# Final Report

## AS2 Interoperability Test

## Second Quarter 2025 (2Q25)

**May 23, 2025**

Prepared & Facilitated by:
Drummond
www.drummondgroup.com

# Table of Contents

# Cover Letter

DRUMMOND is pleased to announce that, for the AS2-2Q25 Interoperability Test Event, these participants have completed all requirements and have passed all required test cases between each product demonstrating interoperability and conformance. (See Interoperability Test Summary below.)

This test event continued to provide test suites with stronger SHA-2 and AES algorithms and HTTPS transport that are more commonly implemented in real-world deployments. Additionally, the previously named AS2 Cloud tests are now referred to as *Authentication* tests since we have found non-Cloud environments also use this security mechanism.

This test event also continued to offer these Optional Profile tests: AS2 Reliability, AS2 Restart, Advanced Encryption Standard (AES), Certificate Exchange Messaging (CEM), Chunked Transfer Encoding (CTE), Filename Preservation (FN), Filename Preservation for MA (FN-MA), Filename Preservation with MDN Responses for Duplicate Filenames (FN-MDN), Multiple Attachments (MA), Secure Hash Algorithm 2 (SHA2) and Chunked Transfer Encoding with AS2 Restart. Full descriptions are contained within this document.

InSitu™, a trusted and proprietary test automation tool, continues to play a crucial role in full-matrix testing, especially as more and more test suites are added to a test run. It allows for automated testing of AS2 Interoperability Required and Optional test cases, in addition to being used for AS2 Pre-Certification testing.

Please note that an AS2 interoperability certification indicates the interoperability of a specific product-with-version, within a specific group of other products-with-version for a given test event, i.e., AS2-2Q25. Products certified in this test event may not be interoperable with products-with-version from previous test events, and interoperability test events must be periodically repeated to verify that as product names, versions or releases change, they remain interoperable. The relevance of an AS2 test event certification within real world deployments diminishes over time as new products enter the market and existing products change with revisions and updates. Given such changes in the product test group, an interoperability certification does not guarantee perpetual interoperability within real world deployments, and interoperability test events must be repeated to include new products, unchanged existing products, and existing products with new versions. From a market perspective, interoperability typically only lasts for 6-12 months.

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

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

# Disclaimer

Drummond conducts interoperability and conformance testing in a neutral test environment for various companies and organizations (referred to hereafter as "the Participant") on open technical standards. At the end of the testing process, Drummond may list the name of the Participant in the Final Report along with an indication that the Participant passed the test. The fact that the name of the Participant appears in this Final Report is not an endorsement of the Participant nor its products or services, and Drummond therefore makes no warranties, either express or implied, regarding any facet of the business conducted by the Participant.

## Test Participants

| | |
|---|---|
| **Amazon Web Services**<br>https://aws.amazon.com/aws-transfer-family/as2/<br>**Product Name:** **AWS Transfer Family** | **Axway**<br>http://www.axway.com<br>**Product Name:** **Axway B2Bi 2.6 / Activator 6.1** |
| **Axway**<br>http://www.axway.com<br>**Product Name:** **Axway TSIM 3.9** | **Axway**<br>http://www.axway.com<br>**Product Name:** **Axway SecureTransport 5.5** |
| **Beijing Sinowintop**<br>www.sinowintop.com<br>**Product Name**: **EasyLink v2.0** | **CData Software**<br>https://arc.cdata.com/<br>**Product Name:** **CData Arc™ 2025 - 25.1.9231.0** |

| | |
|---|---|
| **Cleo**<br><br>*http://www.cleo.com*<br><br>**Product Name:** **Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®)** | **DXC Technology**<br><br>*dxc.com*<br><br>**Product Name:** **ELIT AS2 Connector v4.61 with AS2API v1.27 Engine** |
| **IceCoreSoft AB**<br><br>*https://icecoresoft.com*<br><br>**Product Name:** **Core Connect 4** | **Salesforce**<br><br>*https://www.salesforce.com/mulesoft/*<br><br>**Product Name:** **MuleSoft Anypoint AS2 Connector 6.9** |
| **/n software**<br><br>*https://www.nsoftware.com/*<br><br>**Product Name:** **IPWorks EDI 2024** | |

# Interoperability Test Summary

This is the 48th round of interoperability testing for the IETF AS2 standard and 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 this test event was 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 sent and received specific messages within the Product Test Group. In both sending and receiving, products-with-versions verified the message structure and security requirements were correct, the intended payload was transferred intact, and the receipt of the message was correctly delivered, verifying the transaction was successful.

The test cases covered 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 were all tested. Test data payloads simulating traditional POs and 1Sync messages were used with X12, EDIFACT and XML document formats.

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

This test event offered the following optional profiles: AES, AS2 Reliability, AS2 Restart, Filename Preservation (FN), Multiple Attachment (MA), Multiple Attachment with FN (FN-MA), Filename Preservation with MDN responses (FN-MDN), Certificate Exchange Messaging (CEM), and Secure Hashing Algorithm 2 (SHA2). Additionally, optional Advanced Algorithms and Authentication Certification testing was provided for participants that were able to enable stronger security strategies.

Details of these optional test suites are included later in this document.

# Interoperability Test History

| | |
|---|---|
| AS2 2Q25 Interoperability Test – Mar – May | 2025 |
| AS2 4Q24 Interoperability Test – Sep – Nov | 2024 |
| AS2 2Q24 Interoperability Test – Mar – May | 2024 |
| AS2 4Q23 Interoperability Test – Sep – Nov | 2023 |
| AS2 2Q23 Interoperability Test – Mar – Jun | 2023 |
| AS2 4Q22 Interoperability Test – Sep – Nov | 2022 |
| AS2 2Q22 Interoperability Test – Mar – May | 2022 |
| AS2 4Q21 Interoperability Test – Sep – Nov | 2021 |
| AS2 2Q21 Interoperability Test – Jun – Aug | 2021 |
| AS2 4Q20 Interoperability Test – Sep – Nov | 2020 |
| AS2 2Q20 Interoperability Test – May – Jun | 2020 |
| AS2 4Q19 Interoperability Test – Aug – Nov | 2019 |
| AS2 2Q19 Interoperability Test – Apr – May | 2019 |
| AS2 3Q18 Interoperability Test – Aug – Nov | 2018 |
| AS2 1Q18 Interoperability Test – Apr – May | 2018 |
| AS2 3Q17 Interoperability Test – Aug – Nov | 2017 |
| AS2 1Q17 Interoperability Test – Mar – Apr | 2017 |
| AS2 3Q16 Interoperability Test – Aug – Nov | 2016 |
| 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 – Jun | 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 – Sep – Nov | 2011 |
| AS2 1Q11 Interoperability Test – Mar – May | 2011 |
| AS2 3Q10 Interoperability Test – Sep – Nov | 2010 |
| AS2 1Q10 Interoperability Test – Mar – May | 2010 |
| AS2 3Q09 Interoperability Test – Sep – Nov | 2009 |
| AS2 1Q09 Interoperability Test – Apr – May | 2009 |
| AS2 3Q08 Interoperability Test – Sep – Oct | 2008 |
| AS2 1Q08 Interoperability Test – Mar – Apr | 2008 |
| AS2 3Q07 Interoperability Test – Sep – Nov | 2007 |
| AS2 1Q07 Interoperability Test – Feb – Apr | 2007 |
| AS2 3Q06 Interoperability Test – Sep – Oct | 2006 |
| AS2 1Q06 Interoperability Test – Feb – Mar | 2006 |
| AS2 3Q05 Interoperability Test – Sep – Oct | 2005 |
| AS2 1Q05 Interoperability Test – Feb – Apr | 2005 |
| AS2 3Q04 Interoperability Test – Aug – Sep | 2004 |
| AS2 1Q04 Interoperability Test – Feb – Mar | 2004 |
| AS2 3Q03 Interoperability Test – Jul – Sep | 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 Process

The successful sending and receiving of all Test Case messages among all the products-with-version is the Test Criteria for determining successful interoperability 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 event may be found in the Test Case Summary section of this Final Report.

The Interoperability Test Event (including Optional Profiles) was completed over nine weeks. During the initial weeks, QA and debug testing focused on finding interoperability errors and correcting them. These testing weeks before the Final Certification test run are the most important as they ensure all interoperability issues are found and resolved. All test cases are repeated until no issues remain. The Certification run is then executed where no code changes are allowed during this last week of testing.

During all weeks of testing, including the final week, unless otherwise noted, all products-with-version tested with each other in a full-matrix manner. During the Final Certification run, all products executed all required test cases in a full-matrix manner 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 are 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 test automation tool, and by the participants themselves as they demonstrated by automatically uploading the messages that they exchanged with each other. InSitu™ further checked all exchanged payloads for CRC mismatches as a further verification that the received payload content was identical to the sent payload.

No warranty of product interoperability is implied over and above the publishing of the results of the Test Event as completed by all vendors during the specified period of testing.

Also, please note that products certified in this interoperability test event have only achieved interoperability with the other products-with-version listed within this specific test event. No warranties are made for interoperability between products from two different test events (including optional profile test cases).

# Optional Profiles

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

The AS2-Version header of some AS2 products supporting the optional 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 during this test event. Along with completing the required test case, these participating products completed the optional AS2 Reliability testing during this test event.

"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 during this test event. Along with completing the required test cases, these participating products implemented and completed the optional AS2 Restart testing in this test event. 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/

## Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) continued to be tested during this test event. Along with completing the required test cases, these participating products completed the optional AES tests in this test event.

AES also known by its original name *Rijndael*, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES has been adopted by the U.S. government. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

## Basic Authentication with SSL

With an increasing number of AS2 products hosted on Cloud-based platforms, or in other protected environments, securing the data stream using SSL and restricting access to authorized users using Basic Authentication is a common approach; however not all AS2 products are capable of supporting Basic Authentication. To that end, additional optional suites of test cases were offered that require Basic Authentication and transporting the data stream over SSL and these participating products completed these test cases.

The IETF open standard https://datatracker.ietf.org/doc/html/rfc7617 describes the Basic HTTP Authentication scheme and its usage.

## Certificate Exchange Messaging

The optional Certificate Exchange Messaging (CEM) continued to be tested during this test event. Along with completing the required test cases, these participating products completed the optional CEM tests in this test event.

CEM is a standard for the automation of exchanging digital certificates within EDIINT 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 that are due to expire or have been revoked.

## Chunked Transfer Encoding

The optional Chunked Transfer Encoding (CTE) continued to be tested during this test event. Along with completing the required test cases, these participating products completed the optional CTE tests in this test event.

CTE is a streaming data transfer mechanism available in version 1.1 of the Hypertext Transfer Protocol (HTTP). In chunked transfer encoding, the data stream is divided into a series of non-overlapping "chunks". The chunks are sent out and received independently of one another. No knowledge of the data stream outside the currently-being-processed chunk is necessary for both the sender and the receiver at any given time.

Each chunk is preceded by its size in bytes. The transmission ends when a zero-length chunk is received. The *chunked* keyword in the Transfer-Encoding header is used to indicate chunked transfer.

(Reference: http://en.wikipedia.org/wiki/Chunked_transfer_encoding )

## Filename Preservation

The optional Filename Preservation (FN) profile continued to be tested during this test event. Along with completing the required test cases, these participating products completed the optional FN testing in this test event.

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 participated 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

The optional Filename Preservation for Multiple Attachments (FN-MA) profile continued to be tested during this test event. Along with completing the Required and FN test cases, these participating products completed the FN for MA optional profile test cases in this test event.

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

The test scenarios were comparable 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 during this test event. 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, these participating products completed the optional FN with MDN notification test cases in this test event.

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.

## Multiple Attachment

The optional Multiple Attachment (MA) profile continued to be tested during this test event. Along with completing the required test cases, these participating products completed the optional MA testing in this test event.

AS2 transmissions generally contain only a single EDI or XML payload document, and this is what was solely tested during the initial Drummond interoperability test events. However, some transactions require multiple documents to communicate all relevant information. Multiple attachments allow 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.

## Secure Hashing Algorithm 2

The optional Secure Hashing Algorithm – 2 (SHA2) continued to be tested during this test event. SHA2 features a higher level of security than its predecessor and addresses the need to offer both SHA1 and SHA2, as SHA1 is being phased out, and SHA2 is becoming the preference for security reasons.

SHA2 was designed through the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). It is driven by government applications that use AS2 and require SHA2, such as the CSOS (Controlled Substances Ordering Systems) standard, and in Europe and the U.S. gas and energy industries.

The SHA2 tests verify the interoperability of the signed message digest values and MIC values returned in the MDNs using the more secure SHA-256, SHA-384 and SHA-512 hash algorithms. Along with completing the required test cases, these participating products completed the optional SHA2 testing in this test event.

# Interoperability Required Test Results

In order to obtain a Drummond AS2 Certification Seal, each participating product must successfully complete at least one of the following set of tests.

## 3DES/SHA1 Algorithm Transport Tests

These companies and products participated in and successfully completed the 3DES/SHA1 Algorithm Tests. These tests demonstrated the transport of payload files using 3DES encryption and SHA-1 signature hashing over both HTTP and HTTPS.

| **Company** | **Product** |
|---|---|
| Amazon Web Services | AWS Transfer Family ***** |
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Axway | Axway SecureTransport 5.5 |
| Axway | Axway TSIM 3.9 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| DXC Technology | ELIT AS2 Connector v4.61 with AS2API v1.27 Engine |
| IceCoreSoft AB | Core Connect 4 |
| Salesforce | MuleSoft Anypoint AS2 Connector 6.9 |
| /n software | IPWorks EDI 2024 |

(*****) Participant product required encrypted messages and only supported outbound asynchronous MDNs

## AES-128/SHA-256 Advanced Algorithm Transport Tests

These companies and products participated in and successfully completed the AES-128/SHA-256 Advanced Algorithm Tests. These tests demonstrated the transport of payload files using AES-128 encryption and SHA-256 signature hashing over HTTPS (SSL) only.

| **Company** | **Product** |
|---|---|
| Amazon Web Services | AWS Transfer Family ***** |
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Axway | Axway SecureTransport 5.5 |
| Axway | Axway TSIM 3.9 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| DXC Technology | ELIT AS2 Connector v4.61 with AS2API v1.27 Engine |
| IceCoreSoft AB | Core Connect 4 |
| Salesforce | MuleSoft Anypoint AS2 Connector 6.9 |
| /n software | IPWorks EDI 2024 |

(*****) Participant product only supported outbound asynchronous MDNs

# Optional Profile Test Results

Those companies listed under each of the following profiles 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, unless otherwise indicated.
Please note that products certified in this list have achieved interoperability with the other products-with-version listed within this specific test event. No warranties are made for interoperability between products from two different test events (including optional profile test cases).

## Optional Profile – AS2 Reliability

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

| Company | Product |
|---|---|
| Amazon Web Services | AWS Transfer Family ***** |
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| IceCoreSoft AB | Core Connect 4 |
| /n software | IPWorks EDI 2024 |

(*****) Participant product required encrypted messages and only supported outbound asynchronous MDNs, asynchronous MDN retries were not tested

## Optional Profile – AS2 Restart

These companies and products participated 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 2.6 / Activator 6.1 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| IceCoreSoft AB | Core Connect 4 |
| /n software | IPWorks EDI 2024 |

## Optional Profile - Basic Authentication with SSL

These companies and products participated in and successfully completed the Basic Authentication with SSL tests. These tests demonstrated the transport of payload files over SSL using Basic Authentication to validate the sender and AES-128 encryption and SHA-256 signature hashing to secure the payload.

| Company | Product |
|---|---|
| Amazon Web Services | AWS Transfer Family ***** |
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Axway | Axway SecureTransport 5.5 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) ***** |
| DXC Technology | ELIT AS2 Connector v4.61 with AS2API v1.27 Engine |
| IceCoreSoft AB | Core Connect 4 |
| Salesforce | MuleSoft Anypoint AS2 Connector 6.9 |
| /n software | IPWorks EDI 2024 |

(*****) Participant product only supported outbound messages

## Optional Profile – Certificate Exchange Messaging (CEM)

These companies and products participated in and successfully completed Certificate Exchange Messaging (CEM) Optional testing during this test event. CEM message exchange was tested in both directions.

| Company | Product |
|---|---|
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| IceCoreSoft AB | Core Connect 4 |
| /n software | IPWorks EDI 2024 |

## Optional Profile - Filename Preservation with MDN Notification (FN-MDN)

These companies and products participated in and successfully completed Filename Preservation with MDN Notification (FN-MDN). MDN notifications on error conditions were sent by the receiving side. The filename provided was either preserved or not, depending on the test cases executed and the receiving side's configuration.

| Company | Product |
|---|---|
| Axway | Axway TSIM 3.9 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| IceCoreSoft AB | Core Connect 4 |
| /n software | IPWorks EDI 2024 |

## Optional Profile – Advanced Encryption Standard (AES)

These companies and products participated in and successfully completed AES-128, AES-192, and AES-256 testing.

| Company | Product |
|---|---|
| Amazon Web Services | AWS Transfer Family * |
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Axway | Axway SecureTransport 5.5 |
| Axway | Axway TSIM 3.9 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| DXC Technology | ELIT AS2 Connector v4.61 with AS2API v1.27 Engine |
| IceCoreSoft AB | Core Connect 4 |
| Salesforce | MuleSoft Anypoint AS2 Connector 6.9 |
| /n software | IPWorks EDI 2024 |

(*) Participant product only supported outbound asynchronous MDNs

## Optional Profile – Chunked Transfer Encoding (CTE)

These companies and products participated in and successfully completed Chunked Transfer Encoding (CTE) testing for the specified certification type(s). Participants tested both by sending and receiving Chunked Transfer Encoding messages, unless otherwise noted.

| **Company** | **Product** |
|---|---|
| Amazon Web Services | AWS Transfer Family ***** |
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| DXC Technology | ELIT AS2 Connector v4.61 with AS2API v1.27 Engine |
| IceCoreSoft AB | Core Connect 4 |
| Salesforce | MuleSoft Anypoint AS2 Connector 6.9 |
| /n software | IPWorks EDI 2024 |

(*****) Participant product supported inbound CTE messages only

## Optional Profile - Filename Preservation (FN)

These companies and products participated in and successfully completed both sending and receiving Filename Preservation (FN) messages for the specified certification type(s). The filename provided by the sender was preserved on the receiving side.

| Company | Product |
|---|---|
| Amazon Web Services | AWS Transfer Family * |
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Axway | Axway TSIM 3.9 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| DXC Technology | ELIT AS2 Connector v4.61 with AS2API v1.27 Engine |
| IceCoreSoft AB | Core Connect 4 |
| Salesforce | MuleSoft Anypoint AS2 Connector 6.9 |
| /n software | IPWorks EDI 2024 |

(*****) Participant product only supported outbound asynchronous MDNs

## Optional Profile - Filename Preservation for MA (FN-MA)

These companies and products participated in and successfully completed Filename Preservation for Multiple Attachments (FN-MA) for testing inbound messages for the specified certification type(s). The filename was provided by the sender for each attached payload and was preserved on the receiving side for all attached payloads.

| Company | Product |
|---|---|
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Axway | Axway TSIM 3.9 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| IceCoreSoft AB | Core Connect 4 |
| /n software | IPWorks EDI 2024 |

## Optional Profile – Multiple Attachments (MA)

These companies and products participated in and successfully completed Multiple Attachments (MA) Optional testing during this test event for the specified certification type(s).

| Company | Product |
|---|---|
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Axway | Axway TSIM 3.9 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| IceCoreSoft AB | Core Connect 4 |
| /n software | IPWorks EDI 2024 |

## Optional Profile – Secure Hashing Algorithm – 2 (SHA2)

These companies and products participated in and successfully completed SHA2 testing for the specified certification type(s). The SHA2 message digest was created on the outbound message with the specified SHA2 hash value and was validated on the inbound message.

The Message Integrity Check (MIC) returned in the MDN was also validated to use SHA2.

| **Company** | **Product** |
|---|---|
| Amazon Web Services | AWS Transfer Family * |
| Axway | Axway B2Bi 2.6 / Activator 6.1 |
| Axway | Axway SecureTransport 5.5 |
| Axway | Axway TSIM 3.9 |
| Beijing Sinowintop | EasyLink v2.0 |
| CData Software | CData Arc™ 2025 - 25.1.9231.0 |
| Cleo | Cleo Integration Cloud: Private Cloud Edition (Version 5.8.1 of Cleo LexiCom®, Cleo VLTrader® and Cleo Harmony®) |
| DXC Technology | ELIT AS2 Connector v4.61 with AS2API v1.27 Engine |
| IceCoreSoft AB | Core Connect 4 |
| Salesforce | MuleSoft Anypoint AS2 Connector 6.9 |
| /n software | IPWorks EDI 2024 |

(*****) Participant product only supported outbound asynchronous MDNs

## 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 Event if and only if it demonstrates, the pair wise exchange of data, in a full-matrix manner, covering the *Test Criteria* between all products in the Interoperability Test Event. A product is either fully interoperable or it is not considered interoperable. Waivers or exceptions are not given in demonstrating interoperability for the *Test Criteria* unless the entire *Product Test Group* and Drummond agree.

***Interoperable products*** – Group of products, from the *Product Test Group*, that successfully completed the *Test Criteria*, in a full–matrix manner with every other *Product Test Group* participant in an Interoperability Test Event 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 Test Event.

***Product, product-with-version, or product-with-version-with-release*** – are interchangeable and are defined for the purpose of a Test Event 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: "V.Rx…x," where V is the version numeral designator, R is the single digit release numeral designator and x is the sub-release multiple digit numeral designator. Drummond 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 Event. 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 Event is complete.

***Test Case*** – The test criteria is a set of 10 or more individual test cases that 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, but this is not required) and others 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 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 required tests cases with all other participants. These tests cases, which can be found in the next section, 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 2048 bits, as it was required by at least one of the participants. Triple DES (3DES) or AES-128 was the encryption algorithm used for the required tests depending on the transport used during the test. Other algorithms, such as RC2 or DES, were not tested. Either SHA1 or SHA2 hashing could be used in creating digital signatures, but the MD5 hash algorithm 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 that 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 those 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 connection. Asynchronous receipts are sent to the originator of the transaction over a new connection. Synchronous and asynchronous receipts on both HTTP and HTTP/S connections 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" value MUST always be returned to the requester. The "Received-Content-MIC" value presents the receipts in the form of NRR (Non-Repudiation of Receipt).

## Transports

Both HTTP and HTTP/S transports were used for this test, although some participants did not test HTTP because of stronger security policies . Both HTTP version 1.0 and HTTP version 1.1 servers were involved in this test. For HTTP/S, only server-side authentication (using SSL certificates) was tested. Asynchronous receipts were returned over both HTTP and HTTP/S transports.

## 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 here.

## Micalg Parameters

The latest Bouncy Castle library supports the S/MIME version 3.2 specification, described in RFC 5751, defining the micalg parameters to specify a signed MDN. RFC 5751 has changed the definition of the micalg parameters previously defined in the S/MIME version 3.1 specification, described in RFC 3851. By default, RFC 5751 uses the "micalg=sha-1" parameter when signing the content. However, there may be older products in the field that only support the older RFC 3851 "micalg=sha1" parameter and could cause interoperability issues with newer products that only support RFC 5751.

Within this interoperability test event, all products were compliant with S/MIME version 3.2. To be compliant with all versions, some AS2 products were also backward compatible and were able to support micalg values of both "sha-1" and "sha1".

## Error Reporting (MDN Conformance)

Products were sent erroneously signed, encrypted and compressed messages using the Drummond MDN Test Tool and were required to return MDNs with the appropriate error message.

## Basic Authentication Profile Overview

In the context of an HTTP transaction, **Basic Authentication** is a method for an AS2/HTTP user to provide a username and password when making a request to the server. In basic authentication, a request contains a header field in the form of `Authorization: Basic <credentials>`, where <credentials> is the Base64 encoding of the username and password joined by a single colon `:`. The specification is described in RFC 7617.

Participants that had the capability configured their AS2 servers to require Basic Authentication and specified a username and password. These usernames and passwords were provided by each participant. Senders included the Authorization header with that base64-encoded username and password, for example,

```
Authorization: Basic dXNlcmF1dGg6dXNlclBhc3N3b3JkMSE=
```

Recipients validated the sender's username and password before allowing access to their server.

## Certificate Requirements for Advanced Algorithms and Authentication Tests

To accommodate participant security requirements for all Advanced Algorithms and Authentication tests, CA certificates were required or, if they were self-signed, then they had to include a SAN (Subject Alternative Name) extension with a DNSName and an IP address:

```
ObjectId: 2.5.29.17  Criticality=false
SubjectAlternativeName [
DNSName: my.dns.name
IPAddres: 123.45.678.90
]
```

# Required Transport Tests

In order to obtain a Drummond AS2 Interoperability Certification Seal, all participants were required to successfully execute at least one of the required test profiles with all other participants in their Test Group.

The signing and encryption algorithms used were either 3DES/SHA-1 or AES-128/SHA-256 based on the specific transport being tested.

An AES Optional Test was also provided that encrypted the payload using three different AES key lengths.

## Required Test Cases

| Test Case | Msg Payload | Msg Transport (3DES/SHA1) | Msg Transport (AES/SHA2) | Msg Security | Compressed | MDN Transport (3DES/SHA1) | MDN Transport (AES/SHA2) | MDN Security |
|---|---|---|---|---|---|---|---|---|
| A | Data #1 | HTTP | HTTPS | Signed/Encrypted | No | Sync | Sync | Unsigned |
| B | Data #2 | HTTP | HTTPS | Signed/Encrypted | No | Sync | Sync | Signed |
| C | Data #3 | HTTP | HTTPS | Signed/Encrypted | No | Async/HTTPS | Async/HTTPS | Signed |
| D | Data #4 | HTTP | HTTPS | Encrypted | Yes | Sync | Sync | Signed |
| E | Data #5 | HTTP | HTTPS | Encrypted | No | Sync | Sync | Signed |
| F | Data #6 | HTTP | HTTPS | Signed | No | Sync | Sync | Signed |
| G | Data #7 | HTTPS | HTTPS | Signed | Yes | Sync | Sync | Signed |
| H | Data #8 | HTTPS | HTTPS | Signed | No | Async/HTTP | Async/HTTPS | Signed |
| I | Data #9 | HTTPS | HTTPS | Signed | No | Async/HTTPS | Async/HTTPS | Signed |
| J | Data #10 | HTTP | HTTPS | Signed/Encrypted | Yes | Async/HTTP | Async/HTTPS | Signed |

Test cases K1-K3 are error scenario test cases and were only tested inbound where Drummond's MDN Conformance Tool sent outbound messages. Participants did <u>not</u> send these tests to each other. These test cases were successfully executed by all participants.

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

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

## Required Test Case Test Data

The test data described below was used as payloads in the test cases during this interoperability test event. This test data was provided automatically through the InSitu™ server during the creation of the specified test case.

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

## Required Test Case A:

| | |
|---|---|
| **Test Description** | The initiator creates a signed, encrypted exchange over HTTP (3DES/SHA1) or HTTPS (AES-128/SHA-256) with a request for a synchronous, unsigned MDN. |
| **Message Payload** | Test Data # 1 |
| **Message Transport** | HTTP for 3DES/SHA1, HTTPS for AES-128/SHA-256 |
| **Message Security** | Signature (SHA-1 or SHA-256 hash), Encryption (3DES or AES-128) |
| **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 (3DES/SHA1) or HTTPS (AES-128/SHA-256) with a request for a synchronous, signed MDN. |
| **Message Payload** | Test Data # 2 |
| **Message Transport** | HTTP for 3DES/SHA1, HTTPS for AES-128/SHA-256 |
| **Message Security** | Signature (SHA-1 or SHA-256 hash), Encryption (3DES or AES-128) |
| **Message Compression** | No |
| **MDN Transport** | Synchronous |
| **MDN Security** | Signature (SHA-1 or SHA-256 hash) |
| **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 (3DES/SHA1) or HTTPS (AES-128/SHA-256) with a request for an asynchronous, signed MDN. |
| **Message Payload** | Test Data # 3 |
| **Message Transport** | HTTP for 3DES/SHA1, HTTPS for AES-128/SHA-256 |
| **Message Security** | Signature (SHA-1 or SHA-256 hash), Encryption (3DES or AES-128) |
| **Message Compression** | No |
| **MDN Transport** | Asynchronous/HTTPS |
| **MDN Security** | Signature (SHA-1 or SHA-256 hash) |
| **Expected Results** | The payload is successfully transferred, the initial HTTP or 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 D:

| | |
|---|---|
| ***Test Description*** | The initiator creates an encrypted, compressed exchange over HTTP (3DES/SHA1) or HTTPS (AES-128/SHA-256) with a request for a synchronous, signed MDN. |
| **Message Payload** | Test Data # 4 |
| **Message Transport** | HTTP for 3DES/SHA1, HTTPS for AES-128/SHA-256 |
| **Message Security** | Encryption (3DES or AES-128) |
| **Message Compression** | Yes |
| **MDN Transport** | Synchronous |
| **MDN Security** | Signature (SHA-1 or SHA-256 hash) |
| **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 (3DES/SHA1) or HTTPS (AES-128/SHA-256) with a request for a synchronous, signed MDN. |
| **Message Payload** | Test Data # 5 |
| **Message Transport** | HTTP for 3DES/SHA1, HTTPS for AES-128/SHA-256 |
| **Message Security** | Encryption (3DES or AES-128) |
| **Message Compression** | No |
| **MDN Transport** | Synchronous |
| **MDN Security** | Signature (SHA-1 or SHA-256 hash) |
| **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 (3DES/SHA1) or HTTPS (AES-128/SHA-256) with a request for a synchronous, signed MDN. |
| **Message Payload** | Test Data # 6 |
| **Message Transport** | HTTP for 3DES/SHA1, HTTPS for AES-128/SHA-256 |
| **Message Security** | Signature (SHA-1 or SHA-256 hash) |
| **Message Compression** | No |
| **MDN Transport** | Synchronous |
| **MDN Security** | Signature (SHA-1 or SHA-256 hash) |
| **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 (SHA-1 or SHA-256 hash) |
| **Message Compression** | Yes |
| **MDN Transport** | Synchronous |
| **MDN Security** | Signature (SHA-1 or SHA-256 hash) |
| **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 (3DES/SHA1) or HTTPS (AES-128/SHA-256). |
| **Message Payload** | Test Data # 8 |
| **Message Transport** | HTTPS |
| **Message Security** | Signature (SHA-1 or SHA-256 hash) |
| **Message Compression** | No |
| **MDN Transport** | Asynchronous/HTTP or Asynchronous/HTTPS |
| **MDN Security** | Signature (SHA-1 or SHA-256 hash) |
| **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 or HTTPS 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 (SHA-1 or SHA-256 hash) |
| **Message Compression** | No |
| **MDN Transport** | Asynchronous/HTTPS |
| **MDN Security** | Signature (SHA-1 or SHA-256 hash) |
| **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 (3DES/SHA1) or HTTPS for Adv and BA with a request for an asynchronous, signed MDN. |
| **Message Payload** | Test Data # 10 |
| **Message Transport** | HTTP for 3DES/SHA1, HTTPS for AES-128/SHA-256 |
| **Message Security** | Signature (SHA-1 or SHA-256 hash), Encryption (3DES or AES-128) |
| **Message Compression** | Yes |
| **MDN Transport** | Asynchronous/HTTP or Asynchronous/HTTPS |
| **MDN Security** | Signature (SHA-1 or SHA-256 hash) |
| **Expected Results** | The payload is successfully transferred, the initial HTTP or HTTPS connection is closed with a 200 OK, and then an MDN with a disposition value of "processed" is returned over a new HTTP (3DES/SHA1) or HTTPS (AES-128/SHA-256) connection. |

## Required Test Case K.1:

| | |
|---|---|
| **Test Description** | The Drummond MDN Conformance Tool sends a corrupt signed message to the participant. The signed data 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 an MDN with the disposition value correctly identifying the error. |
| **Message Payload** | Test Data # 1 |
| **Message Transport** | HTTPS |
| **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 MDN Conformance Tool sends an 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 an MDN with the disposition value correctly identifying the decryption error. |
| **Message Payload** | Test Data # 1 |
| **Message Transport** | HTTPS |
| **Message Security** | Encryption (corrupted) |
| **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 MDN Conformance Tool sends a corrupt 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 an MDN with the disposition value correctly identifying the error. |
| **Message Payload** | Test Data # 1 |
| **Message Transport** | HTTPS |
| **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 for the reliability of AS2 transactions has increased tremendously since AS2 was initially introduced and adopted. It is not inconceivable that millions of transactions are processed daily and a wide variety of document types and sizes are exchanged between heterogeneous environments. The requirement for guaranteed message 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 message delivery and duplicate message elimination, which will enable "reliable" communication between AS2 servers. It extends the AS2 RFC 4130 standard and in essence recognizes error scenarios that 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 either a synchronous or asynchronous MDN. The type of MDN is not important. The point is that the Originator did not receive the expected '200 OK' in response to the POST. Instead, for instance, it received a 503 response or no response at all. The following diagram depicts this scenario:

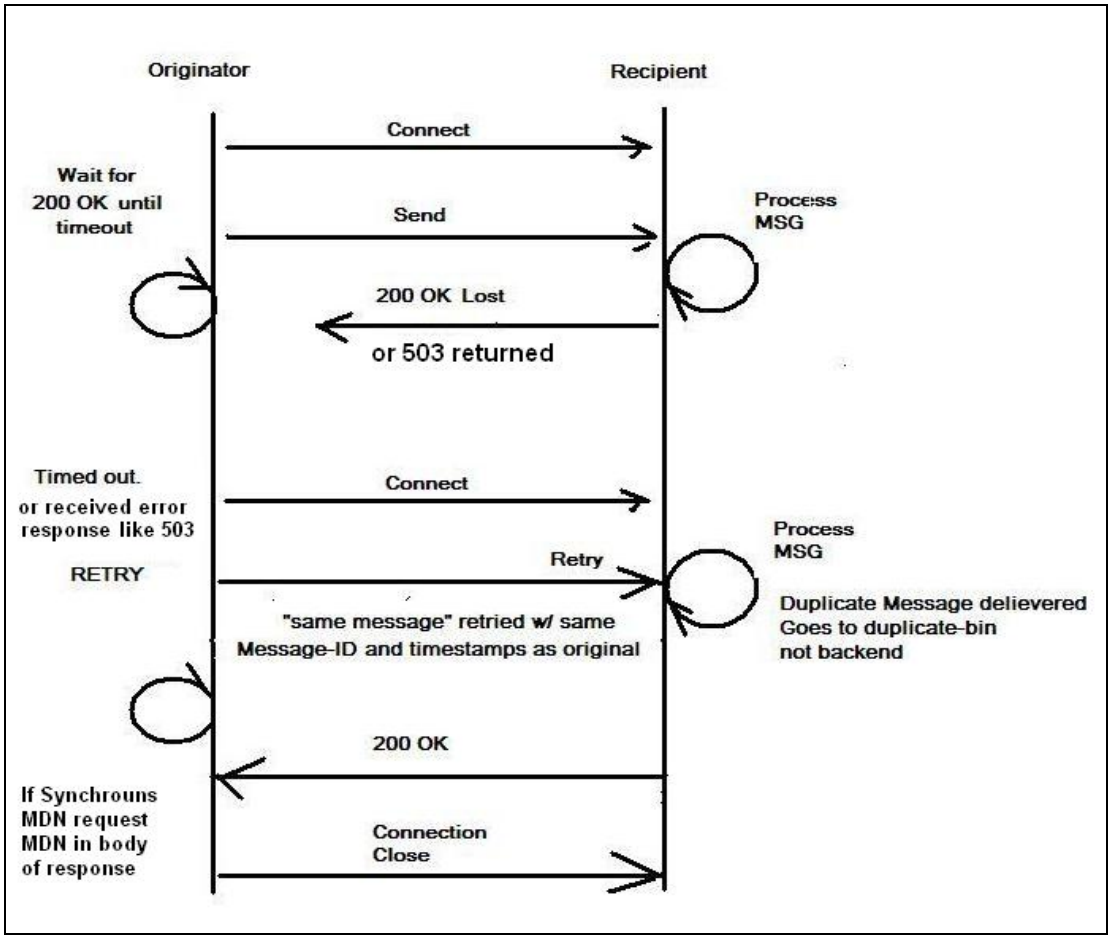


**Figure 1 Diagram showing Retry logic**

The Originator may 'retry' the AS2 message, 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 incoming message is a duplicate (with the same Message-ID) and not deliver the payload to the backend system for processing. Instead, the receiving system can flag it as a duplicate message.

## AS2 Reliability Resends -- Asynchronous AS2 Protocol Breakdown

Resends are 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 incoming message is a duplicate (with the same Message-ID) and not deliver the payload to the backend system for processing. Instead, the receiving system can flag it as a duplicate message.

Furthermore, the Recipient may resend the same asynchronous MDN as originally received. The original-message-id and received-content-mic values must be the same as the original asynchronous MDN with which the Recipient originally responded.

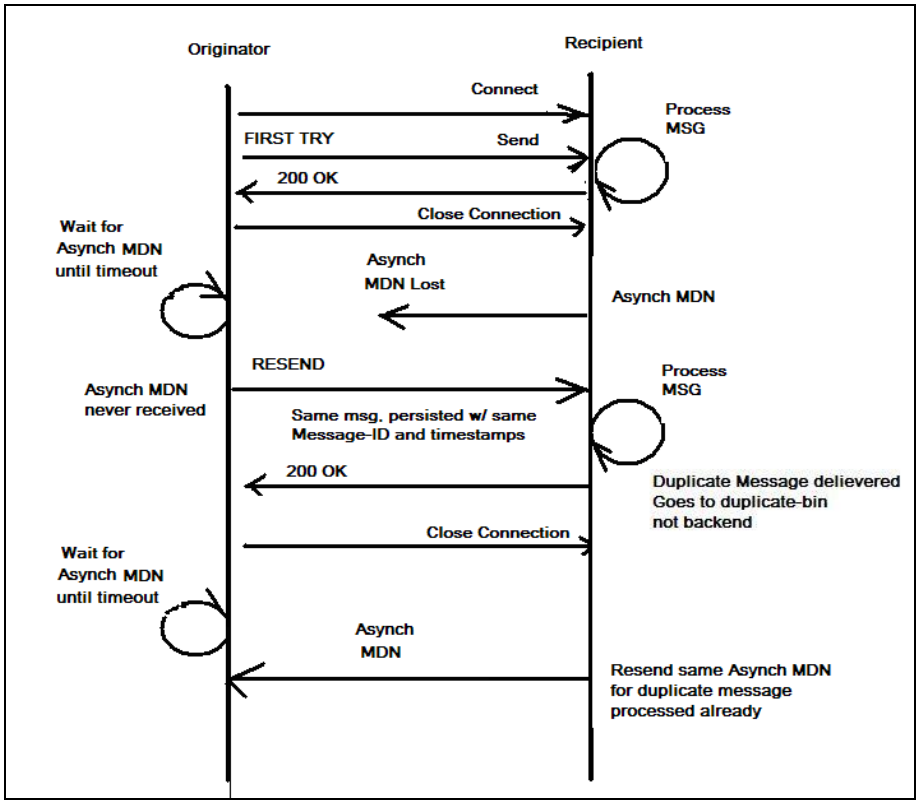


**Figure 2 Diagram showing Resend logic**

# 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 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 |
|---|---|---|---|---|---|---|
| Rel-A<br>Rel-Ax | Data #1 | HTTP | Signed/Encrypted | No | Sync | Unsigned |
| Rel-C<br>Rel-Cx | Data #3 | HTTP | Signed/Encrypted | No | Async/HTTP | Signed |

## AS2 Reliability Test Data

Drummond provides the payload data for all 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. The size is 12kB.
2. Test Data #3 (test_data_3.xml). Sync 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 to be processed by its AS2 product. The HTTP server may be embedded within the AS2 product.

The AS2 product is configured to send outbound messages through an HTTP forward proxy, where the InSitu™ client's Interceptor IP address and port is configured as that Proxy. Based on the test case, the Interceptor determines whether the messages should be passed through to the intended recipient or should be blocked in order to simulate "lost" messages so retries will be attempted.

## AS2 Reliability Test Case Description

### AS2 Reliability Rel-A/Rel-Ax - Retry, Request Synchronous MDN

| | |
|---|---|
| **Test Description** | The initiator creates a signed and encrypted data exchange over HTTP with a request for a synchronous, unsigned MDN. |
| **Message Payload** | Test Data # 1 (X12) |
| **Message Transport** | HTTP |
| **Message Security** | Signature (SHA-1) |
| **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. |

### AS2 Reliability Rel-C/Rel-Cx - Resend, Request Asynchronous MDN

| | |
|---|---|
| **Test Description** | The initiator creates a signed and encrypted data exchange over HTTP with a request for an asynchronous, signed MDN. |
| **Message Payload** | Test Data # 3 (XML) |
| **Message Transport** | HTTP |
| **Message Security** | Signature (SHA-1) |
| **Message Compression** | No |
| **MDN Transport** | Asynchronous/HTTP |
| **MDN Security** | Signature (SHA-1) |
| **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 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.

AS2 Restart testing was built on top of the AS2 Reliability test cases and utilized the InSitu™ client Interceptor as the configured Proxy to introduce network errors during AS2 message exchanges. The J payload was increased to 200 MB, 500 MB and 1 GB 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 then successfully processed the AS2 message.

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

# Optional Profile – Advanced Encryption Standard (AES)

## AES Test Case Execution

The AES tests used the same required encryption test cases, except that each test case was executed 3 times: one time with each key length (AES-128, AES-192 and AES-256).

The signature algorithm used for these tests was either SHA-1 or SHA-256 depending on the transport used during the test. The payloads used for these AES test cases were the same as their required test counterparts.

## AES Test Cases

| Test Case | Msg Payload | Msg Transport (3DES/SHA1) | Msg Transport (AES/SHA2) | Msg Security | Compressed | MDN Transport (3DES/SHA1) | MDN Transport (AES/SHA2) | MDN Security |
|---|---|---|---|---|---|---|---|---|
| B | Data #2 | HTTP | HTTPS | Signed/Encrypted | No | Sync | Sync | Signed |
| C | Data #3 | HTTP | HTTPS | Signed/Encrypted | No | Async/HTTPS | Async/HTTPS | Signed |
| D | Data #4 | HTTP | HTTPS | Encrypted | Yes | Sync | Sync | Signed |
| E | Data #5 | HTTP | HTTPS | Encrypted | No | Sync | Sync | Signed |
| J | Data #10 | HTTP | HTTPS | Signed/Encrypted | Yes | Async/HTTP | Async/HTTPS | Signed |

# 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 with active trading. In order to test, participants must have an existing trading partner relationship. Then, they will exchange new certificates through CEM and confirm the acceptance by sending messages which use the new certificates.

**Note:** These tests are not automated through InSitu™. Participants ran these tests manually and provided copies of all their raw test messages.

## CEM Test Case Execution

Each test participant exchanges 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 – Chunked Transfer Encoding

## CTE Overview

Chunked Transfer Encoding (CTE) is a means for allowing HTTP messages to be split into several parts. This can be applied to both HTTP requests (from client to server) and HTTP responses (from server to client). For example, consider the way in which an HTTP server may transmit data to a client application (usually through a web browser). Normally, data delivered in HTTP responses is sent in one piece and its 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 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 were the same as those used in AS2 Required testing, except that Chunked Transfer Encoding was used to exchange these messages. A subset of the required test cases was used for the CTE tests, specifically, test cases A, B, G and J.

The encryption algorithm used to encrypt the payload was either 3DES or AES-128 and the signature hash algorithm was either SHA-1 or SHA-256 depending on the transport used during the test.

| Test Case | Msg Payload | Msg Transport (3DES/SHA1) | Msg Transport (AES/SHA2) | Msg Security | Compressed | MDN Transport (3DES/SHA1) | MDN Transport (AES/SHA2) | MDN Security |
|---|---|---|---|---|---|---|---|---|
| A | Data #1 | HTTP | HTTPS | Signed/Encrypted | No | Sync | Sync | Unsigned |
| B | Data #2 | HTTP | HTTPS | Signed/Encrypted | No | Sync | Sync | Signed |
| G | Data #7 | HTTPS | HTTPS | Signed | Yes | Sync | Sync | Signed |
| J | Data #10 | HTTP | HTTPS | Signed/Encrypted | Yes | Async/HTTP | Async/HTTPS | Signed |

# Optional Profile – Filename Preservation

The Filename Preservation test cases were optional. Details of these test cases are described 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 with a Content-Disposition header included in the MIME header. The AS2 message is sent to the receiving participant which extracts the payload and names it according to the value provided in the Content-Disposition header.

The recipient should extract a single attachment and return an MDN. The expected MIC calculation should also be included if it is a signed MDN.

If the filename already exists, duplicate file indications should not be reported by the recipient in the returned MDN.

## FN Test Cases

| Test Case | Msg Payload | Msg Transport (3DES/SHA1) | Msg Transport (AES/SHA2) | Msg Security | Compressed | MDN Transport (3DES/SHA1) | MDN Transport (AES/SHA2) | MDN Security |
|---|---|---|---|---|---|---|---|---|
| A | Data #1 | HTTP | HTTPS | Signed/Encrypted | No | Sync | Sync | Unsigned |
| B | Data #2 | HTTP | HTTPS | Signed/Encrypted | No | Sync | Sync | Signed |
| C | Data #3 | HTTP | HTTPS | Signed/Encrypted | No | Async/HTTPS | Async/HTTPS | Signed |
| D | Data #4 | HTTP | HTTPS | Encrypted | Yes | Sync | Sync | Signed |
| E | Data #5 | HTTP | HTTPS | Encrypted | No | Sync | Sync | Signed |
| F | Data #6 | HTTP | HTTPS | Signed | No | Sync | Sync | Signed |
| G | Data #7 | HTTPS | HTTPS | Signed | Yes | Sync | Sync | Signed |
| H | Data #8 | HTTPS | HTTPS | Signed | No | Async/HTTP | Async/HTTPS | Signed |
| I | Data #9 | HTTPS | HTTPS | Signed | No | Async/HTTPS | Async/HTTPS | Signed |
| J | Data #10 | HTTP | HTTPS | Signed/Encrypted | Yes | Async/HTTP | Async/HTTPS | Signed |

## FN Test Data

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

# Optional Profile – Filename Preservation for MA

As in the Filename Preservation (FN) profile, the FN for MA profile 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 body parts of the AS2 MA message.

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

> 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 with a Content-Disposition header included in the MIME body part 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 header of each MIME body part.

The recipient should extract the multiple attachments and return an MDN. The expected MIC calculation should also be included if it is a signed MDN.

If the filename already exists, duplicate file indications should not be reported by the recipient in the returned MDN.

## 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 example, when a filename is already in use. This section describes 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 provides content based MDN responses that 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 and return a warning, or
2. reject the incoming payload and not write it out and return an error

In each case, a content-based MDN is returned to the Sending Trading Partner alerting them of the conflict. Which response the receiving side provides depends on its configuration capability. Some AS2 receiving systems may be capable of being configured on a per trading partner basis, thus the response is contingent on trading partner agreements between the sender and the recipient. 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, the response indicates that the message was delivered without error or to indicate an error in processing, for instance signature validation or decryption errors. 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 MDN responses.

## 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 expected but not received

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

The sending trading partner MUST be notified of any 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 of 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 for the offending payload SHOULD give some indication to the end-user that an error occurred, for instance pre-pending a string “dup_” to the unique filename (e.g., “dup_unique_filename.ext”) or by placing it in an inbound directory reserved for messages with error conditions.

2. **Negative MDN with Error Level:** Recipient rejects incoming AS2 message and replies with a 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 MDN Disposition type MUST be set to the value of "processed", and the MDN Disposition modifier set to the value of "warning".

The "warning" MDN Disposition modifier MUST be used with the "processed" MDN Disposition type to indicate that the message was successfully processed, but that an exception occurred.

A "warning:" MDN Disposition modifier MUST be used to combine the indication of a warning with the payload warning conditions.

The following MDN ‘Disposition’ 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 MDN Disposition type MUST be set to the value of "failed", and the MDN Disposition modifier set to "failure".

A "failure:" MDN Disposition modifier MUST be used to combine the indication of the error with the payload error conditions.

The following Disposition 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 executed test cases with a request for a synchronous MDN first. Each participant then repeated the test with a request for an asynchronous MDN.

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

**Note:** These tests are not automated through InSitu™. Participants ran these tests manually and provided copies of all their test messages.

## FN with MDN Test Data

To avoid duplicate file names, separate EDI files were used for synchronous (fnp_test_data_1.edi) and asynchronous (fnp_test_data_1_async.edi) testing.

# Optional Profile – Multiple Attachments (MA)

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", "image/tiff", or "application/pdf" depending on the content type for each part. The multipart/related structure is signed, signed, and encrypted, or signed, encrypted and compressed and sent requesting a signed or unsigned MDN, either synchronously or asynchronously according to the table below.

The expected results require that the recipient is able to extract the number of attachments included in the AS2 message and return an MDN (as requested) with the expected MIC calculation in the MDN.

As already mentioned in the other optional test descriptions, the encryption algorithm used was either 3DES or AES-128 and the signature hash algorithm used was either SHA-1 or SHA-256 depending on the transport used during the test.

## MA Test Cases

The 10 MA test cases mirrored the 10 required test case counterparts for the required test cases in terms of security, transport, and MDN configuration. For the first nine test cases, two payloads are included and for the last test case, four payloads are included instead of two.

Below is a summary of the test cases and the test data used for the payload parts.

| Test Case | Payload Part - Payload | Msg Transport (3DES/SHA1) | Msg Transport (AES/SHA2) | Msg Security | Compressed | MDN Transport (3DES/SHA1) | MDN Transport (AES/SHA2) | MDN Security |
|---|---|---|---|---|---|---|---|---|
| MA-A | 1 – MA Data 1<br>2 – MA Data 3 | HTTP | HTTPS | Signed/ Encrypted | No | Sync | Sync | Unsigned |
| MA-B | 1 – MA Data 2<br>2 – MA Data 5 | HTTP | HTTPS | Signed/ Encrypted | No | Sync | Sync | Signed |
| MA-C | 1 – MA Data 3<br>2 – MA Data 4 | HTTP | HTTPS | Signed/ Encrypted | No | Async/HTTPS | Async/HTTPS | Signed |
| MA-D | 1 – MA Data 4<br>2 – MA Data 5 | HTTP | HTTPS | Encrypted | Yes | Sync | Sync | Signed |
| MA-E | 1 – MA Data 2<br>2 – MA Data 5 | HTTP | HTTPS | Encrypted | No | Sync | Sync | Signed |
| MA-F | 1 – MA Data 1<br>2 – MA Data 3 | HTTP | HTTPS | Signed | No | Sync | Sync | Signed |
| MA-G | 1 – MA Data 1<br>2 – MA Data 3 | HTTPS | HTTPS | Signed | Yes | Sync | Sync | Signed |
| MA-H | 1 – MA Data 2<br>2 – MA Data 5 | HTTPS | HTTPS | Signed | No | Async/HTTP | Async/HTTPS | Signed |
| MA-I | 1 – MA Data 1<br>2 – MA Data 3 | HTTPS | HTTPS | Signed | No | Async/HTTPS | Async/HTTPS | Signed |
| MA-J | 1 – MA Data 1<br>2 – MA Data 2<br>3 – MA Data 3<br>4 – MA Data 5 | HTTP | HTTPS | Signed/ Encrypted | Yes | Async/HTTP | Async/HTTPS | 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 – Secure Hashing Algorithm 2 (SHA2)

## SHA2 Overview

In cryptography, **SHA2** 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. SHA2 includes a significant number of changes from its predecessor, SHA1. SHA2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits. (Reference: wikipedia.com)

## SHA2 Test Case Execution

The SHA-2 test cases mirrored the 10 required test case counterparts in terms of security, transport, and MDN configuration except that each test case is executed 3 times, one time each with each hash algorithm strength (SHA-256, SHA-384 and SHA-512).

The Message Integrity Check (MIC) returned in the MDN was required to use the same SHA2 hash algorithm. The payloads used for the optional AS2 test cases are also used for the SHA-2 test cases. SHA-224 was not tested.

Note: As already mentioned in the other optional test descriptions, the encryption algorithm used was either 3DES or AES-128 depending on the transport used during the test.

## SHA2 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 participating in this test event. 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 |
|---|---|---|---|
| Amazon Web Services | A m a z o n | ZZ | A m a z o n |
| Axway | axway -> b2bi | ZZ | ax_b2bi |
| Axway | secureTransport ! | ZZ | ax_transport |
| Axway | a x w a y - > T SIM | ZZ | axwaytsim |
| Beijing Sinowintop | Sinowintop AS2 | ZZ | sinowintop |
| CData Software | C D a t a - A r c # | ZZ | cdata |
| Cleo | CLEO | ZZ | cleo |
| DXC Technology | DXC *Elit | ZZ | dxc |
| IceCoreSoft AB | I c e c o r e s o f t ! | ZZ | icecoresoft |
| Salesforce | M u l e s o f t % | ZZ | mulesoft |

# Overview of the Drummond Interoperability Compliance Process®

The interoperability of B2B products for the Internet is essential for the long-term acceptance and growth of electronic commerce. To foster interoperability, Drummond 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 Pre-Certification Test Event

Pre-Certification Test Events are designed to allow participants—with products new to Drummond interoperability testing, or previously certified products that have made significant product changes or have undergone version changes or have missed the most recent test event — to both test and debug their products against the Drummond Test Server.

The Drummond Test Server is a collection of products-with-version from the previous Interoperability Test Event. These products were provided by the vendors on a voluntary basis. The Drummond 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 Pre-Certification Test Events, participants will see their products-with-version become conformant to the AS2 standard and interoperable with the Drummond Test Server products. Products that successfully complete Pre-Certification Test Events are considered compliant to the respective standard and will be listed on the Drummond website as “Pre-Certified", but they will not be given product Interoperability Status on the Drummond website.

Successful test completion also qualifies that product-with-version to participate in the next Drummond Interoperability Test event but does NOT guarantee successful completion of the full Interoperability Test Event. Drummond makes no warranty or guarantee that products passing the Pre-Certification Test Events will pass the Interoperability Tests.

## Drummond Interoperability Test Event

Products-with-version from the previous AS2 Interoperability Test Event and products-with-version from the Pre-Certification 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 Event, each product-with-version must successfully test with each other in order to be certified as interoperable.

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

Products-with-version that 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 Drummond website. Interoperability Test Events are periodically repeated to verify that as product names, versions or releases change, the products continue to remain interoperable.

## InSitu™ Test System

Drummond has created an innovative system for the automation of interoperability testing called InSitu™. InSitu™ is a proprietary and trusted testing tool developed for conducting automated interoperability testing allowing multiple products to coordinate the exchange of test cases without human intervention. Manpower requirements for coordinating testing have been eliminated, allowing participants to focus on debugging their codebase.

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. It does not change the requirements of the test case nor how the test instance result is interpreted. InSitu™ is only a test tool and cannot be utilized to compete with the participating products. All products-with-version have integrated the use of InSitu™ into their systems to enable automated testing.

# About Drummond

Drummond is the trusted interoperability test lab offering global testing services throughout 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 has tested thousands of 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: sales@drummondgroup.com