Final Report

ebMS Interoperability Test - 2023

March 1, 2023

Prepared & Administered By:
DRUMMOND GROUP, LLC
http://www.drummondgroup.com/

Table of Contents

Cover Letter

DRUMMOND GROUP, LLC is pleased to announce that during the Drummond Certified™ ebXML Message Service Interoperability Test for 2023 (ebMS 2023) these participants have completed all requirements and passed all required tests (see Final Test Results) between each product demonstrating interoperability and conformance to a Basic Profile subset of the ebMS version 2.0 specification. The Certification Run for this Test Event was completed March 1, 2023.

These participants also engaged in and successfully completed the following additional optional tests of Technical Profiles which comprise compliant supersets of the ebMS v2.0 standard based on recommendations from industry specific sources:

- Profile for XML Encryption and SSL Client Authentication as described by the Centers for Disease Control and Prevention (CDC)

- Automotive Retail Profile for GZIP based Compression as described by Standards for Technology in Automotive Retail (STAR)

Please note that an ebMS interoperability certification indicates the interoperability of a specific product-with-version, such as ebMS Product X v2.0, within a specific group of other products-with-version for a given test round, such as ebMS 2023. Products certified in this test event may not be interoperable with the products-with-version from future certification test rounds unless these products are retested.

Interoperability test rounds must be periodically repeated to verify that as product names, versions or releases change they remain interoperable. Therefore, passing an interoperability test round does not guarantee perpetual interoperability. The relevance of an ebMS test round certification within real world deployment diminishes with time. 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 deployment, 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 lasts for 6-12 months.

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

Sincerely,
Aaron Gomez
Supply Chain Security
Drummond Group, LLC

Disclaimer

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

Test Participants

Axway http://www.axway.com **Product Name:** **Axway B2Bi 2.6 / Activator 6.1**	**OpenText** http://www.opentext.com **Product Name:** **BizManager v16.6**

Definitions

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

Interoperable products – is that group of products, from the *Product Test Group*, which successfully completed the *Test Criteria*, in a full duplex manner with every other *Product Test Group* participant in an Interoperability Test Event without any errors in the Final Certification Test Phase. Interoperable products receive a Drummond Certified ™ Seal.

Product Test Group – A group of products involved in an interoperability or conformant 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: "VV.Rx…x," where VV is the version numeral designator, R is the single digit release numeral designator and x is the sub-release multiple digit numeral designator. Drummond Group assumes that any digits of less significance than the R place do not indicate code changes on the product-with-version-with-release tested in the Test 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 individual test cases, often 10 to 50 which the product test group exchange among themselves to verify conformance and interoperability.

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

Interoperability Test Summary

ebMS v2.0 is a Message Service protocol for reliable Business-to-Business data interchange. ebMS v2.0 adds quality of service features on top of transfer protocols such as HTTP and SMTP. Key qualities of service features include guaranteed delivery and non-repudiation of receipt. ebMS v2.0 can reliably transfer any data type including XML, X12, EDIFACT, or binary data between two parties over the Internet. The purpose of this test is to provide software vendors a neutral venue to test interoperability of ebMS v2.0 products in a non-competitive environment with the goal to accelerate adoption of high quality ebMS v2.0 deployments.

This is the 22nd round of Drummond Group Interoperability testing of the OASIS ebXML Message Service specification version 2.0 (ebMS v2.0). The Final Certification Test was completed on March 1, 2023.

During ebMS testing 2023, two participants successfully tested the Basic Profile, the additional Industry/Technology profile for XML Encryption and SSL Client Authentication. The same two participants also completed the additional Industry/Technology profile for Automotive Retail with GZIP based data compression of payloads.

Interoperability Test History

This is the 22nd Interoperability Test administered by Drummond Group.

ebMS 2023 Interoperability Test January – March 2023

Previous tests included the following:

ebMS 1Q22 Interoperability Test January – March 2022
ebMS 4Q20 Interoperability Test November 2020 – January 2021
ebMS 4Q19 Interoperability Test November 2019 – January 2020
ebMS 4Q18 Interoperability Test November 2018 – January 2019
ebMS 4Q17 Interoperability Test November - December 2017
ebMS 4Q16 Interoperability Test November - December 2016
ebMS 4Q15 Interoperability Test November - December 2015
ebMS 2Q14 Interoperability Test July - August 2014
ebMS 2Q13 Interoperability Test July - August 2013
ebMS 2Q12 Interoperability Test June 2012
ebMS 2Q11 Interoperability Test June - July 2011
ebMS 2Q10 Interoperability Test June - July 2010
ebMS 3Q09 Interoperability Test July - August 2009
ebMS 4Q08 Interoperability Test October - November 2008
ebMS 4Q07 Interoperability Test October - December 2007
ebMS 4Q06 Interoperability Test October - December 2006
ebMS 3Q05 Interoperability Test September - December 2005
ebMS 3Q04 Interoperability Test September - December 2004
ebMS 3Q03 Interoperability Test September - December 2003
ebMS 3Q02 Interoperability Test August - December 2002
ebMS 4Q01 Interoperability Test September - December 2001

Test Summary: Basic Profile

The following tests were identified as representative of the overall Basic Profile test suite and are composed of the most complex features. These tests comprised the ebMS v2.0 Certification Run Test Suite and were executed as the Final Test.

Test	Description	Transfer	Sync/Async	Payload
E1	Unsigned with Ack	http	async	Small XML
E3	Signed Data/Unsigned Ack	http	async	Small XML
E4	Signed Data/ Signed Ack Sync	http	sync	Small XML
E5	Signed Data/Signed Ack SSL	https	async	Small XML
E6	DSA Signed Data/Unsigned Ack	http	async	Small XML
F3	Two Payloads Signed Data	http	sync	Small XML Medium binary jpeg
F4	Five Payloads Signed Data/Ack SSL	https	async	Medium X12 HCCO Small EDIFACT Small XML Large XML Medium binary jpeg
G1	Ping Pong	http	sync	none
H1	Once and only once	https	async	Small XML
H2	Duplicate Detection	https	async	Small XML

Interoperability is determined by each product-with-version successfully sending and receiving each test case with the others. A test case is successful when the expected result is achieved according to the message specifications.

All products-with-version listed on this test report successfully sent and received all test cases in the Debug Phase Basic Profile Test Suite, that is, B1, B2, C1, D1, E1, E2, E3, E4, E5, E6, E7, F1, F2, F3, F4, G1, G2, G3, H1 and H2 with each and every other participant. The I1-I9 tests were successfully executed between each participant and the Drummond Group hosted test system during the Debug Phase and were not repeated during the Certification Run.

It should also be noted that 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 time period of testing.

Large Messages

The C1 Large Message Test is included in the Basic Profile as a straightforward test of a product-with-version's ability to send, receive and process large messages (50 megabyte). The test is not intended as a stress test or as a performance test. Drummond Group does not require a full matrix test for Large Messages to avoid performance problems related to memory issues, as participant test servers are typically medium sized servers. However, during the entire Interoperability Test Event, each participant exchanged a large message with every other participant. Since the Test Group only consisted of two (2) participants, both Test Participants successfully exchanged Large Messages during both the Debug Phase and Certification Run.

DSA Signature Algorithms

The ebMS v2.0 specification recommends the use of the DSAwithSHA1 algorithm for digitally signing ebMS messages. Historically this ebMS certification event has used the RSAwithSHA1 algorithm because of its widespread use in the marketplace. However, since the ebMS specification does recommend the use of DSA, this Certification Event now offers required tests as part of the Basic Profile Test Suite to certify the interoperability of the use of DSAwithSHA1 digital signatures over both HTTP and HTTPS. Test cases (E6 and E7) for messages signed with the DSAwithSHA1 signature algorithm using DSA digital certificates over both HTTP and HTTPS were executed by all participants during the Debug Phase and Certification Run.

Error Testing

Error tests defined in the Basic Profile are not tested in a round-robin fashion. Messages-in-error originate only from a Drummond Group hosted test system and are sent to the participants (for Tests I1-I8) or are sent from the participant to the Drummond Group hosted test system to test resending when a response is not received (Test I9).

During the Debug Phase, a full range of tests designed to test the error handling of each participant's Product-Under-Test were conducted with each participant. The executed Error Tests are listed in the Debug Phase Basic Profile Test Suite.

Test Summary: XML Encryption with SSL Client Authentication Profile

The following participants successfully completed the XML Encryption with SSL Client Authentication Industry Optional Profile Tests: **Axway** and **OpenText**.

As the ebMS 2.0 specification does not provide detailed requirements or recommendations for the use of XML Encryption, this profile makes use of CDC experience and recommendations for the use of XML Encryption with ebMS.

Beginning with the 4Q08 Interoperability Test Event, the message payload used during these tests was changed from the one used in previous test events. The new payload consisted of a small XML file in which some of the data consisted of accented non-English characters. This change was in response to reports of interoperability issues in the field with respect to payloads of this sort with XML encryption of at least one security toolkit vendor.

The following tests were executed by each participant noted above. Each participant successfully executed each test against the other participants involved in this optional test.

Test	Description	Transfer	Sync/Async	Payload
J1	Client Authentication	https	sync	Small XML w/accented characters
J2	Client Authentication & XML Encryption	https	sync	Small XML w/accented characters
J3	Client Authentication, Digital Signature & XML Encryption	https	sync	Small XML w/accented characters

Test Summary: Automotive Retail Profile - GZIP Based Compression

The following participants successfully completed the Automotive Retail with GZIP based Compression Industry Optional Profile Tests: **Axway** and **OpenText**.

As the ebMS 2.0 specification does not provide detailed requirements or recommendations for the use of payload compression, this profile makes use of the STAR (Standards for Technology in Automotive Retail) Profile experience with ebMS.

The following tests were executed by each participant noted above. Each participant successfully executed each test against the other participants involved in this optional test.

Test	Description	Transfer	Sync / Async	Payload
K1	XML Payload Synchronous	https	sync	Small XML, PartsOrder BOD
K2	XML Payload Asynchronous, Compressed	https	async	Large XML, PartsInvoice BOD
K3	XML Payload Asynchronous, Compressed and Signed	https	async	Large XML, PartsInvoice BOD

Interoperability Issues

During previous ebMS interoperability test events, issues arose that required consensus to achieve interoperability. Some of these items are outside the scope of the ebMS v2.0 specification and are related to underlying technical specifications such as MIME, and some of these issues address ebMS v2.0 features which have been interpreted differently by different readers.

The consensus items from all ebMS Interop Test Events were provided to the participants at the beginning of this Test Event. Additional copies will be provided upon request. There were no new interoperability items identified during the ebMS 2023 Test Event.

Test Requirements

In order to be part of the certified interoperable products-with-versions, each participant must both successfully send and receive all tests cases in the Basic Profile with each and every other participant.

Trading Partner Requirements

All participants were required to establish trading partner relationships with each other. All participants were remote from each other, and all test messages were exchanged over the public Internet. Participants were responsible for distributing their network information and configuring their firewalls to allow all other participants access to their product-with-version.

Each participant provided their security certificates (including SSL server and client 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. All participants generated their own self-signed certificates. Some participants chose to use a single certificate for all purposes, including SSL Server Authentication, SSL Client Authentication, Digital Signature and XML Encryption.

Additionally, all participants generated a second set of DSA certificates for use with the E6 and E7 tests.

Drummond Group provided test payloads and user identification aliases.

Technical Requirements – Basic Profile

Each participant successfully sent and received all tests cases in the Basic Profile with the other participant, with the exception of the Error Tests which are executed between a participant and a Drummond Group hosted test system.

The Basic Profile test cases cover the core requirements of ebMS v2.0 and include some optional features of ebMS v2.0 that are widely implemented and or desired by end users. These requirements are described directly below.

The effect is that all the products-with-version are proven interoperable over a feature-rich, industry horizontal profile and demonstrates that the products-with-version can cover the technical requirements listed below. For additional technical information regarding ebMS v2.0 requirements, please see the Message Service Specification version 2.0 located at:

http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf

Message Packaging

ebMS leverages SOAP with Attachments (SwA) to define an extensible message package that prescribes message headers for routing, partner identification, message identification, time-stamping, digital signature and other quality of service features. The message package is also capable of encapsulating one or more business documents or other binary data as payloads. Participant products-with-version must be capable of formatting SwA messages in the manner described by the specification.

Digital Signature

ebMS v2.0 leverages XMLDigitalSignature to provide proof of content-integrity, authentication of senders and receivers and NonRepudiation. An ebMS v2.0 signature is a signature over the entire message which may include one or more payloads. For the Basic Profile, the RSAwithSHA1 and DSAwithSHA1 digital signing algorithms are used.

Error Handling

ebMS v2.0 leverages SOAP Fault semantics for low level SOAP-related errors, and specifies higher level "ebMS error lists" that can be comprised of a list of warnings and/or errors that occur at the ebMS transport level. For example, a SOAP syntax error will generally result in a SOAP Fault error reply, while a message where TimeToLive has expired will result in an ebMS defined error list reply stating that the message has expired.

Synchronous and Asynchronous Messaging

ebMS supports both synchronous and asynchronous message patterns. The type of message pattern is defined per message. This allows ebMS to be highly transfer protocol neutral and to be used in business scenarios where immediate reply is required and in business scenarios where delayed replies are common due to queuing operations, load balancing, system outages or other technical or business reasons.

Synchronous and Asynchronous Acknowledgments of Receipt

Acknowledgments validate the receipt and persistent storage of a message. Synchronous acknowledgments provide a confirmation of receipt in a message returned over the same session and the same transfer protocol as the original message. Asynchronous acknowledgments are sent back to the originator over a separate session.

Acknowledgments are tested in both synchronous and asynchronous styles, both signed and unsigned. A signed acknowledgment includes hash digests of the original message allowing for true Non Repudiation of Receipt.

Transfer Protocols

Both HTTP & HTTPS transport protocols were tested. SMTP was not tested.

Payloads

The ebMS v2.0 message package provides for multiple payloads. Effectively, more than one business document can be sent in a single message. In some cases, the secondary documents may be binary files such as pictures and are often referred to as attachments; conceptually similar to email attachments.

Tests of single and multiple (up to five) payloads were executed. These tests included Digital Signature and HTTPS transport.

These payloads were used throughout the testing:

- Medium sized HIPAA compliant X12 document, approximately 18K provided by HCCO
- Small EDIFACT EDI document, approximately 2K
- Small XML document, approximately 600 bytes
- Large XML document, approximately 41K
- Medium sized XML automotive PartsOrder BOD, approximately 4K
- Large XML automotive PartsInvoice BOD, approximately 1 megabyte
- Very large X12 EDI file, 50 megabytes
- Medium sized binary jpeg file, approximately 11K

Large Messages

ebMS v2.0 provides the ability to transport any data type including large files. As a message service standard gains wider deployment in the market, invariably end users demand the ability to send very large messages. One test was run with a 50 megabyte EDI payload. This test is intended to prove the ability to send and receive large messages, and is not intended as a performance or stress test. Due to the Test Group comprising only two (2) participants, the large message tests were successfully executed in a full matrix manner during both the Debug Phase and Certification Run.

Reliable Messaging

ebMS v2.0 defines features to enable once-and-only-once delivery of messages. This is often referred to as Guaranteed Delivery; a message is received and persisted to storage successfully or the sender is notified of failure.

Tests are executed that exercise the features needed for once-and-only-once:

- Acknowledgment of receipt
- Sender’s ability to retry failed messages

Message Status

This ebMS v2.0 specific service is used to query the status of a previously sent message. An ebMS v2.0 specific reply is generated listing the previous message as UnAuthorized, NotRecognized, Received, Processed or Forwarded.

Ping/Pong

The Ping/Pong feature of ebMS v2.0 can be used as a “keep alive” status message, allowing parties to query the state of a partner’s message handler for management and troubleshooting purposes. Ping/Pong can also be useful as a simple connectivity test when engaging with new partners.

Error Handling

Each participant was sent messages-in-error from a Drummond Group hosted test system. The replies from the products-with-version were analyzed to determine if the participant system recognized the error and responded with an appropriate error response.

Technical Requirements: XML Encryption & SSL Client Authentication Profiles

Participants successfully executed an optional suite of tests designed to prove interoperability of XML Encryption and SSL Client Authentication implementations. These tests were executed in a full matrix with four participants choosing to opt-in and tested as both sender and receiver with the other participants. The specific details for applying XMLEncryption to ebMS v2.0 payloads originated from the CDC. For more information regarding the relationship between CDC PHIN and ebMS v2.0 see:

http://www.cdc.gov/phin/messaging/index.htm

http://www.cdc.gov/phin/components

Client Authentication

Client Authentication is an option of SSL/TLS that allows a Server to authenticate a client via the client’s possession of a recognizable digital certificate.

RFC 5246 indicates that **TLS 1.2** and previous versions of TLS and SSL utilize a CertificateRequest/Certificate Verify mechanism that occurs during the initial SSL handshake to authenticate a client. The server is in control of the client authentication and will send a CertificateRequest message to the client requesting the client’s certificate and the client will respond with its certificate to allow validation of the client. If the client does not return a valid certificate to the server, the connection will be terminated with an error.

TLS 1.3 now allows for and has described a new Client Authentication extension

whereby the client and server will negotiate client authentication post-handshake. The post handshake authentication is only allowed if the client has indicated that it is willing to perform a post-handshake authentication session. RFC 8446 states that a server MUST NOT send a post-handshake CertificateRequest to a client unless it has been requested by the client. Therefore, it is important to note that the TLS 1.3 post-handshake client authentication will not be executed unless the SSL client has indicated to the server that it supports post-handshake client authentication. If a client does not support post-handshake authentication the server should utilize the older CertificateRequest mechanism during the SSL handshake.

Participants proved interoperability over SSL Client Authentication and used it for all tests within this Profile.

XML Encryption

ebMS v2.0 allows for the use of a persistent encryption mechanism that can be applied to payloads within a message. Persistent encryption can be leveraged as an additional layer of security for Internet based messaging; essentially part or all of a message payload may be encrypted in a manner that allows only the intended receiver to decrypt the message. At the time the ebMS v2.0 standard was approved, XMLEncryption was still a draft standard. As a result, ebMS v2.0 states that XMLEncryption is the preferred encryption method, but ebMS v2.0 does not provide detailed methods for applying XML Encryption to ebMS messages.

This profile requires encryption of whole XML payloads using XMLEncryption. Participants who executed this Profile successfully interoperated with XMLEncryption and also a combination of XMLEncryption with DigitalSignature.

Technical Requirements – Automotive Retail Profile for GZIP-based Compression

Both participants chose to opt-in to the optional Automotive Retail Profile and successfully executed a suite of tests designed to prove interoperability of key features recommended by the Standards for Technology in Automotive Retail (STAR) consortium's ebMS Implementation Guidelines.

For additional technical information regarding the relationship between STAR and ebMS, refer to the STAR documents named Transport Guidelines and ebMS Implementation Guidelines which can be obtained from the Special Interest Groups / Infrastructure section of the public STAR website after completing a free registration. See http://www.starstandards.org.

GZIP Based Compression

The use of large messages (multiple megabytes) is common in many industries. There are several available methods for compressing HTTP based messages. The STAR guidelines recommend the use of gzip based compression where the payload itself is composed of compressed data using the MIME type application/gzip.

Participants proved interoperability over gzip based compression including the ability to combine compression with digital signature. For tests that required signature, the order of operations were implemented as compress-then-sign for message senders, and validate-signature-then-decompress for receivers.

Industry-Recommended Common Header Field Values

To assist in interoperability, the STAR guidelines require common methods for populating some of the key ebMS message header fields. Participants proved interoperability over requirements to populate the Service, Action and Timestamp header fields in accordance with STAR guidelines. Service and Action field values were based on the type of STAR OAG BOD payload in the test message.

Debug Phase Basic Profile Test Suite

A1	Connectivity			Individual Setup Time
B1	Simple Transfer	http	async	Small XML
B2	Simple Transfer SSL	https	async	Small XML
C1	Large Message	http	async	Very Large X12
D1	Signed Data	http	async	Small XML
E1	Unsigned with Ack	http	async	Small XML
E2	Unsigned with ACK sync	http	sync	Small XML
E3	Signed Data/Unsigned Ack	http	async	Small XML
E4	Signed Data/ Signed Ack Sync	http	sync	Small XML
E5	Signed Data/Signed Ack SSL	https	async	Small XML
E6	DSA Signed Data/Unsigned Ack	http	async	Small XML
E7	DSA Signed Data/Signed Ack	https	async	Small XML
F1	2 Payloads	http	async	Small XML Medium binary jpeg
F2	5 Payloads	http	async	Medium X12 HCCO HIPPA Small EDIFACT Small XML Large XML Medium binary jpeg
F3	2 Payloads Signed Data	http	sync	Small EDIFACT Medium binary jpeg
F4	5 Payloads Signed Data/Ack SSL	https	async	Medium X12 HCCO HIPPA Small EDIFACT Small XML Large XML Medium binary jpeg
G1	Ping Pong	http	sync	None
G2	Ping Pong SSL	https	async	None
G3	Message Status SSL	https	Async	None
H1	Once and only once	https	Async	Small XML
H2	Duplicate Detection	https	Async	Small XML Medium binary jpeg
I1	SOAP Fault	http	sync	Small XML
I2	Value not recognized	http	sync	Small XML
I3	Not Supported	http	sync	Small XML
I4	Inconsistent sync	http	async	Small XML
I5	Security Failure	http	sync	Small XML
I6	Time to Live expired	http	sync	Small XML
I7	Message Header format	http	sync	Small XML
I8	Missing Payload	http	sync	none
I9	Delivery Failure	http	async	Small XML

During the Debug Phase, both participants executed each Basic Profile test against the other participant, acting as both receiver and sender.

The only exceptions to this matrix style testing were for the Error Tests where Error Tests I1 through I8 were executed from a Drummond Group hosted test system to the participant's server and Error Test I9 was executed from the participant to a Drummond Group hosted server.

Overview of the Interoperability Compliance Process®

Interoperability of B2B products for the Internet is essential for the long-term acceptance and growth of electronic commerce. To foster interoperability, Drummond Group facilitates interoperability and conformance tests. This section contains a description of the test process involved with creating and listing interoperable products.

Drummond Group In-the-Queue Test Event

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

The Drummond Group Test Server is a collection of products-with-version from the previous Interoperability Test Event. These products were provided by the vendors on a voluntary basis. The Drummond Group Test Server allows products new to the interoperability process to be debugged in a quicker manner by testing with proven products-with-version.

Through the In-the-Queue Test Events, participants will see their products-with-version become conformant to the ebMS v2.0 standard and interoperable with the Drummond Group Test Server products. Products that successfully complete In-the-Queue Test Events are considered compliant to the respective standard and will be listed on the Drummond Group website as “In the Queue," but they will not be given product Interoperability Status on the Drummond Group website.

Successful test completion also qualifies that particular product to participate in the next Drummond Group Interoperability Test Event, but does NOT guarantee successful completion of the full Interoperability Certification Test. Drummond Group makes no warranties nor guarantees that products passing In-the-Queue Test Events will pass the Interoperability Tests.

Drummond Group Interoperability Test Event

Products-with-version from the previous ebMS v2.0 Interoperability Test Event and products-with-version from the In-the-Queue tests come together in a vendor-neutral and non-competitive environment to test with each other in order to become interoperable with each other. In an Interoperability Test Event, each product-with-version must successfully test with each other in order to be certified as interoperable.

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

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

About Drummond Group

Drummond Group offers comprehensive compliance, security, risk management, surveillance, and education services to healthcare, financial, and other regulated industries. We bring thought leadership, expertise, practical tools, and partnership to the compliance and assessment processes for our clients. At Drummond Group, enabling you to feel secure about the ways in which you share your business' sensitive and private data is our primary goal.

EPCS, CSOS, AS2, AS4, ebXML, GDSN, EPCIS GS1 for DSCSA Track and Trace; each is a standard that helps ensure the integrity of the supply chain, and Drummond Group is right there to help you, no matter which trustmark, certification, or assurance you're pursuing.