Final Report

AS2 Interoperability Test

Second Quarter 2018 (2Q18)

June 28, 2018

Prepared & Facilitated by:
Drummond Group
www.drummondgroup.com

Table of Contents

Cover Letter

DRUMMOND GROUP is pleased to announce that the following participants in the AS2-2Q18 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 May 25 – May 30, 2018.

This AS2 interoperability testing continued to offer Optional Profile testing, all of which are very important. This included: AS2 Reliability, AS2 Restart, Certificate Exchange Messaging (CEM), Chunked Transfer Encoding (CTE), Multiple Attachments (MA), Filename Preservation (FN), Filename Preservation for MA (FN-MA), Filename Preservation with MDN Responses for Duplicate Filenames (FN-MDN), Secure Hash Algorithm 2 (SHA-2) and Chunked Transfer Encoding with AS2 Restart. More participants are now starting to support all optional profiles.

AS2 Restart allows the transfer of very large messages to resume from the last point of a network failure, thus allowing transfer of very large messages to be completed without re-sending the entire message.

SHA-2 (Secure Hashing Algorithm) addresses the need to offer both SHA-1 and SHA-2, as SHA-1 is being phased out, and SHA-2 is starting to be preferred for security reasons. Also, adding SHA-2 is driven by government applications that use AS2 and require SHA-2, such as the CSOS (Controlled Substances Ordering Systems) standard, and in Europe and U.S. the gas and energy industries. The SHA-2 optional profile cryptographic hash functions tested were: SHA-256, SHA-384, and SHA-512.

InSitu™, a patented test automation tool, continues to play a critical role. It allows for automated testing of AS2 Interop Required test cases in addition to being used for the Optional Profiles and AS2 ITQ testing.

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

Drummond Group continues to be dedicated to resolving AS2 software interoperability and expanding the AS2 standard to meet the needs of industry. If your company has questions or concerns about AS2 and its use in your industry, please send email to info2@drummondgroup.com. We welcome your input or questions.

Sincerely,

Aaron Gomez
Standards Certification
Drummond Group

Disclaimer

Drummond Group 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, Drummond Group 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 Drummond Group therefore makes no warranties, either express or implied, regarding any facet of the business conducted by the Participant.

Test Participants

Axway http://www.axway.com **Product Name:** **Axway B2Bi 2.3 / Activator 6.0**	**Axway** http://www.axway.com **Product Name:** **Axway Gateway 6.17**
Axway http://www.axway.com **Product Name:** **Axway SecureTransport 5.3**	**Axway** http://www.axway.com **Product Name:** **Axway TSIM 3.9**
Cleo http://www.cleo.com **Product Name:** **Cleo Harmony® v5.5 / Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5**	**Dell Boomi** http://www.boomi.com **Product Name:** **AtomSphere Jun '18**

DXC Technology http://www.dxc.com **Product Name:** **ELIT AS2 Connector v4.32 with AS2API v1.13 Engine**	**IBM** http://www.ibm.com **Product Name:** **IBM® Supply Chain Business Network® 17.1.1.0**
JSCAPE LLC http://www.jscape.com **Product Name:** **JSCAPE MFT Server 11.0**	**HelpSystems** http://www.goanywhere.com/ **Product Name:** **GoAnywhere MFT 5.7**
OpenText GXS www.opentext.com **Product Name:** **BizManager 4.0**	**RSSBus** http://www.rssbus.com/ **Product Name**: **RSSBus Connect 2018 using /n software EDI Integrator 2016**

Interoperability Test Summary

This is the 34th 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 (IETF EDIINT RFC 4130)

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 1Sync 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 MDN's. 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 to identify and resolve the problem.

The test round repeated the following optional profiles: AS2 Reliability, AS2 Restart, Filename Preservation (FN), Multiple Attachment (MA), Multiple Attachment with FN, Filename Preservation with MDN responses, and Certificate Exchange Messaging (CEM), and Secure Hashing Algorithm 2 (SHA-2).

Details of these profiles are included later in this document.

Interoperability Test History

This is the 34th Interoperability Test administered by Drummond Group.

AS2 1Q18 Interoperability Test – April – May	2018

Previous tests included the following:

AS2 3Q17 Interoperability Test – Aug – Nov	2017
AS2 1Q17 Interoperability Test – Mar – Apr	2017
AS2 1Q16 Interoperability Test – Mar – May	2016
AS2 3Q15 Interoperability Test – Aug – Nov	2015
AS2 1Q15 Interoperability Test – Mar – Apr	2015
AS2 3Q14 Interoperability Test – Aug – Nov	2014
AS2 1Q14 Interoperability Test – Mar – June	2014
AS2 3Q13 Interoperability Test – Aug – Nov	2013
AS2 1Q13 Interoperability Test – Mar – Jun	2013
AS2 3Q12 Interoperability Test – Aug – Nov	2012
AS2 1Q12 Interoperability Test – Mar – May	2012
AS2 3Q11 Interoperability Test – Sept – Nov	2011
AS2 1Q11 Interoperability Test – Mar – May	2011
AS2 3Q10 Interoperability Test – Sept – Nov	2010
AS2 1Q10 Interoperability Test – Mar – May	2010
AS2 3Q09 Interoperability Test – Sept – Nov	2009
AS2 1Q09 Interoperability Test – Apr – May	2009
AS2 3Q08 Interoperability Test – Sept – Oct	2008
AS2 1Q08 Interoperability Test – Mar – Apr	2008
AS2 3Q07 Interoperability Test – Sept – Nov	2007
AS2 1Q07 Interoperability Test – Feb – Apr	2007
AS2 3Q06 Interoperability Test – Sept – Oct	2006
AS2 1Q06 Interoperability Test – Feb – Mar	2006
AS2 3Q05 Interoperability Test – Sept – Oct	2005
AS2 1Q05 Interoperability Test – Feb – Apr	2005
AS2 3Q04 Interoperability Test – Aug – Sept	2004
AS2 1Q04 Interoperability Test – Feb – Mar	2004
AS2 3Q03 Interoperability Test – July – Sept	2003
AS2 1Q03 Interoperability Test – Jan – Feb	2003
AS2 2Q02 Interoperability Test – Mar – Aug	2002
AS2 2Q01 Interoperability Test – May – Aug	2001
AS2 4Q00 Interoperability Test – Oct – Dec	2000

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 Profiles) was completed in eight weeks. During the first seven weeks, the debug testing was focused on finding interoperability errors and correcting them. These testing weeks before the Certification test run are the most important as they ensure all interoperability issues are found and resolved. All test cases are repeated until no remaining issues remain. The Certification run is then executed where no code changes are allowed during last week of testing.

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 run, 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, the Drummond Group test automation tool, and by the participants themselves and demonstrated by uploading automatically the messages sent and received between each other. InSitu further checked all payloads exchanged for mismatches.

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 interoperability event have only 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 profile test cases).

To review the list of issues resolved in this and previous AS2 Interoperability tests please see the document found at:

http://www.drummondgroup.com/pdfs/AS2_Interoperability_Issues_Resolved.pdf

Optional Profiles

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

The AS2-Version header of some AS2 products supporting these features is 1.2, and each product includes the additional AS2 header EDIINT-Features (documented in IETF standard https://datatracker.ietf.org/doc/draft-meadors-ediint-features-header/).

The EDIINT-Features feature name (or value) for MA is: "multiple-attachments". The EDIINT-Features header name (or value) for CEM is "CEM". The EDIINT-Features feature name (or value) for Reliability is: "AS2-Reliability". Applications supporting several of these features, would include the following headers in AS2 messages, for example:

AS2-Version: 1.2
EDIINT-Features: CEM, multiple-attachments, AS2-Reliability

AS2 Reliability

The optional AS2 Reliability profile continued to be tested in this round. Along with completing the required test case, the participating products completed the optional AS2 Reliability testing in this test round.

"AS2 Reliability has the goal of ensuring that the AS2 protocol succeeds in exchanging business data payloads exactly once, provided that the network routing and transport (IP and TCP) layers are fully functional. That is, the goals for reliability are, first, that errors associated with HTTP server operation and server initiated sub processes do not prevent delivering messages or their receipt responses (MDNs) at least once and, second, that retry or resending operations made to compensate for these errors do not result in the same message payloads being submitted for further processing more than once. "

It is based on an IETF open standard, https://datatracker.ietf.org/doc/draft-duker-as2-reliability/.

AS2 Restart

The optional AS2 Restart profile continued to be tested in this round. Along with completing the required test case, the participating products implemented and completed the optional AS2 Restart testing in this test round. The introduction paragraph from the draft states:

> AS2 [RFC4130] has experienced widespread adoption and is continually being asked to send or receive larger files by the business community between its trading partners. As the size of the file transfers increase it has become evident that a mechanism is required that will allow trading partners to restart failed transfers from the point of failure. This document will outline a method of implementing a failed transfer restart mechanism using existing HTTP headers so backwards compatibility will exist with AS2 servers not wishing to support AS2 Restart.

It is based on an IETF open standard, https://datatracker.ietf.org/doc/draft-harding-as2-restart/

Certificate Exchange Messaging

The optional Certificate Exchange Messaging (CEM) continued to be tested in this test round. Along with completing the required test case, CEM participating products completed the optional CEM testing in this test round.

CEM is a standard 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. It is based on an IETF open standard, https://datatracker.ietf.org/doc/draft-meadors-certificate-exchange/. CEM provides for a secure and automated way of updating certificates which are due to expire.

Filename Preservation

The optional Filename Preservation (FN) profile continued to be tested in this test round. Along with completing the required test case, the products that took part completed the optional FN testing in this test round.

Based on an IETF open standard, https://datatracker.ietf.org/doc/draft-harding-ediint-filename-preservation/, 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.

Multiple Attachment

The optional Multiple Attachment (MA) profile continued to be tested in this test round. Along with completing the required test case, the products that took part completed the optional MA testing in this test round.

AS2 transmissions generally contain only a single EDI or XML payload document, and this is what has been solely tested within past Drummond Group 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 https://datatracker.ietf.org/doc/draft-meadors-multiple-attachments-ediint/, multiple attachment testing provides for the same security used in single payload AS2 transmission.

Filename Preservation for MA

The optional Filename Preservation for Multiple Attachments (FN-MA) profile continued to be tested in this test round. Along with completing the required and FN test cases the products that took part completed the FN for MA optional profile test cases in this test round.

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 MA test cases test indicated above, except that the participants confirmed the preservation of the payload filename for each attachment.

Filename Preservation with MDN Notification

Filename Preservation with MDN Notification (FN-MDN) continued to be offered. It focuses on preserving the Filename associated with the payloads sent and received during AS2 message exchanges as well, but in addition returns MDN notifications on duplicate filenames and error conditions. Returning MDN notifications on duplicate filenames is configurable as unique filenames may also be generated. Along with completing the required and FN test cases, the products that took part completed the optional FN with MDN notification in this test round.

Drummond Group documented the requirements for this profile, working in conjunction with AS2 vendors and the FSTC Technical Group. The requirements are available on Drummond Group website.

Filename Preservation with MDN Notification is especially important for the banking industry but its implementation is generic so it may be used by any industry.

Secure Hashing Algorithm 2 (SHA-2)

SHA-2 was offered for a second time this test event. Drummond Group continued the discussion and implementation details and documented the results in a document. The SHA-2 enhancement will be submitted to IETF in the future.

Interoperability Test Results - Optional Profiles

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

Also, please note that products certified in this 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 profile test cases).

Optional Profile – AS2 Reliability

The following companies and products took part in and successfully completed AS2 Reliability testing for both automatic Retry and Resend functionality. The "same message" with same MIC and Message-ID is retried or resent.

Company	Product
Axway	Axway B2Bi 2.3 / Activator 6.0
Cleo	Cleo Harmony® v5.5/ Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5
JSCAPE LLC	JSCAPE MFT Server 11.0
OpenText GXS	BizManager 4.0
RSSBus	RSSBus Connect 2018 using /n software EDI Integrator 2016

Optional Profile – AS2 Restart

The following companies and products took part in and successfully completed AS2 Restart testing. Network errors were introduced and the AS2 messages were retried from their last point of failure.

Company	Product
Axway	Axway B2Bi 2.3 / Activator 6.0
Cleo	Cleo Harmony® v5.5 / Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5
JSCAPE LLC	JSCAPE MFT Server 11.0
OpenText GXS	BizManager 4.0
RSSBus	RSSBus Connect 2018 using /n software EDI Integrator 2016

Optional Profile – SHA-2

The following companies and products also took part in and successfully completed SHA-2 testing.

Company	Product
Axway	Axway B2Bi 2.3 / Activator 6.0
Axway*	Axway SecureTransport 5.3
Cleo	Cleo Harmony® v5.5 / Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5
Dell Boomi	AtomSphere Jun ‘18
DXC Technology	ELIT AS2 Connector v4.32 with AS2API v1.13 Engine
HelpSystems	GoAnywhere MFT 5.7
JSCAPE LLC	JSCAPE MFT Server 11.0
OpenText GXS	BizManager 4.0
RSSBus	RSSBus Connect 2018 using /n software EDI Integrator 2016

Axway SecureTransport supported SHA-256, SHA-384 both inbound and outbound. SHA-512 was not supported.

Optional Profile – Chunked Transfer Encoding

The following companies and products also took part in and successfully completed Chunked Transfer Encoding testing. Where the participant only tested Chunked Transfer Encoding as a Recipient an asterisk appears after the company name. Otherwise, participants tested both sending and receiving Chunked Transfer Encoding.

Company	Product
Axway	Axway B2Bi 2.3 / Activator 6.0
Cleo	Cleo Harmony® v5.5 / Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5
DXC Technology	ELIT AS2 Connector v4.32 with AS2API v1.13 Engine
HelpSystems	GoAnywhere MFT 5.7
JSCAPE LLC	JSCAPE MFT Server 11.0
OpenText GXS	BizManager 4.0
RSSBus	RSSBus Connect 2018 using /n software EDI Integrator 2016

(*) Like other test cases, Chunked Transfer Encoding (CTE) was tested outbound and inbound. Participants that only tested Chunked Transfer Encoding (CTE), as a Recipient (inbound), are indicated with an asterisk after CTE.

Optional Profile - Filename Preservation

The following companies and products also took part in and successfully completed Filename Preservation both Inbound and Outbound messages. The filename provided by the sender was preserved on the receiving side.

Company	Product
Axway	Axway B2Bi 2.3 / Activator 6.0
Axway	Axway Gateway 6.17
Axway	Axway TSIM 3.9
Cleo	Cleo Harmony® v5.5 / Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5
DXC Technology	ELIT AS2 Connector v4.32 with AS2API v1.13 Engine
HelpSystems	GoAnywhere MFT 5.7
JSCAPE LLC	JSCAPE MFT Server 11.0
OpenText GXS	BizManager 4.0
RSSBus	RSSBus Connect 2018 using /n software EDI Integrator 2016

Optional Profile - MA

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

Company	Product
Axway	Axway B2Bi 2.3 / Activator 6.0
Axway	Axway TSIM 3.9
Cleo	Cleo Harmony® v5.5 / Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5
HelpSystems	GoAnywhere MFT 5.7
JSCAPE LLC	JSCAPE MFT Server 11.0
OpenText GXS	BizManager 4.0
RSSBus	RSSBus Connect 2018 using /n software EDI Integrator 2016

Optional Profile - Filename Preservation for MA

The following companies and products also took part in and successfully completed Filename Preservation for Inbound MA messages. The filename is provided by the sender for each attached payload, and is preserved on the receiving side for all attached payloads.

Company	Product
Axway	Axway B2Bi 2.3 / Activator 6.0
Axway	Axway TSIM 3.9
Cleo	Cleo Harmony® v5.5 / Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5
HelpSystems	GoAnywhere MFT 5.7
JSCAPE LLC	JSCAPE MFT Server 11.0
OpenText GXS	BizManager 4.0
RSSBus	RSSBus Connect 2018 using /n software EDI Integrator 2016

Optional Profile - Filename Preservation with MDN Notification

The following companies and products also took part in and successfully completed Filename Preservation with MDN Notification. MDN notifications on error conditions were sent by the receiving side. The filename provided is either preserved or not, depending on the test cases executed and the receiving side configuration.

Company	Product
Axway	Axway TSIM 3.9
Cleo	Cleo Harmony® v5.5 / Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5
RSSBus	RSSBus Connect 2018 using /n software EDI Integrator 2016

Optional Profile - CEM

The following companies and products also took part in and successfully completed Certificate Exchange Messaging (CEM) Optional testing for this round. CEM message exchange was tested in both directions.

Company	Product
Axway	Axway B2Bi 2.3 / Activator 6.0
Cleo	Cleo Harmony® v5.5 / Cleo VLTrader® v5.5 / Cleo LexiCom® v5.5
RSSBus	RSSBus Connect 2018 using /n software EDI Integrator 2016

Note on Payload CRC Check Performed by InSitu

For each test case, InSitu computes a CRC on the payloads received and uploaded to the InSitu database by the Originator and Recipient participants. Test Cases with uploaded payloads that do not have a matching CRC are flagged for further inspection. The CRC is performed on all payloads regardless of data type, for instance EDI, XML, PDF, TIF, etc.

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 Drummond Group 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. Drummond Group 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-versions are interoperable under the *Test Criteria*.

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 SSL 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.

Drummond Group 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 tests cases with the other participants. These tests 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

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 https://datatracker.ietf.org/doc/rfc5402/. 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 1Sync 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.
  1Sync 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:

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

Required Test Case B:

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

Required Test Case C:

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

Test Description	The initiator creates an encrypted, compressed exchange over HTTP with a request for a synchronous, signed MDN.
Message Payload	Test Data # 4
Message Transport	HTTP
Message Security	Encryption
Message Compression	Yes
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Required Test Case E:

Test Description	The initiator creates an encrypted exchange over HTTP with a request for a synchronous, signed MDN.
Message Payload	Test Data # 5
Message Transport	HTTP
Message Security	Encryption
Message Compression	No
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Required Test Case F:

Test Description	The initiator creates a signed exchange over HTTP with a request for a synchronous, signed MDN.
Message Payload	Test Data # 6
Message Transport	HTTP
Message Security	Signature
Message Compression	No
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Required Test Case G:

Test Description	The initiator creates a signed, compressed exchange over HTTPs with a request for a synchronous, signed MDN.
Message Payload	Test Data # 7
Message Transport	HTTPs
Message Security	Signature
Message Compression	Yes
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The payload is successfully transferred. The MDN with a disposition value of "processed" is returned.

Required Test Case H:

Test Description	The initiator creates a signed exchange over HTTPs with a request for an asynchronous, signed MDN over HTTP.
Message Payload	Test Data # 8
Message Transport	HTTPs
Message Security	Signature
Message Compression	No
MDN Transport	Asynchronous/HTTP
MDN Security	Signature
Expected Results	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:

Test Description	The initiator creates a signed exchange over HTTPs with a request for an asynchronous, signed MDN.
Message Payload	Test Data # 9
Message Transport	HTTPs
Message Security	Signature
Message Compression	No
MDN Transport	Asynchronous/HTTPs
MDN Security	Signature
Expected Results	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:

Test Description	The initiator creates a signed, encrypted, compressed exchange over HTTP with a request for an asynchronous, signed MDN.
Message Payload	Test Data # 10
Message Transport	HTTP
Message Security	Signed, Encryption
Message Compression	Yes
MDN Transport	Asynchronous/HTTP
MDN Security	Signature
Expected Results	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:

Test Description	The Drummond Group test administrator sends a corrupted signed message to the participant. The data signed over is altered after the digital signature is created and applied. The recipient should not be able to match the digital signature with the payload. The participant must return a MDN with the disposition value correctly identifying the error.
Message Payload	Test Data # 1
Message Transport	HTTP
Message Security	Signed
Message Compression	No
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The MDN is returned with a disposition type, modifier and extension of either "processed/error: authentication-failed" or "processed/error: integrity-check-failed".

Required Test Case K.2:

Test Description	The Drummond Group test administrator sends a improperly encrypted message to the participant. The payload data is encrypted using a different certificate than that of the recipient. As a result, the recipient should not be able to decrypt the encrypted MIME body part. The participant must return a MDN with the disposition value correctly identifying the decryption error.
Message Payload	Test Data # 1
Message Transport	HTTP
Message Security	Encryption
Message Compression	No
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The MDN is returned with a disposition type, modifier and extension of "processed/error: decryption-failed".

Required Test Case K.3:

Test Description	The Drummond Group test administrator sends a corrupted compressed message to the participant. The compressed data structure is altered. The recipient should not be able to decompress the compressed MIME body part. The participant must return a MDN with the disposition value correctly identifying the error.
Message Payload	Test Data # 1
Message Transport	HTTP
Message Security	None
Message Compression	Yes
MDN Transport	Synchronous
MDN Security	Signature
Expected Results	The MDN is returned with a disposition type, modifier and extension of either "processed/error: decompression-failed" or "unexpected-processing-error".

Optional Profile – AS2 Reliability

AS2 Reliability Overview

With the wide use of AS2 in different industry verticals, the demand on the reliability of AS2 transactions has increased tremendously since AS2 was first introduced and adopted. Now, we hear of millions of transactions per day and a wide variety of document types and sizes being exchanged between heterogeneous environments. The requirement for guaranteed delivery has never been greater. To this end, the AS2 Reliability draft has been proposed. This document describes the testing methods that will be used for certifying AS2 products to the AS2 Reliability draft specification.

AS2 Reliability Concepts

AS2 reliability is a draft IETF specification (https://datatracker.ietf.org/doc/draft-duker-as2-reliability/) for guaranteed delivery, duplicate message elimination, which will enable "reliable" communication between AS2 servers. It extends the AS2 RFC 4130 standard and in essence recognizes error scenarios which may occur during message transfers. Recovery from these error scenarios is described as retrying a message and resending a message.

AS2 Reliability Retries – Transient Network Errors

Retries is related to an Originator sending an AS2 message and encountering a network related error in the process. The AS2 message may request a Synchronous or Asynchronous MDN it does not matter. The point is that the Originator did not receive the expected 200 OK in response to the POST, instead it received for instance a 503 response or no response at all. The following diagram depicts this scenario:

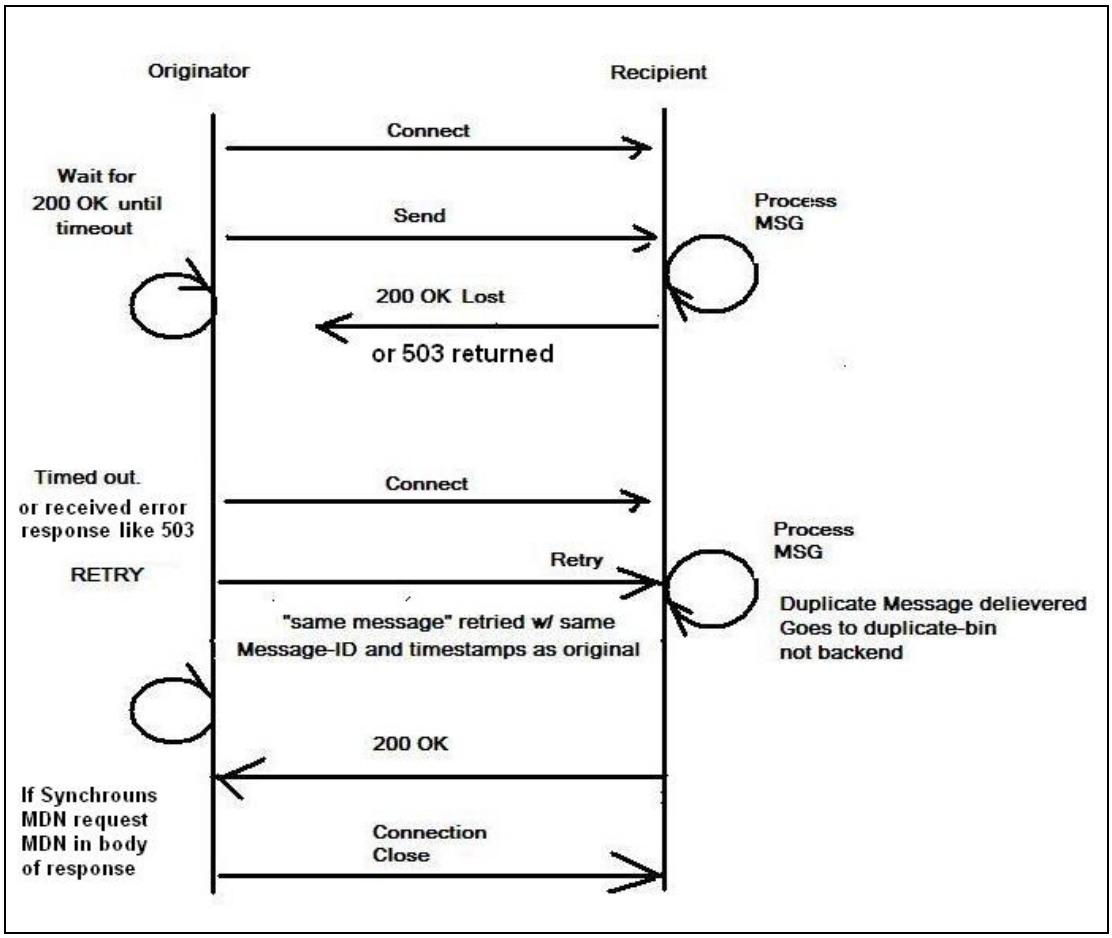

Figure 1 Diagram showing Retry logic

The Originator may 'retry" the AS2 message again, that is send it again in order to recover from this network related failure. If the originating AS2 system is configured to recover from such errors, then it must retry the "same message", and not repackage the payload. The recipient, upon receiving the second message, can now detect that the second (or third, depending on how many retry attempts have been configured on the originator side) incoming message is a duplicate (based on the fact that the same Message-ID) and not deliver to the payload to the backend system for processing. Instead, the receiving system can tag it as a duplicate message.

AS2 Reliability Resends -- Asynchronous AS2 Protocol Breakdown

Resends is related to an Originator sending an AS2 message and requesting an Asynchronous MDN. If the Asynchronous MDN is not received by the Originator, this is considered a failure, but the Originator may 'resend" the original message in order to recover from this failure. If the originating AS2 system is configured to recover from such errors, then it must resend the same message, and not repackage the payload. The recipient, upon receiving the second message, can now detect that the second (or third, depending on how many retry attempts have been configured on the originator side) incoming message is a duplicate (based on the fact that the same Message-ID) and not deliver to the backend system for processing. Instead, the receiving system can tag it as a duplicate message.

Furthermore, the Recipient may resend the same Async MDN as originally received. The original-message-id and received-mic-value must be the same as the original Async MDN the Recipient originally responded with.

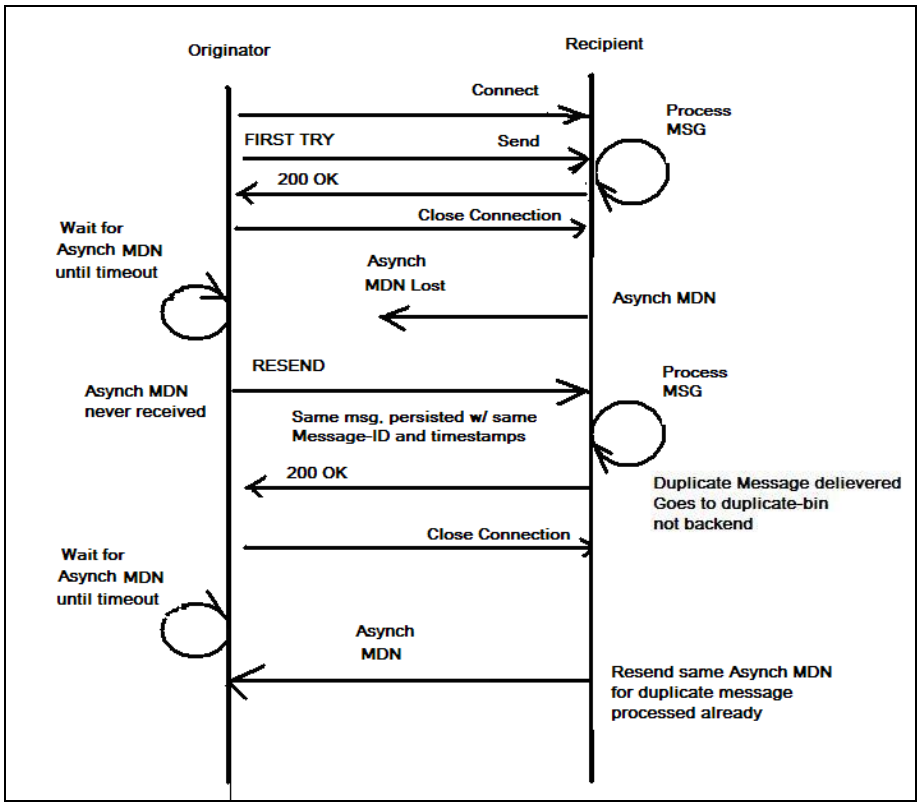

Figure 2 Diagram showing Resend logic

AS2 Reliability Test Criteria

AS2 Reliability Test Case Overview

To demonstrate reliable message exchange, each AS2 product will exchange messages with every other participant in the test group. Failure conditions will be simulated so as to induce “retries” and “resends”. Participants will confirm that the same message as in the original transmission was reused in subsequent retries or resends.

Test Case	Msg Payload	Msg Transport	Msg Security	Compression	MDN Transport	MDN Security
A-R	Data #1	HTTP	Signed	No	Sync	Unsigned
C-R	Data #3	HTTP	Signed	No	Async/HTTP	Signed

AS2 Reliability Test Data

Drummond Group provides the payload data for the test cases. Test data will be supplied and individual payloads assigned to test cases at the beginning of the test.

1. Test Data #1 (test_data_1.edi). X12 PO with an apostrophe (‘!’) for segment terminator. Size is 12kB.
2. Test Data #3 (test_data_3.xml). 1Synch XML file. Size is 9kB.

AS2 Reliability Test Case Execution

Each participant acts as both originator and recipient for each test case with every other participant. For the outbound test case, the originator is to apply the required security to the test data specified for each test case. The recipient of each test case must have a conformant HTTP server listening for the message which is to be processed by its AS2 product (HTTP server may be embedded within AS2 product).

AS2 Reliability Test Case Description

Reliability TC A-R - Retry, Request Synchronous MDN

Test Description: The initiator creates a signed exchange over HTTP with a request for a synchronous, unsigned MDN.

Message Payload: Test Data # 1 (X12)

Message Transport: HTTP

Message Security: Signature

Message Compression: No

MDN Transport: Synchronous

MDN Security: No Signature

Expected Results: The payload is successfully transferred on the second retry. The MDN with a disposition value of "processed" is returned.

Reliability TC C-R - Resend, Request Asynchronous MDN

Test Description: The initiator creates an signed exchange over HTTP with a request for an asynchronous, signed MDN.

Message Payload: Test Data # 3 (XML)

Message Transport: HTTP

Message Security: Signed

Message Compression: No

MDN Transport: Asynchronous/HTTP

MDN Security: Signature

Expected Results: The payload is successfully transferred on the second resend attempt. An asynchronous MDN with a disposition value of "processed" is returned over a new HTTP connection.

Optional Profile – AS2 Restart

AS2 Restart testing built on top of the AS2 Reliability test cases and also utilized the InSituClient Interceptor to introduce network errors on AS2 message exchanges. The J payload was increased to 200 MB and the Interceptor introduced up to 9 network errors. Participants successfully resent from the last point of failure each time a network error occurred and the successfully processed the AS2 message.

The test cases were then repeated with Chunked Transfer Encoding enabled.

Optional Profile – Chunked Transfer Encoding

CTE Overview

Chunked Transfer Encoding (CTE) is a mechanism that allows HTTP messages to be split in several parts. This can be applied to both HTTP requests (from client to server) and HTTP responses (from server to client). For example, let us consider the way in which an HTTP server may transmit data to a client application (usually a web browser). Normally, data delivered in HTTP responses is sent in one piece, whose length is indicated by the Content-Length header field. The length of the data is important, because the client needs to know where the response ends and any following response starts.

With chunked encoding however, the data is broken up into a series of blocks of data and transmitted in one or more "chunks" so that a server may start sending data before it knows the final size of the content that it's sending. Often, the size of these blocks is the same, but this is not always the case. (Reference: http://en.wikipedia.org/wiki/Chunked_transfer_encoding)

CTE Test Cases

The test cases used are similar to those used in AS2 Required testing except that Chunked Transfer Encoding was used to exchange the messages.. In particular, test cases A, B, G and J were used.

Optional Profile – Multiple Attachments

The Multiple Attachment test cases were optional. Details of these test cases follow below. The MA test cases are based on the IETF draft: https://datatracker.ietf.org/doc/draft-meadors-multiple-attachments-ediint/ which states:

> "The primary work of EDI-INT (AS2) was to develop a secure means of transporting EDI documents over the Internet. This was described in the three working group developed standards for secure transport over SMTP [AS1], HTTP [AS2] and FTP [AS3]. For most uses of EDI, all
> relevant information to complete a single business transaction could be stored in a single document. As adoption of EDI-INT grew, new industries and businesses began using AS2 and needing to include multiple documents in a single message to complete a trading partner transaction. These documents were a variety of MIME media types.
>
> This informational draft describes how to use the MIME multipart/related envelope structure within EDI-INT messages to store
> multiple document attachments. Details of computing the MIC value over this envelope is covered. A minimum listing of MIME media types to support within the multipart/related envelope is given along with information on extracting these documents."

MA Test Case Execution

The originator creates a Multipart-Related MIME structure with a type parameter of "application/xml", "application/pdf", "application/tif" depending on the attachments. The attachments (test data) for each test case are indicated in the table, and can be cross referenced to the Test Data list. The Multipart-Related structure has the security settings applied according to the Test Case Table and sent requesting a signed or unsigned MDN as indicated for each test case.

The recipient is able to extract the number of attachments and return an MDN with the expected MIC calculation in the signed or unsigned MDN.

Optional MA Test Cases

The 10 MA test cases mimic the 10 required test cases in terms of security, transport, and MDN configuration except that two payloads are included vs one, except for one test case which has four payloads instead of two. Below is a summary of the test cases and which test data is used for what payload part.

Test Case	Payload Part - Payload	Msg Transport	Msg Security	Compressed	MDN Transport	MDN Security
MA-A	1 – MA Data 1 2 – MA Data 3	HTTP	Signed/Encrypted	No	Sync	Unsigned
MA-B	1 – MA Data 2 2 – MA Data 5	HTTP	Signed/Encrypted	No	Sync	Signed
MA-C	1 – MA Data 3 2 – MA Data 4	HTTP	Signed/Encrypted	No	Async/HTTPS	Signed
MA-D	1 – MA Data 4 2 – MA Data 5	HTTP	Encrypted	Yes	Sync	Signed
MA-E	1 – MA Data 2 2 – MA Data 5	HTTP	Encrypted	No	Sync	Signed
MA-F	1 – MA Data 1 2 – MA Data 3	HTTP	Signed	No	Sync	Signed
MA-G	1 – MA Data 1 2 – MA Data 3	HTTPS	Signed	Yes	Sync	Signed
MA-H	1 – MA Data 2 2 – MA Data 5	HTTPS	Signed	No	Async/HTTP	Signed
MA-I	1 – MA Data 1 2 – MA Data 3	HTTPS	Signed	No	Async/HTTPS	Signed
MA-J	1 – MA Data 1 2 – MA Data 2 3 – MA Data 3 4 – MA Data 5	HTTP	Signed/Encrypted	Yes	Async/HTTP	Signed

MA Test Data

MA Data 1 - ma_test_data_1.xml
MA Data 2 - ma_test_data_2.xml
MA Data 3 - z_ma_test_data_2.pdf
MA Data 4 - z_ma_test_data_3.pdf
MA Data 5 - z_ma_test_data_4.TIF

Optional Profile – Filename Preservation

The Filename Preservation Test cases were optional. Details of these test cases follow below. The FN test cases are based on the IETF draft (mirrored at) : https://datatracker.ietf.org/doc/draft-harding-ediint-filename-preservation/ which states:

"

1. Introduction

   This document describes a method of filename preservation utilizing the Content-Disposition MIME header[RFC 2183]. This document will further define the use of available optional parameters as described in RFC 2183, and any issues involved with implementing this informational document.

2. Requirements

   An EDIINT compliant system that implements this informational document MUST preserve the filename of an EDI business document during packaging and transport of the EDIINT MIME message to its trading partner.

   The recipient of the EDIINT MIME message MUST be able to retrieve the filename of the MIME wrapped EDI business document and transfer the received file to its backend system using the received filename.

   Since there are many ways in which files can be delivered to an EDIINT compliant application from their backend, this document will only focus on preserving the filename within the EDIINT MIME message."

FN Test Case Execution

The originator creates an AS2 message a Content-Disposition included in the MIME header. The AS2 message is sent the receiving participant which extracts the payload and names it according to the value provided in the Content-Disposition.

The recipient is able to extract the single attachment and return an MDN with the expected MIC calculation in the signed or unsigned MDN. In the case of the filename already in existence, no indication of existing duplicate files is reported by the recipient in the returned MDN.

Optional FN Test Cases

Test Case	Msg Payload	Msg Transport	Msg Security	Compression	MDN Transport	MDN Security
VF -A	Data #1	HTTP	Signed/Encrypted	No	Sync	Unsigned
VF -D	Data #4	HTTP	Encrypted	Yes	Sync	Signed
VF -E	Data #5	HTTP	Encrypted	No	Sync	Signed
VF -F	Data #6	HTTP	Signed	No	Sync	Signed
VF -G	Data #7	HTTPs	Signed	Yes	Sync	Signed
VF -J	Data #10	HTTP	Signed/Encrypted	Yes	Async/HTTP	Signed

Test Data

The Test Data used is exactly the same as the required test case. Please see the required test data description for details on the test data.

Optional Profile – Filename Preservation for MA

Similar to the Filename Preservation profile, the FN for MA further enhances FN to include preservation of the filename when Multiple Attachments are sent. The same IETF FN draft specification applies as it documents that the content-disposition header may be included in the MIME bodyParts of an MA AS2 message.

The FN draft specification, in addition to what is indicated under the section Filename Preservation, that:

> The Content-Disposition header will be added to the MIME bodyPart that encapsulates the EDI business document. If the EDIINT MIME message contains multiple attachments(See [MA]) then each individual MIME bodyPart that encapsulates an attachment will have its own Content-Disposition header describing the filename of the attachment.

FN-MA Test Case Execution

The originator creates an AS2 message a Content-Disposition included in the MIME header of each attachment. The AS2 message is sent to the receiving participant who extracts the payloads and names them according to the value provided in the Content-Disposition of each MIME bodyPart.

The recipient is able to extract the multiple attachments and return an MDN with the expected MIC calculation in the signed or unsigned MDN. In the case of the filename already in existence, no indication of existing duplicates is reported by the recipient in the returned MDN.

Optional FN-MA Test Cases

The MA test cases were used as indicated in the MA Optional Profile.

FN-MA Test Data

The Test Data used is the same as the MA test data.. Please see the MA test data description for details on the test data.

Optional Profile – Filename Preservation with MDN

FN with MDN Overview

AS2 Filename Preservation addresses the need to communicate a payload filename provided by the sender to the recipient. This requirement has been document in the IETF Filename Preservation draft (see Addendum). The need for this requirement originated with the Financial Services Technical Consortium (fstc.org).

However, the IETF Filename Preservation draft currently does not address filename preservation error scenarios, for instance when a filename is already in use. The purpose of this document is to document these scenarios where content-based MDN responses are to be returned and under what conditions.

FN with MDN Business Context

Trading Partners that provide a filename with AS2 payloads desire to be notified if that filename is already in existence. This notification takes on the form of content-based MDN responses in AS2 which serve as alerts or notifications to the sending Trading Partner. The receiving AS2 system should therefore not overwrite the existing duplicate filename nor submit this duplicate payload for backend processing.

FN with MDN Functional Requirements

As already stated, sending Trading Partners want to be notified when a filename that was provided for a payload is already in use on the receiving side (or has been submitted for backend processing).

The receiving system may take on one of two responses:

1. write the incoming payload out but give it a unique name, or
2. reject the incoming payload and not write it out

In each case, a content-based MDN is returned to the Sending Trading Partner alerting them of the conflict. Which response the receiving side takes on depends on its configuration capability. Some AS2 receiving systems may be capable of being configured on a Trading Partner bases, thus the response is contingent on trading partner agreements between the recipient and the sender. In other AS2 receiving systems, the only configuration capability is at a global level, thus all trading partners receive one or the other response.

FN MDN Responses

MDNs are typically returned to the Sending Trading Partner to indicate success or failure for the sent message. That is, to indicate that the message was delivered without error, or to indicate an error in processing, for instance signature validation or decryption. These are known as message processing errors.

As discussed here, a content-based MDN response indicates that processing of the incoming AS2 message was successful (i.e., signature validation and decryption succeeded) however, a business-level requirement associated with the content failed. For instance, the content (payload) did not have the appropriate EDI identifiers or the filename suggested for the content (payload) was already in use.

AS2 Filename MDN Responses are content-based MDNs.

Filename Preservation MDN Responses

The three types of errors or warnings that may arise during a filename write operation are:

1. Content-Disposition (filename) duplicate filename
2. Content-Disposition (filename) filename string badly formed
3. Content-Disposition (filename) filename not received but expected

Additional error conditions will be documented in future revisions of this document, if any.

The sending trading partner MUST be notified of either of these types of errors with a Positive MDN/Warning or Negative MDN/Failure. The type of MDN a sending trading partner receives depends on the trading partner configuration on the receiving side derived from upfront trading partner agreements, and AS2 server configuration capability.

FN MDN Rules

The rules for these MDNs are as follows:

1. **Positive MDN with Warning Level**: Recipient Sends back positive MDN with warning level and text describing the error. For instance, “duplicate filename encountered”. This type of MDN is returned when the AS2 receiving system is configured to write out the incoming payload, regardless of any these three error conditions.

   Again, the incoming payload with any of the three types of error conditions is given a unique name and MUST be written out. The incoming payload MUST not be provided to the backend system for processing until the transaction (payload) error condition is reconciled between the two parties. The unique name generated of the offending payload SHOULD give some indication to the end-user that an error of some sort occurred, for instance pre-pending a string “dup_” to the unique filename (e.g., dup_unique_filename.ext) or by placing it an inbound directory reserved for messages with error conditions.

2. **Negative MDN with Error Level:** Recipient Rejects incoming AS2 message and replies back with negative MDN, and text describing the error for instance, “payload rejected, duplicate filename” error. The incoming payload MUST not be written out. It is the responsibility of the sending trading partner to resend the message without any error conditions.

Format of Positive MDNs with Warnings

In the situation described above, the "AS2-disposition-type" MUST be set to the value of "processed", and the AS2-disposition-modifier set to the "warning" value.

The "warning" AS2-disposition-modifier MUST be used with the "processed" disposition-type to indicate that the message was successfully processed but that an exception condition occurred.

A "warning:" AS2-disposition-modifier-extension MUST be used to combine the indication of a warning with the payload warning conditions.

The following Dispositions examples MUST be supported

```
Disposition: automatic-action/MDN-sent-automatically;
  processed/warning: Duplicate-filename-encountered, unique filename
generated

Disposition: automatic-action/MDN-sent-automatically;
  processed/warning: Illegal filename, unique filename generated

Disposition: automatic-action/MDN-sent-automatically;
 processed/warning: Filename for payload not provided, unique filename generated
```

Format of Negative MDNs with Failures

In the situation described above, the "AS2-disposition-type" MUST be set to the value of "failed", and the AS2-disposition-modifier set to the "failure" value.

A "failure:" AS2-disposition-modifier-extension MUST be used to combine the indication of the error with the payload error conditions.

The following Dispositions examples MUST be supported

```
Disposition: automatic-action/MDN-sent-automatically;
  failed/failure: Duplicate-filename-encountered, payload rejected

Disposition: automatic-action/MDN-sent-automatically;
  failed/failure: Illegal filename, payload rejected

 Disposition: automatic-action/MDN-sent-automatically;
  failed/failure: Filename for payload not provided, payload rejected
```

FN with MDN Test Case Execution

Each participant ran Test Cases for Synchronous MDN request first. Each participant then repeated for Asynchronous MDN request.

The recipient is able to extract the single attachment and return an MDN with the expected MIC and correct MDN Disposition.

FN with MDN Test Data

An EDI file was used (FN_test_data_1.edi) for testing. Each participant modified the payload's to and from so as to make valid for each participant to participant message exchange.

Optional Profile - Certificate Exchange Messaging

CEM Overview

Certificate Exchange Messaging (CEM), https://datatracker.ietf.org/doc/draft-meadors-certificate-exchange/, 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.

CEM Test Case Execution

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.

CEM Test Cases

CEM Test Case: 1 – Handling of New Signature Certificate
CEM Test Case: 2 – Handling of New Encryption Certificate
CEM Test Case: 3 – Handling of New TLS Certificate
CEM Test Case: 4 – Sending Multiple Certificates in a CEM Request
CEM Test Case: 5 – Sending One Certificate for Multiple Usages
CEM Test Case: 6 – Handling of Different Certificates among Different Trading Partners

Optional Profile – Secure Hashing Algorithm 2 (SHA-2)

SHA-2 Overview

In cryptography, **SHA-2** is a set of cryptographic hash functions (**SHA-224, SHA-256, SHA-384, SHA-512**) designed by the National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. SHA-2 includes a significant number of changes from its predecessor, SHA-1. SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits. (ref: wikipedia.com)

SHA-2 Test Case Execution

The SHA-2 test cases mimic the 10 required test cases in terms of security, transport, and MDN configuration except that each test case is executed 3 times, one time each algorithm strength. The payloads used for the required test cases were also used for the SHA-2 test cases. SHA-224 was not tested as the products, by design, did not include it.

SHA-2 Test Cases

Test Case A - Executed with 256, 384, 512 strengths
Test Case B - Executed with 256, 384, 512 strengths
Test Case C - Executed with 256, 384, 512 strengths
Test Case D - Executed with 256, 384, 512 strengths
Test Case E - Executed with 256, 384, 512 strengths
Test Case F - Executed with 256, 384, 512 strengths
Test Case G - Executed with 256, 384, 512 strengths
Test Case H - Executed with 256, 384, 512 strengths
Test Case I - Executed with 256, 384, 512 strengths
Test Case J - Executed with 256, 384, 512 strengths

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 -> interchange	ZZ	ax_interchange
Axway	axway <> gateway	ZZ	ax_gateway
Axway	secureTransport !	ZZ	ax_transport
Axway	a x w a y - > T SIM	ZZ	axwaytsim
Cleo	CLEO	ZZ	cleo
Dell Boomi	d e l l boomi *	ZZ	dellboomi
DXC Technology	DXC *Elit	ZZ	hp
HelpSystems	Help _ S y s t em s !	ZZ	linoma
IBM®	ibm s c b n - /	ZZ	ibmscbn
JSCAPE LLC	J S c a p e * / -	ZZ	jscape
OpenText GXS	opentext [test]	ZZ	opentext
RSSBus	r s s - b u s *	ZZ	rssbus

Overview of the Drummond Group 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, Drummond Group facilitates interoperability and conformance tests on open standards. This section contains a description of the test process involved with creating and listing interoperable products.

Drummond Group In-the-Queue Test Round

In-the-Queue Test Rounds are designed to allow participants—with products new to Drummond Group 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 Drummond Group Test Server.

The Drummond Group 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 Drummond Group 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 Drummond Group Test Server products. Products which successfully complete In the Queue Test Rounds are considered compliant to the respective standard and will be listed on the www.drummondgroup.com website as “In the Queue," but they will not be given product Interoperability Status on the www.drummondgroup.com website.

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

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

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

InSitu™ Test System

Drummond Group 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

Drummond Group is the trusted interoperability test lab offering global testing services through the product life cycle. Auditing, QA, conformance testing, custom software test lab services, and consulting are offered in addition to interoperability testing. Founded in 1999, Drummond Group has tested over a thousand international software products used in vertical industries such as automotive, consumer product goods, healthcare, energy, financial services, government, petroleum, pharmaceutical and retail. For more information, please visit www.drummondgroup.com or email: info2@drummondgroup.com