



Creating A Single Global Electronic Market

1 **Message Service Specification**

2 **Version 2.0**

3 **OASIS ebXML Messaging Services Technical Committee**

4 1 April 2002

5 Status of this Document

6 This document specifies an ebXML Message Specification for the eBusiness community. Distribution of
7 this document is unlimited.

8 The document formatting is based on the Internet Society's Standard RFC format converted to Microsoft
9 Word 2000 format.

10 Note: Implementers of this specification should consult the OASIS ebXML Messaging Services Technical
11 Committee web site for current status and revisions to the specification
12 (<http://www.oasis-open.org/committees/ebxml-msg/>).

13 *Specification*

14 Version 1.0 of this Technical Specification document was approved by the ebXML Plenary in May 2001.

15 Version 2.0 of this Technical Specification document was approved by the OASIS Messaging Team, as a
16 Technical Committee(TC) Specification, March 1, 2002.

17 Version 2.0 of this Technical Specification document is presented to the OASIS membership for
18 consideration as an OASIS Technical Specification, April 2002.

19 *This version*

20 V2.0 – http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf

21 *Errata to this version*

22 V2.0 – http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0_errata.html

23 *Previous version*

24 V1.0 – <http://www.ebxml.org/specs/ebMS.doc>

25 ebXML Participants

26 The authors wish to acknowledge the support of the members of the Messaging Services Team who
27 contributed ideas, comments and text to this specification by the group's discussion eMail list, on
28 conference calls and during face-to-face meetings.

Ralph Berwanger	Individual Member	Ian Jones	Individual Member
Dick Brooks	Individual Member	Brad Lund	Intel™ Corporation
Doug Bunting	Sun Microsystems, Inc	Bob Miller	GE Global eXchange
David Burdett	Commerce One	Dale Moberg	Cyclone Commerce
Arvola Chan	TIBCO	Himagiri Mulkamala	Sybase
Sanjay Cherian	Sterling Commerce	Bruce Pedretti	Hewlett-Packard
Cliff Collins	Sybase	Yukinori Saito	Individual Member
Philippe DeSmedt	Individual Member	Martin Sachs	IBM Research
Colleen Evans	Sonic Software	Jeff Turpin	Cyclone Commerce
Chris Ferris	Sun Microsystems, Inc	Aynur Unal	E2Open
David Fischer	Drummond Group	Cedrec Vessell	DISA
Jim Galvin	Drummond Group	Daniel Weinreb	eXcelon
Brian Gibb	Sterling Commerce	Pete Wenzel	SeeBeyond
Scott Hinkelman	IBM	Prasad Yendluri	WebMethods
Jim Hughes	Hewlett Packard	Sinisa Zimek	SAP
Kazunori Iwasa	Fujitsu Limited		

29 The UN/CEFACT-OASIS v1.0 Team – see Acknowledgments

30 Table of Contents

31 Status of this Document 2

32 ebXML Participants 2

33 Introduction 6

34 1 Summary of Contents of this Document 6

35 1.1.1 Document Conventions 7

36 1.1.2 Audience 7

37 1.1.3 Caveats and Assumptions 7

38 1.1.4 Related Documents 7

39 1.2 Concept of Operation 8

40 1.2.1 Scope 8

41 1.2.2 Background and Objectives 8

42 1.2.3 Operational Policies and Constraints 9

43 1.2.4 Modes of Operation 10

44 1.3 Minimal Requirements for Conformance 11

45 Part I. Core Functionality 12

46 2 ebXML with SOAP 12

47 2.1 Packaging Specification 12

48 2.1.1 SOAP Structural Conformance 13

49 2.1.2 Message Package 13

50 2.1.3 Header Container 13

51 2.1.4 Payload Container 14

52 2.1.5 Additional MIME Parameters 14

53 2.1.6 Reporting MIME Errors 15

54 2.2 XML Prolog 15

55 2.2.1 XML Declaration 15

56 2.2.2 Encoding Declaration 15

57 2.3 ebXML SOAP Envelope extensions 15

58 2.3.1 Namespace pseudo attribute 15

59 2.3.2 xsi:schemaLocation attribute 15

60 2.3.3 SOAP Header Element 16

61 2.3.4 SOAP Body Element 16

62 2.3.5 ebXML SOAP Extensions 16

63 2.3.6 #wildcard Element Content 17

64 2.3.7 id attribute 17

65 2.3.8 version attribute 17

66 2.3.9 SOAP mustUnderstand attribute 18

67 2.3.10 ebXML "Next MSH" actor URI 18

68 2.3.11 ebXML "To Party MSH" actor URI 18

69 3 Core Extension Elements 18

70 3.1 MessageHeader Element 18

71 3.1.1 From and To Elements 19

72 3.1.2 CPAlid Element 19

73 3.1.3 ConversationId Element 20

74 3.1.4 Service Element 20

75 3.1.5 Action Element 21

76 3.1.6 MessageData Element 21

77 3.1.7 DuplicateElimination Element 22

78 3.1.8 Description Element 22

79 3.1.9 MessageHeader Sample 22

80 3.2 Manifest Element 22

81 3.2.1 Reference Element 23

82 3.2.2 Manifest Validation 23

83 3.2.3 Manifest Sample 24

84 4 Core Modules 24

85 4.1 Security Module 24

86 4.1.1 Signature Element 24

87 4.1.2 Security and Management 25

88 4.1.3 Signature Generation 25

89 4.1.4 Countermeasure Technologies 27

90	4.1.5	Security Considerations	28
91	4.2	Error Handling Module	29
92	4.2.2	Types of Errors	29
93	4.2.3	ErrorList Element	30
94	4.2.4	Implementing Error Reporting and Handling.....	32
95	4.3	SyncReply Module	33
96	4.3.1	SyncReply Element.....	33
97	5	Combining ebXML SOAP Extension Elements	33
98	5.1.1	MessageHeader Element Interaction	33
99	5.1.2	Manifest Element Interaction.....	34
100	5.1.3	Signature Element Interaction	34
101	5.1.4	ErrorList Element Interaction.....	34
102	5.1.5	SyncReply Element Interaction	34
103		Part II. Additional Features.....	35
104	6	Reliable Messaging Module.....	35
105	6.1	Persistent Storage and System Failure	35
106	6.2	Methods of Implementing Reliable Messaging.....	35
107	6.3	Reliable Messaging SOAP Header Extensions.....	36
108	6.3.1	AckRequested Element.....	36
109	6.3.2	Acknowledgment Element.....	37
110	6.4	Reliable Messaging Parameters.....	38
111	6.4.1	DuplicateElimination.....	38
112	6.4.2	AckRequested.....	39
113	6.4.3	Retries	39
114	6.4.4	RetryInterval	39
115	6.4.5	TimeToLive	39
116	6.4.6	PersistDuration	39
117	6.4.7	syncReplyMode	39
118	6.5	ebXML Reliable Messaging Protocol.....	40
119	6.5.1	Sending Message Behavior	40
120	6.5.2	Receiving Message Behavior.....	40
121	6.5.3	Generating an Acknowledgment Message	41
122	6.5.4	Resending Lost Application Messages.....	41
123	6.5.5	Resending Acknowledgments	42
124	6.5.6	Duplicate Message Handling.....	43
125	6.5.7	Failed Message Delivery	43
126	6.6	Reliable Messaging Combinations	44
127	7	Message Status Service	44
128	7.1	Message Status Messages	45
129	7.1.1	Message Status Request Message	45
130	7.1.2	Message Status Response Message	45
131	7.1.3	Security Considerations	45
132	7.2	StatusRequest Element.....	45
133	7.2.1	RefToMessageId Element.....	46
134	7.2.2	StatusRequest Sample	46
135	7.2.3	StatusRequest Element Interaction	46
136	7.3	StatusResponse Element.....	46
137	7.3.1	RefToMessageId Element.....	46
138	7.3.2	Timestamp Element	46
139	7.3.3	messageStatus attribute.....	46
140	7.3.4	StatusResponse Sample.....	47
141	7.3.5	StatusResponse Element Interaction	47
142	8	Message Service Handler Ping Service.....	47
143	8.1	Message Service Handler Ping Message.....	47
144	8.2	Message Service Handler Pong Message	48
145	8.3	Security Considerations	49
146	9	MessageOrder Module.....	49
147	9.1	MessageOrder Element	49
148	9.1.1	SequenceNumber Element	49
149	9.1.2	MessageOrder Sample	50
150	9.2	MessageOrder Element Interaction.....	50
151	10	Multi-Hop Module	50
152	10.1	Multi-hop Reliable Messaging	51
153	10.1.1	AckRequested Sample.....	51

154	10.1.2	Acknowledgment Sample.....	51
155	10.1.3	Multi-Hop Acknowledgments.....	51
156	10.1.4	Signing Multi-Hop Acknowledgments.....	52
157	10.1.5	Multi-Hop Security Considerations.....	52
158	10.2	Message Ordering and Multi-Hop.....	52
159	Part III. Normative Appendices.....		53
160	Appendix A	The ebXML SOAP Extension Elements Schema.....	53
161	Appendix B	Communications Protocol Bindings.....	58
162	B.1	Introduction.....	58
163	B.2	HTTP.....	58
164	B.2.1	Minimum level of HTTP protocol.....	58
165	B.2.2	Sending ebXML Service messages over HTTP.....	58
166	B.2.3	HTTP Response Codes.....	59
167	B.2.4	SOAP Error conditions and Synchronous Exchanges.....	60
168	B.2.5	Synchronous vs. Asynchronous.....	60
169	B.2.6	Access Control.....	60
170	B.2.7	Confidentiality and Transport Protocol Level Security.....	60
171	B.3	SMTP.....	61
172	B.3.1	Minimum Level of Supported Protocols.....	61
173	B.3.2	Sending ebXML Messages over SMTP.....	61
174	B.3.3	Response Messages.....	63
175	B.3.4	Access Control.....	63
176	B.3.5	Confidentiality and Transport Protocol Level Security.....	63
177	B.3.6	SMTP Model.....	63
178	B.4	Communication Errors during Reliable Messaging.....	64
179	Appendix C	Supported Security Services.....	65
180	References.....		67
181	Normative References.....		67
182	Non-Normative References.....		68
183	Contact Information.....		69
184	Acknowledgments.....		69
185	Disclaimer.....		70
186	Copyright Statement.....		70
187	Intellectual Property Rights Statement.....		70
188			

188 Introduction

189 This specification is one of a series of specifications realizing the vision of creating a single global
190 electronic marketplace where enterprises of any size and in any geographical location can meet and
191 conduct business with each other through the exchange of XML based messages. The set of
192 specifications enable a modular, yet complete electronic business framework.

193 This specification focuses on defining a communications-protocol neutral method for exchanging
194 electronic business messages. It defines specific enveloping constructs supporting reliable, secure
195 delivery of business information. Furthermore, the specification defines a flexible enveloping technique,
196 permitting messages to contain payloads of any format type. This versatility ensures legacy electronic
197 business systems employing traditional syntaxes (i.e. UN/EDIFACT, ASC X12, or HL7) can leverage the
198 advantages of the ebXML infrastructure along with users of emerging technologies.

199 1 Summary of Contents of this Document

200 This specification defines the *ebXML Message Service Protocol* enabling the secure and reliable
201 exchange of messages between two parties. It includes descriptions of:

- 202 • the ebXML Message structure used to package payload data for transport between parties,
- 203 • the behavior of the Message Service Handler sending and receiving those messages over a data
204 communications protocol.

205 This specification is independent of both the payload and the communications protocol used. Appendices
206 to this specification describe how to use this specification with HTTP [RFC2616] and SMTP [RFC2821].

207 This specification is organized around the following topics:

208 Core Functionality

- 209 • **Packaging Specification** – A description of how to package an ebXML Message and its associated parts
210 into a form that can be sent using a communications protocol such as HTTP or SMTP (section 2.1),
- 211 • **ebXML SOAP Envelope Extensions** – A specification of the structure and composition of the information
212 necessary for an *ebXML Message Service* to generate or process an ebXML Message (section 2.3),
- 213 • **Error Handling** – A description of how one *ebXML Message Service* reports errors it detects to another
214 ebXML Message Service Handler (section 4.2),
- 215 • **Security** – Provides a specification of the security semantics for ebXML Messages (section 4.1),
- 216 • **SyncReply** – Indicates to the Next MSH whether or not replies are to be returned synchronously
217 (section 4.3).

218 Additional Features

- 219 • **Reliable Messaging** – The Reliable Messaging function defines an interoperable protocol where any two
220 Message Service implementations can reliably exchange messages sent using once-and-only-once delivery
221 semantics (section 6),
- 222 • **Message Status Service** – A description of services enabling one service to discover the status of another
223 Message Service Handler (MSH) or an individual message (section 7 and 8),
- 224 • **Message Order** – The Order of message receipt by the *To Party MSH* can be guaranteed (section 9),
- 225 • **Multi-Hop** – Messages may be sent through intermediary MSH nodes (section 10).

226 Appendices to this specification cover the following:

- 227 • **Appendix A Schema** – This normative appendix contains XML schema definition [XMLSchema] for the
228 ebXML SOAP *Header* and *Body* Extensions,
- 229 • **Appendix B Communications Protocol Envelope Mappings** – This normative appendix describes how to
230 transport *ebXML Message Service* compliant messages over HTTP and SMTP,
- 231 • **Appendix C Security Profiles** – a discussion concerning Security Service Profiles.

232 1.1.1 Document Conventions

233 Terms in *Italics* are defined in the ebXML Glossary of Terms [ebGLOSS]. Terms listed in **Bold Italics**
234 represent the element and/or attribute content. Terms listed in `Courier` font relate to MIME
235 components. Notes are listed in Times New Roman font and are informative (non-normative). Attribute
236 names begin with lowercase. Element names begin with Uppercase.

237 The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT,
238 RECOMMENDED, MAY and OPTIONAL, when they appear in this document, are to be interpreted as
239 described in [RFC2119] as quoted here:

- 240 • *MUST: This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute*
241 *requirement of the specification.*
- 242 • *MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of*
243 *the specification.*
- 244 • *SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in*
245 *particular circumstances to ignore a particular item, but the full implications must be understood and*
246 *carefully weighed before choosing a different course.*
- 247 • *SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED", means that there may exist valid*
248 *reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full*
249 *implications should be understood and the case carefully weighed before implementing any behavior*
250 *described with this label.*
- 251 • *MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose*
252 *to include the item because a particular marketplace requires it or because the vendor feels that it enhances*
253 *the product while another vendor may omit the same item. An implementation which does not include a*
254 *particular option MUST be prepared to interoperate with another implementation which does include the*
255 *option, though perhaps with reduced functionality. In the same vein an implementation which does include a*
256 *particular option MUST be prepared to interoperate with another implementation which does not include the*
257 *option (except, of course, for the feature the option provides).*

258 1.1.2 Audience

259 The target audience for this specification is the community of software developers who will implement the
260 *ebXML Message Service*.

261 1.1.3 Caveats and Assumptions

262 It is assumed the reader has an understanding of communications protocols, MIME, XML, SOAP, SOAP
263 Messages with Attachments and security technologies.

264 All examples are to be considered non-normative. If inconsistencies exist between the specification and
265 the examples, the specification supersedes the examples.

266 It is strongly RECOMMENDED implementors read and understand the Collaboration Protocol Profile/
267 Agreement [ebCPP] specification and its implications prior to implementation.

268 1.1.4 Related Documents

269 The following set of related specifications are developed independent of this specification as part of the
270 ebXML initiative:

- 271 • **ebXML Technical Architecture Specification** [ebTA] – defines the overall technical architecture for ebXML
- 272 • **ebXML Technical Architecture Risk Assessment Technical Report** [secRISK] – defines the security
273 mechanisms necessary to negate anticipated, selected threats
- 274 • **ebXML Collaboration Protocol Profile and Agreement Specification** [ebCPP] – defines how one party
275 can discover and/or agree upon the information the party needs to know about another party prior to sending
276 them a message that complies with this specification
- 277 • **ebXML Registry/Repository Services Specification** [ebRS] – defines a registry service for the ebXML
278 environment

279 1.2 Concept of Operation

280 1.2.1 Scope

281 The ebXML Message Service (ebMS) defines the message enveloping and header document schema
282 used to transfer ebXML messages over a communications protocol such as HTTP or SMTP and the
283 behavior of software sending and receiving ebXML messages. The ebMS is defined as a set of layered
284 extensions to the base Simple Object Access Protocol [SOAP] and SOAP Messages with Attachments
285 [SOAPAttach] specifications. This document provides security and reliability features necessary to
286 support international electronic business. These security and reliability features are not provided in the
287 SOAP or SOAP with Attachments specifications.

288 The ebXML infrastructure is composed of several independent, but related, components. Specifications
289 for the individual components are fashioned as stand-alone documents. The specifications are totally
290 self-contained; nevertheless, design decisions within one document can and do impact the other
291 documents. Considering this, the ebMS is a closely coordinated definition for an ebXML message service
292 handler (MSH).

293 The ebMS provides the message packaging, routing and transport facilities for the ebXML infrastructure.
294 The ebMS is not defined as a physical component, but rather as an abstraction of a process. An
295 implementation of this specification could be delivered as a wholly independent software application or an
296 integrated component of some larger business process.

297 1.2.2 Background and Objectives

298 Traditional business information exchanges have conformed to a variety of standards-based syntaxes.
299 These exchanges were largely based on electronic data interchange (EDI) standards born out of
300 mainframe and batch processing. Some of the standards defined bindings to specific communications
301 protocols. These EDI techniques worked well; however, they were difficult and expensive to implement.
302 Therefore, use of these systems was normally limited to large enterprises possessing mature information
303 technology capabilities.

304 The proliferation of XML-based business interchanges served as the catalyst for defining a new global
305 paradigm that ensured all business activities, regardless of size, could engage in electronic business
306 activities. The prime objective of ebMS is to facilitate the exchange of electronic business messages
307 within an XML framework. Business messages, identified as the 'payloads' of the ebXML messages, are
308 not necessarily expressed in XML. XML-based messages, as well as traditional EDI formats, are
309 transported by the ebMS. Actually, the ebMS payload can take any digital form—XML, ASC X12, HL7,
310 AIAG E5, database tables, binary image files, etc.

311 The ebXML architecture requires that the ebXML Message Service protocol be capable of being carried
312 over any available communications protocol. Therefore, this document does not mandate use of a
313 specific communications protocol. This version of the specification provides bindings to HTTP and SMTP,
314 but other protocols can, and reasonably will, be used.

315 The ebXML Requirements Specification [ebREQ] mandates the need for secure, reliable
316 communications. The ebXML work focuses on leveraging existing and emerging technology—attempts to
317 create new protocols are discouraged. Therefore, this document defines security within the context of
318 existing security standards and protocols. Those requirements satisfied with existing standards are
319 specified in the ebMS, others must be deferred until new technologies or standards are available, for
320 example encryption of individual message header elements.

321 Reliability requirements defined in the ebREQ relate to delivery of ebXML messages over the
322 communications channels. The ebMS provides mechanisms to satisfy the ebREQ requirements. The
323 reliable messaging elements of the ebMS supply reliability to the communications layer; they are not
324 intended as business-level acknowledgments to the applications supported by the ebMS. This is an
325 important distinction. Business processes often anticipate responses to messages they generate. The
326 responses may take the form of a simple acknowledgment of message receipt by the application
327 receiving the message or a companion message reflecting action on the original message. Those
328 messages are outside of the MSH scope. The acknowledgment defined in this specification does not

329 indicate the payload of the ebXML message was syntactically correct. It does not acknowledge the
330 accuracy of the payload information. It does not indicate business acceptance of the information or
331 agreement with the content of the payload. The ebMS is designed to provide the sender with the
332 confidence the receiving MSH has received the message securely and intact.

333 The underlying architecture of the MSH assumes messages are exchanged between two ebMS-
334 compliant MSH nodes. This pair of MSH nodes provides a hop-to-hop model extended as required to
335 support a multi-hop environment. The multi-hop environment allows the next destination of the message
336 to be an intermediary MSH other than the 'receiving MSH' identified by the original sending MSH. The
337 ebMS architecture assumes the sender of the message MAY be unaware of the specific path used to
338 deliver a message. However, it MUST be assumed the original sender has knowledge of the final
339 recipient of the message and the first of one or more intermediary hops.

340 The MSH supports the concept of 'quality of service.' The degree of service quality is controlled by an
341 agreement existing between the parties directly involved in the message exchange. In practice, multiple
342 agreements may be required between the two parties. The agreements might be tailored to the particular
343 needs of the business exchanges. For instance, business partners may have a contract defining the
344 message exchanges related to buying products from a domestic facility and another defining the
345 message exchanges for buying from an overseas facility. Alternatively, the partners might agree to follow
346 the agreements developed by their trade association. Multiple agreements may also exist between the
347 various parties handling the message from the original sender to the final recipient. These agreements
348 could include:

- 349 • an agreement between the MSH at the message origination site and the MSH at the final destination; and
- 350 • agreement between the MSH at the message origination site and the MSH acting as an intermediary; and
- 351 • an agreement between the MSH at the final destination and the MSH acting as an intermediary. There
352 would, of course, be agreements between any additional intermediaries; however, the originating site MSH
353 and final destination MSH MAY have no knowledge of these agreements.

354 An ebMS-compliant MSH shall respect the in-force agreements between itself and any other ebMS-
355 compliant MSH with which it communicates. In broad terms, these agreements are expressed as
356 Collaboration Protocol Agreements (CPA). This specification identifies the information that must be
357 agreed. It does not specify the method or form used to create and maintain these agreements. It is
358 assumed, in practice, the actual content of the contracts may be contained in initialization/configuration
359 files, databases, or XML documents complying with the ebXML Collaboration Protocol Profile and
360 Agreement Specification [ebCPP].

361 **1.2.3 Operational Policies and Constraints**

362 The ebMS is a service logically positioned between one or more business applications and a
363 communications service. This requires the definition of an abstract service interface between the
364 business applications and the MSH. This document acknowledges the interface, but does not provide a
365 definition for the interface. Future versions of the ebMS MAY define the service interface structure.

366 Bindings to two communications protocols are defined in this document; however, the MSH is specified
367 independent of any communications protocols. While early work focuses on HTTP for transport, no
368 preference is being provided to this protocol. Other protocols may be used and future versions of the
369 specification may provide details related to those protocols.

370 The ebMS relies on external configuration information. This information is determined either through
371 defined business processes or trading partner agreements. These data are captured for use within a
372 Collaboration Protocol Profile (CPP) or Collaboration Protocol Agreement (CPA). The ebXML
373 Collaboration Protocol Profile and Agreement Specification [ebCPP] provides definitions for the
374 information constituting the agreements. The ebXML architecture defines the relationship between this
375 component of the infrastructure and the ebMS. As regards the MSH, the information composing a
376 CPP/CPA must be available to support normal operation. However, the method used by a specific
377 implementation of the MSH does not mandate the existence of a discrete instance of a CPA. The CPA is
378 expressed as an XML document. Some implementations may elect to populate a database with the
379 information from the CPA and then use the database. This specification does not prescribe how the CPA

380 information is derived, stored, or used: it only states specific information items must be available for the
 381 MSH to achieve successful operations.

382 1.2.4 Modes of Operation

383 This specification does not mandate how the MSH will be installed within the overall ebXML framework. It
 384 is assumed some MSH implementations will not implement all functionality defined in this specification.
 385 For instance, a set of trading partners may not require reliable messaging services; therefore, no reliable
 386 messaging capabilities exist within their MSH. But, all MSH implementations shall comply with the
 387 specification with regard to the functions supported in the specific implementation and provide error
 388 notifications for functionality requested but not supported. Documentation for a MSH implementation
 389 SHALL identify all ebMS features not satisfied in the implementation.

390 The *ebXML Message Service* may be conceptually broken down into the following three parts:
 391 (1) an abstract *Service Interface*, (2) functions provided by the MSH and (3) the mapping to underlying
 392 transport service(s).

393 *Figure 1* depicts a logical arrangement of the functional
 394 modules existing within one possible implementation of the
 395 *ebXML Message Services* architecture. These modules are
 396 arranged in a manner to indicate their inter-relationships
 397 and dependencies.

398 **Header Processing** – the creation of the ebXML Header
 399 elements for the *ebXML Message* uses input from the
 400 application, passed through the Message Service Interface,
 401 information from the *Collaboration Protocol Agreement*
 402 governing the message, and generated information such as
 403 digital signature, timestamps and unique identifiers.

404 **Header Parsing** – extracting or transforming information
 405 from a received ebXML Header element into a form suitable
 406 for processing by the MSH implementation.

407 **Security Services** – digital signature creation and
 408 verification, encryption, authentication and authorization.
 409 These services MAY be used by other components of the
 410 MSH including the Header Processing and Header Parsing
 411 components.

412 **Reliable Messaging Services** – handles the delivery and
 413 acknowledgment of ebXML Messages. The service
 414 includes handling for persistence, retry, error notification
 415 and acknowledgment of messages requiring reliable
 416 delivery.

417 **Message Packaging** – the final enveloping of an *ebXML*
 418 *Message* (ebXML header elements and payload) into its
 419 SOAP Messages with Attachments [SOAPAttach] container.

420 **Error Handling** – this component handles the reporting of
 421 errors encountered during MSH or Application processing of
 422 a message.

423 **Message Service Interface** – an abstract service interface
 424 applications use to interact with the MSH to send and
 425 receive messages and which the MSH uses to interface
 426 with applications handling received messages (Delivery
 427 Module).

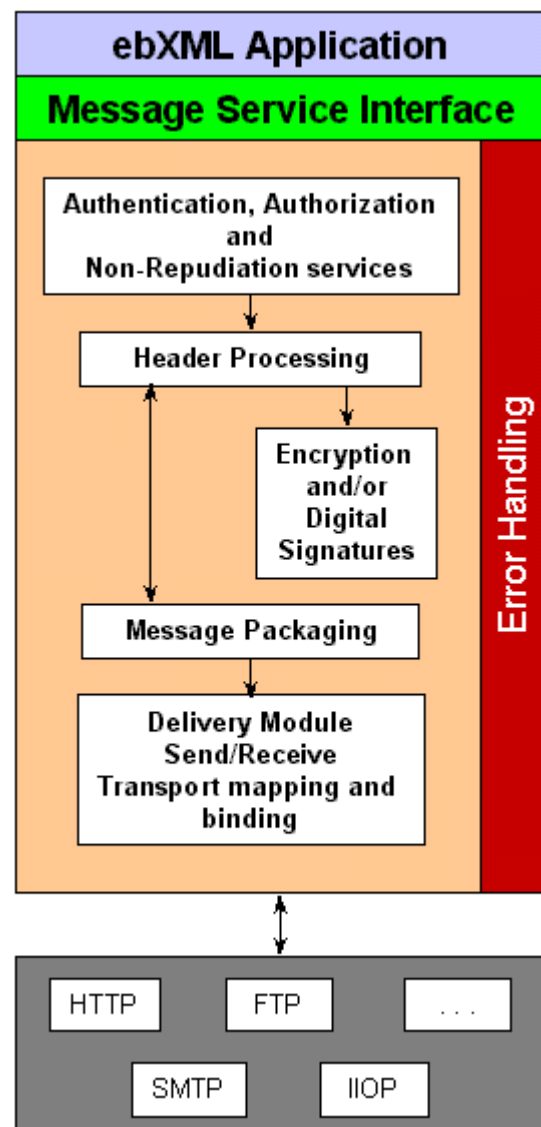


Figure 1.1 Typical Relationship between ebXML Message Service Handler Components

428 1.3 Minimal Requirements for Conformance

429 An implementation of this specification MUST satisfy ALL of the following conditions to be considered a
430 conforming implementation:

- 431 • It supports all the mandatory syntax, features and behavior (as identified by the [RFC2119] key words
432 MUST, MUST NOT, REQUIRED, SHALL and SHALL NOT) defined in Part I – Core Functionality.
- 433 • It supports all the mandatory syntax, features and behavior defined for each of the additional module(s),
434 defined in Part II – Additional Features, the implementation has chosen to implement.
- 435 • It complies with the following interpretation of the keywords OPTIONAL and MAY: When these keywords
436 apply to the behavior of the implementation, the implementation is free to support these behaviors or not, as
437 meant in [RFC2119]. When these keywords apply to message contents relevant to a module of features, a
438 conforming implementation of such a module MUST be capable of processing these optional message
439 contents according to the described ebXML semantics.
- 440 • If it has implemented optional syntax, features and/or behavior defined in this specification, it MUST be
441 capable of interoperating with another implementation that has not implemented the optional syntax,
442 features and/or behavior. It MUST be capable of processing the prescribed failure mechanism for those
443 optional features it has chosen to implement.
- 444 • It is capable of interoperating with another implementation that has chosen to implement optional syntax,
445 features and/or behavior, defined in this specification, it has chosen not to implement. Handling of
446 unsupported features SHALL be implemented in accordance with the prescribed failure mechanism defined
447 for the feature.

448 More details on Conformance to this specification – conformance levels or profiles and on their
449 recommended implementation – are described in a companion document, "*Message Service
450 Implementation Guidelines*" from the OASIS ebXML Implementation, Interoperability and Conformance
451 (IIC) Technical Committee.

452

Part I. Core Functionality

453

2 ebXML with SOAP

454 The ebXML Message Service Specification defines a set of namespace-qualified SOAP **Header** and
 455 **Body** element extensions within the SOAP **Envelope**. These are packaged within a MIME multipart to
 456 allow payloads or attachments to be included with the SOAP extension elements. In general, separate
 457 ebXML SOAP extension elements are used where:

- 458 • different software components may be used to generate ebXML SOAP extension elements,
- 459 • an ebXML SOAP extension element is not always present or,
- 460 • the data contained in the ebXML SOAP extension element MAY be digitally signed separately from the other
 461 ebXML SOAP extension elements.

462

2.1 Packaging Specification

463 An ebXML Message is a communications protocol independent MIME/Multipart message envelope,
 464 structured in compliance with the SOAP Messages with Attachments [SOAPAttach] specification, referred
 465 to as a *Message Package*.

466 There are two logical MIME parts within the *Message Package*:

- 467 • The first MIME part, referred to as the *Header Container*, containing one SOAP 1.1 compliant
 468 message. This XML document is referred to as a *SOAP Message* for the remainder of this
 469 specification,
 470 as a *SOAP Message* for the remainder of this
 471 specification,
- 472 • zero or more additional MIME parts, referred to as *Payload Containers*, containing application
 473 level payloads.
 474

475 The general structure and composition of an ebXML
 476 Message is described in the following figure (2.1).
 477

478

478 The *SOAP Message* is an XML document consisting
 479 of a SOAP **Envelope** element. This is the root
 480 element of the XML document representing a *SOAP
 481 Message*. The SOAP **Envelope** element consists of:

- 482 • One SOAP **Header** element. This is a generic
 483 mechanism for adding features to a *SOAP
 484 Message*, including ebXML specific header
 485 elements.
- 486 • One SOAP **Body** element. This is a container for
 487 message service handler control data and
 488 information related to the payload parts of the
 489 message.

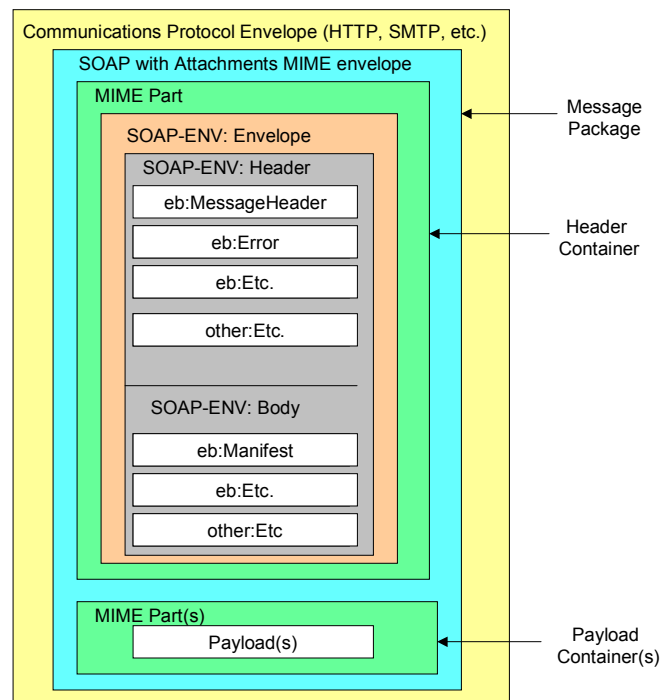


Figure 2.1 ebXML Message Structure

490 2.1.1 SOAP Structural Conformance

491 The *ebXML Message* packaging complies with the following specifications:

- 492 • Simple Object Access Protocol (SOAP) 1.1 [SOAP]
- 493 • SOAP Messages with Attachments [SOAPAttach]

494 Carrying ebXML headers in *SOAP Messages* does not mean ebXML overrides existing semantics of
495 SOAP, but rather the semantics of ebXML over SOAP maps directly onto SOAP semantics.

496 2.1.2 Message Package

497 All MIME header elements of the *Message Package* are in conformance with the SOAP Messages with
498 Attachments [SOAPAttach] specification. In addition, the `Content-Type` MIME header in the *Message*
499 *Package* contain a `type` attribute matching the MIME media type of the MIME body part containing the
500 *SOAP Message* document. In accordance with the [SOAP] specification, the MIME media type of the
501 *SOAP Message* has the value "text/xml".

502 It is strongly RECOMMENDED the initial headers contain a `Content-ID` MIME header structured in
503 accordance with MIME [RFC2045], and in addition to the required parameters for the Multipart/Related
504 media type, the `start` parameter (OPTIONAL in MIME Multipart/Related [RFC2387]) always be present.
505 This permits more robust error detection. The following fragment is an example of the MIME headers for
506 the multipart/related *Message Package*:

```
507 Content-Type: multipart/related; type="text/xml"; boundary="boundaryValue";  
508 start=messagepackage-123@example.com  
509  
510 --boundaryValue  
511 Content-ID: <messagepackage-123@example.com>
```

512 Implementations MUST support non-multipart messages, which may occur when there are no ebXML
513 payloads. An ebXML message with no payload may be sent either as a plain SOAP message or as a
514 [SOAPAttach] multipart message with only one body part.

515 2.1.3 Header Container

516 The root body part of the *Message Package* is referred to in this specification as the *Header Container*.
517 The *Header Container* is a MIME body part consisting of one *SOAP Message* as defined in the SOAP
518 Messages with Attachments [SOAPAttach] specification.

519 2.1.3.1 Content-Type

520 The MIME `Content-Type` header for the *Header Container* MUST have the value "text/xml" in
521 accordance with the [SOAP] specification. The `Content-Type` header MAY contain a "charset"
522 attribute. For example:

```
523 Content-Type: text/xml; charset="UTF-8"
```

524 2.1.3.2 charset attribute

525 The MIME `charset` attribute identifies the character set used to create the *SOAP Message*. The
526 semantics of this attribute are described in the "charset parameter / encoding considerations" of
527 `text/xml` as specified in XML [XMLMedia]. The list of valid values can be found at <http://www.iana.org/>.

528 If both are present, the MIME `charset` attribute SHALL be equivalent to the encoding declaration of the
529 *SOAP Message*. If provided, the MIME `charset` attribute MUST NOT contain a value conflicting with the
530 encoding used when creating the *SOAP Message*.

531 For maximum interoperability it is RECOMMENDED UTF-8 [UTF-8] be used when encoding this
532 document. Due to the processing rules defined for media types derived from `text/xml` [XMLMedia],
533 this MIME attribute has no default.

534 2.1.3.3 Header Container Example

535 The following fragment represents an example of a *Header Container*:

```

536 Content-ID: <messagepackage-123@example.com> --- | Header
537 Content-Type: text/xml; charset="UTF-8"
538
539 <SOAP:Envelope -- | SOAP Message
540   xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
541   <SOAP:Header>
542     ...
543   </SOAP:Header>
544   <SOAP:Body>
545     ...
546   </SOAP:Body>
547 </SOAP:Envelope> -- |
548
549 --boundaryValue --- |

```

550 2.1.4 Payload Container

551 Zero or more *Payload Containers* MAY be present within a *Message Package* in conformance with the
 552 SOAP Messages with Attachments [SOAPAttach] specification.

553 If the *Message Package* contains an application payload, it SHOULD be enclosed within a *Payload*
 554 *Container*.

555 If there is no application payload within the *Message Package* then a *Payload Container* MUST NOT be
 556 present.

557 The contents of each *Payload Container* MUST be identified in the ebXML Message **Manifest** element
 558 within the SOAP **Body** (see section 3.2).

559 The ebXML Message Service Specification makes no provision, nor limits in any way, the structure or
 560 content of application payloads. Payloads MAY be simple-plain-text objects or complex nested multipart
 561 objects. The specification of the structure and composition of payload objects is the prerogative of the
 562 organization defining the business process or information exchange using the *ebXML Message Service*.

563 2.1.4.1 Example of a Payload Container

564 The following fragment represents an example of a *Payload Container* and a payload:

```

565 Content-ID: <domainname.example.com> ----- | ebXML MIME
566 Content-Type: application/xml ----- |
567
568 <Invoice> ----- |
569   <Invoicedata> ----- | Payload
570     ...
571   </Invoicedata> ----- |
572 </Invoice> ----- |

```

573 Note: It might be noticed the content-type used in the preceding example (application/XML) is different than the
 574 content-type in the example SOAP envelope in section 2.1.2 above (text/XML). The SOAP 1.1 specification states
 575 the content-type used for the SOAP envelope MUST be 'text/xml'. However, many MIME experts disagree with
 576 the choice of the primary media type designation of 'text/*' for XML documents as most XML is not "human
 577 readable" in the sense the MIME designation of 'text' was meant to infer. They believe XML documents should be
 578 classified as 'application/XML'.

579 2.1.5 Additional MIME Parameters

580 Any MIME part described by this specification MAY contain additional MIME headers in conformance with
 581 the MIME [RFC2045] specification. Implementations MAY ignore any MIME header not defined in this
 582 specification. Implementations MUST ignore any MIME header they do not recognize.

583 For example, an implementation could include `content-length` in a message. However, a recipient of
 584 a message with `content-length` could ignore it.

585 **2.1.6 Reporting MIME Errors**

586 If a MIME error is detected in the *Message Package* then it MUST be reported as specified in SOAP with
587 Attachments [SOAPAttach].

588 **2.2 XML Prolog**

589 The SOAP *Message*'s XML Prolog, if present, MAY contain an XML declaration. This specification has
590 defined no additional comments or processing instructions appearing in the XML prolog. For example:

```
591 Content-Type: text/xml; charset="UTF-8"  
592 <?xml version="1.0" encoding="UTF-8"?>  
593
```

594 **2.2.1 XML Declaration**

595 The XML declaration MAY be present in a SOAP *Message*. If present, it MUST contain the version
596 specification required by the XML Recommendation [XML] and MAY contain an encoding declaration.
597 The semantics described below MUST be implemented by a compliant *ebXML Message Service*.

598 **2.2.2 Encoding Declaration**

599 If both the encoding declaration and the *Header Container* MIME charset are present, the XML prolog for
600 the SOAP *Message* SHALL contain the encoding declaration SHALL be equivalent to the `charset`
601 attribute of the MIME `Content-Type` of the *Header Container* (see section 2.1.3).

602 If provided, the encoding declaration MUST NOT contain a value conflicting with the encoding used when
603 creating the SOAP *Message*. It is RECOMMENDED UTF-8 be used when encoding the SOAP *Message*.

604 If the character encoding cannot be determined by an XML processor using the rules specified in section
605 4.3.3 of XML [XML], the XML declaration and its contained encoding declaration SHALL be provided in
606 the ebXML SOAP *Header* Document.

607 Note: the encoding declaration is not required in an XML document according to XML v1.0 specification [XML].

608 **2.3 ebXML SOAP Envelope extensions**

609 In conformance with the [SOAP] specification, all extension element content is namespace qualified. All of
610 the ebXML SOAP extension element content defined in this specification is namespace qualified to the
611 ebXML SOAP *Envelope* extensions namespace as defined in section 2.2.2.

612 Namespace declarations (`xmlns` pseudo attributes) for the ebXML SOAP extensions may be included in
613 the SOAP *Envelope*, *Header* or *Body* elements, or directly in each of the ebXML SOAP extension
614 elements.

615 **2.3.1 Namespace pseudo attribute**

616 The namespace declaration for the ebXML SOAP *Envelope* extensions (`xmlns` pseudo attribute) (see
617 [XMLNS]) has a REQUIRED value of:

```
618 http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2\_0.xsd
```

619 **2.3.2 xsi:schemaLocation attribute**

620 The SOAP namespace:

```
621 http://schemas.xmlsoap.org/soap/envelope/
```

622 resolves to a W3C XML Schema specification. The ebXML OASIS ebXML Messaging TC has provided
623 an equivalent version of the SOAP schema conforming to the W3C Recommendation version of the XML
624 Schema specification [XMLSchema].

```
625 http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
```

626 All ebXML MSH implementations are strongly RECOMMENDED to include the XMLSchema-instance
 627 namespace qualified **schemaLocation** attribute in the SOAP **Envelope** element to indicate to validating
 628 parsers a location of the schema document that should be used to validate the document. Failure to
 629 include the **schemaLocation** attribute could prevent XML schema validation of received messages.

630 For example:

```
631 <SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
632             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
633             xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
634             http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
```

635 In addition, ebXML SOAP **Header** and **Body** extension element content may be similarly qualified so as
 636 to identify the location where validating parsers can find the schema document containing the ebXML
 637 namespace qualified SOAP extension element definitions. The ebXML SOAP extension element schema
 638 has been defined using the W3C Recommendation version of the XML Schema specification
 639 [XMLSchema] (see Appendix A). The XMLSchema-instance namespace qualified **schemaLocation**
 640 attribute should include a mapping of the ebXML SOAP **Envelope** extensions namespace to its schema
 641 document in the same element that declares the ebXML SOAP **Envelope** extensions namespace.

642 The **schemaLocation** for the namespace described above in section 2.3.1 is:

```
643 http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
```

644 Separate **schemaLocation** attribute are RECOMMENDED so tools, which may not correctly use the
 645 **schemaLocation** attribute to resolve schema for more than one namespace, will still be capable of
 646 validating an ebXML SOAP *message*. For example:

```
647 <SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
648             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
649             xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
650             http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
651   <SOAP:Header
652     xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
653     xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
654     http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
655     <eb:MessageHeader ...>
656       ...
657     </eb:MessageHeader>
658   </SOAP:Header>
659   <SOAP:Body
660     xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
661     xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
662     http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
663     <eb:Manifest eb:version="2.0">
664       ...
665     </eb:Manifest>
666   </SOAP:Body>
667 </SOAP:Envelope>
```

668 2.3.3 SOAP Header Element

669 The SOAP **Header** element is the first child element of the SOAP **Envelope** element. It MUST have a
 670 namespace qualifier that matches the SOAP **Envelope** namespace declaration for the namespace
 671 "http://schemas.xmlsoap.org/soap/envelope/".

672 2.3.4 SOAP Body Element

673 The SOAP **Body** element is the second child element of the SOAP **Envelope** element. It MUST have a
 674 namespace qualifier that matches the SOAP **Envelope** namespace declaration for the namespace
 675 "http://schemas.xmlsoap.org/soap/envelope/".

676 2.3.5 ebXML SOAP Extensions

677 An ebXML Message extends the SOAP *Message* with the following principal extension elements:

678 2.3.5.1 SOAP Header extensions:

- 679 • **MessageHeader** – a REQUIRED element containing routing information for the message (To/From, etc.) as
680 well as other context information about the message.
- 681 • **SyncReply** – an element indicating the required transport state to the next SOAP node.

682 2.3.5.2 SOAP Body extension:

- 683 • **Manifest** – an element pointing to any data present either in the *Payload Container(s)* or elsewhere, e.g. on
684 the web. This element MAY be omitted.

685 2.3.5.3 Core ebXML Modules:

- 686 • Error Handling Module
 - 687 - **ErrorList** – a SOAP Header element containing a list of the errors being reported against a previous
688 message. The **ErrorList** element is only used if reporting an error or warning on a previous message.
689 This element MAY be omitted.
- 690 • Security Module
 - 691 - **Signature** – an element that contains a digital signature that conforms to [XMLDSIG] that signs data
692 associated with the message. This element MAY be omitted.

693 2.3.6 #wildcard Element Content

694 Some ebXML SOAP extension elements, as indicated in the schema, allow for foreign namespace-
695 qualified element content to be added for extensibility. The extension element content MUST be
696 namespace-qualified in accordance with XMLNS [XMLNS] and MUST belong to a foreign namespace. A
697 foreign namespace is one that is NOT [http://www.oasis-open.org/committees/ebxml-
699 msg/schema/msg-header-2_0.xsd](http://www.oasis-open.org/committees/ebxml-
698 msg/schema/msg-header-2_0.xsd). The wildcard elements are provided wherever extensions might be
required for private extensions or future expansions to the protocol.

700 An implementation of the MSH MAY ignore the namespace-qualified element and its content.

701 2.3.7 id attribute

702 Each of the ebXML SOAP extension elements defined in this specification has an **id** attribute which is an
703 XML ID that MAY be added to provide for the ability to uniquely identify the element within the SOAP
704 *Message*. This MAY be used when applying a digital signature to the ebXML SOAP *Message* as
705 individual ebXML SOAP extension elements can be targeted for inclusion or exclusion by specifying a
706 URI of "#<idvalue>" in the **Reference** element.

707 2.3.8 version attribute

708 The REQUIRED **version** attribute indicates the version of the ebXML Message Service Header
709 Specification to which the ebXML SOAP **Header** extensions conform. Its purpose is to provide future
710 versioning capabilities. For conformance to this specification, all of the version attributes on any SOAP
711 extension elements defined in this specification MUST have a value of "2.0". An ebXML message MAY
712 contain SOAP header extension elements that have a value other than "2.0". An implementation
713 conforming to this specification that receives a message with ebXML SOAP extensions qualified with a
714 version other than "2.0" MAY process the message if it recognizes the version identified and is capable of
715 processing it. It MUST respond with an error (details TBD) if it does not recognize the identified version.
716 The **version** attribute MUST be namespace qualified for the ebXML SOAP **Envelope** extensions
717 namespace defined above.

718 Use of multiple versions of ebXML SOAP extensions elements within the same ebXML SOAP document,
719 while supported, should only be used in extreme cases where it becomes necessary to semantically
720 change an element, which cannot wait for the next ebXML Message Service Specification version
721 release.

722 2.3.9 SOAP *mustUnderstand* attribute

723 The REQUIRED SOAP *mustUnderstand* attribute on SOAP *Header* extensions, namespace qualified to
724 the SOAP namespace (<http://schemas.xmlsoap.org/soap/envelope/>), indicates whether the contents of
725 the element MUST be understood by a receiving process or else the message MUST be rejected in
726 accordance with SOAP [SOAP]. This attribute with a value of '1' (true) indicates the element MUST be
727 understood or rejected. This attribute with a value of '0' (false), the default, indicates the element may be
728 ignored if not understood.

729 2.3.10 ebXML "Next MSH" actor URI

730 The URI *urn:oasis:names:tc:ebxml-msg:actor:nextMSH* when used in the context of the SOAP *actor*
731 attribute value SHALL be interpreted to mean an entity that acts in the role of an instance of the ebXML
732 MSH conforming to this specification.

733 This *actor* URI has been established to allow for the possibility that SOAP nodes that are NOT ebXML
734 MSH nodes MAY participate in the message path of an *ebXML Message*. An example might be a SOAP
735 node that digitally signs or encrypts a message.

736 All ebXML MSH nodes MUST act in this role.

737 2.3.11 ebXML "To Party MSH" actor URI

738 The URI *urn:oasis:names:tc:ebxml-msg:actor:toPartyMSH* when used in the context of the SOAP
739 *actor* attribute value SHALL be interpreted to mean an instance of an ebXML MSH node, conforming to
740 this specification, acting in the role of the Party identified in the *MessageHeader/To/PartyId* element of
741 the same message. An ebXML MSH MAY be configured to act in this role. How this is done is outside
742 the scope of this specification.

743 The MSH that is the ultimate destination of ebXML messages MUST act in the role of the *To Party MSH*
744 actor URI in addition to acting in the default actor as defined by SOAP.

745 3 Core Extension Elements

746 3.1 MessageHeader Element

747 The *MessageHeader* element is REQUIRED in all ebXML Messages. It MUST be present as a child
748 element of the SOAP *Header* element.

749 The *MessageHeader* element is a composite element comprised of the following subordinate elements:

- 750 • an *id* attribute (see section 2.3.7 for details)
- 751 • a *version* attribute (see section 2.3.8 for details)
- 752 • a SOAP *mustUnderstand* attribute with a value of "1" (see section 2.3.9 for details)
- 753 • *From* element
- 754 • *To* element
- 755 • *CPAId* element
- 756 • *ConversationId* element
- 757 • *Service* element
- 758 • *Action* element
- 759 • *MessageData* element
- 760 • *DuplicateElimination* element
- 761 • *Description* element

762 3.1.1 From and To Elements

763 The REQUIRED **From** element identifies the *Party* that originated the message. The REQUIRED **To**
764 element identifies the *Party* that is the intended recipient of the message. Both **To** and **From** can contain
765 logical identifiers, such as a DUNS number, or identifiers that also imply a physical location such as an
766 eMail address.

767 The **From** and the **To** elements each contains:

- 768 • **PartyId** elements – occurs one or more times
- 769 • **Role** element – occurs zero or one times.

770 If either the **From** or **To** elements contains multiple **PartyId** elements, all members of the list MUST
771 identify the same organization. Unless a single **type** value refers to multiple identification systems, the
772 value of any given **type** attribute MUST be unique within the list of **PartyId** elements contained within
773 either the From or To element.

774 Note: This mechanism is particularly useful when transport of a message between the parties may involve multiple
775 intermediaries. More generally, the *From Party* should provide identification in all domains it knows in support of
776 intermediaries and destinations that may give preference to particular identification systems.

777 The **From** and **To** elements contain zero or one **Role** child element that, if present, SHALL immediately
778 follow the last **PartyId** child element.

779 3.1.1.1 PartyId Element

780 The **PartyId** element has a single attribute, **type** and the content is a string value. The **type** attribute
781 indicates the domain of names to which the string in the content of the **PartyId** element belongs. The
782 value of the **type** attribute MUST be mutually agreed and understood by each of the *Parties*. It is
783 RECOMMENDED that the value of the **type** attribute be a URI. It is further recommended that these
784 values be taken from the EDIRA (ISO 6523), EDIFACT ISO 9735 or ANSI ASC X12 I05 registries.

785 If the **PartyId type** attribute is not present, the content of the **PartyId** element MUST be a URI
786 [RFC2396], otherwise the *Receiving MSH* SHOULD report an error (see section 4.1.5) with **errorCode**
787 set to **Inconsistent** and **severity** set to **Error**. It is strongly RECOMMENDED that the content of the
788 **PartyId** element be a URI.

789 3.1.1.2 Role Element

790 The **Role** element identifies the authorized role (**fromAuthorizedRole** or **toAuthorizedRole**) of the *Party*
791 sending (when present as a child of the **From** element) and/or receiving (when present as a child of the
792 **To** element) the message. The value of the **Role** element is a non-empty string, which is specified in the
793 *CPA*.

794 Note: Role is better defined as a URI – e.g. <http://rosettanet.org/roles/buyer>.

795 The following fragment demonstrates usage of the **From** and **To** elements.

```
796 <eb:From>
797   <eb:PartyId eb:type="urn:duns">123456789</eb:PartyId>
798   <eb:PartyId eb:type="SCAC">RDWY</eb:PartyId>
799   <eb:Role>http://rosettanet.org/roles/Buyer</eb:Role>
800 </eb:From>
801 <eb:To>
802   <eb:PartyId>mailto:joe@example.com</eb:PartyId>
803   <eb:Role>http://rosettanet.org/roles/Seller</eb:Role>
804 </eb:To>
```

805 3.1.2 CPAId Element

806 The REQUIRED **CPAId** element is a string that identifies the parameters governing the exchange of
807 messages between the parties. The recipient of a message MUST be able to resolve the **CPAId** to an
808 individual set of parameters, taking into account the sender of the message.

809 The value of a **CPAId** element MUST be unique within a namespace mutually agreed by the two parties.
 810 This could be a concatenation of the **From** and **To PartyId** values, a URI prefixed with the Internet
 811 domain name of one of the parties, or a namespace offered and managed by some other naming or
 812 registry service. It is RECOMMENDED that the **CPAId** be a URI.

813 The **CPAId** MAY reference an instance of a **CPA** as defined in the ebXML Collaboration Protocol Profile
 814 and Agreement Specification [ebCPP]. An example of the **CPAId** element follows:

```
815 <eb:CPAId>http://example.com/cpas/ourcpawithyou.xml</eb:CPAId>
```

816 The messaging parameters are determined by the appropriate elements from the **CPA**, as identified by
 817 the **CPAId** element.

818 If a receiver determines that a message is in conflict with the **CPA**, the appropriate handling of this conflict
 819 is undefined by this specification. Therefore, senders SHOULD NOT generate such messages unless
 820 they have prior knowledge of the receiver's capability to deal with this conflict.

821 If a *Receiving MSH* detects an inconsistency, then it MUST report it with an **errorCode** of **Inconsistent**
 822 and a **severity** of **Error**. If the **CPAId** is not recognized, then it MUST report it with an **errorCode** of
 823 **NotRecognized** and a **severity** of **Error**.

824 3.1.3 ConversationId Element

825 The REQUIRED **ConversationId** element is a string identifying the set of related messages that make up
 826 a conversation between two *Parties*. It MUST be unique within the context of the specified **CPAId**. The
 827 *Party* initiating a conversation determines the value of the **ConversationId** element that SHALL be
 828 reflected in all messages pertaining to that conversation.

829 The **ConversationId** enables the recipient of a message to identify the instance of an application or
 830 process that generated or handled earlier messages within a conversation. It remains constant for all
 831 messages within a conversation.

832 The value used for a **ConversationId** is implementation dependent. An example of the **ConversationId**
 833 element follows:

```
834 <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
```

835 Note: Implementations are free to choose how they will identify and store conversational state related to a specific
 836 conversation. Implementations SHOULD provide a facility for mapping between their identification scheme and a
 837 **ConversationId** generated by another implementation.

838 3.1.4 Service Element

839 The REQUIRED **Service** element identifies the *service* that acts on the message and it is specified by the
 840 designer of the *service*. The designer of the *service* may be:

- 841 • a standards organization, or
- 842 • an individual or enterprise

843 Note: In the context of an ebXML business process model, an action equates to the lowest possible role based
 844 activity in the Business Process [ebBPSS] (requesting or responding role) and a service is a set of related actions for
 845 an authorized role within a party.

846 An example of the **Service** element follows:

```
847 <eb:Service>urn:services:SupplierOrderProcessing</eb:Service>
```

848 Note: URIs in the **Service** element that start with the namespace **urn:oasis:names:tc:ebxml-msg:service** are
 849 reserved for use by this specification.

850 The **Service** element has a single **type** attribute.

851 3.1.4.1 type attribute

852 If the **type** attribute is present, it indicates the parties sending and receiving the message know, by some
853 other means, how to interpret the content of the **Service** element. The two parties MAY use the value of
854 the **type** attribute to assist in the interpretation.

855 If the **type** attribute is not present, the content of the **Service** element MUST be a URI [RFC2396]. If it is
856 not a URI then report an error with **errorCode** of **Inconsistent** and **severity** of **Error** (see section 4.1.5).

857 3.1.5 Action Element

858 The REQUIRED **Action** element identifies a process within a **Service** that processes the Message.
859 **Action** SHALL be unique within the **Service** in which it is defined. The value of the **Action** element is
860 specified by the designer of the **service**. An example of the **Action** element follows:

```
861 <eb:Action>NewOrder</eb:Action>
```

862 If the value of either the **Service** or **Action** element are unrecognized by the *Receiving MSH*, then it
863 MUST report the error with an **errorCode** of **NotRecognized** and a **severity** of **Error**.

864 3.1.6 MessageData Element

865 The REQUIRED **MessageData** element provides a means of uniquely identifying an ebXML Message. It
866 contains the following:

- 867 • **MessageId** element
- 868 • **Timestamp** element
- 869 • **RefToMessageId** element
- 870 • **TimeToLive** element

871 The following fragment demonstrates the structure of the **MessageData** element:

```
872 <eb:MessageData>
873   <eb:MessageId>20001209-133003-28572@example.com</eb:MessageId>
874   <eb:Timestamp>2001-02-15T11:12:12</eb:Timestamp>
875   <eb:RefToMessageId>20001209-133003-28571@example.com</eb:RefToMessageId>
876 </eb:MessageData>
```

877 3.1.6.1 MessageId Element

878 The REQUIRED element **MessageId** is a globally unique identifier for each message conforming to
879 MessageId [RFC2822].

880 Note: In the Message-Id and Content-Id MIME headers, values are always surrounded by angle brackets. However
881 references in mid: or cid: scheme URI's and the MessageId and RefToMessageId elements MUST NOT include
882 these delimiters.

883 3.1.6.2 Timestamp Element

884 The REQUIRED **Timestamp** is a value representing the time that the message header was created
885 conforming to a dateTime [XMLSchema] and MUST be expressed as UTC. Indicating UTC in the
886 **Timestamp** element by including the 'Z' identifier is optional.

887 3.1.6.3 RefToMessageId Element

888 The **RefToMessageId** element has a cardinality of zero or one. When present, it MUST contain the
889 **MessageId** value of an earlier ebXML Message to which this message relates. If there is no earlier
890 related message, the element MUST NOT be present.

891 For Error messages, the **RefToMessageId** element is REQUIRED and its value MUST be the
892 **MessageId** value of the message in error (as defined in section 4.2).

893 3.1.6.4 TimeToLive Element

894 If the **TimeToLive** element is present, it MUST be used to indicate the time, expressed as UTC, by which
895 a message should be delivered to the *To Party MSH*. It MUST conform to an XML Schema dateTime.

896 In this context, the **TimeToLive** has expired if the time of the internal clock, adjusted for UTC, of the
897 *Receiving MSH* is greater than the value of **TimeToLive** for the message.

898 If the *To Party's MSH* receives a message where **TimeToLive** has expired, it SHALL send a message to
899 the *From Party MSH*, reporting that the **TimeToLive** of the message has expired. This message SHALL
900 be comprised of an **ErrorList** containing an error with the **errorCode** attribute set to **TimeToLiveExpired**
901 and the **severity** attribute set to **Error**.

902 The **TimeToLive** element is discussed further under Reliable Messaging in section 6.4.5.

903 3.1.7 DuplicateElimination Element

904 The **DuplicateElimination** element, if present, identifies a request by the sender for the receiving MSH to
905 check for duplicate messages (see section 6.4.1 for more details).

906 Valid values for **DuplicateElimination**:

- 907 • **DuplicateElimination** present – duplicate messages SHOULD be eliminated.
- 908 • **DuplicateElimination** not present – this results in a delivery behavior of Best-Effort.

909 The **DuplicateElimination** element MUST NOT be present if the CPA has **duplicateElimination** set to
910 **never** (see section 6.4.1 and section 6.6 for more details).

911 3.1.8 Description Element

912 The **Description** element may be present zero or more times. Its purpose is to provide a human
913 readable description of the purpose or intent of the message. The language of the description is defined
914 by a required **xml:lang** attribute. The **xml:lang** attribute MUST comply with the rules for identifying
915 languages specified in XML [XML]. Each occurrence SHOULD have a different value for **xml:lang**.

916 3.1.9 MessageHeader Sample

917 The following fragment demonstrates the structure of the **MessageHeader** element within the SOAP
918 **Header**:

```
919 <eb:MessageHeader eb:id="..." eb:version="2.0" SOAP:mustUnderstand="1">
920   <eb:From>
921     <eb:PartyId>uri:example.com</eb:PartyId>
922     <eb:Role>http://rosettanet.org/roles/Buyer</eb:Role>
923   </eb:From>
924   <eb:To>
925     <eb:PartyId eb:type="someType">QRS543</eb:PartyId>
926     <eb:Role>http://rosettanet.org/roles/Seller</eb:Role>
927   </eb:To>
928   <eb:CPAId>http://www.oasis-open.org/cpa/123456</eb:CPAId>
929   <eb:ConversationId>987654321</eb:ConversationId>
930   <eb:Service eb:type="myservicetypes">QuoteToCollect</eb:Service>
931   <eb:Action>NewPurchaseOrder</eb:Action>
932   <eb:MessageData>
933     <eb:MessageId>UUID-2</eb:MessageId>
934     <eb:Timestamp>2000-07-25T12:19:05</eb:Timestamp>
935     <eb:RefToMessageId>UUID-1</eb:RefToMessageId>
936   </eb:MessageData>
937   <eb:DuplicateElimination/>
938 </eb:MessageHeader>
```

939 3.2 Manifest Element

940 The **Manifest** element MAY be present as a child of the SOAP **Body** element. The **Manifest** element is
941 a composite element consisting of one or more **Reference** elements. Each **Reference** element identifies

942 payload data associated with the message, whether included as part of the message as payload
 943 document(s) contained in a *Payload Container*, or remote resources accessible via a URL. It is
 944 RECOMMENDED that no payload data be present in the SOAP **Body**. The purpose of the **Manifest** is:

- 945 • to make it easier to directly extract a particular payload associated with this ebXML Message,
- 946 • to allow an application to determine whether it can process the payload without having to parse it.

947 The **Manifest** element is comprised of the following:

- 948 • an **id** attribute (see section 2.3.7 for details)
- 949 • a **version** attribute (see section 2.3.8 for details)
- 950 • one or more **Reference** elements

951 3.2.1 Reference Element

952 The **Reference** element is a composite element consisting of the following subordinate elements:

- 953 • zero or more **Schema** elements – information about the schema(s) that define the instance document
 954 identified in the parent **Reference** element
- 955 • zero or more **Description** elements – a textual description of the payload object referenced by the parent
 956 **Reference** element

957 The **Reference** element itself is a simple link [XLINK]. It should be noted that the use of XLINK in this
 958 context is chosen solely for the purpose of providing a concise vocabulary for describing an association.
 959 Use of an XLINK processor or engine is NOT REQUIRED, but may prove useful in certain
 960 implementations.

961 The **Reference** element has the following attribute content in addition to the element content described
 962 above:

- 963 • **id** – an XML ID for the **Reference** element,
- 964 • **xlink:type** – this attribute defines the element as being an XLINK simple link. It has a fixed value of 'simple',
- 965 • **xlink:href** – this REQUIRED attribute has a value that is the URI of the payload object referenced. It SHALL
 966 conform to the XLINK [XLINK] specification criteria for a simple link.
- 967 • **xlink:role** – this attribute identifies some resource that describes the payload object or its purpose. If
 968 present, then it SHALL have a value that is a valid URI in accordance with the [XLINK] specification,
- 969 • Any other namespace-qualified attribute MAY be present. A *Receiving MSH* MAY choose to ignore any
 970 foreign namespace attributes other than those defined above.

971 The designer of the business process or information exchange using ebXML Messaging decides what
 972 payload data is referenced by the **Manifest** and the values to be used for **xlink:role**.

973 3.2.1.1 Schema Element

974 If the item being referenced has schema(s) of some kind that describe it (e.g. an XML Schema, DTD
 975 and/or a database schema), then the **Schema** element SHOULD be present as a child of the **Reference**
 976 element. It provides a means of identifying the schema and its version defining the payload object
 977 identified by the parent **Reference** element. The **Schema** element contains the following attributes:

- 978 • **location** – the REQUIRED URI of the schema
- 979 • **version** – a version identifier of the schema

980 3.2.1.2 Description Element

981 See section 3.1.8 for more details. An example of a **Description** element follows.

```
982 <eb:Description xml:lang="en-GB">Purchase Order for 100,000 widgets</eb:Description>
```

983 3.2.2 Manifest Validation

984 If an **xlink:href** attribute contains a URI that is a content id (URI scheme "cid") then a MIME part with
 985 that `content-id` MUST be present in the corresponding *Payload Container* of the message. If it is not,

986 then the error SHALL be reported to the *From Party* with an **errorCode** of **MimeProblem** and a **severity**
987 of **Error**.

988 If an **xlink:href** attribute contains a URI, not a content id (URI scheme "cid"), and the URI cannot be
989 resolved, it is an implementation decision whether to report the error. If the error is to be reported, it
990 SHALL be reported to the *From Party* with an **errorCode** of **MimeProblem** and a **severity** of **Error**.

991 Note: If a payload exists, which is not referenced by the *Manifest*, that payload SHOULD be discarded.

992 3.2.3 Manifest Sample

993 The following fragment demonstrates a typical *Manifest* for a single payload MIME body part:

```
994 <eb:Manifest eb:id="Manifest" eb:version="2.0">
995   <eb:Reference eb:id="pay01"
996     xlink:href="cid:payload-1"
997     xlink:role="http://regrep.org/gci/purchaseOrder">
998     <eb:Schema eb:location="http://regrep.org/gci/purchaseOrder/po.xsd" eb:version="2.0"/>
999     <eb:Description xml:lang="en-US">Purchase Order for 100,000 widgets</eb:Description>
1000   </eb:Reference>
1001 </eb:Manifest>
```

1002 4 Core Modules

1003 4.1 Security Module

1004 The *ebXML Message Service*, by its very nature, presents certain security risks. A Message Service may
1005 be at risk by means of:

- 1006 • Unauthorized access
- 1007 • Data integrity and/or confidentiality attacks (e.g. through man-in-the-middle attacks)
- 1008 • Denial-of-Service and spoofing

1009 Each security risk is described in detail in the ebXML Technical Architecture Risk Assessment Technical
1010 Report [secRISK].

1011 Each of these security risks may be addressed in whole, or in part, by the application of one, or a
1012 combination, of the countermeasures described in this section. This specification describes a set of
1013 profiles, or combinations of selected countermeasures, selected to address key risks based upon
1014 commonly available technologies. Each of the specified profiles includes a description of the risks that
1015 are not addressed. See Appendix C for a table of security profiles.

1016 Application of countermeasures SHOULD be balanced against an assessment of the inherent risks and
1017 the value of the asset(s) that might be placed at risk. For this specification, a *Signed Message* is any
1018 message containing a **Signature** element.

1019 4.1.1 Signature Element

1020 An ebXML Message MAY be digitally signed to provide security countermeasures. Zero or more
1021 **Signature** elements, belonging to the XML Signature [XMLDSIG] defined namespace, MAY be present
1022 as a child of the SOAP **Header**. The **Signature** element MUST be namespace qualified in accordance
1023 with XML Signature [XMLDSIG]. The structure and content of the **Signature** element MUST conform to
1024 the XML Signature [XMLDSIG] specification. If there is more than one **Signature** element contained
1025 within the SOAP **Header**, the first MUST represent the digital signature of the ebXML Message as signed
1026 by the *From Party MSH* in conformance with section 4.1. Additional **Signature** elements MAY be
1027 present, but their purpose is undefined by this specification.

1028 Refer to section 4.1.3 for a detailed discussion on how to construct the **Signature** element when digitally
1029 signing an ebXML Message.

1030 4.1.2 Security and Management

1031 No technology, regardless of how advanced it might be, is an adequate substitute to the effective
1032 application of security management policies and practices.

1033 It is strongly RECOMMENDED that the site manager of an *ebXML Message Service* apply due diligence
1034 to the support and maintenance of its security mechanisms, site (or physical) security procedures,
1035 cryptographic protocols, update implementations and apply fixes as appropriate. (See
1036 <http://www.cert.org/> and <http://ciac.llnl.gov/>)

1037 4.1.2.1 Collaboration Protocol Agreement

1038 The configuration of Security for MSHs is specified in the *CPA*. Two areas of the *CPA* have security
1039 definitions as follows:

- 1040 • The Document Exchange section addresses security to be applied to the payload of the message. The
1041 MSH is not responsible for any security specified at this level but may offer these services to the message
1042 sender.
- 1043 • The Transport section addresses security applied to the entire ebXML Document, which includes the header
1044 and the payload(s).

1045 4.1.3 Signature Generation

1046 An ebXML Message is signed using [XMLDSIG] following these steps:

- 1047 1) Create a **SignedInfo** element with **SignatureMethod**, **CanonicalizationMethod** and **Reference**
1048 elements for the SOAP **Envelope** and any required payload objects, as prescribed by XML
1049 Signature [XMLDSIG].
- 1050 2) Canonicalize and then calculate the **SignatureValue** over **SignedInfo** based on algorithms
1051 specified in **SignedInfo** as specified in XML Signature [XMLDSIG].
- 1052 3) Construct the **Signature** element that includes the **SignedInfo**, **KeyInfo** (RECOMMENDED) and
1053 **SignatureValue** elements as specified in XML Signature [XMLDSIG].
- 1054 4) Include the namespace qualified **Signature** element in the SOAP **Header** just signed.

1055 The **SignedInfo** element SHALL have a **CanonicalizationMethod** element, a **SignatureMethod** element
1056 and one or more **Reference** elements, as defined in XML Signature [XMLDSIG].

1057 The RECOMMENDED canonicalization method applied to the data to be signed is

```
1058 <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

1059 described in [XMLC14N]. This algorithm excludes comments.

1060 The **SignatureMethod** element SHALL be present and SHALL have an **Algorithm** attribute. The
1061 RECOMMENDED value for the **Algorithm** attribute is:

```
1062 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmlsig#dsa-sha1"/>
```

1063 This RECOMMENDED value SHALL be supported by all compliant *ebXML Message Service* software
1064 implementations.

1065 The [XMLDSIG] **Reference** element for the SOAP **Envelope** document SHALL have a URI attribute
1066 value of "" to provide for the signature to be applied to the document that contains the **Signature** element.

1067 The [XMLDSIG] **Reference** element for the SOAP **Envelope** MAY include a **Type** attribute that has a
1068 value "http://www.w3.org/2000/09/xmlsig#Object" in accordance with XML Signature [XMLDSIG]. This
1069 attribute is purely informative. It MAY be omitted. Implementations of the ebXML MSH SHALL be
1070 prepared to handle either case. The **Reference** element MAY include the **id** attribute.

1071 The [XMLDSIG] **Reference** element for the SOAP **Envelope** SHALL include a child **Transforms**
1072 element. The **Transforms** element SHALL include the following **Transform** child elements.

1073 The first **Transform** element has an **Algorithm** attribute with a value of:

```
1074 <Transform Algorithm="http://www.w3.org/2000/09/xmlsig#enveloped-signature"/>
```

1075 The result of this statement excludes the parent **Signature** element and all its descendants.

1076 The second **Transform** element has a child **XPath** element that has a value of:

```
1077 <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
1078   <XPath> not (ancestor-or-self::node() [@SOAP:actor="urn:oasis:names:tc:ebxml-msg:actor:nextMSH"] |
1079     ancestor-or-self::node() [@SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next" ] )
1080   </XPath>
1081 </Transform>
```

1082 The result of this [XPath] statement excludes all elements within the SOAP **Envelope** which contain a
 1083 SOAP:**actor** attribute targeting the **nextMSH**, and all their descendants. It also excludes all elements
 1084 with **actor** attributes targeting the element at the next node (which may change en route). Any
 1085 intermediate node or MSH MUST NOT change, format or in any way modify any element not targeted to
 1086 the intermediary. Intermediate nodes MUST NOT add or delete white space. Any such change may
 1087 invalidate the signature.

1088 The last **Transform** element SHOULD have an **Algorithm** attribute with a value of:

```
1089 <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

1090 The result of this algorithm is to canonicalize the SOAP **Envelope** XML and exclude comments.

1091 Note: These transforms are intended for the SOAP Envelope and its contents. These transforms are NOT intended
 1092 for the payload objects. The determination of appropriate transforms for each payload is left to the implementation.

1093 Each payload object requiring signing SHALL be represented by a [XMLDSIG] **Reference** element that
 1094 SHALL have a **URI** attribute resolving to the payload object. This can be either the **Content-Id** URI of
 1095 the MIME body part of the payload object, or a URI matching the **Content-Location** of the MIME body part
 1096 of the payload object, or a URI that resolves to a payload object external to the Message Package. It is
 1097 strongly RECOMMENDED that the URI attribute value match the **xlink:href** URI value of the
 1098 corresponding **Manifest/Reference** element for the payload object.

1099 Note: When a transfer encoding (e.g. base64) specified by a **Content-Transfer-Encoding** MIME header is used for
 1100 the SOAP Envelope or payload objects, the signature generation MUST be executed before the encoding.

1101 Example of digitally signed ebXML SOAP Message:

```
1102 <?xml version="1.0" encoding="utf-8"?>
1103 <SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
1104   xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
1105   xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
1106   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1107   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
1108     http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
1109     http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
1110     http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
1111   <SOAP:Header>
1112     <eb:MessageHeader eb:id="..." eb:version="2.0" SOAP:mustUnderstand="1">
1113       ...
1114     </eb:MessageHeader>
1115     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
1116       <SignedInfo>
1117         <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
1118         <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
1119         <Reference URI="">
1120           <Transforms>
1121             <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
1122             <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
1123               <XPath> not (ancestor-or-self::node() [@SOAP:actor=
1124                 &quot;urn:oasis:names:tc:ebxml-msg:actor:nextMSH&quot;]
1125                 | ancestor-or-self::node() [@SOAP:actor=
1126                 &quot;http://schemas.xmlsoap.org/soap/actor/next&quot;] )
1127               </XPath>
1128             </Transform>
1129             <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
1130           </Transforms>
1131           <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```

1132     <DigestValue>...</DigestValue>
1133   </Reference>
1134   <Reference URI="cid://blahblahblah/">
1135     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>
1136     <DigestValue>...</DigestValue>
1137   </Reference>
1138 </SignedInfo>
1139 <SignatureValue>...</SignatureValue>
1140 <KeyInfo>...</KeyInfo>
1141 </Signature>
1142 </SOAP:Header>
1143 <SOAP:Body>
1144   <eb:Manifest eb:id="Mani01" eb:version="2.0">
1145     <eb:Reference xlink:href="cid://blahblahblah/" xlink:role="http://ebxml.org/gci/invoice">
1146       <eb:Schema eb:version="2.0" eb:location="http://ebxml.org/gci/busdocs/invoice.dtd"/>
1147     </eb:Reference>
1148   </eb:Manifest>
1149 </SOAP:Body>
1150 </SOAP:Envelope>

```

1151 4.1.4 Countermeasure Technologies

1152 4.1.4.1 Persistent Digital Signature

1153 The only available technology that can be applied to the purpose of digitally signing an ebXML Message
 1154 (the ebXML SOAP **Header** and **Body** and its associated payload objects) is provided by technology that
 1155 conforms to the W3C/IETF joint XML Signature specification [XMLDSIG]. An XML Signature conforming
 1156 to this specification can selectively sign portions of an XML document(s), permitting the documents to be
 1157 augmented (new element content added) while preserving the validity of the signature(s).

1158 If signatures are being used to digitally sign an ebXML Message then XML Signature [DSIG] MUST be
 1159 used to bind the ebXML SOAP **Header** and **Body** to the ebXML Payload Container(s) or data elsewhere
 1160 on the web that relate to the message.

1161 An ebXML Message requiring a digital signature SHALL be signed following the process defined in this
 1162 section of the specification and SHALL be in full compliance with XML Signature [XMLDSIG].

1163 4.1.4.2 Persistent Signed Receipt

1164 An *ebXML Message* that has been digitally signed MAY be acknowledged with an *Acknowledgment*
 1165 *Message* that itself is digitally signed in the manner described in the previous section. The
 1166 *Acknowledgment Message* MUST contain a [XMLDSIG] **Reference** element list consistent with those
 1167 contained in the [XMLDSIG] **Signature** element of the original message.

1168 4.1.4.3 Non-persistent Authentication

1169 Non-persistent authentication is provided by the communications channel used to transport the *ebXML*
 1170 *Message*. This authentication MAY be either in one direction or bi-directional. The specific method will be
 1171 determined by the communications protocol used. For instance, the use of a secure network protocol,
 1172 such as TLS [RFC2246] or IPSEC [RFC2402] provides the sender of an *ebXML Message* with a way to
 1173 authenticate the destination for the TCP/IP environment.

1174 4.1.4.4 Non-persistent Integrity

1175 A secure network protocol such as TLS [RFC2246] or IPSEC [RFC2402] MAY be configured to provide
 1176 for digests and comparisons of the packets transmitted via the network connection.

1177 4.1.4.5 Persistent Confidentiality

1178 XML Encryption is a W3C/IETF joint activity actively engaged in the drafting of a specification for the
 1179 selective encryption of an XML document(s). It is anticipated that this specification will be completed
 1180 within the next year. The ebXML Transport, Routing and Packaging team for v1.0 of this specification
 1181 has identified this technology as the only viable means of providing persistent, selective confidentiality of
 1182 elements within an *ebXML Message* including the SOAP **Header**.

1183 Confidentiality for ebXML Payload Containers MAY be provided by functionality possessed by a MSH.
1184 Payload confidentiality MAY be provided by using XML Encryption (when available) or some other
1185 cryptographic process (such as S/MIME [S/MIME], [S/MIMEV3], or PGP MIME [PGP/MIME]) bilaterally
1186 agreed upon by the parties involved. The XML Encryption standard shall be the default encryption
1187 method when XML Encryption has achieved W3C Recommendation status.

1188 Note: When both signature and encryption are required of the MSH, sign first and then encrypt.

1189 **4.1.4.6 Non-persistent Confidentiality**

1190 A secure network protocol, such as TLS [RFC2246] or IPSEC [RFC2402], provides transient
1191 confidentiality of a message as it is transferred between two ebXML adjacent MSH nodes.

1192 **4.1.4.7 Persistent Authorization**

1193 The OASIS Security Services Technical Committee (TC) is actively engaged in the definition of a
1194 specification that provides for the exchange of security credentials, including Name Assertion and
1195 Entitlements, based on Security Assertion Markup Language [SAML]. Use of technology based on this
1196 anticipated specification may provide persistent authorization for an *ebXML Message* once it becomes
1197 available.

1198 **4.1.4.8 Non-persistent Authorization**

1199 A secure network protocol such as TLS [RFC2246] or IPSEC [RFC2402] MAY be configured to provide
1200 for bilateral authentication of certificates prior to establishing a session. This provides for the ability for an
1201 ebXML MSH to authenticate the source of a connection and to recognize the source as an authorized
1202 source of *ebXML Messages*.

1203 **4.1.4.9 Trusted Timestamp**

1204 At the time of this specification, services offering trusted timestamp capabilities are becoming available.
1205 Once these become more widely available, and a standard has been defined for their use and
1206 expression, these standards, technologies and services will be evaluated and considered for use in later
1207 versions of this specification.

1208 **4.1.5 Security Considerations**

1209 Implementors should take note, there is a vulnerability present even when an XML Digital Signature is
1210 used to protect to protect the integrity and origin of ebXML messages. The significance of the
1211 vulnerability necessarily depends on the deployed environment and the transport used to exchange
1212 ebXML messages.

1213 The vulnerability is present because ebXML messaging is an integration of both XML and MIME
1214 technologies. Whenever two or more technologies are conjoined there are always additional (sometimes
1215 unique) security issues to be addressed. In this case, MIME is used as the framework for the message
1216 package, containing the SOAP *Envelope* and any payload containers. Various elements of the SOAP
1217 *Envelope* make reference to the payloads, identified via MIME mechanisms. In addition, various labels
1218 are duplicated in both the SOAP *Envelope* and the MIME framework, for example, the type of the content
1219 in the payload. The issue is how and when all of this information is used.

1220 Specifically, the MIME Content-ID: header is used to specify a unique, identifying label for each payload.
1221 The label is used in the SOAP *Envelope* to identify the payload whenever it is needed. The MIME
1222 Content-Type: header is used to identify the type of content carried in the payload; some content types
1223 may contain additional parameters serving to further qualify the actual type. This information is available
1224 in the SOAP *Envelope*.

1225 The MIME headers are not protected, even when an XML-based digital signature is applied. Although
1226 XML Encryption is not currently available and thus not currently used, its application is developing
1227 similarly to XML digital signatures. Insofar as its application is the same as that of XML digital signatures,
1228 its use will not protect the MIME headers. Thus, an ebXML message may be at risk depending on how

1229 the information in the MIME headers is processed as compared to the information in the SOAP
1230 **Envelope**.

1231 The Content-ID: MIME header is critical. An adversary could easily mount a denial-of-service attack by
1232 mixing and matching payloads with the Content-ID: headers. As with most denial-of-service attacks, no
1233 specific protection is offered for this vulnerability. However, it should be detected since the digest
1234 calculated for the actual payload will not match the digest included in the SOAP **Envelope** when the
1235 digital signature is validated.

1236 The presence of the content type in both the MIME headers and SOAP **Envelope** is a problem. Ordinary
1237 security practices discourage duplicating information in two places. When information is duplicated,
1238 ordinary security practices require the information in both places to be compared to ensure they are
1239 equal. It would be considered a security violation if both sets of information fail to match.

1240 An adversary could change the MIME headers while a message is en route from its origin to its
1241 destination and this would not be detected when the security services are validated. This threat is less
1242 significant in a peer-to-peer transport environment as compared to a multi-hop transport environment. All
1243 implementations are at risk if the ebXML message is ever recorded in a long-term storage area since a
1244 compromise of that area puts the message at risk for modification.

1245 The actual risk depends on how an implementation uses each of the duplicate sets of information. If any
1246 processing beyond the MIME parsing for body part identification and separation is dependent on the
1247 information in the MIME headers, then the implementation is at risk of being directed to take unintended
1248 or undesirable actions. How this might be exploited is best compared to the common programming
1249 mistake of permitting buffer overflows: it depends on the creativity and persistence of the adversary.

1250 Thus, an implementation could reduce the risk by ensuring that the unprotected information in the MIME
1251 headers is never used except by the MIME parser for the minimum purpose of identifying and separating
1252 the body parts. This version of the specification makes no recommendation regarding whether or not an
1253 implementation should compare the duplicate sets of information nor what action to take based on the
1254 results of the comparison.

1255 4.2 Error Handling Module

1256 This section describes how one ebXML Message Service Handler (MSH) reports errors it detects in an
1257 ebXML Message to another MSH. The *ebXML Message Service* error reporting and handling module is
1258 to be considered as a layer of processing above the SOAP processor layer. This means the ebXML MSH
1259 is essentially an application-level handler of a *SOAP Message* from the perspective of the SOAP
1260 Processor. The SOAP processor MAY generate a SOAP **Fault** message if it is unable to process the
1261 message. A *Sending MSH* MUST be prepared to accept and process these SOAP **Fault** values.

1262 It is possible for the ebXML MSH software to cause a SOAP **Fault** to be generated and returned to the
1263 sender of a *SOAP Message*. In this event, the returned message MUST conform to the [SOAP]
1264 specification processing guidelines for SOAP **Fault** values.

1265 An ebXML *SOAP Message* reporting an error with a **highestSeverity** of **Warning** SHALL NOT be
1266 reported or returned as a SOAP **Fault**.

1267 4.2.1.1 Definitions:

1268 For clarity, two phrases are defined for use in this section:

- 1269 • "message in error" – A *message* containing or causing an error or warning of some kind
- 1270 • "message reporting the error" – A *message* containing an ebXML **ErrorList** element that describes the
1271 warning(s) and/or error(s) found in a message in error (also referred to as an *Error Message* elsewhere in
1272 this document).

1273 4.2.2 Types of Errors

1274 One MSH needs to report errors to another MSH. For example, errors associated with:

- 1275 • ebXML namespace qualified content of the *SOAP Message* document (see section 2.3.1)
- 1276 • reliable messaging failures (see section 6.5.7)
- 1277 • security (see section 4.1)

1278 Unless specified to the contrary, all references to "an error" in the remainder of this specification imply
1279 any or all of the types of errors listed above or defined elsewhere.

1280 Errors associated with data communications protocols are detected and reported using the standard
1281 mechanisms supported by that data communications protocol and do not use the error reporting
1282 mechanism described here.

1283 4.2.3 ErrorList Element

1284 The existence of an **ErrorList** extension element within the SOAP **Header** element indicates the
1285 message identified by the **RefToMessageId** in the **MessageHeader** element has an error.

1286 The **ErrorList** element consists of:

- 1287 • **id** attribute (see section 2.3.7 for details)
- 1288 • a **version** attribute (see section 2.3.8 for details)
- 1289 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)
- 1290 • **highestSeverity** attribute
- 1291 • one or more **Error** elements

1292 If there are no errors to be reported then the **ErrorList** element MUST NOT be present.

1293 4.2.3.1 highestSeverity attribute

1294 The **highestSeverity** attribute contains the highest severity of any of the **Error** elements. Specifically, if
1295 any of the **Error** elements have a **severity** of **Error**, **highestSeverity** MUST be set to **Error**, otherwise,
1296 **highestSeverity** MUST be set to **Warning**.

1297 4.2.3.2 Error Element

1298 An **Error** element consists of:

- 1299 • **id** attribute (see section 2.3.7 for details)
- 1300 • **codeContext** attribute
- 1301 • **errorCode** attribute
- 1302 • **severity** attribute
- 1303 • **location** attribute
- 1304 • **Description** element

1305 4.2.3.2.1 id attribute

1306 If the error is a part of an ebXML element, the **id** of the element MAY be provided for error tracking.

1307 4.2.3.2.2 codeContext attribute

1308 The **codeContext** attribute identifies the namespace or scheme for the **errorCodes**. It MUST be a URI.
1309 Its default value is **urn:oasis:names:tc:ebxml-msg:service:errors**. If it does not have the default value,
1310 then it indicates an implementation of this specification has used its own **errorCode** attribute values.

1311 Use of a **codeContext** attribute value other than the default is NOT RECOMMENDED. In addition, an
1312 implementation of this specification should not use its own **errorCode** attribute values if an existing
1313 **errorCode** as defined in this section has the same or very similar meaning.

1314 4.2.3.2.3 **errorCode attribute**

1315 The REQUIRED **errorCode** attribute indicates the nature of the error in the message in error. Valid
1316 values for the **errorCode** and a description of the code's meaning are given in the next section.

1317 4.2.3.2.4 **severity attribute**

1318 The REQUIRED **severity** attribute indicates the severity of the error. Valid values are:

- 1319 • **Warning** – This indicates other messages in the conversation could be generated in the normal way in spite
1320 of this problem.
- 1321 • **Error** – This indicates there is an unrecoverable error in the message and no further message processing
1322 should occur. Appropriate failure conditions should be communicated to the Application.

1323 4.2.3.2.5 **location attribute**

1324 The **location** attribute points to the part of the message containing the error.

1325 If an error exists in an ebXML element and the containing document is "well formed" (see XML [XML]),
1326 then the content of the **location** attribute MUST be an XPointer [XPointer].

1327 If the error is associated with an ebXML Payload Container, then **location** contains the `content-id` of
1328 the MIME part in error, using URI scheme "cid".

1329 4.2.3.2.6 **Description Element**

1330 The content of the **Description** element provides a narrative description of the error in the language
1331 defined by the **xml:lang** attribute. The XML parser or other software validating the message typically
1332 generates the message. The content is defined by the vendor/developer of the software that generated
1333 the **Error** element. (See section 3.1.8)

1334 4.2.3.3 **ErrorList Sample**

1335 An example of an **ErrorList** element is given below.

```
1336 <eb:ErrorList eb:id="3490sdo", eb:highestSeverity="error" eb:version="2.0" SOAP:mustUnderstand="1">
1337   <eb:Error eb:errorCode="SecurityFailure" eb:severity="Error" eb:location="URI_of_ds:Signature">
1338     <eb:Description xml:lang="en-US">Validation of signature failed<eb:Description>
1339   </eb:Error>
1340   <eb:Error ...> ... </eb:Error>
1341 </eb:ErrorList>
```

1342 4.2.3.4 **errorCode values**

1343 This section describes the values for the **errorCode** attribute used in a *message reporting an error*. They
1344 are described in a table with three headings:

- 1345 • the first column contains the value to be used as an **errorCode**, e.g. **SecurityFailure**
- 1346 • the second column contains a "Short Description" of the **errorCode**. This narrative MUST NOT be used in
1347 the content of the **Error** element.
- 1348 • the third column contains a "Long Description" that provides an explanation of the meaning of the error and
1349 provides guidance on when the particular **errorCode** should be used.

1350 4.2.3.4.1 **Reporting Errors in the ebXML Elements**

1351 The following list contains error codes that can be associated with ebXML elements:

Error Code	Short Description	Long Description
ValueNotRecognized	Element content or attribute value not recognized.	Although the document is well formed and valid, the element/attribute contains a value that could not be recognized and therefore could not be used by the <i>ebXML Message Service</i> .
NotSupported	Element or attribute not	Although the document is well formed and valid, a module is

	supported	present consistent with the rules and constraints contained in this specification, but is not supported by the <i>ebXML Message Service</i> processing the message.
Inconsistent	Element content or attribute value inconsistent with other elements or attributes.	Although the document is well formed and valid, according to the rules and constraints contained in this specification the content of an element or attribute is inconsistent with the content of other elements or their attributes.
OtherXml	Other error in an element content or attribute value.	Although the document is well formed and valid, the element content or attribute value contains values that do not conform to the rules and constraints contained in this specification and is not covered by other error codes. The content of the Error element should be used to indicate the nature of the problem.

1352 4.2.3.4.2 Non-XML Document Errors

1353 The following are error codes that identify errors not associated with the ebXML elements:

Error Code	Short Description	Long Description
DeliveryFailure	Message Delivery Failure	A message has been received that either probably or definitely could not be sent to its next destination. Note: if <i>severity</i> is set to Warning then there is a small probability that the message was delivered.
TimeToLiveExpired	Message Time To Live Expired	A message has been received that arrived after the time specified in the TimeToLive element of the MessageHeader element.
SecurityFailure	Message Security Checks Failed	Validation of signatures or checks on the authenticity or authority of the sender of the message have failed.
MimeProblem	URI resolve error	If an xlink:href attribute contains a URI, not a content id (URI scheme "cid"), and the URI cannot be resolved, then it is an implementation decision whether to report the error.
Unknown	Unknown Error	Indicates that an error has occurred not covered explicitly by any of the other errors. The content of the Error element should be used to indicate the nature of the problem.

1354 4.2.4 Implementing Error Reporting and Handling

1355 4.2.4.1 When to Generate Error Messages

1356 When a MSH detects an error in a message it is strongly RECOMMENDED the error is reported to the
1357 MSH that sent the message in error. This is possible when:

- 1358 • the Error Reporting Location (see section 4.2.4.2) to which the message reporting the error should be sent
1359 can be determined
- 1360 • the message in error does not have an **ErrorList** element with **highestSeverity** set to **Error**.

1361 If the Error Reporting Location cannot be found or the message in error has an **ErrorList** element with
1362 **highestSeverity** set to **Error**, it is RECOMMENDED:

- 1363 • the error is logged
- 1364 • the problem is resolved by other means
- 1365 • no further action is taken.

1366 4.2.4.2 Identifying the Error Reporting Location

1367 The Error Reporting Location is a URI specified by the sender of the message in error that indicates
1368 where to send a *message reporting the error*.

1369 The **ErrorURI** implied by the **CPA**, identified by the **CPAId** on the message, SHOULD be used.
 1370 Otherwise, the recipient MAY resolve an **ErrorURI** using the **From** element of the message in error. If
 1371 neither is possible, no error will be reported to the sending **Party**.

1372 Even if the message in error cannot be successfully analyzed, MSH implementers MAY try to determine
 1373 the Error Reporting Location by other means. How this is done is an implementation decision.

1374 4.2.4.3 Service and Action Element Values

1375 An **ErrorList** element can be included in a SOAP **Header** that is part of a *message* being sent as a result
 1376 of processing of an earlier message. In this case, the values for the **Service** and **Action** elements are
 1377 set by the designer of the Service. This method MUST NOT be used if the **highestSeverity** is **Error**.

1378 An **ErrorList** element can also be included in an independent *message*. In this case the values of the
 1379 **Service** and **Action** elements MUST be set as follows:

- 1380 • The **Service** element MUST be set to: **urn:oasis:names:tc:ebxml-msg:service**
- 1381 • The **Action** element MUST be set to **MessageError**.

1382 4.3 SyncReply Module

1383 It may be necessary for the sender of a message, using a synchronous communications protocol, such as
 1384 HTTP, to receive the associated response message over the same connection the request message was
 1385 delivered. In the case of HTTP, the sender of the HTTP request message containing an ebXML message
 1386 needs to have the response ebXML message delivered to it on the same HTTP connection.

1387 If there are intermediary nodes (either ebXML MSH nodes or possibly other SOAP nodes) involved in the
 1388 message path, it is necessary to provide some means by which the sender of a message can indicate it is
 1389 expecting a response so the intermediary nodes can keep the connection open.

1390 The **SyncReply** ebXML SOAP extension element is provided for this purpose.

1391 4.3.1 SyncReply Element

1392 The **SyncReply** element MAY be present as a direct child descendant of the SOAP **Header** element. It
 1393 consists of:

- 1394 • an **id** attribute (see section 2.3.7 for details)
- 1395 • a **version** attribute (see section 2.3.8 for details)
- 1396 • a SOAP **actor** attribute with the REQUIRED value of "**http://schemas.xmlsoap.org/soap/actor/next**"
- 1397 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)

1398 If present, this element indicates to the receiving SOAP or ebXML MSH node the connection over which
 1399 the message was received SHOULD be kept open in expectation of a response message to be returned
 1400 via the same connection.

1401 This element MUST NOT be used to override the value of **syncReplyMode** in the CPA. If the value of
 1402 **syncReplyMode** is **none** and a **SyncReply** element is present, the *Receiving MSH* should issue an error
 1403 with **errorCode** of **Inconsistent** and a **severity** of **Error** (see section 4.1.5).

1404 An example of a **SyncReply** element:

```
1405 <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"  
1406 SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
```

1407 5 Combining ebXML SOAP Extension Elements

1408 This section describes how the various ebXML SOAP extension elements may be used in combination.

1409 5.1.1 MessageHeader Element Interaction

1410 The **MessageHeader** element MUST be present in every message.

1411 **5.1.2 Manifest Element Interaction**

1412 The **Manifest** element MUST be present if there is any data associated with the message not present in
1413 the *Header Container*. This applies specifically to data in the *Payload Container(s)* or elsewhere, e.g. on
1414 the web.

1415 **5.1.3 Signature Element Interaction**

1416 One or more XML Signature [XMLDSIG] **Signature** elements MAY be present on any message.

1417 **5.1.4 ErrorList Element Interaction**

1418 If the **highestSeverity** attribute on the **ErrorList** is set to **Warning**, then this element MAY be present
1419 with any element.

1420 If the **highestSeverity** attribute on the **ErrorList** is set to **Error**, then this element MUST NOT be present
1421 with the **Manifest** element

1422 **5.1.5 SyncReply Element Interaction**

1423 The **SyncReply** element MAY be present on any outbound message sent using synchronous
1424 communication protocol.

1425

Part II. Additional Features

1426

6 Reliable Messaging Module

1427 Reliable Messaging defines an interoperable protocol such that two Message Service Handlers (MSH)
1428 can reliably exchange messages, using acknowledgment, retry and duplicate detection and elimination
1429 mechanisms, resulting in the *To Party* receiving the message Once-And-Only-Once. The protocol is
1430 flexible, allowing for both store-and-forward and end-to-end reliable messaging.

1431 Reliability is achieved by a *Receiving MSH* responding to a message with an *Acknowledgment Message*.
1432 An *Acknowledgment Message* is any ebXML message containing an **Acknowledgment** element. Failure
1433 to receive an *Acknowledgment Message* by a *Sending MSH* MAY trigger successive retries until such
1434 time as an *Acknowledgment Message* is received or the predetermined number of retries has been
1435 exceeded at which time the *From Party* MUST be notified of the probable delivery failure.

1436 Whenever an identical message may be received more than once, some method of duplicate detection
1437 and elimination is indicated, usually through the mechanism of a *persistent store*.

1438

6.1 Persistent Storage and System Failure

1439 A MSH that supports Reliable Messaging MUST keep messages sent or received reliably in *persistent*
1440 *storage*. In this context *persistent storage* is a method of storing data that does not lose information after
1441 a system failure or interruption.

1442 This specification recognizes different degrees of resilience may be realized depending upon the
1443 technology used to store the data. However, at a minimum, persistent storage with the resilience
1444 characteristics of a hard disk (or equivalent) SHOULD be used. It is strongly RECOMMENDED that
1445 implementers of this specification use technology resilient to the failure of any single hardware or
1446 software component.

1447 After a system interruption or failure, a MSH MUST ensure that messages in persistent storage are
1448 processed as if the system failure or interruption had not occurred. How this is done is an implementation
1449 decision.

1450 In order to support the filtering of duplicate messages, a *Receiving MSH* MUST save the **MessageId** in
1451 *persistent storage*. It is also RECOMMENDED the following be kept in *persistent storage*:

- 1452 • the complete message, at least until the information in the message has been passed to the application or
1453 other process needing to process it,
- 1454 • the time the message was received, so the information can be used to generate the response to a *Message*
1455 *Status Request* (see section 7.1.1),
- 1456 • the complete response message.

1457

6.2 Methods of Implementing Reliable Messaging

1458 Support for Reliable Messaging is implemented in one of the following ways:

- 1459 • using the ebXML Reliable Messaging protocol,
- 1460 • using ebXML SOAP structures together with commercial software products that are designed to provide
1461 reliable delivery of messages using alternative protocols,
- 1462 • user application support for some features, especially duplicate elimination, or
- 1463 • some mixture of the above options on a per-feature basis.

1464 6.3 Reliable Messaging SOAP Header Extensions

1465 6.3.1 AckRequested Element

1466 The **AckRequested** element is an OPTIONAL extension to the SOAP **Header** used by the *Sending MSH*
 1467 to request a *Receiving MSH*, acting in the role of the actor URI identified in the SOAP **actor** attribute,
 1468 returns an *Acknowledgment Message*.

1469 The **AckRequested** element contains the following:

- 1470 • a **id** attribute (see section 2.3.7 for details)
- 1471 • a **version** attribute (see section 2.3.8 for details)
- 1472 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)
- 1473 • a SOAP **actor** attribute
- 1474 • a **signed** attribute

1475 This element is used to indicate to a *Receiving MSH*, acting in the role identified by the SOAP **actor**
 1476 attribute, whether an *Acknowledgment Message* is expected, and if so, whether the message should be
 1477 signed by the *Receiving MSH*.

1478 An *ebXML Message* MAY have zero, one, or two instances of an **AckRequested** element. A single MSH
 1479 node SHOULD only insert one **AckRequested** element. If there are two **AckRequested** elements
 1480 present, they MUST have different values for their respective SOAP **actor** attributes. At most one
 1481 **AckRequested** element can be targeted at the **actor** URI meaning *Next MSH* (see section 2.3.10) and at
 1482 most one **AckRequested** element can be targeted at the **actor** URI meaning *To Party MSH* (see section
 1483 2.3.11) for any given message.

1484 6.3.1.1 SOAP actor attribute

1485 The **AckRequested** element MUST be targeted at either the *Next MSH* or the *To Party MSH* (these are
 1486 equivalent for single-hop routing). This is accomplished by including a SOAP **actor** with a URN value
 1487 with one of the two ebXML **actor** URNs defined in sections 2.3.10 and 2.3.11 or by leaving this attribute
 1488 out. The default **actor** targets the *To Party MSH*.

1489 6.3.1.2 signed attribute

1490 The REQUIRED **signed** attribute is used by a *From Party* to indicate whether or not a message received
 1491 by the *To Party MSH* should result in the *To Party* returning a signed *Acknowledgment Message* –
 1492 containing a [XMLDSIG] **Signature** element as described in section 4.1. Valid values for **signed** are:

- 1493 • **true** - a signed *Acknowledgment Message* is requested, or
- 1494 • **false** - an unsigned *Acknowledgment Message* is requested.

1495 Before setting the value of the **signed** attribute in **AckRequested**, the *Sending MSH* SHOULD check if
 1496 the *Receiving MSH* supports *Acknowledgment Messages* of the type requested (see also [ebCPP]).

1497 When a *Receiving MSH* receives a message with **signed** attribute set to **true** or **false** then it should verify
 1498 it is able to support the type of *Acknowledgment Message* requested.

- 1499 • If the *Receiving MSH* can produce the *Acknowledgment Message* of the type requested, then it MUST
 1500 return to the *Sending MSH* a message containing an **Acknowledgment** element.
- 1501 • If the *Receiving MSH* cannot return an *Acknowledgment Message* as requested it MUST report the error to
 1502 the *Sending MSH* using an **errorCode** of **Inconsistent** and a **severity** of either **Error** if inconsistent with the
 1503 CPA, or **Warning** if not supported..

1504 6.3.1.3 AckRequested Sample

1505 In the following example, an *Acknowledgment Message* is requested of a MSH node acting in the role of
 1506 the *To Party* (see section 2.3.11). The **Acknowledgment** element generated MUST be targeted to the

1507 ebXML MSH node acting in the role of the *From Party* along the reverse message path (end-to-end
1508 acknowledgment).

```
1509 <eb:AckRequested SOAP:mustUnderstand="1" eb:version="2.0" eb:signed="false"/>
```

1510 6.3.1.4 AckRequested Element Interaction

1511 An **AckRequested** element MUST NOT be included on a message with only an **Acknowledgment**
1512 element (no payload). This restriction is imposed to avoid endless loops of *Acknowledgment Messages*.
1513 An *Error Message* MUST NOT contain an **AckRequested** element.

1514 6.3.2 Acknowledgment Element

1515 The **Acknowledgment** element is an OPTIONAL extension to the SOAP **Header** used by one Message
1516 Service Handler to indicate to another Message Service Handler that it has received a message. The
1517 **RefToMessageId** element in an **Acknowledgment** element is used to identify the message being
1518 acknowledged by its **MessageId**.

1519 The **Acknowledgment** element consists of the following elements and attributes:

- 1520 • an **id** attribute (see section 2.3.7 for details)
- 1521 • a **version** attribute (see section 2.3.8 for details)
- 1522 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)
- 1523 • a SOAP **actor** attribute
- 1524 • a **Timestamp** element
- 1525 • a **RefToMessageId** element
- 1526 • a **From** element
- 1527 • zero or more [XMLDSIG] **Reference** element(s)

1528 6.3.2.1 SOAP actor attribute

1529 The SOAP **actor** attribute of the **Acknowledgment** element SHALL have a value corresponding to the
1530 **AckRequested** element of the message being acknowledged. If there is no SOAP **actor** attribute
1531 present on an **Acknowledgment** element, the default target is the *To Party MSH* (see section for 10.1.3).

1532 6.3.2.2 Timestamp Element

1533 The REQUIRED **Timestamp** element is a value representing the time that the message being
1534 acknowledged was received by the *MSH* generating the acknowledgment message. It must conform to a
1535 dateTime [XMLSchema] and is expressed as UTC (section 3.1.6.2).

1536 6.3.2.3 RefToMessageId Element

1537 The REQUIRED **RefToMessageId** element contains the **MessageId** of the message whose delivery is
1538 being reported.

1539 6.3.2.4 From Element

1540 This is the same element as the **From** element within **MessageHeader** element (see section 3.1.1).
1541 However, when used in the context of an **Acknowledgment** element, it contains the identifier of the *Party*
1542 generating the *Acknowledgment Message*.

1543 If the **From** element is omitted then the *Party* sending the element is identified by the **From** element in
1544 the **MessageHeader** element.

1545 6.3.2.5 [XMLDSIG] Reference Element

1546 An *Acknowledgment Message* MAY be used to enable non-repudiation of receipt by a MSH by including
1547 one or more **Reference** elements, from the XML Signature [XMLDSIG] namespace, derived from the
1548 *message being acknowledged* (see section 4.1.3 for details). The **Reference** element(s) MUST be

1549 namespace qualified to the aforementioned namespace and MUST conform to the XML Signature
 1550 [XMLDSIG] specification. If the *message being acknowledged* contains an **AckRequested** element with
 1551 a **signed** attribute set to **true**, then the [XMLDSIG] **Reference** list is REQUIRED.

1552 Receipt of an *Acknowledgment Message*, indicates the original message reached its destination. Receipt
 1553 of a signed *Acknowledgment Message* validates the sender of the *Acknowledgment Message*. However,
 1554 a signed *Acknowledgment Message* does not indicate whether the message arrived intact. Including a
 1555 digest (see [XMLDSIG] section 4.3.3) of the original message in the *Acknowledgment Message* indicates
 1556 to the original sender what was received by the recipient of the message being acknowledged. The
 1557 digest contained in the *Acknowledgment Message* may be compared to a digest of the original message.
 1558 If the digests match, the message arrived intact. Such a digest already exists in the original message, if it
 1559 is signed, contained within the [XMLDSIG] **Signature / Reference** element(s).

1560 If the original message is signed, the [XMLDSIG] **Signature / Reference** element(s) of the original
 1561 message will be identical to the **Acknowledgment / Reference** element(s) in the
 1562 *Acknowledgment Message*. If the original message is not signed, the [XMLDSIG] **Reference** element
 1563 must be derived from the original message (see section 4.1.3).

1564 Upon receipt of an end-to-end *Acknowledgment Message*, the *From Party MSH* MAY notify the
 1565 application of successful delivery for the referenced message. This MSH SHOULD ignore subsequent
 1566 *Error* or *Acknowledgment Messages* with the same **RefToMessageId** value.

1567 6.3.2.6 Acknowledgment Sample

1568 An example **Acknowledgment** element targeted at the *To Party MSH*:

```
1569 <eb:Acknowledgment SOAP:mustUnderstand="1" eb:version="2.0">
1570   <eb:Timestamp>2001-03-09T12:22:30</eb:Timestamp>
1571   <eb:RefToMessageId>323210:e52151ec74:7ffc@xtacy</eb:RefToMessageId>
1572   <eb:From> <eb:PartyId>uri:www.example.com</eb:PartyId> </eb:From>
1573 </eb:Acknowledgment>
```

1574 6.3.2.7 Sending an Acknowledgment Message by Itself

1575 If there are no errors in the message received and an *Acknowledgment Message* is being sent on its own,
 1576 not as a message containing payload data, then the **Service** and **Action** MUST be set as follows:

- 1577 • the **Service** element MUST be set to **urn:oasis:names:tc:ebxml-msg:service**
- 1578 • the **Action** element MUST be set to **Acknowledgment**

1579 6.3.2.8 Acknowledgment Element Interaction

1580 An **Acknowledgment** element MAY be present on any message, except as noted in section 6.3.1.4. An
 1581 *Acknowledgment Message* MUST NOT be returned for an *Error Message*.

1582 6.4 Reliable Messaging Parameters

1583 This section describes the parameters required to control reliable messaging. Many of these parameters
 1584 can be obtained from a CPA.

1585 6.4.1 DuplicateElimination

1586 The **DuplicateElimination** element MUST be used by the *From Party MSH* to indicate whether the
 1587 *Receiving MSH* MUST eliminate duplicates (see section 6.6 for Reliable Messaging behaviors). If the
 1588 value of **duplicateElimination** in the CPA is **never**, **DuplicateElimination** MUST NOT be present.

- 1589 • If **DuplicateElimination** is present – The *To Party MSH* must persist messages in a persistent store so
 1590 duplicate messages will be presented to the *To Party Application At-Most-Once*, or
- 1591 • If **DuplicateElimination** is not present – The *To Party MSH* is not required to maintain the message in
 1592 persistent store and is not required to check for duplicates.

1593 If **DuplicateElimination** is present, the *To Party MSH* must adopt a reliable messaging behavior (see
 1594 section 6.6) causing duplicate messages to be ignored.

1595 If **DuplicateElimination** is not present, a *Receiving MSH* is not required to check for duplicate message
1596 delivery. Duplicate messages might be delivered to an application and persistent storage of messages is
1597 not required – although elimination of duplicates is still allowed.

1598 If the *To Party* is unable to support the requested functionality, or if the value of **duplicateElimination** in
1599 the CPA does not match the implied value of the element, the *To Party* SHOULD report the error to the
1600 *From Party* using an **errorCode** of **Inconsistent** and a **Severity** of **Error**.

1601 **6.4.2 AckRequested**

1602 The **AckRequested** parameter is used by the *Sending MSH* to request a *Receiving MSH*, acting in the
1603 role of the actor URI identified in the SOAP **actor** attribute, return an *Acknowledgment Message*
1604 containing an **Acknowledgment** element (see section 6.3.1).

1605 **6.4.3 Retries**

1606 The **Retries** parameter, from a CPA, is an integer value specifying the maximum number of times a
1607 *Sending MSH* SHOULD attempt to redeliver an unacknowledged *message* using the same
1608 communications protocol.

1609 **6.4.4 RetryInterval**

1610 The **RetryInterval** parameter, from a CPA, is a time value, expressed as a duration in accordance with
1611 the **duration** [XMLSchema] data type. This value specifies the minimum time a *Sending MSH* SHOULD
1612 wait between **Retries**, if an *Acknowledgment Message* is not received or if a communications error was
1613 detected during an attempt to send the message. **RetryInterval** applies to the time between sending of
1614 the original message and the first retry as well as the time between retries.

1615 **6.4.5 TimeToLive**

1616 **TimeToLive** is defined in section 3.1.6.4.

1617 For a reliably delivered message, **TimeToLive** MUST conform to:

1618
$$\mathbf{TimeToLive} > \mathbf{Timestamp} + ((\mathbf{Retries} + 1) * \mathbf{RetryInterval}).$$

1619 where **TimeStamp** comes from **MessageData**.

1620 **6.4.6 PersistDuration**

1621 The **PersistDuration** parameter, from a CPA, is the minimum length of time, expressed as a **duration**
1622 [XMLSchema], data from a reliably sent *Message*, is kept in *Persistent Storage* by a *Receiving MSH*.

1623 If the **PersistDuration** has passed since the message was first sent, a *Sending MSH* SHOULD NOT
1624 resend a message with the same **MessageId**.

1625 If a message cannot be sent successfully before **PersistDuration** has passed, then the *Sending MSH*
1626 should report a delivery failure (see section 6.5.7).

1627 **TimeStamp** for a reliably sent message (found in the message header), plus its **PersistDuration** (found
1628 in the CPA), must be greater than its **TimeToLive** (found in the message header).

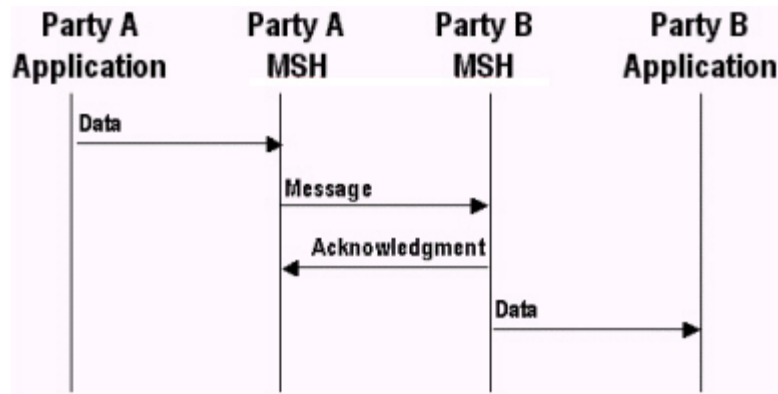
1629 **6.4.7 syncReplyMode**

1630 The **syncReplyMode** parameter from the CPA is used only if the data communications protocol is
1631 *synchronous* (e.g. HTTP). If the communications protocol is not *synchronous*, then the value of
1632 **syncReplyMode** is ignored. If the **syncReplyMode** attribute is not present, it is semantically equivalent
1633 to its presence with a value of **none**. If the **syncReplyMode** parameter is not **none**, a **SyncReply**
1634 element MUST be present and the MSH must return any response from the application or business
1635 process in the payload of the *synchronous* reply message, as specified in the CPA. Valid values of
1636 **syncReplyMode** are **mshSignalsOnly**, **signalsOnly**, **signalsAndResponse**, **responseOnly**, and **none**.
1637 See also the description of **syncReplyMode** in the CPPA [ebCPP] specification.

1638 If the value of *syncReplyMode* is *none* and a *SyncReply* element is present, the *Receiving MSH* should
 1639 issue an error with *errorCode* of *Inconsistent* and a *severity* of *Error* (see section 4.1.5).

1640 6.5 ebXML Reliable Messaging Protocol

1641 The ebXML Reliable Messaging Protocol is illustrated by the following figure.



1642

1643

Figure 6-1 Indicating a message has been received

1644 The receipt of the *Acknowledgment Message* indicates the message being acknowledged has been
 1645 successfully received and either processed or persisted by the *Receiving MSH*.

1646 An *Acknowledgment Message* MUST contain an *Acknowledgment* element as described in section 6.3.1
 1647 with a *RefToMessageId* containing the same value as the *MessageId* element in the *message being*
 1648 *acknowledged*.

1649 6.5.1 Sending Message Behavior

1650 If a MSH is given data by an application needing to be sent reliably, the MSH MUST do the following:

- 1651 1. Create a message from components received from the application.
- 1652 2. Insert an *AckRequested* element as defined in section 6.3.1.
- 1653 3. Save the message in *persistent storage* (see section 6.1).
- 1654 4. Send the message to the *Receiving MSH*.
- 1655 5. Wait for the return of an *Acknowledgment Message* acknowledging receipt of this specific
 1656 message and, if it does not arrive before *RetryInterval* has elapsed, or if a communications
 1657 protocol error is encountered, then take the appropriate action as described in section 6.5.4.

1658 6.5.2 Receiving Message Behavior

1659 If this is an *Acknowledgment Message* as defined in section 6 then:

- 1660 1 Look for a message in *persistent storage* with a *MessageId* the same as the value of
 1661 *RefToMessageId* on the received Message.
- 1662 2 If a message is found in *persistent storage* then mark the persisted message as delivered.

1663 If the *Receiving MSH* is NOT the *To Party MSH* (as defined in section 2.3.10 and 2.3.11), then see
 1664 section 10.1.3 for the behavior of the *AckRequested* element.

1665 If an *AckRequested* element is present (not an *Acknowledgment Message*) then:

- 1666 1 If the message is a duplicate (i.e. there is a *MessageId* held in persistent storage containing the
 1667 same value as the *MessageId* in the received message), generate an *Acknowledgment Message*
 1668 (see section 6.5.3). Follow the procedure in section 6.5.5 for resending lost *Acknowledgment*

1669 *Messages*. The *Receiving MSH* MUST NOT deliver the message to the application interface.
 1670 Note: The check for duplicates is only performed when **DuplicateElimination** is present.

- 1671 2 If the message is not a duplicate or (there is no **MessageId** held in persistent storage
 1672 corresponding to the **MessageId** in the received message) then:
- 1673 a If there is a **DuplicateElimination** element, save the **MessageId** of the received message in
 1674 persistent storage. As an implementation decision, the whole message MAY be stored.
- 1675 b Generate an *Acknowledgment Message* in response (this may be as part of another
 1676 message). The *Receiving MSH* MUST NOT send an *Acknowledgment Message* until the
 1677 message has been safely stored in *persistent storage* or delivered to the application
 1678 interface. Delivery of an *Acknowledgment Message* constitutes an obligation by the
 1679 *Receiving MSH* to deliver the message to the application or forward to the next MSH in the
 1680 message path as appropriate.

1681 If there is no **AckRequested** element then do the following:

- 1682 1 If there is a **DuplicateElimination** element, and the message is a duplicate, then do nothing.
 1683 2 Otherwise, deliver the message to the application interface

1684 If the *Receiving MSH* node is operating as an intermediary along the message's message path, then it
 1685 MAY use store-and-forward behavior. However, it MUST NOT filter out perceived duplicate messages
 1686 from their normal processing at that node.

1687 If an *Acknowledgment Message* is received unexpectedly, it should be ignored. No error should be sent.

1688 **6.5.3 Generating an Acknowledgment Message**

1689 An *Acknowledgment Message* MUST be generated whenever a message is received with an
 1690 **AckRequested** element having a SOAP **actor** URI targeting the *Receiving MSH* node.

1691 As a minimum, it MUST contain an **Acknowledgment** element with a **RefToMessageId** containing the
 1692 same value as the **MessageId** element in the message being acknowledged. This message MUST be
 1693 placed in persistent storage with the same **PersistDuration** as the original message.

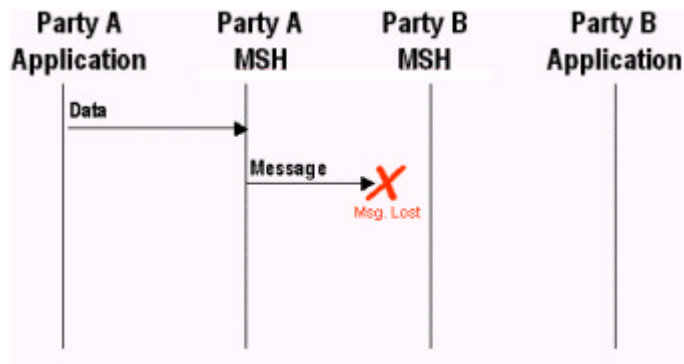
1694 The *Acknowledgment Message* can be sent at the same time as the response to the received message.
 1695 In this case, the values for the **MessageHeader** elements of the *Acknowledgment Message* are
 1696 determined by the **Service** and **Action** associated with the business response.

1697 If an *Acknowledgment Message* is being sent on its own, then the value of the **MessageHeader** elements
 1698 MUST be set as follows:

- 1699 • The **Service** element MUST be set to: **urn:oasis:names:tc:ebxml-msg:service**
- 1700 • The **Action** element MUST be set to **Acknowledgment**.
- 1701 • The **From** element MAY be populated with the **To** element extracted from the message received and all
 1702 child elements from the **To** element received SHOULD be included in this **From** element.
- 1703 • The **To** element MAY be populated with the **From** element extracted from the message received and all
 1704 child elements from the **From** element received SHOULD be included in this **To** element.
- 1705 • The **RefToMessageId** element MUST be set to the **MessageId** of the message received.

1706 **6.5.4 Resending Lost Application Messages**

1707 This section describes the behavior required by the sender and receiver of a message in order to handle
 1708 lost messages. A message is "lost" when a *Sending MSH* does not receive a positive acknowledgment to
 1709 a message. For example, it is possible a *message* was lost:



1710

1711 **Figure 6-2 Undelivered Message**1712 It is also possible the *Acknowledgment Message* was lost, for example:

1713

1714 **Figure 6-3 Lost Acknowledgment Message**1715 Note: *Acknowledgment Messages* are never acknowledged.1716 The rules applying to the non-receipt of an anticipated *Acknowledgment Message* due to the loss of either the
1717 application message or the *Acknowledgment Message* are as follows:

- 1718 • The *Sending MSH* MUST resend the original message if an *Acknowledgment Message* has been requested
1719 but has not been received and the following are true:
 - 1720 • At least the time specified in the **RetryInterval** parameter has passed since the message was last sent,
 - 1721 • The message has been resent less than the number of times specified in the **Retries** parameter.
- 1722 • If the *Sending MSH* does not receive an *Acknowledgment Message* after the maximum number of retries,
1723 the *Sending MSH* SHALL notify the application and/or system administrator function of the failure to receive
1724 an *Acknowledgment Message* (see also section 4.2.3.2.4 concerning treatment of errors).
- 1725 • If the *Sending MSH* detects a communications protocol error, the *Sending MSH* MUST resend the message
1726 using the same algorithm as if it has not received an *Acknowledgment Message*.

1727 **6.5.5 Resending Acknowledgments**1728 If the *Receiving MSH* receives a message it discovers to be a duplicate, it should resend the original
1729 *Acknowledgment Message* if the message is stored in *persistent store*. In this case, do the following:1730 Look in persistent storage for the first response to the received message (i.e. it contains a
1731 **RefToMessageId** that matches the **MessageId** of the received message).1732 If a response message was found in *persistent storage* then resend the persisted message back to the
1733 MSH that sent the received message. If no response message was found in *persistent storage*, then:

- 1734 (1) If **syncReplyMode** is not set to **none** and if the CPA indicates an application response is
1735 included, then it must be the case that the application has not finished processing the earlier

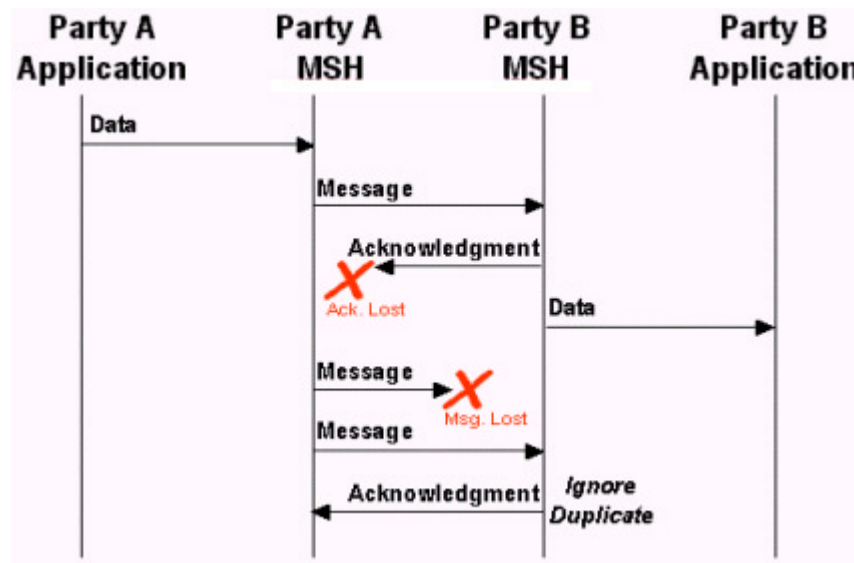
1736 copy of the same message. Therefore, wait for the response from the application and then
 1737 return that response synchronously over the same connection that was used for the
 1738 retransmission.

1739 (2) Otherwise, generate an *Acknowledgment Message*.

1740 6.5.6 Duplicate Message Handling

1741 In the context of this specification:

- 1742 • an "identical message" – a *message* containing the same ebXML SOAP **Header**, **Body** and ebXML Payload
 1743 Container(s) as the earlier sent *message*.
- 1744 • a "duplicate message" – a *message* containing the same **MessageId** as a previously received message.
- 1745 • the "first response message" – the message with the earliest **Timestamp** in the **MessageData** element
 1746 having the same **RefToMessageId** as the duplicate message.



1747

1748 **Figure 6-4 Resending Unacknowledged Messages**

1749 The diagram above shows the behavior to be followed by the *Sending* and *Receiving* MSH for messages
 1750 sent with an **AckRequested** element and a **DuplicateElimination** element. Specifically:

- 1751 1) The sender of the *message* (e.g. Party A MSH) MUST resend the "identical message" if no
 1752 *Acknowledgment Message* is received.
- 1753 2) When the recipient (Party B MSH) of the *message* receives a "duplicate message", it MUST resend to
 1754 the sender (Party A MSH) an *Acknowledgment Message* identical to the *first response message* sent
 1755 to the sender Party A MSH).
- 1756 3) The recipient of the *message* (Party B MSH) MUST NOT forward the message a second time to the
 1757 application/process.

1758 6.5.7 Failed Message Delivery

1759 If a message sent with an **AckRequested** element cannot be delivered, the MSH or process handling the
 1760 message (as in the case of a routing intermediary) SHALL send a delivery failure notification to the *From*
 1761 *Party*. The delivery failure notification message is an *Error Message* with **errorCode** of **DeliveryFailure**
 1762 and a **severity** of:

- 1763 • **Error** if the party who detected the problem could not transmit the message (e.g. the communications
 1764 transport was not available)
- 1765 • **Warning** if the message was transmitted, but an *Acknowledgment Message* was not received. This means
 1766 the message probably was not delivered.

1767 It is possible an error message with an **Error** element having an **errorCode** set to **DeliveryFailure**
 1768 cannot be delivered successfully for some reason. If this occurs, then the *From Party*, the ultimate
 1769 destination for the *Error Message*, MUST be informed of the problem by other means. How this is done is
 1770 outside the scope of this specification

1771 Note: If the *From Party MSH* receives an *Acknowledgment Message* from the *To Party MSH*, it should ignore all
 1772 other **DeliveryFailure** or *Acknowledgment Messages*.

1773 6.6 Reliable Messaging Combinations

	Duplicate- Elimination [§]	AckRequested ToPartyMSH	AckRequested NextMSH	Comment
1	Y	Y	Y	Once-And-Only-Once Reliable Messaging at the End-To-End and At-Least-Once to the Intermediate. Intermediate and To Party can issue Delivery Failure Notifications if they cannot deliver.
2	Y	Y	N	Once-And-Only-Once Reliable Message at the End-To-End level only based upon end-to-end retransmission
3	Y	N	Y	At-Least-Once Reliable Messaging at the Intermediate Level – Once-And-Only-Once end-to-end if all Intermediates are Reliable. No End-to-End notification.
4	Y	N	N	At-Most-Once Duplicate Elimination only at the To Party. No retries at the Intermediate or the End.
5	N	Y	Y	At-Least-Once Reliable Messaging with duplicates possible at the Intermediate and the To Party.
6	N	Y	N	At-Least-Once Reliable Messaging duplicates possible at the Intermediate and the To Party.
7	N	N	Y	At-Least-Once Reliable Messaging to the Intermediate and at the End. No End-to-End notification.
8	N	N	N	Best Effort

1774 [§]Duplicate Elimination is only performed at the To Party MSH, not at the Intermediate Level.

1775 7 Message Status Service

1776 The Message Status Request Service consists of the following:

- 1777 • A Message Status Request message containing details regarding a message previously sent is sent to a
 1778 Message Service Handler (MSH)
- 1779 • The Message Service Handler receiving the request responds with a Message Status Response message.

1780 A Message Service Handler SHOULD respond to Message Status Requests for messages that have
 1781 been sent reliably and the **MessageId** in the **RefToMessageId** is present in *persistent storage* (see
 1782 section 6.1).

1783 A Message Service Handler MAY respond to Message Status Requests for messages that have not been
 1784 sent reliably.

1785 A Message Service SHOULD NOT use the Message Status Request Service to implement Reliable
 1786 Messaging.

1787 If a *Receiving MSH* does not support the service requested, it SHOULD return an *Error Message* with an
 1788 **errorCode** of **NotSupported** and a **highestSeverity** attribute set to **Error**. Each service is described
 1789 below.

1790 7.1 Message Status Messages

1791 7.1.1 Message Status Request Message

1792 A Message Status Request message consists of an *ebXML Message* with no ebXML Payload Container
1793 and the following:

- 1794 • a **MessageHeader** element containing:
 - 1795 • a **From** element identifying the *Party* that created the Message Status Request message
 - 1796 • a **To** element identifying a *Party* who should receive the message.
 - 1797 • a **Service** element that contains: *urn:oasis:names:tc:ebxml-msg:service*
 - 1798 • an **Action** element that contains **StatusRequest**
 - 1799 • a **MessageData** element
- 1800 • a **StatusRequest** element containing:
 - 1801 • a **RefToMessageld** element in **StatusRequest** element containing the **MessageId** of the message
1802 whose status is being queried.
- 1803 • an [XMLDSIG] **Signature** element (see section 4.1 for more details)

1804 The message is then sent to the *To Party*.

1805 7.1.2 Message Status Response Message

1806 Once the *To Party* receives the Message Status Request message, they SHOULD generate a Message
1807 Status Response message with no ebXML Payload Container consisting of the following:

- 1808 • a **MessageHeader** element containing:
 - 1809 ▪ a **From** element that identifies the sender of the Message Status Response message
 - 1810 ▪ a **To** element set to the value of the **From** element in the Message Status Request message
 - 1811 ▪ a **Service** element that contains *urn:oasis:names:tc:ebxml-msg:service*
 - 1812 ▪ an **Action** element that contains **StatusResponse**
 - 1813 ▪ a **MessageData** element containing:
 - 1814 • a **RefToMessageId** that identifies the Message Status Request message.
- 1815 • **StatusResponse** element (see section 7.2.3)
- 1816 • an [XMLDSIG] **Signature** element (see section 4.1 for more details)

1817 The message is then sent to the *To Party*.

1818 7.1.3 Security Considerations

1819 Parties who receive a Message Status Request message SHOULD always respond to the message.
1820 However, they MAY ignore the message instead of responding with **messageStatus** set to
1821 **Unauthorized** if they consider the sender of the message to be unauthorized. The decision process
1822 resulting in this course of action is implementation dependent.

1823 7.2 StatusRequest Element

1824 The OPTIONAL **StatusRequest** element is an immediate child of a SOAP **Body** and is used to identify
1825 an earlier message whose status is being requested (see section 7.3.5).

1826 The **StatusRequest** element consists of the following:

- 1827 • an **id** attribute (see section 2.3.7 for details)
- 1828 • a **version** attribute (see section 2.3.8 for details)
- 1829 • a **RefToMessageId** element

1830 7.2.1 RefToMessageId Element

1831 A REQUIRED *RefToMessageId* element contains the *MessageId* of the message whose status is being
1832 requested.

1833 7.2.2 StatusRequest Sample

1834 An example of the *StatusRequest* element is given below:

```
1835 <eb:StatusRequest eb:version="2.0" >
1836   <eb:RefToMessageId>323210:e52151ec74:-7ffc@xtacy</eb:RefToMessageId>
1837 </eb:StatusRequest>
```

1838 7.2.3 StatusRequest Element Interaction

1839 A *StatusRequest* element MUST NOT be present with the following elements:

- 1840 • a *Manifest* element
- 1841 • a *StatusResponse* element
- 1842 • an *ErrorList* element

1843 7.3 StatusResponse Element

1844 The OPTIONAL *StatusResponse* element is an immediate child of a SOAP *Body* and is used by one
1845 MSH to describe the status of processing of a message.

1846 The *StatusResponse* element consists of the following elements and attributes:

- 1847 • an *id* attribute (see section 2.3.7 for details)
- 1848 • a *version* attribute (see section 2.3.8 for details)
- 1849 • a *RefToMessageId* element
- 1850 • a *Timestamp* element
- 1851 • a *messageStatus* attribute

1852 7.3.1 RefToMessageId Element

1853 A REQUIRED *RefToMessageId* element contains the *MessageId* of the message whose status is being
1854 reported. *RefToMessageId* element child of the *MessageData* element of a message containing a
1855 *StatusResponse* element SHALL have the *MessageId* of the message containing the *StatusRequest*
1856 element to which the *StatusResponse* element applies. The *RefToMessageId* child element of the
1857 *StatusRequest* or *StatusResponse* element SHALL contain the *MessageId* of the message whose
1858 status is being queried.

1859 7.3.2 Timestamp Element

1860 The *Timestamp* element contains the time the message, whose status is being reported, was received
1861 (section 3.1.6.2.). This MUST be omitted if the message, whose status is being reported, is
1862 *NotRecognized* or the request was *Unauthorized*.

1863 7.3.3 messageStatus attribute

1864 The REQUIRED *messageStatus* attribute identifies the status of the message identified by the
1865 *RefToMessageId* element. It SHALL be set to one of the following values:

- 1866 • *Unauthorized* – the Message Status Request is not authorized or accepted
- 1867 • *NotRecognized* – the message identified by the *RefToMessageId* element in the *StatusResponse*
1868 element is not recognized
- 1869 • *Received* – the message identified by the *RefToMessageId* element in the *StatusResponse* element has
1870 been received by the MSH
- 1871 • *Processed* – the message identified by the *RefToMessageId* element in the *StatusResponse* element has
1872 been processed by the MSH

- 1873 • **Forwarded** – the message identified by the **RefToMessageId** element in the **StatusResponse** element has
1874 been forwarded by the MSH to another MSH

1875 Note: if a Message Status Request is sent after the elapsed time indicated by **PersistDuration** has passed since the
1876 message being queried was sent, the Message Status Response may indicate the **MessageId** was **NotRecognized** –
1877 the **MessageId** is no longer in persistent storage.

1878 7.3.4 StatusResponse Sample

1879 An example of the **StatusResponse** element is given below:

```
1880 <eb:StatusResponse eb:version="2.0" eb:messageStatus="Received">
1881   <eb:RefToMessageId>323210:e52151ec74:-7ffc@xtacy</eb:RefToMessageId>
1882   <eb:Timestamp>2001-03-09T12:22:30</eb:Timestamp>
1883 </eb:StatusResponse>
```

1884 7.3.5 StatusResponse Element Interaction

1885 This element MUST NOT be present with the following elements:

- 1886 • a **Manifest** element
1887 • a **StatusRequest** element
1888 • an **ErrorList** element with a **highestSeverity** attribute set to **Error**

1889 8 Message Service Handler Ping Service

1890 The OPTIONAL Message Service Handler Ping Service enables one MSH to determine if another MSH is
1891 operating. It consists of:

- 1892 • one MSH sending a Message Service Handler Ping message to a MSH, and
1893 • another MSH, receiving the Ping, responding with a Message Service Handler Pong message.

1894 If a *Receiving MSH* does not support the service requested, it SHOULD return an *Error Message* with an
1895 **errorCode** of **NotSupported** and a **highestSeverity** attribute set to **Error**.

1896 8.1 Message Service Handler Ping Message

1897 A Message Service Handler Ping (MSH Ping) message consists of an *ebXML Message* containing no
1898 ebXML Payload Container and the following:

- 1899 • a **MessageHeader** element containing the following:
- 1900 • a **From** element identifying the *Party* creating the MSH Ping message
 - 1901 • a **To** element identifying the *Party* being sent the MSH Ping message
 - 1902 • a **CPAId** element
 - 1903 • a **ConversationId** element
 - 1904 • a **Service** element containing: **urn:oasis:names:tc:ebxml-msg:service**
 - 1905 • an **Action** element containing **Ping**
 - 1906 • a **MessageData** element
- 1907 • an [XMLDSIG] **Signature** element (see section 4.1 for details).

1908 The message is then sent to the *To Party*.

1909 An example Ping:

```
1910 . . .Transport Headers
1911 SOAPAction: "ebXML"
1912 Content-type: multipart/related; boundary="ebXMLBoundary"
1913
1914 --ebXMLBoundary
1915 Content-Type: text/xml
1916
```

```

1917 <?xml version="1.0" encoding="UTF-8"?>
1918 <SOAP:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1919     xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
1920     xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
1921         http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
1922 <SOAP:Header xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
1923     xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
1924         http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
1925   <eb:MessageHeader version="2.0" SOAP:mustUnderstand="1"
1926     xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
1927     xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
1928         http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
1929     <eb:From> <eb:PartyId>urn:duns:123456789</eb:PartyId> </eb:From>
1930     <eb:To> <eb:PartyId>urn:duns:912345678</eb:PartyId> </eb:To>
1931     <eb:CPAId>20001209-133003-28572</eb:CPAId>
1932     <eb:ConversationId>20010215-111213-28572</eb:ConversationId>
1933     <eb:Service>urn:oasis:names:tc:ebxml-msg:service</eb:Service>
1934     <eb:Action>Ping</eb:Action>
1935     <eb:MessageData>
1936       <eb:MessageId>20010215-111212-28572@example.com</eb:MessageId>
1937       <eb:Timestamp>2001-02-15T11:12:12</eb:Timestamp>
1938     </eb:MessageData>
1939   </eb:MessageHeader>
1940 </SOAP:Header>
1941 <SOAP:Body/>
1942 </SOAP:Envelope>
1943
1944 --ebXMLBoundary--

```

1945 Note: The above example shows a Multipart/Related MIME structure with only one bodypart.

1946 8.2 Message Service Handler Pong Message

1947 Once the *To Party* receives the MSH Ping message, they MAY generate a Message Service Handler
 1948 Pong (MSH Pong) message consisting of an ebXML Message containing no ebXML Payload Container
 1949 and the following:

- 1950 • a **MessageHeader** element containing the following:
 - 1951 • a **From** element identifying the creator of the MSH Pong message
 - 1952 • a **To** element identifying a *Party* that generated the MSH Ping message
 - 1953 • a **CPAId** element
 - 1954 • a **ConversationId** element
 - 1955 • a **Service** element containing the value: *urn:oasis:names:tc:ebxml-msg:service*
 - 1956 • an **Action** element containing the value **Pong**
 - 1957 • a **MessageData** element containing:
 - 1958 • a **RefToMessageId** identifying the MSH Ping message.
- 1959 • an [XMLDSIG] **Signature** element (see section 4.1.1 for details).

1960 An example Pong:

```

1961 . . .Transport Headers
1962 SOAPAction: "ebXML"
1963 Content-Type: text/xml
1964
1965 <?xml version="1.0" encoding="UTF-8"?>
1966 <SOAP:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1967     xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
1968     xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
1969         http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
1970 <SOAP:Header xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
1971     xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
1972         http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
1973   <eb:MessageHeader eb:version="2.0" SOAP:mustUnderstand="1">
1974     <eb:From> <eb:PartyId>urn:duns:912345678</eb:PartyId> </eb:From>
1975     <eb:To> <eb:PartyId>urn:duns:123456789</eb:PartyId> </eb:To>

```



```

1976 <eb:CPAId>20001209-133003-28572</eb:CPAId>
1977 <eb:ConversationId>20010215-111213-28572</eb:ConversationId>
1978 <eb:Service>urn:oasis:names:tc:ebxml-msg:service</eb:Service>
1979 <eb:Action>Pong</eb:Action>
1980 <eb:MessageData>
1981 <eb:MessageId>20010215-111213-395884@example2.com</eb:MessageId>
1982 <eb:Timestamp>2001-02-15T11:12:13</eb:Timestamp>
1983 <eb:RefToMessageId>20010215-111212-28572@example.com</eb:RefToMessageId>
1984 </eb:MessageData>
1985 </eb:MessageHeader>
1986 </SOAP:Header>
1987 <SOAP:Body/>
1988 </SOAP:Envelope>

```

1989 Note: This example shows a non-multipart MIME structure.

1990 8.3 Security Considerations

1991 Parties who receive a MSH Ping message SHOULD always respond to the message. However, there is
 1992 a risk some parties might use the MSH Ping message to determine the existence of a Message Service
 1993 Handler as part of a security attack on that MSH. Therefore, recipients of a MSH Ping MAY ignore the
 1994 message if they consider that the sender of the message received is unauthorized or part of some attack.
 1995 The decision process that results in this course of action is implementation dependent.

1996 9 MessageOrder Module

1997 The **MessageOrder** module allows messages to be presented to the *To Party* in a particular order. This
 1998 is accomplished through the use of the **MessageOrder** element. Reliable Messaging MUST be used
 1999 when a **MessageOrder** element is present.

2000 **MessageOrder** module MUST only be used in conjunction with the ebXML Reliable Messaging Module
 2001 (section 6) with a scheme of Once-And-Only-Once (sections 6.6). If a sequence is sent and one
 2002 message fails to arrive at the *To Party MSH*, all subsequent messages will also fail to be presented to the
 2003 *To Party Application* (see **status** attribute section 9.1.1).

2004 9.1 MessageOrder Element

2005 The **MessageOrder** element is an OPTIONAL extension to the SOAP **Header** requesting the
 2006 preservation of message order in this conversation.

2007 The **MessageOrder** element contains the following:

- 2008 • a **id** attribute (see section 2.3.7)
- 2009 • a **version** attribute (see section 2.3.8 for details)
- 2010 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)
- 2011 • a **SequenceNumber** element

2012 When the **MessageOrder** element is present, **DuplicateElimination** MUST also be present and
 2013 **SyncReply** MUST NOT be present.

2014 9.1.1 SequenceNumber Element

2015 The REQUIRED **SequenceNumber** element indicates the sequence a *Receiving MSH* MUST process
 2016 messages. The **SequenceNumber** is unique within the **ConversationId** and MSH. The *From Party MSH*
 2017 and the *To Party MSH* each set an independent **SequenceNumber** as the *Sending MSH* within the
 2018 **ConversationId**. It is set to zero on the first message from that MSH within a conversation and then
 2019 incremented by one for each subsequent message sent.

2020 A MSH that receives a message with a **SequenceNumber** element MUST NOT pass the message to an
 2021 application until all the messages with a lower **SequenceNumber** have been passed to the application.

2022 If the implementation defined limit for saved out-of-sequence messages is reached, then the *Receiving*
 2023 *MSH* MUST indicate a delivery failure to the *Sending MSH* with **errorCode** set to **DeliveryFailure** and
 2024 **severity** set to **Error** (see section 4.1.5).

2025 The **SequenceNumber** element is an integer value incremented by the *Sending MSH* (e.g. 0, 1, 2, 3, 4...)
 2026 for each application-prepared message sent by that MSH within the **ConversationId**. The next value after
 2027 99999999 in the increment is "0". The value of **SequenceNumber** consists of ASCII numerals in the
 2028 range 0-99999999. In following cases, **SequenceNumber** takes the value "0":

- 2029 1. First message from the *Sending MSH* within the conversation
- 2030 2. First message after resetting **SequenceNumber** information by the *Sending MSH*
- 2031 3. First message after wraparound (next value after 99999999)

2032 The **SequenceNumber** element has a single attribute, **status**. This attribute is an enumeration, which
 2033 SHALL have one of the following values:

- 2034 • **Reset** – the **SequenceNumber** is reset as shown in 1 or 2 above
- 2035 • **Continue** – the **SequenceNumber** continues sequentially (including 3 above)

2036 When the **SequenceNumber** is set to "0" because of 1 or 2 above, the *Sending MSH* MUST set the
 2037 **status** attribute of the message to **Reset**. In all other cases, including 3 above, the **status** attribute
 2038 MUST be set to **Continue**. The default value of the **status** attribute is **Continue**.

2039 A *Sending MSH* MUST wait before resetting the **SequenceNumber** of a conversation until it has received
 2040 confirmation of all the messages previously sent for the conversation. Only when all the sent Messages
 2041 are accounted for, can the *Sending MSH* reset the **SequenceNumber**.

2042 9.1.2 MessageOrder Sample

2043 An example of the **MessageOrder** element is given below:

```
2044 <eb:MessageOrder eb:version="2.0" SOAP:mustUnderstand="1">
2045   <eb:SequenceNumber>00000010</eb:SequenceNumber>
2046 </eb:MessageOrder>
```

2047 9.2 MessageOrder Element Interaction

2048 For this version of the ebXML Messaging Specification, the **MessageOrder** element MUST NOT be
 2049 present with the **SyncReply** element. If these two elements are received in the same message, the
 2050 *Receiving MSH* SHOULD report an error (see section 4.1.5) with **errorCode** set to **Inconsistent** and
 2051 **severity** set to **Error**.

2052 10 Multi-Hop Module

2053 Multi-hop is the process of passing the message through one or more intermediary nodes or MSH's. An
 2054 Intermediary is any node or MSH where the message is received, but is not the *Sending* or *Receiving*
 2055 *MSH*. This node is called an Intermediary.

2056 Intermediaries may be for the purpose of Store-and-Forward or may be involved in some processing
 2057 activity such as a trusted third-party timestamp service. For the purposes of this version of this
 2058 specification, Intermediaries are considered only as Store-and-Forward entities.

2059 Intermediaries MAY be involved in removing and adding SOAP extension elements or modules targeted
 2060 either to the **Next** SOAP node or the **NextMSH**. SOAP rules specify, the receiving node must remove
 2061 any element or module targeted to the **Next** SOAP node. If the element or module needs to continue to
 2062 appear on the SOAP message destined to the **Next** SOAP node, or in this specification the **NextMSH**, it
 2063 must be reapplied. This deleting and adding of elements or modules poses potential difficulties for signed
 2064 ebXML messages. Any Intermediary node or MSH MUST NOT change, format or in any way modify any
 2065 element not targeted to the Intermediary. Any such change may invalidate the signature.

2066 10.1 Multi-hop Reliable Messaging

2067 Multi-hop (hop-to-hop) Reliable Messaging is accomplished using the **AckRequested** element (section
2068 6.3.1) and an **Acknowledgment Message** containing an **Acknowledgment** element (section 6.3.1.4) each
2069 with a SOAP **actor** of **Next MSH** (section 2.3.10) between the **Sending MSH** and the **Receiving MSH**.
2070 This MAY be used in store-and-forward multi-hop situations.

2071 The use of the duplicate elimination is not required for Intermediate nodes. Since duplicate elimination by
2072 an intermediate MSH can interfere with End-to-End Reliable Messaging Retries, the intermediate MSH
2073 MUST know it is an intermediate and MUST NOT perform duplicate elimination tasks.

2074 At this time, the values of **Retry** and **RetryInterval** between Intermediate MSHs remains implementation
2075 specific. See section 6.4 for more detail on Reliable Messaging.

2076 10.1.1 AckRequested Sample

2077 An example of the **AckRequested** element targeted at the **NextMSH** is given below:

```
2078 <eb:AckRequested SOAP:mustUnderstand="1" eb:version="2.0" eb:signed="false"  
2079 SOAP:actor="urn:oasis:names:tc:ebxml-msg:actor:nextMSH"/>
```

2080 In the preceding example, an **Acknowledgment Message** is requested of the next ebXML MSH node (see
2081 section 2.3.10) in the message. The **Acknowledgment** element generated MUST be targeted at the next
2082 ebXML MSH node along the reverse message path (the **Sending MSH**) using the SOAP **actor** with a
2083 value of **NextMSH** (section 2.3.10).

2084 Any Intermediary receiving an **AckRequested** with SOAP **actor** of **NextMSH** MUST remove the
2085 **AckRequested** element before forwarding to the next MSH. Any Intermediary MAY insert a single
2086 **AckRequested** element into the SOAP **Header** with a SOAP **actor** of **NextMSH**. There SHALL NOT be
2087 two **AckRequested** elements targeted at the next MSH.

2088 When the **SyncReply** element is present, an **AckRequested** element with SOAP **actor** of **NextMSH**
2089 MUST NOT be present. If the **SyncReply** element is not present, the Intermediary MAY return the
2090 Intermediate **Acknowledgment Message** synchronously with a synchronous transport protocol. If these
2091 two elements are received in the same message, the **Receiving MSH** SHOULD report an error (see
2092 section 4.1.5) with **errorCode** set to **Inconsistent** and **severity** set to **Error**.

2093 10.1.2 Acknowledgment Sample

2094 An example of the **Acknowledgment** element targeted at the **NextMSH** is given below:

```
2095 <eb:Acknowledgment SOAP:mustUnderstand="1" eb:version="2.0"  
2096 SOAP:actor="urn:oasis:names:tc:ebxml-msg:actor:nextMSH">  
2097 <eb:Timestamp>2001-03-09T12:22:30</eb:Timestamp>  
2098 <eb:RefToMessageId>323210:e52151ec74:-7ffc@xtacy</eb:RefToMessageId>  
2099 <eb:From> <eb:PartyId>uri:www.example.com</eb:PartyId> </eb:From>  
2100 </eb:Acknowledgment>
```

2101 10.1.3 Multi-Hop Acknowledgments

2102 There MAY be two **AckRequested** elements on the same message. An **Acknowledgment** MUST be
2103 sent for each **AckRequested** using an identical SOAP **actor** attribute as the **AckRequested** element.

2104 If the **Receiving MSH** is the **To Party MSH**, then see section 6.5.2. If the **Receiving MSH** is the **To Party**
2105 **MSH** and there is an **AckRequested** element targeting the Next MSH (the **To Party MSH** is acting in both
2106 roles), then perform both procedures (this section and section 6.5.2) for generating **Acknowledgment**
2107 **Messages**. This MAY require sending two **Acknowledgment** elements, possibly on the same message,
2108 one targeted for the **Next MSH** and one targeted for the **To Party MSH**.

2109 There MAY be multiple **Acknowledgements** elements, on the same message or on different messages,
2110 returning from either the Next MSH or from the **To Party MSH**. A MSH supporting Multi-hop MUST
2111 differentiate, based upon the **actor**, which **Acknowledgment** is being returned and act accordingly.

2112 If this is an **Acknowledgment Message** as defined in section 6 then:

- 2113 1 Look for a message in *persistent storage* with a **MessageId** the same as the value of
2114 **RefToMessageId** on the received Message.
- 2115 2 If a message is found in *persistent storage* then mark the persisted message as delivered.

2116 If an **AckRequested** element is present (not an *Acknowledgment Message*) then generate an
2117 *Acknowledgment Message* in response (this may be as part of another message). The *Receiving MSH*
2118 MUST NOT send an *Acknowledgment Message* until the message has been persisted or delivered to the
2119 *Next MSH*.

2120 **10.1.4 Signing Multi-Hop Acknowledgments**

2121 When a signed Intermediate *Acknowledgment Message* is requested (i.e. a signed *Acknowledgment*
2122 *Message* with a SOAP **actor** of *NextMSH*), it MUST be sent by itself and not bundled with any other
2123 message. The XML Signature [XMLDSIG] **Signature** element with **Transforms**, as described in section
2124 4.1.3, will exclude this **Acknowledgment** element. To send a signed *Acknowledgment Message* with
2125 SOAP **actor** of *NextMSH*, create a message with no payloads, including a single **Acknowledgment**
2126 element (see section 6.3.2.6), and a [XMLDSIG] **Signature** element with the following **Transforms**:

```
2127           <Transforms>
2128             <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
2129             <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
2130           </Transforms>
```

2131 **10.1.5 Multi-Hop Security Considerations**

2132 SOAP messaging allows intermediaries to add or remove elements targeted to the intermediary node.
2133 This has potential conflicts with end-to-end signatures since the slightest change in any character of the
2134 SOAP **Envelope** or to a payload will invalidate the **ds:Signature** by changing the calculated digest.
2135 Intermediaries MUST NOT add or remove elements unless they contain a SOAP **actor** of *next* or
2136 *nextMSH*. Intermediaries MUST NOT disturb white space – line terminators (CR/LF), tabs, spaces, etc. –
2137 outside those elements being added or removed.

2138 **10.2 Message Ordering and Multi-Hop**

2139 Intermediary MSH nodes MUST NOT participate in Message Order processing as specified in section 9.

2140

Part III. Normative Appendices

2141 Appendix A The ebXML SOAP Extension Elements Schema

2142 The OASIS ebXML Messaging Technical Committee has provided a version of the SOAP 1.1 envelope
2143 schema specified using the schema vocabulary that conforms to the W3C XML Schema
2144 Recommendation specification [XMLSchema].

2145 SOAP1.1- <http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd>

2146 It was necessary to craft a schema for the XLINK [XLINK] attribute vocabulary to conform to the W3C
2147 XML Schema Recommendation [XMLSchema]. This schema is referenced from the ebXML SOAP
2148 extension elements schema and is available from the following URL:

2149 Xlink - <http://www.oasis-open.org/committees/ebxml-msg/schema/xlink.xsd>

```

2150 <?xml version="1.0" encoding="UTF-8"?>
2151 <!-- Some parsers may require explicit declaration of xmlns:xml="http://www.w3.org/XML/1998/namespace".
2152      In that case, a copy of this schema augmented with the above declaration should be cached and used
2153      for the purpose of schema validation on ebXML messages. -->
2154 <schema targetNamespace="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2155       xmlns:tns="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2156       xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2157       xmlns:xlink="http://www.w3.org/1999/xlink"
2158       xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
2159       xmlns="http://www.w3.org/2001/XMLSchema"
2160       elementFormDefault="qualified"
2161       attributeFormDefault="qualified"
2162       version="2.0">
2163   <import namespace="http://www.w3.org/2000/09/xmldsig#"
2164     schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
2165   <import namespace="http://www.w3.org/1999/xlink"
2166     schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/xlink.xsd"/>
2167   <import namespace="http://schemas.xmlsoap.org/soap/envelope/"
2168     schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd"/>
2169   <import namespace="http://www.w3.org/XML/1998/namespace"
2170     schemaLocation="http://www.w3.org/2001/03/xml.xsd"/>
2171   <!-- MANIFEST, for use in soap:Body element -->
2172   <element name="Manifest">
2173     <complexType>
2174       <sequence>
2175         <element ref="tns:Reference" maxOccurs="unbounded"/>
2176         <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2177       </sequence>
2178       <attributeGroup ref="tns:bodyExtension.grp"/>
2179     </complexType>
2180   </element>
2181   <element name="Reference">
2182     <complexType>
2183       <sequence>
2184         <element ref="tns:Schema" minOccurs="0" maxOccurs="unbounded"/>
2185         <element ref="tns:Description" minOccurs="0" maxOccurs="unbounded"/>
2186         <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2187       </sequence>
2188       <attribute ref="tns:id"/>
2189       <attribute ref="xlink:type" fixed="simple"/>
2190       <attribute ref="xlink:href" use="required"/>
2191       <attribute ref="xlink:role"/>
2192       <anyAttribute namespace="##other" processContents="lax"/>
2193     </complexType>
2194   </element>
2195   <element name="Schema">
2196     <complexType>
2197       <attribute name="location" type="anyURI" use="required"/>
2198       <attribute name="version" type="tns:non-empty-string"/>
2199     </complexType>

```

```

2200 </element>
2201 <!-- MESSAGEHEADER, for use in soap:Header element -->
2202 <element name="MessageHeader">
2203   <complexType>
2204     <sequence>
2205       <element ref="tns:From"/>
2206       <element ref="tns:To"/>
2207       <element ref="tns:CPAId"/>
2208       <element ref="tns:ConversationId"/>
2209       <element ref="tns:Service"/>
2210       <element ref="tns:Action"/>
2211       <element ref="tns:MessageData"/>
2212       <element ref="tns:DuplicateElimination" minOccurs="0"/>
2213       <element ref="tns:Description" minOccurs="0" maxOccurs="unbounded"/>
2214       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2215     </sequence>
2216     <attributeGroup ref="tns:headerExtension.grp"/>
2217   </complexType>
2218 </element>
2219 <element name="CPAId" type="tns:non-empty-string"/>
2220 <element name="ConversationId" type="tns:non-empty-string"/>
2221 <element name="Service">
2222   <complexType>
2223     <simpleContent>
2224       <extension base="tns:non-empty-string">
2225         <attribute name="type" type="tns:non-empty-string"/>
2226       </extension>
2227     </simpleContent>
2228   </complexType>
2229 </element>
2230 <element name="Action" type="tns:non-empty-string"/>
2231 <element name="MessageData">
2232   <complexType>
2233     <sequence>
2234       <element ref="tns:MessageId"/>
2235       <element ref="tns:Timestamp"/>
2236       <element ref="tns:RefToMessageId" minOccurs="0"/>
2237       <element ref="tns:TimeToLive" minOccurs="0"/>
2238     </sequence>
2239   </complexType>
2240 </element>
2241 <element name="MessageId" type="tns:non-empty-string"/>
2242 <element name="TimeToLive" type="dateTime"/>
2243 <element name="DuplicateElimination">
2244 </element>
2245 <!-- SYNC REPLY, for use in soap:Header element -->
2246 <element name="SyncReply">
2247   <complexType>
2248     <sequence>
2249       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2250     </sequence>
2251     <attributeGroup ref="tns:headerExtension.grp"/>
2252     <attribute ref="soap:actor" use="required"/>
2253   </complexType>
2254 </element>
2255 <!-- MESSAGE ORDER, for use in soap:Header element -->
2256 <element name="MessageOrder">
2257   <complexType>
2258     <sequence>
2259       <element ref="tns:SequenceNumber"/>
2260       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2261     </sequence>
2262     <attributeGroup ref="tns:headerExtension.grp"/>
2263   </complexType>
2264 </element>
2265 <element name="SequenceNumber" type="tns:sequenceNumber.type"/>
2266 <!-- ACK REQUESTED, for use in soap:Header element -->
2267 <element name="AckRequested">
2268   <complexType>
2269     <sequence>
2270       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

```

```

2271     </sequence>
2272     <attributeGroup ref="tns:headerExtension.grp"/>
2273     <attribute ref="soap:actor"/>
2274     <attribute name="signed" type="boolean" use="required"/>
2275   </complexType>
2276 </element>
2277 <!-- ACKNOWLEDGMENT, for use in soap:Header element -->
2278 <element name="Acknowledgment">
2279   <complexType>
2280     <sequence>
2281       <element ref="tns:Timestamp"/>
2282       <element ref="tns:RefToMessageId"/>
2283       <element ref="tns:From" minOccurs="0"/>
2284       <element ref="ds:Reference" minOccurs="0" maxOccurs="unbounded"/>
2285       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2286     </sequence>
2287     <attributeGroup ref="tns:headerExtension.grp"/>
2288     <attribute ref="soap:actor"/>
2289   </complexType>
2290 </element>
2291 <!-- ERROR LIST, for use in soap:Header element -->
2292 <element name="ErrorList">
2293   <complexType>
2294     <sequence>
2295       <element ref="tns:Error" maxOccurs="unbounded"/>
2296       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2297     </sequence>
2298     <attributeGroup ref="tns:headerExtension.grp"/>
2299     <attribute name="highestSeverity" type="tns:severity.type" use="required"/>
2300   </complexType>
2301 </element>
2302 <element name="Error">
2303   <complexType>
2304     <sequence>
2305       <element ref="tns:Description" minOccurs="0"/>
2306       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2307     </sequence>
2308     <attribute ref="tns:id"/>
2309     <attribute name="codeContext" type="anyURI"
2310       default="urn:oasis:names:tc:ebxml-msg:service:errors"/>
2311     <attribute name="errorCode" type="tns:non-empty-string" use="required"/>
2312     <attribute name="severity" type="tns:severity.type" use="required"/>
2313     <attribute name="location" type="tns:non-empty-string"/>
2314     <anyAttribute namespace="##other" processContents="lax"/>
2315   </complexType>
2316 </element>
2317 <!-- STATUS RESPONSE, for use in soap:Body element -->
2318 <element name="StatusResponse">
2319   <complexType>
2320     <sequence>
2321       <element ref="tns:RefToMessageId"/>
2322       <element ref="tns:Timestamp" minOccurs="0"/>
2323       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2324     </sequence>
2325     <attributeGroup ref="tns:bodyExtension.grp"/>
2326     <attribute name="messageStatus" type="tns:messageStatus.type" use="required"/>
2327   </complexType>
2328 </element>
2329 <!-- STATUS REQUEST, for use in soap:Body element -->
2330 <element name="StatusRequest">
2331   <complexType>
2332     <sequence>
2333       <element ref="tns:RefToMessageId"/>
2334       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2335     </sequence>
2336     <attributeGroup ref="tns:bodyExtension.grp"/>
2337   </complexType>
2338 </element>
2339 <!-- COMMON TYPES -->
2340 <complexType name="sequenceNumber.type">
2341   <simpleContent>

```

```

2342     <extension base="nonNegativeInteger">
2343         <attribute name="status" type="tns:status.type" default="Continue"/>
2344     </extension>
2345 </simpleContent>
2346 </complexType>
2347 <simpleType name="status.type">
2348     <restriction base="NMTOKEN">
2349         <enumeration value="Reset"/>
2350         <enumeration value="Continue"/>
2351     </restriction>
2352 </simpleType>
2353 <simpleType name="messageStatus.type">
2354     <restriction base="NMTOKEN">
2355         <enumeration value="Unauthorized"/>
2356         <enumeration value="NotRecognized"/>
2357         <enumeration value="Received"/>
2358         <enumeration value="Processed"/>
2359         <enumeration value="Forwarded"/>
2360     </restriction>
2361 </simpleType>
2362 <simpleType name="non-empty-string">
2363     <restriction base="string">
2364         <minLength value="1"/>
2365     </restriction>
2366 </simpleType>
2367 <simpleType name="severity.type">
2368     <restriction base="NMTOKEN">
2369         <enumeration value="Warning"/>
2370         <enumeration value="Error"/>
2371     </restriction>
2372 </simpleType>
2373 <!-- COMMON ATTRIBUTES and ATTRIBUTE GROUPS -->
2374 <attribute name="id" type="ID"/>
2375 <attribute name="version" type="tns:non-empty-string"/>
2376 <attributeGroup name="headerExtension.grp">
2377     <attribute ref="tns:id"/>
2378     <attribute ref="tns:version" use="required"/>
2379     <attribute ref="soap:mustUnderstand" use="required"/>
2380     <anyAttribute namespace="##other" processContents="lax"/>
2381 </attributeGroup>
2382 <attributeGroup name="bodyExtension.grp">
2383     <attribute ref="tns:id"/>
2384     <attribute ref="tns:version" use="required"/>
2385     <anyAttribute namespace="##other" processContents="lax"/>
2386 </attributeGroup>
2387 <!-- COMMON ELEMENTS -->
2388 <element name="PartyId">
2389     <complexType>
2390         <simpleContent>
2391             <extension base="tns:non-empty-string">
2392                 <attribute name="type" type="tns:non-empty-string"/>
2393             </extension>
2394         </simpleContent>
2395     </complexType>
2396 </element>
2397 <element name="To">
2398     <complexType>
2399         <sequence>
2400             <element ref="tns:PartyId" maxOccurs="unbounded"/>
2401             <element name="Role" type="tns:non-empty-string" minOccurs="0"/>
2402         </sequence>
2403     </complexType>
2404 </element>
2405 <element name="From">
2406     <complexType>
2407         <sequence>
2408             <element ref="tns:PartyId" maxOccurs="unbounded"/>
2409             <element name="Role" type="tns:non-empty-string" minOccurs="0"/>
2410         </sequence>
2411     </complexType>
2412 </element>

```



```
2413 <element name="Description">
2414   <complexType>
2415     <simpleContent>
2416       <extension base="tns:non-empty-string">
2417         <attribute ref="xml:lang" use="required"/>
2418       </extension>
2419     </simpleContent>
2420   </complexType>
2421 </element>
2422 <element name="RefToMessageId" type="tns:non-empty-string"/>
2423 <element name="Timestamp" type="dateTime"/>
2424 </schema>
```

2425

2425 Appendix B Communications Protocol Bindings

2426 B.1 Introduction

2427 One of the goals of this specification is to design a message handling service usable over a variety of
2428 network and application level transport protocols. These protocols serve as the "carrier" of ebXML
2429 Messages and provide the underlying services necessary to carry out a complete ebXML Message
2430 exchange between two parties. HTTP, FTP, Java Message Service (JMS) and SMTP are examples of
2431 application level transport protocols. TCP and SNA/LU6.2 are examples of network transport protocols.
2432 Transport protocols vary in their support for data content, processing behavior and error handling and
2433 reporting. For example, it is customary to send binary data in raw form over HTTP. However, in the case
2434 of SMTP it is customary to "encode" binary data into a 7-bit representation. HTTP is equally capable of
2435 carrying out *synchronous* or *asynchronous* message exchanges whereas it is likely that message
2436 exchanges occurring over SMTP will be *asynchronous*. This section describes the technical details
2437 needed to implement this abstract ebXML Message Handling Service over particular transport protocols.

2438 This section specifies communications protocol bindings and technical details for carrying *ebXML*
2439 *Message Service* messages for the following communications protocols:

- 2440 • Hypertext Transfer Protocol [RFC2616], in both *asynchronous* and *synchronous* forms of transfer.
- 2441 • Simple Mail Transfer Protocol [RFC2821], in *asynchronous* form of transfer only.

2442 B.2 HTTP

2443 B.2.1 Minimum level of HTTP protocol

2444 Hypertext Transfer Protocol Version 1.1 [RFC2616] is the minimum level of protocol that **MUST** be used.

2445 B.2.2 Sending ebXML Service messages over HTTP

2446 Even though several HTTP request methods are available, this specification only defines the use of HTTP
2447 POST requests for sending *ebXML Message Service* messages over HTTP. The identity of the ebXML
2448 MSH (e.g. ebxmlhandler) may be part of the HTTP POST request:

```
2449 POST /ebxmlhandler HTTP/1.1
```

2450 Prior to sending over HTTP, an ebXML Message **MUST** be formatted according to ebXML Message
2451 Service Specification. Additionally, the messages **MUST** conform to the HTTP specific MIME canonical
2452 form constraints specified in section 19.4 of RFC 2616 [RFC2616] specification.

2453 HTTP protocol natively supports 8-bit and Binary data. Hence, transfer encoding is **OPTIONAL** for such
2454 parts in an ebXML Service Message prior to sending over HTTP. However, content-transfer-encoding of
2455 such parts (e.g. using base64 encoding scheme) is not precluded by this specification.

2456 The rules for forming an HTTP message containing an ebXML Service Message are as follows:

- 2457 • The **Content-Type: Multipart/Related** MIME header with the associated parameters, from the
2458 ebXML Service Message Envelope **MUST** appear as an HTTP header.
- 2459 • All other MIME headers that constitute the ebXML Message Envelope **MUST** also become part of the HTTP
2460 header.
- 2461 • The mandatory `SOAPAction` HTTP header field must also be included in the HTTP header and **MAY** have
2462 a value of "ebXML"

```
2463 SOAPAction: "ebXML"
```

- 2464 • Other headers with semantics defined by MIME specifications, such as Content-Transfer-Encoding, **SHALL**
2465 **NOT** appear as HTTP headers. Specifically, the "MIME-Version: 1.0" header **MUST NOT** appear as an
2466 HTTP header. However, HTTP-specific MIME-like headers defined by HTTP 1.1 **MAY** be used with the
2467 semantic defined in the HTTP specification.

- All ebXML Service Message parts that follow the ebXML Message Envelope, including the MIME boundary string, constitute the HTTP entity body. This encompasses the SOAP **Envelope** and the constituent ebXML parts and attachments including the trailing MIME boundary strings.

The example below shows an example instance of an HTTP POST ebXML Service Message:

```

2472 POST /servlet/ebXMLhandler HTTP/1.1
2473 Host: www.example2.com
2474 SOAPAction: "ebXML"
2475 Content-type: multipart/related; boundary="BoundaryY"; type="text/xml";
2476         start="<ebxmhheader111@example.com>"
2477
2478 --BoundaryY
2479 Content-ID: <ebxmhheader111@example.com>
2480 Content-Type: text/xml
2481
2482 <?xml version="1.0" encoding="UTF-8"?>
2483 <SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
2484     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
2485     xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
2486     xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2487     xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
2488         http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
2489         http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
2490         http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
2491 <SOAP:Header>
2492   <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
2493     <eb:From>
2494       <eb:PartyId>urn:duns:123456789</eb:PartyId>
2495     </eb:From>
2496     <eb:To>
2497       <eb:PartyId>urn:duns:912345678</eb:PartyId>
2498     </eb:To>
2499     <eb:CPAId>20001209-133003-28572</eb:CPAId>
2500     <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
2501     <eb:Service>urn:services:SupplierOrderProcessing</eb:Service>
2502     <eb:Action>NewOrder</eb:Action>
2503     <eb:MessageData>
2504       <eb:MessageId>20001209-133003-28572@example.com</eb:MessageId>
2505       <eb:Timestamp>2001-02-15T11:12:12</eb:Timestamp>
2506     </eb:MessageData>
2507   </eb:MessageHeader>
2508 </SOAP:Header>
2509 <SOAP:Body>
2510   <eb:Manifest eb:version="2.0">
2511     <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
2512       xlink:role="XLinkRole" xlink:type="simple">
2513       <eb:Description xml:lang="en-US">Purchase Order 1</eb:Description>
2514     </eb:Reference>
2515   </eb:Manifest>
2516 </SOAP:Body>
2517 </SOAP:Envelope>
2518
2519 --BoundaryY
2520 Content-ID: <ebxmlpayload111@example.com>
2521 Content-Type: text/xml
2522
2523 <?xml version="1.0" encoding="UTF-8"?>
2524 <purchase_order>
2525   <po_number>1</po_number>
2526   <part_number>123</part_number>
2527   <price currency="USD">500.00</price>
2528 </purchase_order>
2529
2530 --BoundaryY--

```

2531 B.2.3 HTTP Response Codes

2532 In general, semantics of communicating over HTTP as specified in the [RFC2616] MUST be followed, for
 2533 returning the HTTP level response codes. A 2xx code MUST be returned when the HTTP Posted

2534 message is successfully received by the receiving HTTP entity. However, see exception for SOAP error
2535 conditions below. Similarly, other HTTP codes in the 3xx, 4xx, 5xx range MAY be returned for conditions
2536 corresponding to them. However, error conditions encountered while processing an ebXML Service
2537 Message MUST be reported using the error mechanism defined by the ebXML Message Service
2538 Specification (see section 4.1.5).

2539 **B.2.4 SOAP Error conditions and Synchronous Exchanges**

2540 The SOAP 1.1 specification states:

2541 *"In case of a SOAP error while processing the request, the SOAP HTTP server MUST issue an HTTP*
2542 *500 "Internal Server Error" response and include a SOAP message in the response containing a SOAP*
2543 *Fault element indicating the SOAP processing error. "*

2544 However, the scope of the SOAP 1.1 specification is limited to *synchronous* mode of message exchange
2545 over HTTP, whereas the ebXML Message Service Specification specifies both *synchronous* and
2546 *asynchronous* modes of message exchange over HTTP. Hence, the SOAP 1.1 specification MUST be
2547 followed for *synchronous* mode of message exchange, where the SOAP *Message* containing a SOAP
2548 **Fault** element indicating the SOAP processing error MUST be returned in the HTTP response with a
2549 response code of "HTTP 500 Internal Server Error". When *asynchronous* mode of message exchange is
2550 being used, a HTTP response code in the range 2xx MUST be returned when the message is received
2551 successfully and any error conditions (including SOAP errors) must be returned via separate HTTP Post.

2552 **B.2.5 Synchronous vs. Asynchronous**

2553 When a synchronous transport is in use, the MSH response message(s) SHOULD be returned on the
2554 same HTTP connection as the inbound request, with an appropriate HTTP response code, as described
2555 above. When the **syncReplyMode** parameter is set to values other than **none**, the application response
2556 messages, if any, are also returned on the same HTTP connection as the inbound request, rather than
2557 using an independent HTTP Post request. If the **syncReplyMode** has a value of **none**, an HTTP
2558 response with a response code as defined in section B.2.3 above and with an empty HTTP body MUST
2559 be returned in response to the HTTP Post.

2560 **B.2.6 Access Control**

2561 Implementers MAY protect their ebXML Message Service Handlers from unauthorized access through the
2562 use of an access control mechanism. The HTTP access authentication process described in "HTTP
2563 Authentication: Basic and Digest Access Authentication" [RFC2617] defines the access control
2564 mechanisms allowed to protect an ebXML Message Service Handler from unauthorized access.

2565 Implementers MAY support all of the access control schemes defined in [RFC2617] including support of
2566 the Basic Authentication mechanism, as described in [RFC2617] section 2, when Access Control is used.

2567 Implementers that use basic authentication for access control SHOULD also use communications
2568 protocol level security, as specified in the section titled "Confidentiality and Transport Protocol Level
2569 Security" in this document.

2570 **B.2.7 Confidentiality and Transport Protocol Level Security**

2571 An ebXML Message Service Handler MAY use transport layer encryption to protect the confidentiality of
2572 ebXML Messages and HTTP transport headers. The IETF Transport Layer Security specification TLS
2573 [RFC2246] provides the specific technical details and list of allowable options, which may be used by
2574 ebXML Message Service Handlers. ebXML Message Service Handlers MUST be capable of operating in
2575 backwards compatibility mode with SSL [SSL3], as defined in Appendix E of TLS [RFC2246].

2576 ebXML Message Service Handlers MAY use any of the allowable encryption algorithms and key sizes
2577 specified within TLS [RFC2246]. At a minimum ebXML Message Service Handlers MUST support the key
2578 sizes and algorithms necessary for backward compatibility with [SSL3].

2579 The use of 40-bit encryption keys/algorithms is permitted, however it is RECOMMENDED that stronger
2580 encryption keys/algorithms SHOULD be used.

2581 Both TLS [RFC2246] and SSL [SSL3] require the use of server side digital certificates. Client side
2582 certificate based authentication is also permitted. All ebXML Message Service handlers MUST support
2583 hierarchical and peer-to-peer or direct-trust trust models.

2584 **B.3 SMTP**

2585 The Simple Mail Transfer Protocol (SMTP) [RFC2821] specification is commonly referred to as Internet
2586 Electronic Mail. This specifications has been augmented over the years by other specifications, which
2587 define additional functionality "layered on top" of this baseline specifications. These include:

2588 Multipurpose Internet Mail Extensions (MIME) [RFC2045], [RFC2046], [RFC2387]

2589 SMTP Service Extension for Authentication [RFC2554]

2590 SMTP Service Extension for Secure SMTP over TLS [RFC2487]

2591 Typically, Internet Electronic Mail Implementations consist of two "agent" types:

2592 Message Transfer Agent (MTA): Programs that send and receive mail messages with other MTA's on
2593 behalf of MUA's. Microsoft Exchange Server is an example of a MTA

2594 Mail User Agent (MUA): Electronic Mail programs are used to construct electronic mail messages and
2595 communicate with an MTA to send/retrieve mail messages. Microsoft Outlook is an example of a MUA.

2596 MTA's often serve as "mail hubs" and can typically service hundreds or more MUA's.

2597 MUA's are responsible for constructing electronic mail messages in accordance with the Internet
2598 Electronic Mail Specifications identified above. This section describes the "binding" of an ebXML
2599 compliant message for transport via eMail from the perspective of a MUA. No attempt is made to define
2600 the binding of an ebXML Message exchange over SMTP from the standpoint of a MTA.

2601 **B.3.1 Minimum Level of Supported Protocols**

2602 Simple Mail Transfer Protocol [RFC2821]

2603 MIME [RFC2045] and [RFC2046]

2604 Multipart/Related MIME [RFC2387]

2605 **B.3.2 Sending ebXML Messages over SMTP**

2606 Prior to sending messages over SMTP an ebXML Message MUST be formatted according to the ebXML
2607 Message Service Specification. Additionally the messages must also conform to the syntax, format and
2608 encoding rules specified by MIME [RFC2045], [RFC2046] and [RFC2387].

2609 Many types of data that a party might desire to transport via email are represented as 8bit characters or
2610 binary data. Such data cannot be transmitted over SMTP [RFC2821], which restricts mail messages to
2611 7bit US-ASCII data with lines no longer than 1000 characters including any trailing CRLF line separator. If
2612 a sending Message Service Handler knows that a receiving MTA, or ANY intermediary MTA's, are
2613 restricted to handling 7-bit data then any document part that uses 8 bit (or binary) representation must be
2614 "transformed" according to the encoding rules specified in section 6 of MIME [RFC2045]. In cases where
2615 a Message Service Handler knows that a receiving MTA and ALL intermediary MTA's are capable of
2616 handling 8-bit data then no transformation is needed on any part of the ebXML Message.

2617 The rules for forming an ebXML Message for transport via SMTP are as follows:

- 2618 • If using SMTP [RFC2821] restricted transport paths, apply transfer encoding to all 8-bit data that will be
2619 transported in an ebXML message, according to the encoding rules defined in section 6 of MIME
2620 [RFC2045]. The Content-Transfer-Encoding MIME header MUST be included in the MIME envelope portion
2621 of any body part that has been transformed (encoded).

- 2622 • The Content-Type: Multipart/Related MIME header with the associated parameters, from the
2623 ebXML Message Envelope MUST appear as an eMail MIME header.
- 2624 • All other MIME headers that constitute the ebXML Message Envelope MUST also become part of the eMail
2625 MIME header.
- 2626 • The SOAPAction MIME header field must also be included in the eMail MIME header and MAY have the
2627 value of ebXML:
2628 SOAPAction: "ebXML"
- 2629 • The "MIME-Version: 1.0" header must appear as an eMail MIME header.
- 2630 • The eMail header "To:" MUST contain the SMTP [RFC2821] compliant eMail address of the ebXML
2631 Message Service Handler.
- 2632 • The eMail header "From:" MUST contain the SMTP [RFC2821] compliant eMail address of the senders
2633 ebXML Message Service Handler.
- 2634 • Construct a "Date:" eMail header in accordance with SMTP [RFC2821]
- 2635 • Other headers MAY occur within the eMail message header in accordance with SMTP [RFC2821] and
2636 MIME [RFC2045], however ebXML Message Service Handlers MAY choose to ignore them.

2637 The example below shows a minimal example of an eMail message containing an ebXML Message:

```

2638 From: ebXMLhandler@example.com
2639 To: ebXMLhandler@example2.com
2640 Date: Thu, 08 Feb 2001 19:32:11 CST
2641 MIME-Version: 1.0
2642 SOAPAction: "ebXML"
2643 Content-type: multipart/related; boundary="Boundary"; type="text/xml";
2644 start="<ebxhmheader111@example.com>"
2645
2646 This is an ebXML SMTP Example
2647
2648 --Boundary
2649 Content-ID: <ebxhmheader111@example.com>
2650 Content-Type: text/xml
2651
2652 <?xml version="1.0" encoding="UTF-8"?>
2653 <SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
2654 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
2655 xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
2656 xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
2657 http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
2658 <SOAP:Header xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2659 xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
2660 http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
2661 <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
2662 <eb:From>
2663 <eb:PartyId>urn:duns:123456789</eb:PartyId>
2664 </eb:From>
2665 <eb:To>
2666 <eb:PartyId>urn:duns:912345678</eb:PartyId>
2667 </eb:To>
2668 <eb:CPAId>20001209-133003-28572</eb:CPAId>
2669 <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
2670 <eb:Service>urn:services:SupplierOrderProcessing</eb:Service>
2671 <eb:Action>NewOrder</eb:Action>
2672 <eb:MessageData>
2673 <eb:MessageId>20001209-133003-28572@example.com</eb:MessageId>
2674 <eb:Timestamp>2001-02-15T11:12:12</eb:Timestamp>
2675 </eb:MessageData>
2676 <eb:DuplicateElimination/>
2677 </eb:MessageHeader>
2678 </SOAP:Header>
2679 <SOAP:Body xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2680 xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
2681 http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
2682 <eb:Manifest eb:version="2.0">
2683 <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
2684 xlink:role="XLinkRole"
2685 xlink:type="simple">

```

```

2686     <eb:Description xml:lang="en-US">Purchase Order 1</eb:Description>
2687     </eb:Reference>
2688     </eb:Manifest>
2689 </SOAP:Body>
2690 </SOAP:Envelope>
2691
2692 --Boundary
2693 Content-ID: <ebxhmheader111@example.com>
2694 Content-Type: text/xml
2695
2696 <?xml version="1.0" encoding="UTF-8"?>
2697 <purchase_order>
2698   <po_number>1</po_number>
2699   <part_number>123</part_number>
2700   <price currency="USD">500.00</price>
2701 </purchase_order>
2702
2703 --Boundary--

```

2704 **B.3.3 Response Messages**

2705 All ebXML response messages, including errors and acknowledgments, are delivered *asynchronously*
 2706 between ebXML Message Service Handlers. Each response message MUST be constructed in
 2707 accordance with the rules specified in the section B.3.2.

2708 All ebXML Message Service Handlers MUST be capable of receiving a delivery failure notification
 2709 message sent by an MTA. A MSH that receives a delivery failure notification message SHOULD examine
 2710 the message to determine which ebXML message, sent by the MSH, resulted in a message delivery
 2711 failure. The MSH SHOULD attempt to identify the application responsible for sending the offending
 2712 message causing the failure. The MSH SHOULD attempt to notify the application that a message
 2713 delivery failure has occurred. If the MSH is unable to determine the source of the offending message the
 2714 MSH administrator should be notified.

2715 MSH's which cannot identify a received message as a valid ebXML message or a message delivery
 2716 failure SHOULD retain the unidentified message in a "dead letter" folder.

2717 A MSH SHOULD place an entry in an audit log indicating the disposition of each received message.

2718 **B.3.4 Access Control**

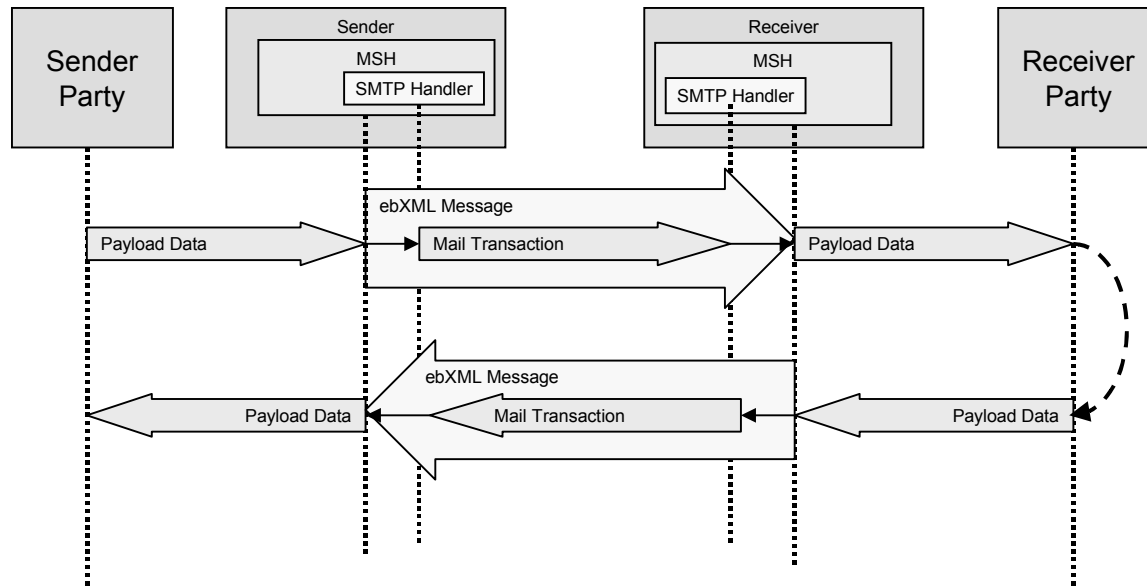
2719 Implementers MAY protect their ebXML Message Service Handlers from unauthorized access through the
 2720 use of an access control mechanism. The SMTP access authentication process described in "SMTP
 2721 Service Extension for Authentication" [RFC2554] defines the ebXML recommended access control
 2722 mechanism to protect a SMTP based ebXML Message Service Handler from unauthorized access.

2723 **B.3.5 Confidentiality and Transport Protocol Level Security**

2724 An ebXML Message Service Handler MAY use transport layer encryption to protect the confidentiality of
 2725 ebXML messages. The IETF "SMTP Service Extension for Secure SMTP over TLS" specification
 2726 [RFC2487] provides the specific technical details and list of allowable options, which may be used.

2727 **B.3.6 SMTP Model**

2728 All *ebXML Message Service* messages carried as mail in an SMTP [RFC2821] Mail Transaction as
 2729 shown in Figure B1.



2730

2731 **Figure B-1 SMTP Mail Depiction**

2732 **B.4 Communication Errors during Reliable Messaging**

2733 When the Sender or the Receiver detects a communications protocol level error (such as an HTTP,
 2734 SMTP or FTP error) and Reliable Messaging is being used then the appropriate transport recovery
 2735 handler will execute a recovery sequence. Only if the error is unrecoverable, does Reliable Messaging
 2736 recovery take place (see section 6).

2737

2737 **Appendix C Supported Security Services**

2738 The general architecture of the ebXML Message Service Specification is intended to support all the
 2739 security services required for electronic business. The following table combines the security services of
 2740 the *Message Service Handler* into a set of security profiles. These profiles, or combinations of these
 2741 profiles, support the specific security policy of the ebXML user community. Due to the immature state of
 2742 XML security specifications, this version of the specification requires support for profiles 0 and 1 only.
 2743 This does not preclude users from employing additional security features to protect ebXML exchanges;
 2744 however, interoperability between parties using any profiles other than 0 and 1 cannot be guaranteed.

2745

Present in baseline MSH		Persistent digital signature	Non-persistent authentication	Persistent signed receipt	Non-persistent integrity	Persistent confidentiality	Non-persistent confidentiality	Persistent authorization	Non-persistent authorization	Trusted timestamp	Description of Profile
✓	Profile 0										no security services are applied to data
✓	Profile 1	✓									<i>Sending MSH</i> applies XML/DSIG structures to message
	Profile 2		✓						✓		<i>Sending MSH</i> authenticates and <i>Receiving MSH</i> authorizes sender based on communication channel credentials.
	Profile 3		✓				✓				<i>Sending MSH</i> authenticates and both MSHs negotiate a secure channel to transmit data
	Profile 4		✓		✓						<i>Sending MSH</i> authenticates, the <i>Receiving MSH</i> performs integrity checks using communications protocol
	Profile 5		✓								<i>Sending MSH</i> authenticates the communication channel only (e.g., SSL 3.0 over TCP/IP)
	Profile 6	✓					✓				<i>Sending MSH</i> applies XML/DSIG structures to message and passes in secure communications channel
	Profile 7	✓		✓							<i>Sending MSH</i> applies XML/DSIG structures to message and <i>Receiving MSH</i> returns a signed receipt
	Profile 8	✓		✓			✓				combination of profile 6 and 7
	Profile 9	✓								✓	Profile 5 with a trusted timestamp applied
	Profile 10	✓		✓						✓	Profile 9 with <i>Receiving MSH</i> returning a signed receipt
	Profile 11	✓					✓			✓	Profile 6 with the <i>Receiving MSH</i> applying a trusted timestamp
	Profile 12	✓		✓			✓			✓	Profile 8 with the <i>Receiving MSH</i> applying a trusted timestamp

Present in baseline MSH		Persistent digital signature	Non-persistent authentication	Persistent signed receipt	Non-persistent integrity	Persistent confidentiality	Non-persistent confidentiality	Persistent authorization	Non-persistent authorization	Trusted timestamp	Description of Profile
	Profile 13	✓				✓					<i>Sending MSH</i> applies XML/DSIG structures to message and applies confidentiality structures (XML-Encryption)
	Profile 14	✓		✓		✓					Profile 13 with a signed receipt
	Profile 15	✓		✓						✓	<i>Sending MSH</i> applies XML/DSIG structures to message, a trusted timestamp is added to message, <i>Receiving MSH</i> returns a signed receipt
	Profile 16	✓				✓				✓	Profile 13 with a trusted timestamp applied
	Profile 17	✓		✓		✓				✓	Profile 14 with a trusted timestamp applied
	Profile 18	✓						✓			<i>Sending MSH</i> applies XML/DSIG structures to message and forwards authorization credentials [SAML]
	Profile 19	✓		✓				✓			Profile 18 with <i>Receiving MSH</i> returning a signed receipt
	Profile 20	✓		✓				✓		✓	Profile 19 with the a trusted timestamp being applied to the <i>Sending MSH</i> message
	Profile 21	✓		✓		✓		✓		✓	Profile 19 with the <i>Sending MSH</i> applying confidentiality structures (XML-Encryption)
	Profile 22					✓					<i>Sending MSH</i> encapsulates the message within confidentiality structures (XML-Encryption)

2746

2747 **References**2748 **Normative References**

- 2749 [\[RFC2119\]](#) Key Words for use in RFCs to Indicate Requirement Levels, Internet Engineering Task Force, March 1997
- 2751 [\[RFC2045\]](#) Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, N Freed & N Borenstein, Published November 1996
- 2753 [\[RFC2046\]](#) Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. N. Freed, N. Borenstein. November 1996.
- 2755 [\[RFC2246\]](#) Dierks, T. and C. Allen, "The TLS Protocol", January 1999.
- 2756 [\[RFC2387\]](#) The MIME Multipart/Related Content-type. E. Levinson. August 1998.
- 2757 [\[RFC2392\]](#) Content-ID and Message-ID Uniform Resource Locators. E. Levinson, August 1998
- 2758 [\[RFC2396\]](#) Uniform Resource Identifiers (URI): Generic Syntax. T Berners-Lee, August 1998
- 2759 [\[RFC2402\]](#) IP Authentication Header. S. Kent, R. Atkinson. November 1998. RFC2406 IP Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998.
- 2761 [\[RFC2487\]](#) SMTP Service Extension for Secure SMTP over TLS. P. Hoffman, January 1999.
- 2762 [\[RFC2554\]](#) SMTP Service Extension for Authentication. J. Myers. March 1999.
- 2763 [\[RFC2821\]](#) Simple Mail Transfer Protocol, J. Klensin, Editor, April 2001 Obsoletes RFC 821
- 2764 [\[RFC2616\]](#) Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol, HTTP/1.1", June 1999.
- 2766 [\[RFC2617\]](#) Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., Sink, E. and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", June 1999.
- 2769 [\[RFC2817\]](#) Khare, R. and S. Lawrence, "Upgrading to TLS Within HTTP/1.1", May 2000.
- 2770 [\[RFC2818\]](#) Rescorla, E., "HTTP Over TLS", May 2000 [SOAP] Simple Object Access Protocol
- 2771 [SOAP] W3C-Draft-Simple Object Access Protocol (SOAP) v1.1, Don Box, DevelopMentor; David
- 2772 Ehnebuske, IBM; Gopal Kakivaya, Andrew Layman, Henrik Frystyk Nielsen, Satish
- 2773 Thatte, Microsoft; Noah Mendelsohn, Lotus Development Corp.; Dave Winer, UserLand
- 2774 Software, Inc.; W3C Note 08 May 2000,
- 2775 <http://www.w3.org/TR/2000/NOTE-SOAP-20000508/>
- 2776 [SOAPAttach] SOAP Messages with Attachments, John J. Barton, Hewlett Packard Labs; Satish Thatte
- 2777 and Henrik Frystyk Nielsen, Microsoft, Published Oct 09 2000
- 2778 <http://www.w3.org/TR/2000/NOTE-SOAP-attachments-20001211>
- 2779 [SSL3] A. Frier, P. Karlton and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications
- 2780 Corp., Nov 18, 1996.
- 2781 [UTF-8] UTF-8 is an encoding that conforms to ISO/IEC 10646. See [XML] for usage conventions.
- 2782 [XLINK] W3C XML Linking Recommendation, <http://www.w3.org/TR/2001/REC-xlink-20010627/>
- 2783 [XML] W3C Recommendation: Extensible Markup Language (XML) 1.0 (Second Edition),
- 2784 October 2000, <http://www.w3.org/TR/2000/REC-xml-20001006>
- 2785 [XMLC14N] W3C Recommendation Canonical XML 1.0,
- 2786 <http://www.w3.org/TR/2001/REC-xml-c14n-20010315>

- 2787 [XMLNS] W3C Recommendation for Namespaces in XML, World Wide Web Consortium, 14
2788 January 1999, <http://www.w3.org/TR/1999/REC-xml-names-19990114/>
- 2789 [XMLDSIG] Joint W3C/IETF XML-Signature Syntax and Processing specification,
2790 <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/>.
- 2791 [XMLMedia] [RFC 3023](#), XML Media Types. M. Murata, S. St. Laurent, January 2001
- 2792 [XPointer] XML Pointer Language (XPointer) Version 1.0, W3C Candidate Recommendation 11
2793 September 2001, <http://www.w3.org/TR/2001/CR-xptr-20010911/>
- 2794

2795 **Non-Normative References**

- 2796 [ebCPP] ebXML Collaboration Protocol Profile and Agreement specification, Version 1.0,
2797 published 10 May, 2001, <http://www.ebxml.org/specs/ebCCP.doc>
- 2798 [ebBPSS] ebXML Business Process Specification Schema, version 1.0, published 27 April 2001,
2799 <http://www.ebxml.org/specs/ebBPSS.pdf>.
- 2800 [ebTA] ebXML Technical Architecture, version 1.04 published 16 February, 2001,
2801 <http://www.ebxml.org/specs/ebTA.doc>
- 2802 [ebRS] ebXML Registry Services Specification, version 2.0, published 6 December 2001
2803 <http://www.oasis-open.org/committees/regrep/documents/2.0/specs/ebRS.pdf>,
2804 published, 5 December 2001.
2805 <http://www.oasis-open.org/committees/regrep/documents/2.0/specs/ebRim.pdf>
- 2806 [ebREQ] ebXML Requirements Specification, <http://www.ebxml.org/specs/ebREQ.pdf>,
2807 published 8 May 2001.
- 2808 [ebGLOSS] ebXML Glossary, <http://www.ebxml.org/specs/ebGLOSS.doc>, published 11 May, 2001.
- 2809 [PGP/MIME] [RFC2015](#), "MIME Security with Pretty Good Privacy (PGP)", M. Elkins. October 1996.
- 2810 [SAML] Security Assertion Markup Language,
2811 <http://www.oasis-open.org/committees/security/docs/draft-sstc-use-strawman-03.html>
- 2812 [S/MIME] [RFC 2311](#), "S/MIME Version 2 Message Specification", S. Dusse, P. Hoffman, B.
2813 Ramsdell, L. Lundblade, L. Repka. March 1998.
- 2814 [S/MIMECH] [RFC 2312](#), "S/MIME Version 2 Certificate Handling", S. Dusse, P. Hoffman, B. Ramsdell,
2815 J. Weinstein. March 1998.
- 2816 [S/MIMEV3] [RFC 2633](#) S/MIME Version 3 Message Specification. B. Ramsdell, Ed June 1999.
- 2817 [secRISK] ebXML Technical Architecture Risk Assessment Technical Report, version 0.36
2818 published 20 April 2001
- 2819 [XMLSchema] W3C XML Schema Recommendation,
2820 <http://www.w3.org/TR/2001/REC-xmlschema-0-20010502/>
2821 <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>
2822 <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>
- 2823 [XMTP] XMTP - Extensible Mail Transport Protocol
2824 <http://www.openhealth.org/documents/xmtp.htm>

2825 **Contact Information**2826 **Team Leader**

Name Ian Jones
Company British Telecommunications
Address Enterprise House, 84-85 Adam Street
 Cardiff, CF24 2XF United Kingdom
Phone: +44 29 2072 4063
EMail: ian.c.jones@bt.com

2827 **Vice Team Leader**

Name Brian Gibb
Company Sterling Commerce
Address 750 W. John Carpenter Freeway
 Irving, Texas 75039 USA
Phone: +1 (469) 524.2628
EMail: brian_gibb@stercomm.com

2828 **Team Editor**

Name David Fischer
Company Drummond Group, Inc
Address P.O. Box 101567
 Fort Worth, Texas 76105 USA
Phone +1 (817) 294-7339
EMail david@drummondgroup.com

2829 **Acknowledgments**

2830 The OASIS ebXML-MS Technical Committee would like to thank the members of the original joint
 2831 UN/CEFACT-OASIS ebXML Messaging Team for their work to produce v1.0 of this specification.

2832

Ralph Berwanger	bTrade.com	Ravi Kacker	Kraft Foods
Jonathan Borden	Author of XMTP	Henry Lowe	OMG
Jon Bosak	Sun Microsystems	Jim McCarthy	webXI
Marc Breissinger	webMethods	Bob Miller	GXS
Dick Brooks	Group 8760	Dale Moberg	Sterling Commerce
Doug Bunting	Ariba	Joel Munter	Intel
David Burdett	Commerce One	Shumpei Nakagaki	NEC Corporation
David Craft	VerticalNet	Farrukh Najmi	Sun Microsystems
Philippe De Smedt	Viquity	Akira Ochi	Fujitsu
Lawrence Ding	WorldSpan	Martin Sachs	IBM
Rik Drummond	Drummond Group (Chair)	Saikat Saha	Commerce One
Andrew Eisenberg	Progress Software	Masayoshi Shimamura	Fujitsu
Colleen Evans	Sonic Software	Prakash Sinha	Netfish Technologies
David Fischer	Drummond Group	Rich Salz	Zolera Systems
Christopher Ferris	Sun Microsystems	Tae Joon Song	eSum Technologies, Inc.
Robert Fox	Softshare	Kathy Spector	Extricity
Brian Gibb	Sterling Commerce	Nikola Stojanovic	Encoda Systems, Inc.
Maryann Hondo	IBM	David Turner	Microsoft
Jim Hughes	Fujitsu	Gordon Van Huizen	Progress Software
John Ibbotson	IBM	Martha Warfelt	DaimlerChrysler Corporation
Ian Jones	British Telecommunications	Prasad Yendluri	Web Methods

2833

2833 **Disclaimer**

2834 The views and specification expressed in this document are those of the authors and are not necessarily
2835 those of their employers. The authors and their employers specifically disclaim responsibility for any
2836 problems arising from correct or incorrect implementation or use of this design.

2837 *This document and the information contained herein is provided on an "AS IS" basis and OASIS
2838 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
2839 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR
2840 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."*

2841

2842 **Copyright Statement**

2843 *Copyright (C) The Organization for the Advancement of Structured Information Standards [OASIS]
2844 January 2002. All Rights Reserved.*

2845 *This document and translations of it may be copied and furnished to others, and derivative works that
2846 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published
2847 and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice
2848 and this paragraph are included on all such copies and derivative works. However, this document itself
2849 may not be modified in any way, such as by removing the copyright notice or references to OASIS,
2850 except as needed for the purpose of developing OASIS specifications, in which case the procedures for
2851 copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to
2852 translate it into languages other than English.*

2853 *The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
2854 or assigns.*

2855

2856 **Intellectual Property Rights Statement**

2857 *"OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
2858 might be claimed to pertain to the implementation or use of the technology described in this document or
2859 the extent to which any license under such rights might or might not be available; neither does it
2860 represent that it has made any effort to identify any such rights. Information on OASIS's procedures with
2861 respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights
2862 made available for publication and any assurances of licenses to be made available, or the result of an
2863 attempt made to obtain a general license or permission for the use of such proprietary rights by
2864 implementors or users of this specification, can be obtained from the OASIS Executive Director."*

2865 *"OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications,
2866 or other proprietary rights which may cover technology that may be required to implement this
2867 specification. Please address the information to the OASIS Executive Director."*

2868 *"OASIS has been notified of intellectual property rights claimed in regard to some or all of the contents of
2869 this specification. For more information consult the online list of claimed rights."*