Product Test Group* and DGI agree.

**Interoperable products** – Group of products, from the *Product Test Group*, which successfully completed the *Test Criteria*, in a full-matrix manner with every other *Product Test Group* participant in an Interoperability Test Round without any errors in the final test Phase. Interoperable products receive a Drummond Certified™ Seal.

**Product Test Group** – A group of products involved in an interoperability or conformant Test Round.

**Product, product-with-version, or product-with-version-with-release** – are interchangeable and are defined for the purpose of a Test Round as a product name, followed by a product version, followed by a single digit release. The assumption is that version and release syntax is as: “VV.Rx...x,” where VV is the version numeral designator, R is the single digit release numeral designator and x is the sub-release multiple digit numeral designator. DGI assumes that any digits of less significance than the R place do not indicate code changes on the product-with-version-with-release tested in the Test Round. A vendor must list a product as product name, followed by version digits followed by a decimal point followed by a single release designator digit before the Test Round is complete.

**Test Case** – The test criteria is a set of individual test cases, often 10 to 50 which the product test group exchange among themselves to verify conformance and interoperability.

**Test Criteria** – A set of individual tests, based on one or more standard specifications, that is used to verify that a product is conformant to the specification(s) or that a set of Product-with-version's are interoperable under the *Test Criteria*.

## Interoperability Issues

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

### Interoperability Issues Resolved or Affirmed AS2-1Q07

1. One participant issued certificates with a Country Code using three characters (USA) vs. two (US). Two characters are required, three characters caused Interop issues with some participants.
2. One participant issued certificates using IAString vs. the correct DirectoryString type for organizational unit name field which caused Interop issues.
3. AS2 Identifiers containing embedded spaces MUST be enclosed in double quotes. When the AS2 Identifier is not enclosed in double quotes, the agreed rule is to parse up to the first blank space, however this caused Interop issues. The solution was to enclose the AS2 Identifier with double quotes.
4. The ability to calculate a message integrity check (MIC) on the received message and return it to the sender of the message inside the signed receipt (MDN) is a basic requirement of AS2. The MIC should be calculated over the signed data. One participant was uncompressing the signed data first, then calculating the MIC, thus generating an incorrect value and causing Interop issues. The solution was to calculate the MIC over the signed payload.
5. Several participants were sending folded headers in the MDNs. However, an earlier Consensus item stated that headers should not be folded. The participants unfolded their headers to resolve Interop issues.
6. One participant was encoding their data as 8bit (used in SMTP), however, binary transfer encoding is the default over HTTP. The participant switched to binary encoding to resolve Interop issues as a result of using 8bit encoding.
7. The Message-ID in the MDN is not required. One participant was failing test cases because of the misunderstanding that the Message-ID was required in the MDN's. This continues to be a source for

misinterpretation. The Original-Message-ID, however, is required in the MDNs.

8. AS2-From and AS2-To do not have to be UPPER CASE. One participant was failing test cases because they of their misunderstanding that the AS2 portion must be UPPERCASE. MIME/HTTP headers are not case sensitive.

## **Interoperability Issues Resolved or Affirmed AS2-3Q06**

1. Certificates and security toolkit related errors continued to be observed in this test round. Certificates using unusual fields or extensions could create problems within supply-chains. Not all possible certificate fields or extensions were tested against every AS2 product's toolkit, and potential issues could still exist due to certain certificate fields and extensions. Also, it is becoming apparent that not every version of security toolkits is interoperable with every other version.
2. MDN were rejected by at least one participant, based on misunderstanding that Message-ID header is not required. The Message-ID is optional, and the Original-Message-ID is required.
3. Certificates with serialNumber equal to zero could not be processed by at least one participant's security toolkit. Therefore, the consensus from previous Interop's was amended to further constrain serial number to be non-negative integers, greater than, but not including zero.
4. Folded-Headers once again caused Interop issues in this round. Folded-Headers, although allowed in the standards, cause Interop issues with some participants, and thus are not allowed. Several participants were using folded headers, and at least one participant could not accept MDN messages with folded headers (that is a CR LF in the string value of a header).
5. Participant was missing a CRLF for the MIME boundary, or not following CR with a LF, or adding an extra CR LF, causing receiving applications to fail the test. See RFC 2045-2049.
6. Participant was missing the report-type, as in: Content-Type: multipart/report; report-type=disposition-notification; for in the MDN header, however, it was required.
7. Although not required, the To: and From: headers, if used, should follow the MIME header formatting rules. At least one participant was not enclosing the values with quotes when they were required. Same issue appeared for AS2-To and AS2-From headers.

8. Base64 encoding the entire HTTP body was being used. Note however, that Content Transfer Encoding (CTE) of MIME body parts within the AS2 message is allowed. Consensus was arrived that if the MIME bodies were already encrypted and or compressed, CTE was neither necessary nor practical for performance reasons. Participants agreed to remove Base64 encoding over the entire HTTP body, which helped resolve Interop issues, and theoretically improved processing performance of messages. Performance metrics are not measured in Interop testing
9. It was agreed that HTTP/1.0 servers are required to close HTTP connections, and it is not the responsibility of HTTP clients. At least one participant was relying on a timeout for the connection to close on the server-side, or for the HTTP client to close the connection. When the HTTP /1.0 Server waited for the HTTP /1.1 Client to close the connection and the Client waited for the Server to close the connection but the Server did not close then the Client timed-out and perceived it as an aborted connection and flagged the test failed. The HTTP 1.0 Servers must close the connection based on the HTTP/1.0 specification.
10. Certificates needed to have two-character country code. This was in the list “Interoperability Issues Resolved or Affirmed from previous Test Rounds”, but it occurred in this round as well.
11. A participant had a certificate organizational unit name specified as “R&D” and it was encoded as an IA5String. This is supposed to be a DirectoryString. The participant discovered that their certificate generation tool used to create their certificates was using the outdated IA5String encoding for some of the elements within the Subject and or Issuer name fields.
12. At least one participant found an issue with LF of CRLF being removed on the outgoing payload data which was causing payload mismatches (the sent payload did not match the received).

## **Interoperability Issues Resolved or Affirmed AS2-1Q06**

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

For example, there was an issue with a participant SSL certificate was not properly formatted (for DER encoding). It caused another participant to reject it during the SSL handshake. The participant's certificate had

an explicit default value in the version identifier. The certificate had a 0 in this field, when it should be version 1 (everyone else's certificates had version 1).

2. Also, it was discovered that security toolkit versions are not always interoperable from version to version, and this Interop revealed and helped resolve these incompatibility in the security toolkits. However, security toolkits were not exhaustively tested for interoperability.
3. The AS2 specification requires that human-readable portion of MDN must contain "Final-Recipient". Please see <http://www.ietf.org/rfc/rfc4130.txt> section 7.4.2. A participant was not sending "Final-Recipient" however it was required.
4. A participant was sending "folded headers" in the MDN's and this caused an error because at least one other participant did not process "folded headers". In previous Interop's, it was a consensus item to not fold the headers.

Example:

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

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

## Interoperability Issues Resolved or Affirmed from previous Test Rounds

1. Some products could not accept certain characters or certain strings of AS2 identifiers. Two specific issues were: 1) having a space (" ") at the third location, e.g. "AS 2", and 2) identifiers containing a comma (","). While these conflicts were very rare and not associated with every participant, supply-chain implementers of these products should avoid identifiers with this syntax and discuss with their AS2 vendor any potential AS2 Identifier issues.

2. Trailing long white spaces (LWS) at the end of HTTP headers is not permitted. Leading LWS is allowed within HTTP (RFC2616) but not clear if trailing LWS is or is not.
3. The value "RSA-SHA1" was used by some participants for the MIC algorithm of the digital signature. It is a valid value and should be considered equal to that of the more common "SHA1" value. "RSA-SHA1" is a legacy value from an earlier S/MIME implementation.
4. Field names in MDNs, such as Original-Message-ID, are case-insensitive. According to RFC2298, section 3.1.1, "field names are case-insensitive, so the names of notification fields may be spelled in any combination of upper and lower case letters." As well, it is permissible to have a white space character (" ") before the message-id value of the Original-Message-ID field in the MDN. Thus, the two examples below are considered identical:
  - a. Original-Message-ID:<123foo@example>
  - b. Original-Message-ID: <123foo@example>
5. The Message-ID header is not required in MDNs.
6. Chunked encoding for HTTP 1.1 requests and responses is acceptable for AS2. Rules for implementing, supporting and understanding chunked encoding can be found in the HTTP 1.1 standard, RFC2616.
7. Some products require valid EDI/XML documents on inbound messages and will generate MDNs with errors if they are invalid. This includes both valid formatting and/or recognized identifiers.
8. Certificate serial numbers must not be negative, per RFC3280. While some AS2 systems accept negative serial numbers, other systems cannot accept negative values.
9. Certificates are uniquely identified through their Issuer name and their serial number. As with negative serial numbers, certain AS2 systems will reject duplicate certificates, but others can accept them.
10. Some products utilizing the open source OpenSSL experienced problems in SSL transactions. The cause was due to the sending of empty fragments in the transaction which caused some trading partner products to corrupt the inbound document. The solution was to modify configuration flags within OpenSSL.
11. HTTP Content-length header is not necessarily required on MDN. The HTTP standard specifies the use and requirement of this header, and the AS2 draft is being updated to refer back to the HTTP standard for the use of content-length.

12. MIME Folded headers continue to cause problems with several products due to their associated web server. Folded headers were not used during the test and should be avoided in actual implementation.
13. The use of quotation marks on AS2 System Identifiers should not be used for atomic names. Also, the use of quotation marks on AS2 System Identifiers must be consistent for both the payload messages as well as for the MDNs. That is, if quotation marks are used in the payload message, they also must be present in MDNs.
14. A 204 (No content) HTTP response would be acceptable in an HTTP response of an async MDN request. This should be accepted (assuming the response has no body). From the latest version (13) of the AS2 draft, section 7.6, notice the comment of the response being "in the 200 range." HTTP RFC2616 states that if a 204 is returned, there is to be no message body and the message is terminated by the first empty line after the header fields. So, the 204 will work as long as there are only HTTP headers in the response.
15. If certificates use the country attribute, the country attribute may only contain two characters. For example, "C=USA" is invalid and instead should be listed as "C=US".
16. Encrypted messages can contain multiple RecipientInfo structures within the CMS data, including one describing the originator. Refer to RFC 2630 Section 6 for more details.
17. Consensus was reached that AS2 messages with EDI payloads should identify the content-type either as application/EDI-X12 or application/EDIFACT and NOT application/EDI-CONSENT.
18. The Message-ID is not required in Asynch MDN's because the AS2 standard states it SHOULD be contained, that is, it is not required. Asynch MDN's should not be rejected if MDN's do not contain Message-ID because it is not required. It is recommended that it be present. Please refer to the meanings of SHOULD and MUST.

## Test Requirements

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

### Trading Partner Requirements

All participants were required to establish trading partner relationships with each other. Each participant provided their security certificates (including TLS server certificates) to the other participants for storage in their trusted store.

Each certificate conformed to the X.509 standards but varied with respect to the fields used in the certificates. 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 certificates for S/MIME and SSL while others used one certificate for all forms of security.

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

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

### Technical Requirements

In order to be part of the certified interoperable products-with-versions, each participant must both successfully send and receive all test cases with the other participants. These test cases, which can be found in the Appendix, cover the basis of the open AS2 standard. The test cases demonstrate the products-with-versions can cover the technical requirements listed in the sections below. For additional technical information concerning these sections, refer to ***RFC 4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)*** found at <http://www.ietf.org/rfc/rfc4130.txt?number=4130>

#### **S/MIME encryption and digital signatures**

S/MIME encryption and digital signatures provide confidentiality and content-integrity of the data being transported. Key length in the security certificates was between 512 bits and 2048 bits. Triple DES (3DES) was the encryption algorithm used, and other algorithms, such as RC2 or DES, were not tested. SHA-1 hashing was used in creating the digital signatures, but the MD5 was not used.

#### **Compression**

While not a part of the AS2 draft document, compression is part of AS2 interoperability testing, and is based on <http://www.ietf.org/internet->

[drafts/draft-ietf-ediint-compression-06.txt](#). 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.

## Required Test Cases

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

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

Test cases K1-K3 are error scenario test cases.

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

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

## Test Data for Required Test Cases

The test data described below was used as payloads in the test cases of the interoperability test round. This test data was distributed to the participants prior to the test.

- Test Data #1.  
X12 PO with an apostrophe (!) for segment terminator.  
Size is 12kB.
- Test Data #2.  
X12 PO with line feed (0x0a) for segment terminator.  
Size is 3kB.
- Test Data #3.  
UCCnet XML file.  
Size is 9kB.
- Test Data #4.  
XML PO.  
Size is 36kB.
- Test Data #5.  
EDIFACT Purchase Order (PO) with standard apostrophe (")  
for segment terminator.  
Size is 6kB.
- Test Data #6.  
EDIFACT Purchase Order (PO) with standard apostrophe (")  
for segment terminator.  
Size is 10kB.
- Test Data #7.  
EDIFACT Purchase Order (PO) with standard apostrophe (")  
for segment terminator.  
Size is 15kB.
- Test Data #8.  
EDIFACT Purchase Order (PO) with standard apostrophe (")  
for segment terminator.  
Size is 2kB.
- Test Data #9.  
Large X12 file.  
Size is 2MB.
- Test Data #10.  
Very large X12 file.  
Size is 50MB.

## Required Test Cases - Detail

### Required 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.        |

### Required 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.      |

## Required 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. |

## Required 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 # 4   |
| <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.           |

## Required 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 # 5   |
| <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. |

## Required 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 # 6   |
| <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. |

## Required 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 # 7  |
| <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.        |

## Required 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 # 8  |
| <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. |

## Required 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 # 9   |
| <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. |

## Required 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 # 10  |
| <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. |

## Required 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”.  |

## Required 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”.  |

### Required 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 - Multiple Attachments

The Multiple Attachment test cases were optional. Details of these test cases follow.

### Optional Test Cases - Detail

#### Test Case M.1: XML and PDF Attachments

##### *M.1 Description*

The originator creates a Multipart-Related MIME structure with a type parameter of "application/xml". The two attachments are ma\_test\_data\_1.xml (root body part) and ma\_test\_data\_2.pdf attachments. The Multipart-Related structure is signed and sent requesting a signed MDN.

##### *M.1 Test Configuration*

**Transport:** HTTP

**Security:** Signature

**Compression:** No

**MDN Transport:** Synchronous, signed

**Attachments:** ma\_test\_data\_1.xml (root) and ma\_test\_data\_2.pdf

##### *M.1 Expected Results*

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

#### Test Case M.2: XML and TIF Attachments

##### *M.2 Description*

The originator creates a Multipart-Related MIME structure with a type parameter of "application/xml". The two attachments are ma\_test\_data\_3.xml (root body part) which uses the "application/xml" media type and ma\_test\_data\_4.tif which uses the "image/tiff" media type. The Multipart-Related structure is signed and encrypted sent requesting a signed MDN.

##### *M.2 Test Configuration*

**Transport:** HTTP

**Security:** Signature, Encrypted

**Compression:** No

**MDN Transport:** Synchronous, signed

**Attachments:** ma\_test\_data\_3.xml (root) and ma\_test\_data\_4.tif

##### *M.2 Expected Results*

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

## Optional Test - Certificate Exchange Messaging

### Overview

[Certificate Exchange Messaging](#) (CEM) is designed for proper exchanging and loading of new certificates within a working trading partner arrangement without interfering the active trading. In order to test, participants will have an existing trading partner relationship. Then, they will exchange new certificates through CEM and confirm the acceptance by sending messages which utilize the new certificates.

### Test Goal and Setup

Each test participant will exchange [CEM Request](#) and [CEM Response](#) messages with all other participants to demonstrate CEM message protocol interoperability. The CEM functional protocol of utilizing multiple certificates in active trading partner relationships and controlled returning (i.e. non-automatic but manual decision) of [CEM Response](#) messages is demonstrated.

Each test participant will establish trading partner relationships with all other participants. All AS2 connections utilize synchronous MDNs. The "Trading Partners" in each test case will be specified by DGI at test time. Unless otherwise state in the Test Case, Test Participant may include other certificates in their [CEM Request](#) message than the certificate specifically under test. For example, a Test Participant exchanging a New Signing Certificate **Bravo** may include its existing Encryption and SSL certificates in the same [CEM Request](#).

If multiple certificates (and thus multiple *TrustRequest* elements) are sent within the same [CEM Request](#) message, the corresponding *TrustResponse* elements may be returned in a single [CEM Response](#) message or multiple [CEM Response](#) messages. Test Participants must be able to handle both scenarios.

If multiple certificates (and thus multiple *TrustRequest* elements) are sent within multiple [CEM Request](#) messages, the corresponding *TrustResponse* elements may be returned in a single [CEM Response](#) message or multiple [CEM Response](#) messages. Test Participants must be able to handle both scenarios.

### Test Certificates

Each participant provides two certificates for data encryption, digital signatures and TLS transport encryption. For testing, these certificate sets with the associated certificates will be used.

Certificate Set A: Signing Cert **Alpha**, Encryption Cert **Charley**, TLS Cert **Echo**

Certificate Set B: Signing Cert **Bravo**, Encryption Cert **Delta**, TLS Cert **Foxtrot**

Certificate Set C: Signing Cert **Golf** and Encryption Cert **Hotel**

Certificate Set D: Signing and Encryption Cert **Zulu**

For Certificate Sets A and B, the different certificate designation (e.g. **Alpha**, **Charley**, etc.) can be different X.509 certificate or the same individual X.509 certificate but must be a different X.509 certificate from the certificates in the other Sets. For Certificate Set C, Cert **Golf** and **Hotel** must be different X.509 certificates from each other and must be different X.509 certificates from the certificates in the other Sets. For Certificate Set D, Cert **Zulu** must be a different X.509 certificate from the certificates in the other Sets. Each Certificate in all Sets can be either self-signed or chained to Root CA. If certificate chains are used, all certificates in the chain must be included in the CEM Request message.

To complete this test, each Participant needs between a minimum of 5 end-entity X.509 certificates or maximum of 9 end-entity X.509 certificates.

## Test Cases Detail

### Test Case N: Handling of Multiple Signature Certificates among Trading Partners

#### Test Steps

1. Test Participant has Signing Cert **Alpha** loaded and in use with all Trading Partners. Test Participant sends a signed message (Signed Message #1) with Signing Cert **Alpha** to all Trading Partners. Test Participant receives back good MDNs for each message.
2. Test Participant loads new Signing Cert **Bravo**. Test Participant sends it to all Trading Partners via CEM Request message with *CertUsage* set to *digitalSignature*. Good MDN is received for all CEM Request messages.
3. Trading Partners 1 and 2 accept Signing Cert **Bravo**. Trading Partners 1 and 2 return CEM Response messages with an *Accepted* state. Other Trading Partners do not return a CEM Response. Test Participant returns good MDNs for each message and then processes the CEM Response accordingly.
4. Test Participant sends a signed message (Signed Message #2) to all Trading Partners. All Trading Partners besides Trading Partners 1 and 2 receive message signed by Signing Cert **Alpha**. Trading Partners 1 and 2 receive message signed either by Signing Cert **Alpha** or **Bravo**. Good MDNs are returned for all messages.
5. Remaining Trading Partners besides 1 and 2 return CEM Response message with an *Accepted* state for Signing Cert **Bravo**. Test Participant returns good MDNs for each message and then processes the CEM Response accordingly.
6. Test Participant sends a signed message (Signed Message #3) to all Trading Partners using Signing Cert **Bravo** and receives back good MDNs for each message.

## Test Case O: Handling of Multiple Encryption Certificates among Trading Partners

### Test Steps

1. Test Participant has Encryption Cert **Charley** loaded and in use with all Trading Partners. All Trading Partners send Test Participant an encrypted message (Encrypted Message #1) with Encryption Cert **Charley** and receive back good MDNs for their messages.
2. Test Participant loads new Encryption Cert **Delta** and sends it to all Trading Partners via CEM Request message with *CertUsage* set to *keyEncipherment*. Good MDN is received for all CEM Request messages.
3. Trading Partners 3 and 4 accept Encryption Cert **Delta** and return CEM Response messages with an *Accepted* state.
4. All Trading Partners send Test Participant an encrypted message (Encrypted Message #2). Trading Partners 3 and 4 use Encryption Cert **Delta** while all other Trading Partners use Encryption Cert **Charley**. Good MDNs are returned for all messages.
5. Remaining Trading Partners besides 3 and 4 return CEM Response message with an *Accepted* state for Encryption Cert **Delta**.
6. All Trading Partners send Test Participant an encrypted message (Encrypted Message #3) with Encryption Cert **Delta** and receive back good MDNs for their messages.

## Test Case P: Handling of Multiple TLS Certificates among Trading Partners

### Test Steps

1. All Trading Partners initiate an TLS connection (TLS Connection #1) with Test Participant. Within the TLS Handshaking, Test Participant sends TLS Cert **Echo** as TLS Server Cert. All Trading Partners accept TLS Cert **Echo** as the TLS Server Cert and use it to successfully complete the TLS Handshaking. The AS2 message is delivered, a good MDN received and the TLS connection completed with all Trading Partners.
2. Test Participant sends new TLS Cert **Foxtrot** to all Trading Partners via CEM Request message with *CertUsage* set to *tlsServer*. Good MDN is received for all CEM Request messages. However, TLS Cert **Echo** is still loaded as active TLS Server Cert.
3. Trading Partners 1 and 2 accept TLS Cert **Foxtrot** and return CEM Response messages with an *Accepted* state.
4. All Trading Partners initiate an TLS connection (TLS Connection #1) with Test Participant. Within the TLS Handshaking, Test Participant sends TLS Cert **Echo** as TLS Server Cert. All Trading Partners, include Trading Partners 1 and 2, accept TLS Cert **Echo** as the TLS Server Cert and use it successfully completes the TLS Handshaking. The AS2 message is delivered, a good MDN is received and the TLS connection is completed with all Trading Partners.
5. Remaining Trading Partners besides 1 and 2 return CEM Response message with an *Accepted* state for TLS Cert **Foxtrot**. Test Participant loads TLS Cert **Foxtrot** as the active TLS Server Cert.
6. All Trading Partners initiate an TLS connection (TLS Connection #3) with Test Participant. Within the TLS Handshaking, Test Participant sends TLS Cert **Foxtrot** as TLS Server Cert. All Trading Partners accept TLS Cert **Foxtrot** as the TLS Server Cert and use it to successfully complete the TLS Handshaking. The AS2 message is delivered, a good MDN received and the TLS connection completed with all Trading Partners.

## Test Case Q: Sending Multiple Certificates in a CEM Request

### Test Steps

1. Test Participant has Signing Cert **Bravo** and Encryption Cert **Delta** loaded and in use with all Trading Partners. Test Participant receives from all Trading Partners an encrypted message (Encrypted Message #4) with Encryption Cert **Delta** and return back good MDNs signed with Signing Cert **Bravo**.
2. Test Participant loads new Signing Cert **Golf** and new Encryption Cert **Hotel** and sends it to all Trading Partners. The two certificates can be sent via the same individual CEM Request message or in two separate CEM Request message at the discretion of the Test Participant. Good MDNs are received for all CEM Request messages.
3. All Trading Partners return CEM Response message with an *Accepted* state for Signing Cert **Golf** and Encryption Cert **Hotel**.
4. Test Participant receives from all Trading Partners an encrypted message (Encrypted Message #5) with Encryption Cert **Hotel** and returns back good MDNs signed with Signing Cert **Golf**.

## Test Case R: Sending One Certificate for Multiple Usages

### Test Steps

1. Test Participant has Signing Cert **Golf** and Encryption Cert **Hotel** loaded and in use with all Trading Partners. Test Participant receives from all Trading Partners an encrypted message (Encrypted Message #6) with Encryption Cert **Hotel** and return back good MDNs signed with Signing Cert **Golf**.
2. Test Participant loads new Cert **Zulu** for both Signing and Encryption and sends it to all Trading Partners in a CEM Request message. Good MDNs are received for all CEM Request messages.
3. All Trading Partners return CEM Response message with an *Accepted* state for Signing and Encryption Cert **Zulu**.
4. Test Participant receives from all Trading Partners an encrypted message (Encrypted Message #7) with Encryption Cert **Zulu** and returns back good MDNs signed with Signing Cert **Zulu**.

## Assigned AS2 and EDI Identifiers

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

| Company                           | AS2 Identifier       | EDI Qualifier | EDI Identifier |
|-----------------------------------|----------------------|---------------|----------------|
| Axway                             | axway -> transfer    | ZZ            | ax_transfer    |
| Axway                             | axway <> gateway     | ZZ            | ax_gateway     |
| BridgeGate                        | Bridge*Gate ]        | ZZ            | bridgegate     |
| Bridgeware                        | Bridge W a r e       | ZZ            | bridgeware     |
| Boomi Software                    | boomi                | ZZ            | boomi          |
| Cleo Communications               | CLEO                 | ZZ            | cleo           |
| Click Commerce, Inc.              | click(commerce)      | ZZ            | click          |
| The Descartes Systems Group, Inc. | D e s c a r t e s    | ZZ            | descartes      |
| EDS                               | EDS *Elit            | ZZ            | eds            |
| Extol International               | Extol;AS2            | ZZ            | extol          |
| GXS                               | GXS Interop          | ZZ            | gxs            |
| IBM                               | IBM_1                | ZZ            | ibm1           |
| IBM                               | 2nd IBM              | ZZ            | ibm2           |
| Inovis                            | inovis [test]        | ZZ            | inovis         |
| /n software inc.                  | n/Software           | ZZ            | nsoftware      |
| nuBridges, Inc.                   | truEDIINT            | ZZ            | nu_truedi      |
| nuBridges, Inc.                   | tru_Commerce         | ZZ            | nu_trucommerce |
| SEEBURGER AG                      | Seeburger            | ZZ            | seeburger      |
| Sterling Commerce                 | Sterling_1           | ZZ            | sterling1      |
| Sterling Commerce                 | SterComm-2           | ZZ            | sterling2      |
| Sterling Commerce                 | SC_No. 3             | ZZ            | sterling3      |
| Sterling Commerce                 | Sterling Commerce #4 | ZZ            | sterling4      |
| TIBCO Software Inc.               | www.tibco.com        | ZZ            | tibco          |
| Tumbleweed Communications Corp.   | Tumbleweed           | ZZ            | tumbleweed     |

## Overview of the DGI Interoperability Compliance Process®

Interoperability of B2B products for the Internet is essential for the long-term acceptance and growth of electronic commerce. To foster interoperability, DGI facilitates interoperability and conformance tests on open standards. 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 the [www.drummondgroup.com](http://www.drummondgroup.com) website.

Successful test completion also qualifies that particular product to participate in the next DGI Interoperability Test round, but does NOT guarantee successful completion of the full Interoperability Test Round. DGI makes no warrants or guarantees that products passing in the Queue Test Rounds will pass the Interoperability Tests.

## **DGI Interoperability Test Round**

Products-with-version from the previous AS2 Interoperability Test Round and products-with-version from the In-the-Queue tests come together in a vendor-neutral and non-competitive environment to test with each other in order to become interoperable with each other. In an Interoperability Test Round, each product-with-version must successfully test with each other in order to be certified as interoperable.

The DGI Interoperability Test Round verifies conformance to a standard and then verifies that members of the Product Test Group are interoperable among themselves. Interoperability is an all or nothing within the Product Test Group over the Test Criteria. A product is either interoperable with all other products in the Test Group or not.

Products-with-version which demonstrate complete interoperability among the passing members of the Product Test Group are given a Drummond Certified™ Seal and are listed with Interoperability Status on the [www.drummondgroup.com](http://www.drummondgroup.com) website. Interoperability Test Rounds are periodically repeated to verify that as product names, versions or releases change, the products remain interoperable.

## **InSitu™ Test System**

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

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

## **About Drummond Group Inc.**

Drummond Group Inc. (DGI) is an independent, privately held company that works with software vendors, vertical industries and the standards community to drive adoption of open 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).