



Creating A Single Global Electronic Market

1 **Message Service Specification**

2 **Version 2.0 rev C**

3 **OASIS ebXML Messaging Services Technical Committee**

4 **21 February 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, January 22, 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 –**Error! Hyperlink reference not valid.** [http://www.oasis-open.org/committees/ebxml-
msg/documents/ebMS_v2_0.pdf](http://www.oasis-open.org/committees/ebxml-
21 msg/documents/ebMS_v2_0.pdf)

22 *Errata to this version*

23 V2.0 –**Error! Hyperlink reference not valid.** [http://www.oasis-open.org/committees/ebxml-
msg/documents/ebMS_v2_0_errata.html](http://www.oasis-open.org/committees/ebxml-
24 msg/documents/ebMS_v2_0_errata.html)

25 *Previous version*

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

27 **ebXML Participants**

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



Creating A Single Global Electronic Market

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

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

Table of Contents

32			
33	Status of this Document	2
34	ebXML Participants	2
35	Introduction	7
36	1	Summary of Contents of this Document7
37	1.1.1	Document Conventions8
38	1.1.2	Audience8
39	1.1.3	Caveats and Assumptions8
40	1.1.4	Related Documents8
41	1.2	Concept of Operation9
42	1.2.1	Scope9
43	1.2.2	Background and Objectives9
44	1.2.3	Operational Policies and Constraints10
45	1.2.4	Modes of Operation11
46	1.3	Minimal Requirements for Conformance12
47	Part I. Core Functionality	13
48	2	ebXML with SOAP13
49	2.1	Packaging Specification13
50	2.1.1	SOAP Structural Conformance14
51	2.1.2	Message Package14
52	2.1.3	Header Container14
53	2.1.4	Payload Container15
54	2.1.5	Additional MIME Parameters15
55	2.1.6	Reporting MIME Errors16
56	2.2	XML Prolog16
57	2.2.1	XML Declaration16
58	2.2.2	Encoding Declaration16
59	2.3	ebXML SOAP Envelope extensions16
60	2.3.1	Namespace pseudo attribute16
61	2.3.2	xsi:schemaLocation attribute16
62	2.3.3	SOAP Header Element17
63	2.3.4	SOAP Body Element17
64	2.3.5	ebXML SOAP Extensions17
65	2.3.6	#wildcard Element Content18
66	2.3.7	id attribute18
67	2.3.8	version attribute18
68	2.3.9	SOAP mustUnderstand attribute19
69	2.3.10	ebXML "Next MSH" actor URI19
70	2.3.11	ebXML "To Party MSH" actor URI19
71	3	Core Extension Elements19
72	3.1	MessageHeader Element19
73	3.1.1	From and To Elements20
74	3.1.2	CPAId Element20
75	3.1.3	ConversationId Element21
76	3.1.4	Service Element21
77	3.1.5	Action Element22
78	3.1.6	MessageData Element22
79	3.1.7	DuplicateElimination Element23
80	3.1.8	Description Element23
81	3.1.9	MessageHeader Sample23
82	3.2	Manifest Element23
83	3.2.1	Reference Element24
84	3.2.2	Manifest Validation24
85	3.2.3	Manifest Sample25
86	4	Core Modules25
87	4.1	Security Module25
88	4.1.1	Signature Element25
89	4.1.2	Security and Management26
90	4.1.3	Signature Generation26
91	4.1.4	Countermeasure Technologies28

92	4.1.5	Security Considerations	29
93	4.2	Error Handling Module	30
94	4.2.2	Types of Errors	30
95	4.2.3	ErrorList Element	31
96	4.2.4	Implementing Error Reporting and Handling	33
97	4.3	SyncReply Module	34
98	4.3.1	SyncReply Element	34
99	5	Combining ebXML SOAP Extension Elements	34
100	5.1.1	MessageHeader Element Interaction	34
101	5.1.2	Manifest Element Interaction	35
102	5.1.3	Signature Element Interaction	35
103	5.1.4	ErrorList Element Interaction	35
104	5.1.5	SyncReply Element Interaction	35
105		Part II. Additional Features	36
106	6	Reliable Messaging Module	36
107	6.1	Persistent Storage and System Failure	36
108	6.2	Methods of Implementing Reliable Messaging	36
109	6.3	Reliable Messaging SOAP Header Extensions	37
110	6.3.1	AckRequested Element	37
111	6.3.2	Acknowledgment Element	38
112	6.4	Reliable Messaging Parameters	39
113	6.4.1	DuplicateElimination	39
114	6.4.2	AckRequested	40
115	6.4.3	Retries	40
116	6.4.4	RetryInterval	40
117	6.4.5	TimeToLive	40
118	6.4.6	PersistDuration	40
119	6.4.7	syncReplyMode	40
120	6.5	ebXML Reliable Messaging Protocol	41
121	6.5.1	Sending Message Behavior	41
122	6.5.2	Receiving Message Behavior	41
123	6.5.3	Generating an Acknowledgment Message	42
124	6.5.4	Resending Lost Application Messages	42
125	6.5.5	Resending Acknowledgments	43
126	6.5.6	Duplicate Message Handling	44
127	6.5.7	Failed Message Delivery	44
128	6.6	Reliable Messaging Combinations	45
129	7	Message Status Service	45
130	7.1	Message Status Messages	46
131	7.1.1	Message Status Request Message	46
132	7.1.2	Message Status Response Message	46
133	7.1.3	Security Considerations	46
134	7.2	StatusRequest Element	46
135	7.2.1	RefToMessageId Element	47
136	7.2.2	StatusRequest Sample	47
137	7.2.3	StatusRequest Element Interaction	47
138	7.3	StatusResponse Element	47
139	7.3.1	RefToMessageId Element	47
140	7.3.2	Timestamp Element	47
141	7.3.3	messageStatus attribute	47
142	7.3.4	StatusResponse Sample	48
143	7.3.5	StatusResponse Element Interaction	48
144	8	Message Service Handler Ping Service	48
145	8.1	Message Service Handler Ping Message	48
146	8.2	Message Service Handler Pong Message	49
147	8.3	Security Considerations	50
148	9	MessageOrder Module	50
149	9.1	MessageOrder Element	50
150	9.1.1	SequenceNumber Element	50
151	9.1.2	MessageOrder Sample	51
152	9.2	MessageOrder Element Interaction	51
153	10	Multi-Hop Module	51
154	10.1	Multi-hop Reliable Messaging	52
155	10.1.1	AckRequested Sample	52

156	10.1.2	Acknowledgment Sample	52
157	10.1.3	Multi-Hop Acknowledgments	52
158	10.1.4	Signing Multi-Hop Acknowledgments	53
159	10.1.5	Multi-Hop Security Considerations	53
160	10.2	Message Ordering and Multi-Hop	53
161	Part III. Normative Appendices		54
162	Appendix A	The ebXML SOAP Extension Elements Schema	54
163	Appendix B	Communications Protocol Bindings	59
164	B.1	Introduction	59
165	B.2	HTTP	59
166	B.2.1	Minimum level of HTTP protocol	59
167	B.2.2	Sending ebXML Service messages over HTTP	59
168	B.2.3	HTTP Response Codes	60
169	B.2.4	SOAP Error conditions and Synchronous Exchanges	61
170	B.2.5	Synchronous vs. Asynchronous	61
171	B.2.6	Access Control	61
172	B.2.7	Confidentiality and Transport Protocol Level Security	61
173	B.3	SMTP	62
174	B.3.1	Minimum Level of Supported Protocols	62
175	B.3.2	Sending ebXML Messages over SMTP	62
176	B.3.3	Response Messages	64
177	B.3.4	Access Control	64
178	B.3.5	Confidentiality and Transport Protocol Level Security	64
179	B.3.6	SMTP Model	64
180	B.4	Communication Errors during Reliable Messaging	65
181	Appendix C	Supported Security Services	66
182	References		68
183	Normative References		68
184	Non-Normative References		69
185	Contact Information		70
186	Acknowledgments		71
187	Disclaimer		71
188	Copyright Statement		71

189 Introduction

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

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

200 1 Summary of Contents of this Document

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

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

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

208 This specification is organized around the following topics:

209 Core Functionality

- 210 • **Packaging Specification** – A description of how to package an ebXML Message and its associated parts
211 into a form that can be sent using a communications protocol such as HTTP or SMTP (section 2.1),
- 212 • **ebXML SOAP Envelope Extensions** – A specification of the structure and composition of the information
213 necessary for an *ebXML Message Service* to generate or process an ebXML Message (section 2.3),
- 214 • **Error Handling** – A description of how one *ebXML Message Service* reports errors it detects to another
215 ebXML Message Service Handler (section 4.2),
- 216 • **Security** – Provides a specification of the security semantics for ebXML Messages (section 4.1),
- 217 • **SyncReply** – Indicates to the Next MSH whether or not replies are to be returned synchronously (section
218 4.3).

219 Additional Features

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

227 Appendices to this specification cover the following:

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

233 1.1.1 Document Conventions

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

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

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

259 1.1.2 Audience

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

262 1.1.3 Caveats and Assumptions

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

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

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

269 1.1.4 Related Documents

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

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

280 1.2 Concept of Operation

281 1.2.1 Scope

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

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

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

298 1.2.2 Background and Objectives

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

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

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

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

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

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

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

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

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

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

362 **1.2.3 Operational Policies and Constraints**

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

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

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

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

383 1.2.4 Modes of Operation

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

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

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

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

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

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

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

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

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

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

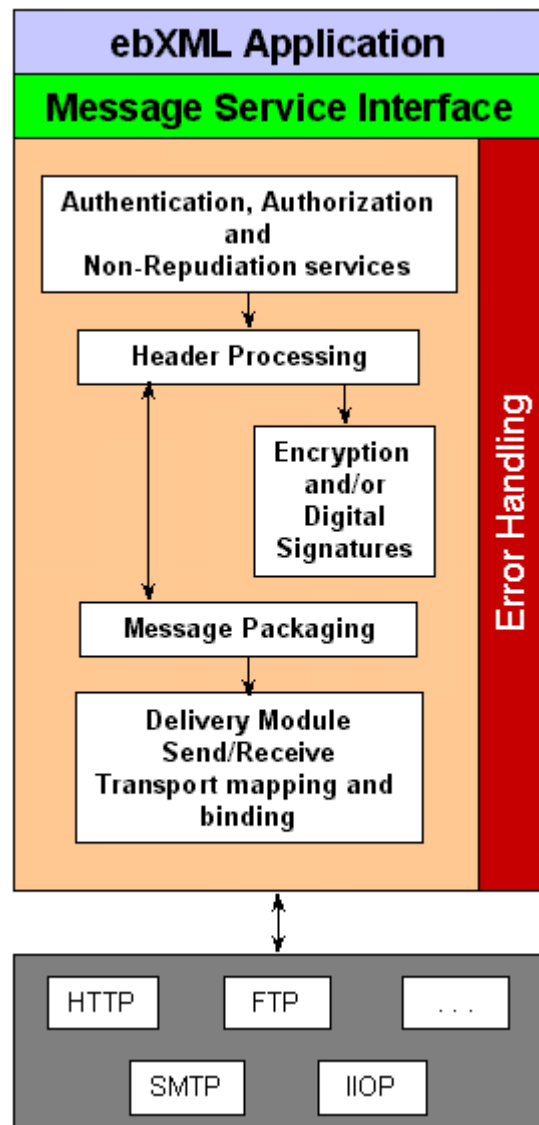


Figure 1.1 Typical Relationship between ebXML Message Service Handler Components

429 **1.3 Minimal Requirements for Conformance**

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

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

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

453

Part I. Core Functionality

454

2 ebXML with SOAP

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

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

463

2.1 Packaging Specification

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

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

- 468 • The first MIME part, referred to as the *Header Container*, containing one SOAP 1.1 compliant
 469 message. This XML document is referred to as a *SOAP Message* for the remainder of this
 470 specification,
 471 as a *SOAP Message* for the remainder of this
 472 specification,
- 473 • zero or more additional MIME parts, referred to as *Payload Containers*, containing application
 474 level payloads.
 475

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

478

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

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

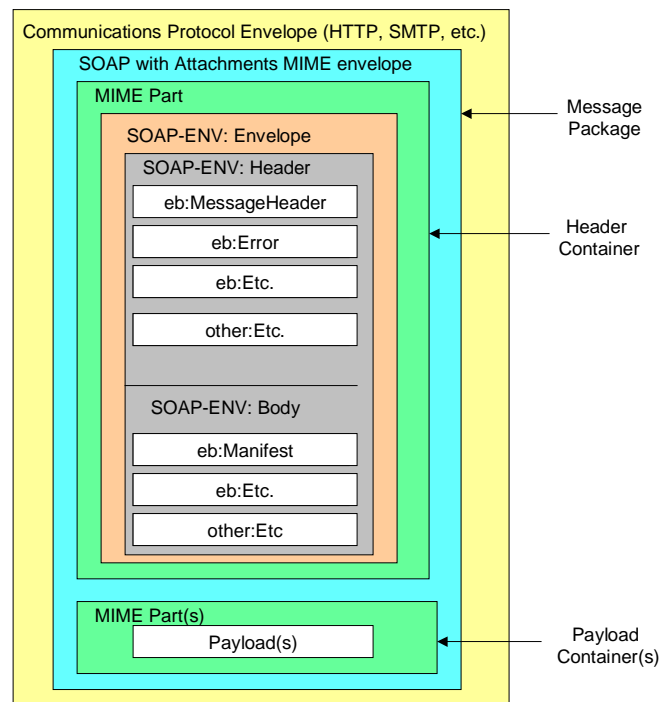


Figure 2.1 ebXML Message Structure

491 **2.1.1 SOAP Structural Conformance**

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

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

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

497 **2.1.2 Message Package**

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

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

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

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

516 **2.1.3 Header Container**

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

520 **2.1.3.1 Content-Type**

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

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

525 **2.1.3.2 charset attribute**

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

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

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

535 2.1.3.3 Header Container Example

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

```

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

```

551 2.1.4 Payload Container

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

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

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

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

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

564 2.1.4.1 Example of a Payload Container

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

```

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

```

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

580 2.1.5 Additional MIME Parameters

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

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

586 **2.1.6 Reporting MIME Errors**

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

589 **2.2 XML Prolog**

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

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

595 **2.2.1 XML Declaration**

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

599 **2.2.2 Encoding Declaration**

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

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

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

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

609 **2.3 ebXML SOAP Envelope extensions**

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

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

616 **2.3.1 Namespace pseudo attribute**

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

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

620 **2.3.2 xsi:schemaLocation attribute**

621 The SOAP namespace:

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

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

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


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

631 For example:

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

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

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

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

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

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

669 2.3.3 SOAP Header Element

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

673 2.3.4 SOAP Body Element

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

677 2.3.5 ebXML SOAP Extensions

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

679 2.3.5.1 SOAP Header extensions:

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

683 2.3.5.2 SOAP Body extension:

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

686 2.3.5.3 Core ebXML Modules:

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

694 2.3.6 #wildcard Element Content

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

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

702 2.3.7 id attribute

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

708 2.3.8 version attribute

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

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

723 2.3.9 SOAP *mustUnderstand* attribute

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

730 2.3.10 ebXML "Next MSH" actor URI

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

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

737 All ebXML MSH nodes MUST act in this role.

738 2.3.11 ebXML "To Party MSH" actor URI

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

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

746 3 Core Extension Elements

747 3.1 MessageHeader Element

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

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

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

763 3.1.1 From and To Elements

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

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

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

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

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

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

780 3.1.1.1 PartyId Element

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

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

790 3.1.1.2 Role Element

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

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

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

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

806 3.1.2 CPAId Element

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

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

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

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

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

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

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

825 3.1.3 ConversationId Element

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

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

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

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

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

839 3.1.4 Service Element

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

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

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

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

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

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

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

852 3.1.4.1 type attribute

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

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

858 3.1.5 Action Element

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

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

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

865 3.1.6 MessageData Element

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

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

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

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

878 3.1.6.1 MessageId Element

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

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

884 3.1.6.2 Timestamp Element

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

888 3.1.6.3 RefToMessageId Element

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

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

894 3.1.6.4 TimeToLive Element

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

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

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

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

904 3.1.7 DuplicateElimination Element

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

907 Valid values for **DuplicateElimination**:

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

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

912 3.1.8 Description Element

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

917 3.1.9 MessageHeader Sample

918 The following fragment demonstrates the structure of the **MessageHeader** element within the SOAP
919 **Header**.

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

940 3.2 Manifest Element

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

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

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

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

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

952 3.2.1 Reference Element

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

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

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

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

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

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

974 3.2.1.1 Schema Element

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

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

981 3.2.1.2 Description Element

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

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

984 3.2.2 Manifest Validation

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

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

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

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

993 3.2.3 Manifest Sample

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

```
995 <eb:Manifest eb:id="Manifest" eb:version="2.0">
996   <eb:Reference eb:id="pay01"
997     xlink:href="cid:payload-1"
998     xlink:role="http://regrep.org/gci/purchaseOrder">
999     <eb:Schema eb:location="http://regrep.org/gci/purchaseOrder/po.xsd" eb:version="2.0"/>
1000     <eb:Description xml:lang="en-US">Purchase Order for 100,000 widgets</eb:Description>
1001   </eb:Reference>
1002 </eb:Manifest>
```

1003 4 Core Modules

1004 4.1 Security Module

1005 The *ebXML Message Service*, by its very nature, presents certain security risks. A Message Service may
1006 be at risk by means of:

- 1007 • Unauthorized access
- 1008 • Data integrity and/or confidentiality attacks (e.g. through man-in-the-middle attacks)
- 1009 • Denial-of-Service and spoofing

1010 Each security risk is described in detail in the ebXML Technical Architecture Risk Assessment Technical
1011 Report [secRISK].

1012 Each of these security risks may be addressed in whole, or in part, by the application of one, or a
1013 combination, of the countermeasures described in this section. This specification describes a set of
1014 profiles, or combinations of selected countermeasures, selected to address key risks based upon
1015 commonly available technologies. Each of the specified profiles includes a description of the risks that
1016 are not addressed. See Appendix C for a table of security profiles.

1017 Application of countermeasures SHOULD be balanced against an assessment of the inherent risks and
1018 the value of the asset(s) that might be placed at risk. For this specification, a *Signed Message* is any
1019 message containing a **Signature** element.

1020 4.1.1 Signature Element

1021 An ebXML Message MAY be digitally signed to provide security countermeasures. Zero or more
1022 **Signature** elements, belonging to the XML Signature [XMLDSIG] defined namespace, MAY be present
1023 as a child of the SOAP **Header**. The **Signature** element MUST be namespace qualified in accordance
1024 with XML Signature [XMLDSIG]. The structure and content of the **Signature** element MUST conform to
1025 the XML Signature [XMLDSIG] specification. If there is more than one **Signature** element contained
1026 within the SOAP **Header**, the first MUST represent the digital signature of the ebXML Message as signed
1027 by the *From Party MSH* in conformance with section 4.1. Additional **Signature** elements MAY be
1028 present, but their purpose is undefined by this specification.

1029 Refer to section 4.1.3 for a detailed discussion on how to construct the **Signature** element when digitally
1030 signing an ebXML Message.

1031 4.1.2 Security and Management

1032 No technology, regardless of how advanced it might be, is an adequate substitute to the effective
1033 application of security management policies and practices.

1034 It is strongly RECOMMENDED that the site manager of an *ebXML Message Service* apply due diligence
1035 to the support and maintenance of its security mechanisms, site (or physical) security procedures,
1036 cryptographic protocols, update implementations and apply fixes as appropriate. (See
1037 <http://www.cert.org/> and <http://ciac.llnl.gov/>)

1038 4.1.2.1 Collaboration Protocol Agreement

1039 The configuration of Security for MSHs is specified in the *CPA*. Two areas of the *CPA* have security
1040 definitions as follows:

- 1041 • The Document Exchange section addresses security to be applied to the payload of the message. The
1042 MSH is not responsible for any security specified at this level but may offer these services to the message
1043 sender.
- 1044 • The Transport section addresses security applied to the entire ebXML Document, which includes the header
1045 and the payload(s).

1046 4.1.3 Signature Generation

1047 An ebXML Message is signed using [XMLDSIG] following these steps:

- 1048 1) Create a **SignedInfo** element with **SignatureMethod**, **CanonicalizationMethod** and **Reference**
1049 elements for the SOAP **Envelope** and any required payload objects, as prescribed by XML
1050 Signature [XMLDSIG].
- 1051 2) Canonicalize and then calculate the **SignatureValue** over **SignedInfo** based on algorithms
1052 specified in **SignedInfo** as specified in XML Signature [XMLDSIG].
- 1053 3) Construct the **Signature** element that includes the **SignedInfo**, **KeyInfo** (RECOMMENDED) and
1054 **SignatureValue** elements as specified in XML Signature [XMLDSIG].
- 1055 4) Include the namespace qualified **Signature** element in the SOAP **Header** just signed.

1056 The **SignedInfo** element SHALL have a **CanonicalizationMethod** element, a **SignatureMethod** element
1057 and one or more **Reference** elements, as defined in XML Signature [XMLDSIG].

1058 The RECOMMENDED canonicalization method applied to the data to be signed is

```
1059 <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

1060 described in [XMLC14N]. This algorithm excludes comments.

1061 The **SignatureMethod** element SHALL be present and SHALL have an **Algorithm** attribute. The
1062 RECOMMENDED value for the **Algorithm** attribute is:

```
1063 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
```

1064 This RECOMMENDED value SHALL be supported by all compliant *ebXML Message Service* software
1065 implementations.

1066 The [XMLDSIG] **Reference** element for the SOAP **Envelope** document SHALL have a URI attribute
1067 value of "" to provide for the signature to be applied to the document that contains the **Signature** element.

1068 The [XMLDSIG] **Reference** element for the SOAP **Envelope** MAY include a **Type** attribute that has a
1069 value "http://www.w3.org/2000/09/xmldsig#Object" in accordance with XML Signature [XMLDSIG]. This
1070 attribute is purely informative. It MAY be omitted. Implementations of the ebXML MSH SHALL be
1071 prepared to handle either case. The **Reference** element MAY include the **id** attribute.

1072 The [XMLDSIG] **Reference** element for the SOAP **Envelope** SHALL include a child **Transforms**
1073 element. The **Transforms** element SHALL include the following **Transform** child elements.

1074 The first **Transform** element has an **Algorithm** attribute with a value of:

```
1075 <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
```

1076 The result of this statement excludes the parent **Signature** element and all its descendants.

1077 The second **Transform** element has a child **XPath** element that has a value of:

```
1078 <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
1079   <XPath> not (ancestor-or-self::() [ @SOAP:actor="urn:oasis:names:tc:ebxml-msg:actor:nextMSH" ] |
1080     ancestor-or-self::() [ @SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next" ] )
1081   </XPath>
1082 </Transform>
```

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

1089 The last **Transform** element SHOULD have an **Algorithm** attribute with a value of:

```
1090 <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
```

1091 The result of this algorithm is to canonicalize the SOAP **Envelope** XML and exclude comments.

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

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

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

1102 Example of digitally signed ebXML SOAP Message:

```
1103 <?xml version="1.0" encoding="utf-8"?>
1104 <SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
1105   xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
1106   xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
1107   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1108   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
1109     http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
1110     http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
1111     http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
1112   <SOAP:Header>
1113     <eb:MessageHeader eb:id="..." eb:version="2.0" SOAP:mustUnderstand="1">
1114       ...
1115     </eb:MessageHeader>
1116     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
1117       <SignedInfo>
1118         <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
1119         <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
1120         <Reference URI="">
1121           <Transforms>
1122             <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
1123             <Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
1124               <XPath> not (ancestor-or-self::() [ @SOAP:actor=
1125                 &quot;urn:oasis:names:tc:ebxml-msg:actor:nextMSH&quot; ]
1126                 | ancestor-or-self::() [ @SOAP:actor=
1127                 &quot;http://schemas.xmlsoap.org/soap/actor/next&quot; ] )
1128               </XPath>
1129             </Transform>
1130             <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
1131           </Transforms>
1132         <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
```

```

1133     <DigestValue>...</DigestValue>
1134     </Reference>
1135     <Reference URI="cid://blahblahblah/">
1136         <DigestMethod Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>
1137         <DigestValue>...</DigestValue>
1138     </Reference>
1139 </SignedInfo>
1140 <SignatureValue>...</SignatureValue>
1141 <KeyInfo>...</KeyInfo>
1142 </Signature>
1143 </SOAP:Header>
1144 <SOAP:Body>
1145     <eb:Manifest eb:id="Mani01" eb:version="2.0">
1146         <eb:Reference xlink:href="cid://blahblahblah/" xlink:role="http://ebxml.org/gci/invoice">
1147             <eb:Schema eb:version="2.0" eb:location="http://ebxml.org/gci/busdocs/invoice.dtd"/>
1148         </eb:Reference>
1149     </eb:Manifest>
1150 </SOAP:Body>
1151 </SOAP:Envelope>

```

1152 4.1.4 Countermeasure Technologies

1153 4.1.4.1 Persistent Digital Signature

1154 The only available technology that can be applied to the purpose of digitally signing an ebXML Message
 1155 (the ebXML SOAP **Header** and **Body** and its associated payload objects) is provided by technology that
 1156 conforms to the W3C/IETF joint XML Signature specification [XMLDSIG]. An XML Signature conforming
 1157 to this specification can selectively sign portions of an XML document(s), permitting the documents to be
 1158 augmented (new element content added) while preserving the validity of the signature(s).

1159 If signatures are being used to digitally sign an ebXML Message then XML Signature [DSIG] MUST be
 1160 used to bind the ebXML SOAP **Header** and **Body** to the ebXML Payload Container(s) or data elsewhere
 1161 on the web that relate to the message.

1162 An ebXML Message requiring a digital signature SHALL be signed following the process defined in this
 1163 section of the specification and SHALL be in full compliance with XML Signature [XMLDSIG].

1164 4.1.4.2 Persistent Signed Receipt

1165 An *ebXML Message* that has been digitally signed MAY be acknowledged with an *Acknowledgment*
 1166 *Message* that itself is digitally signed in the manner described in the previous section. The
 1167 *Acknowledgment Message* MUST contain a [XMLDSIG] **Reference** element list consistent with those
 1168 contained in the [XMLDSIG] **Signature** element of the original message.

1169 4.1.4.3 Non-persistent Authentication

1170 Non-persistent authentication is provided by the communications channel used to transport the *ebXML*
 1171 *Message*. This authentication MAY be either in one direction or bi-directional. The specific method will be
 1172 determined by the communications protocol used. For instance, the use of a secure network protocol,
 1173 such as TLS [RFC2246] or IPSEC [RFC2402] provides the sender of an *ebXML Message* with a way to
 1174 authenticate the destination for the TCP/IP environment.

1175 4.1.4.4 Non-persistent Integrity

1176 A secure network protocol such as TLS [RFC2246] or IPSEC [RFC2402] MAY be configured to provide
 1177 for digests and comparisons of the packets transmitted via the network connection.

1178 4.1.4.5 Persistent Confidentiality

1179 XML Encryption is a W3C/IETF joint activity actively engaged in the drafting of a specification for the
 1180 selective encryption of an XML document(s). It is anticipated that this specification will be completed
 1181 within the next year. The ebXML Transport, Routing and Packaging team for v1.0 of this specification
 1182 has identified this technology as the only viable means of providing persistent, selective confidentiality of
 1183 elements within an *ebXML Message* including the SOAP **Header**.

1184 Confidentiality for ebXML Payload Containers MAY be provided by functionality possessed by a MSH.
1185 Payload confidentiality MAY be provided by using XML Encryption (when available) or some other
1186 cryptographic process (such as S/MIME [S/MIME], [S/MIMEV3], or PGP MIME [PGP/MIME]) bilaterally
1187 agreed upon by the parties involved. The XML Encryption standard shall be the default encryption
1188 method when XML Encryption has achieved W3C Recommendation status.

1189 Note: When both signature and encryption are required of the MSH, sign first and then encrypt.

1190 **4.1.4.6 Non-persistent Confidentiality**

1191 A secure network protocol, such as TLS [RFC2246] or IPSEC [RFC2402], provides transient
1192 confidentiality of a message as it is transferred between two ebXML adjacent MSH nodes.

1193 **4.1.4.7 Persistent Authorization**

1194 The OASIS Security Services Technical Committee (TC) is actively engaged in the definition of a
1195 specification that provides for the exchange of security credentials, including Name Assertion and
1196 Entitlements, based on Security Assertion Markup Language [SAML]. Use of technology based on this
1197 anticipated specification may provide persistent authorization for an *ebXML Message* once it becomes
1198 available.

1199 **4.1.4.8 Non-persistent Authorization**

1200 A secure network protocol such as TLS [RFC2246] or IPSEC [RFC2402] MAY be configured to provide
1201 for bilateral authentication of certificates prior to establishing a session. This provides for the ability for an
1202 ebXML MSH to authenticate the source of a connection and to recognize the source as an authorized
1203 source of *ebXML Messages*.

1204 **4.1.4.9 Trusted Timestamp**

1205 At the time of this specification, services offering trusted timestamp capabilities are becoming available.
1206 Once these become more widely available, and a standard has been defined for their use and
1207 expression, these standards, technologies and services will be evaluated and considered for use in later
1208 versions of this specification.

1209 **4.1.5 Security Considerations**

1210 Implementors should take note, there is a vulnerability present even when an XML Digital Signature is
1211 used to protect to protect the integrity and origin of ebXML messages. The significance of the
1212 vulnerability necessarily depends on the deployed environment and the transport used to exchange
1213 ebXML messages.

1214 The vulnerability is present because ebXML messaging is an integration of both XML and MIME
1215 technologies. Whenever two or more technologies are conjoined there are always additional (sometimes
1216 unique) security issues to be addressed. In this case, MIME is used as the framework for the message
1217 package, containing the SOAP *Envelope* and any payload containers. Various elements of the SOAP
1218 *Envelope* make reference to the payloads, identified via MIME mechanisms. In addition, various labels
1219 are duplicated in both the SOAP *Envelope* and the MIME framework, for example, the type of the content
1220 in the payload. The issue is how and when all of this information is used.

1221 Specifically, the MIME Content-ID: header is used to specify a unique, identifying label for each payload.
1222 The label is used in the SOAP *Envelope* to identify the payload whenever it is needed. The MIME
1223 Content-Type: header is used to identify the type of content carried in the payload; some content types
1224 may contain additional parameters serving to further qualify the actual type. This information is available
1225 in the SOAP *Envelope*.

1226 The MIME headers are not protected, even when an XML-based digital signature is applied. Although
1227 XML Encryption is not currently available and thus not currently used, its application is developing
1228 similarly to XML digital signatures. Insofar as its application is the same as that of XML digital signatures,
1229 its use will not protect the MIME headers. Thus, an ebXML message may be at risk depending on how

1230 the information in the MIME headers is processed as compared to the information in the SOAP
1231 **Envelope**.

1232 The Content-ID: MIME header is critical. An adversary could easily mount a denial-of-service attack by
1233 mixing and matching payloads with the Content-ID: headers. As with most denial-of-service attacks, no
1234 specific protection is offered for this vulnerability. However, it should be detected since the digest
1235 calculated for the actual payload will not match the digest included in the SOAP **Envelope** when the
1236 digital signature is validated.

1237 The presence of the content type in both the MIME headers and SOAP **Envelope** is a problem. Ordinary
1238 security practices discourage duplicating information in two places. When information is duplicated,
1239 ordinary security practices require the information in both places to be compared to ensure they are
1240 equal. It would be considered a security violation if both sets of information fail to match.

1241 An adversary could change the MIME headers while a message is en route from its origin to its
1242 destination and this would not be detected when the security services are validated. This threat is less
1243 significant in a peer-to-peer transport environment as compared to a multi-hop transport environment. All
1244 implementations are at risk if the ebXML message is ever recorded in a long-term storage area since a
1245 compromise of that area puts the message at risk for modification.

1246 The actual risk depends on how an implementation uses each of the duplicate sets of information. If any
1247 processing beyond the MIME parsing for body part identification and separation is dependent on the
1248 information in the MIME headers, then the implementation is at risk of being directed to take unintended
1249 or undesirable actions. How this might be exploited is best compared to the common programming
1250 mistake of permitting buffer overflows: it depends on the creativity and persistence of the adversary.

1251 Thus, an implementation could reduce the risk by ensuring that the unprotected information in the MIME
1252 headers is never used except by the MIME parser for the minimum purpose of identifying and separating
1253 the body parts. This version of the specification makes no recommendation regarding whether or not an
1254 implementation should compare the duplicate sets of information nor what action to take based on the
1255 results of the comparison.

1256 4.2 Error Handling Module

1257 This section describes how one ebXML Message Service Handler (MSH) reports errors it detects in an
1258 ebXML Message to another MSH. The *ebXML Message Service* error reporting and handling module is
1259 to be considered as a layer of processing above the SOAP processor layer. This means the ebXML MSH
1260 is essentially an application-level handler of a *SOAP Message* from the perspective of the SOAP
1261 Processor. The SOAP processor MAY generate a SOAP **Fault** message if it is unable to process the
1262 message. A *Sending MSH* MUST be prepared to accept and process these SOAP **Fault** values.

1263 It is possible for the ebXML MSH software to cause a SOAP **Fault** to be generated and returned to the
1264 sender of a *SOAP Message*. In this event, the returned message MUST conform to the [SOAP]
1265 specification processing guidelines for SOAP **Fault** values.

1266 An ebXML *SOAP Message* reporting an error with a **highestSeverity** of **Warning** SHALL NOT be
1267 reported or returned as a SOAP **Fault**.

1268 4.2.1.1 Definitions:

1269 For clarity, two phrases are defined for use in this section:

- 1270 • "message in error" – A *message* containing or causing an error or warning of some kind
- 1271 • "message reporting the error" – A *message* containing an ebXML **ErrorList** element that describes the
1272 warning(s) and/or error(s) found in a message in error (also referred to as an *Error Message* elsewhere in
1273 this document).

1274 4.2.2 Types of Errors

1275 One MSH needs to report errors to another MSH. For example, errors associated with:

- 1276 • ebXML namespace qualified content of the *SOAP Message* document (see section 2.3.1)
- 1277 • reliable messaging failures (see section 6.5.7)
- 1278 • security (see section 4.1)

1279 Unless specified to the contrary, all references to "an error" in the remainder of this specification imply
1280 any or all of the types of errors listed above or defined elsewhere.

1281 Errors associated with data communications protocols are detected and reported using the standard
1282 mechanisms supported by that data communications protocol and do not use the error reporting
1283 mechanism described here.

1284 4.2.3 ErrorList Element

1285 The existence of an **ErrorList** extension element within the SOAP **Header** element indicates the
1286 message identified by the **RefToMessageId** in the **MessageHeader** element has an error.

1287 The **ErrorList** element consists of:

- 1288 • **id** attribute (see section 2.3.7 for details)
- 1289 • a **version** attribute (see section 2.3.8 for details)
- 1290 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)
- 1291 • **highestSeverity** attribute
- 1292 • one or more **Error** elements

1293 If there are no errors to be reported then the **ErrorList** element MUST NOT be present.

1294 4.2.3.1 highestSeverity attribute

1295 The **highestSeverity** attribute contains the highest severity of any of the **Error** elements. Specifically, if
1296 any of the **Error** elements have a **severity** of **Error**, **highestSeverity** MUST be set to **Error**, otherwise,
1297 **highestSeverity** MUST be set to **Warning**.

1298 4.2.3.2 Error Element

1299 An **Error** element consists of:

- 1300 • **id** attribute (see section 2.3.7 for details)
- 1301 • **codeContext** attribute
- 1302 • **errorCode** attribute
- 1303 • **severity** attribute
- 1304 • **location** attribute
- 1305 • **Description** element

1306 4.2.3.2.1 id attribute

1307 If the error is a part of an ebXML element, the **id** of the element MAY be provided for error tracking.

1308 4.2.3.2.2 codeContext attribute

1309 The **codeContext** attribute identifies the namespace or scheme for the **errorCodes**. It MUST be a URI.
1310 Its default value is **urn:oasis:names:tc:ebxml-msg:service:errors**. If it does not have the default value,
1311 then it indicates an implementation of this specification has used its own **errorCode** attribute values.

1312 Use of a **codeContext** attribute value other than the default is NOT RECOMMENDED. In addition, an
1313 implementation of this specification should not use its own **errorCode** attribute values if an existing
1314 **errorCode** as defined in this section has the same or very similar meaning.

1315 4.2.3.2.3 **errorCode attribute**

1316 The REQUIRED **errorCode** attribute indicates the nature of the error in the message in error. Valid
1317 values for the **errorCode** and a description of the code's meaning are given in the next section.

1318 4.2.3.2.4 **severity attribute**

1319 The REQUIRED **severity** attribute indicates the severity of the error. Valid values are:

- 1320 • **Warning** – This indicates other messages in the conversation could be generated in the normal way in spite
1321 of this problem.
- 1322 • **Error** – This indicates there is an unrecoverable error in the message and no further message processing
1323 should occur. Appropriate failure conditions should be communicated to the Application.

1324 4.2.3.2.5 **location attribute**

1325 The **location** attribute points to the part of the message containing the error.

1326 If an error exists in an ebXML element and the containing document is "well formed" (see XML [XML]),
1327 then the content of the **location** attribute MUST be an XPointer [XPointer].

1328 If the error is associated with an ebXML Payload Container, then **location** contains the `content-id` of
1329 the MIME part in error, using URI scheme "cid".

1330 4.2.3.2.6 **Description Element**

1331 The content of the **Description** element provides a narrative description of the error in the language
1332 defined by the **xml:lang** attribute. The XML parser or other software validating the message typically
1333 generates the message. The content is defined by the vendor/developer of the software that generated
1334 the **Error** element. (See section 3.1.8)

1335 4.2.3.3 **ErrorList Sample**

1336 An example of an **ErrorList** element is given below.

```
1337 <eb:ErrorList eb:id="3490sdo", eb:highestSeverity="error" eb:version="2.0" SOAP:mustUnderstand="1">
1338   <eb:Error eb:errorCode="SecurityFailure" eb:severity="Error" eb:location="URI_of_ds:Signature">
1339     <eb:Description xml:lang="en-US">Validation of signature failed<eb:Description>
1340   </eb:Error>
1341   <eb:Error ...> ... </eb:Error>
1342 </eb:ErrorList>
```

1343 4.2.3.4 **errorCode values**

1344 This section describes the values for the **errorCode** attribute used in a *message reporting an error*. They
1345 are described in a table with three headings:

- 1346 • the first column contains the value to be used as an **errorCode**, e.g. **SecurityFailure**
- 1347 • the second column contains a "Short Description" of the **errorCode**. This narrative MUST NOT be used in
1348 the content of the **Error** element.
- 1349 • the third column contains a "Long Description" that provides an explanation of the meaning of the error and
1350 provides guidance on when the particular **errorCode** should be used.

1351 4.2.3.4.1 **Reporting Errors in the ebXML Elements**

1352 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.

1353 **4.2.3.4.2 Non-XML Document Errors**

1354 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.

1355 **4.2.4 Implementing Error Reporting and Handling**1356 **4.2.4.1 When to Generate Error Messages**1357 When a MSH detects an error in a message it is strongly RECOMMENDED the error is reported to the
1358 MSH that sent the message in error. This is possible when:

- 1359 • the Error Reporting Location (see section 4.2.4.2) to which the message reporting the error should be sent
1360 can be determined
- 1361 • the message in error does not have an **ErrorList** element with **highestSeverity** set to **Error**.

1362 If the Error Reporting Location cannot be found or the message in error has an **ErrorList** element with
1363 **highestSeverity** set to **Error**, it is RECOMMENDED:

- 1364 • the error is logged
- 1365 • the problem is resolved by other means
- 1366 • no further action is taken.

1367 **4.2.4.2 Identifying the Error Reporting Location**1368 The Error Reporting Location is a URI specified by the sender of the message in error that indicates
1369 where to send a *message reporting the error*.

1370 The **ErrorURI** implied by the **CPA**, identified by the **CPAId** on the message, SHOULD be used.
 1371 Otherwise, the recipient MAY resolve an **ErrorURI** using the **From** element of the message in error. If
 1372 neither is possible, no error will be reported to the sending **Party**.

1373 Even if the message in error cannot be successfully analyzed, MSH implementers MAY try to determine
 1374 the Error Reporting Location by other means. How this is done is an implementation decision.

1375 4.2.4.3 Service and Action Element Values

1376 An **ErrorList** element can be included in a SOAP **Header** that is part of a *message* being sent as a result
 1377 of processing of an earlier message. In this case, the values for the **Service** and **Action** elements are
 1378 set by the designer of the Service. This method MUST NOT be used if the **highestSeverity** is **Error**.

1379 An **ErrorList** element can also be included in an independent *message*. In this case the values of the
 1380 **Service** and **Action** elements MUST be set as follows:

- 1381 • The **Service** element MUST be set to: **urn:oasis:names:tc:ebxml-msg:service**
- 1382 • The **Action** element MUST be set to **MessageError**.

1383 4.3 SyncReply Module

1384 It may be necessary for the sender of a message, using a synchronous communications protocol, such as
 1385 HTTP, to receive the associated response message over the same connection the request message was
 1386 delivered. In the case of HTTP, the sender of the HTTP request message containing an ebXML message
 1387 needs to have the response ebXML message delivered to it on the same HTTP connection.

1388 If there are intermediary nodes (either ebXML MSH nodes or possibly other SOAP nodes) involved in the
 1389 message path, it is necessary to provide some means by which the sender of a message can indicate it is
 1390 expecting a response so the intermediary nodes can keep the connection open.

1391 The **SyncReply** ebXML SOAP extension element is provided for this purpose.

1392 4.3.1 SyncReply Element

1393 The **SyncReply** element MAY be present as a direct child descendant of the SOAP **Header** element. It
 1394 consists of:

- 1395 • an **id** attribute (see section 2.3.7 for details)
- 1396 • a **version** attribute (see section 2.3.8 for details)
- 1397 • a SOAP **actor** attribute with the REQUIRED value of "**http://schemas.xmlsoap.org/soap/actor/next**"
- 1398 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)

1399 If present, this element indicates to the receiving SOAP or ebXML MSH node the connection over which
 1400 the message was received SHOULD be kept open in expectation of a response message to be returned
 1401 via the same connection.

1402 This element MUST NOT be used to override the value of **syncReplyMode** in the CPA. If the value of
 1403 **syncReplyMode** is **none** and a **SyncReply** element is present, the *Receiving MSH* should issue an error
 1404 with **errorCode** of **Inconsistent** and a **severity** of **Error** (see section 4.1.5).

1405 An example of a **SyncReply** element:

```
1406 <eb:SyncReply eb:id="3833kkj9" eb:version="2.0" SOAP:mustUnderstand="1"  
1407 SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
```

1408 5 Combining ebXML SOAP Extension Elements

1409 This section describes how the various ebXML SOAP extension elements may be used in combination.

1410 5.1.1 MessageHeader Element Interaction

1411 The **MessageHeader** element MUST be present in every message.

1412 **5.1.2 Manifest Element Interaction**

1413 The **Manifest** element MUST be present if there is any data associated with the message not present in
1414 the *Header Container*. This applies specifically to data in the *Payload Container(s)* or elsewhere, e.g. on
1415 the web.

1416 **5.1.3 Signature Element Interaction**

1417 One or more XML Signature [XMLDSIG] **Signature** elements MAY be present on any message.

1418 **5.1.4 ErrorList Element Interaction**

1419 If the **highestSeverity** attribute on the **ErrorList** is set to **Warning**, then this element MAY be present
1420 with any element.

1421 If the **highestSeverity** attribute on the **ErrorList** is set to **Error**, then this element MUST NOT be present
1422 with the **Manifest** element

1423 **5.1.5 SyncReply Element Interaction**

1424 The **SyncReply** element MAY be present on any outbound message sent using synchronous
1425 communication protocol.

1426

Part II. Additional Features

1427

6 Reliable Messaging Module

1428 Reliable Messaging defines an interoperable protocol such that two Message Service Handlers (MSH)
1429 can reliably exchange messages, using acknowledgment, retry and duplicate detection and elimination
1430 mechanisms, resulting in the *To Party* receiving the message Once-And-Only-Once. The protocol is
1431 flexible, allowing for both store-and-forward and end-to-end reliable messaging.

1432 Reliability is achieved by a *Receiving MSH* responding to a message with an *Acknowledgment Message*.
1433 An *Acknowledgment Message* is any ebXML message containing an **Acknowledgment** element. Failure
1434 to receive an *Acknowledgment Message* by a *Sending MSH* MAY trigger successive retries until such
1435 time as an *Acknowledgment Message* is received or the predetermined number of retries has been
1436 exceeded at which time the *From Party* MUST be notified of the probable delivery failure.

1437 Whenever an identical message may be received more than once, some method of duplicate detection
1438 and elimination is indicated, usually through the mechanism of a *persistent store*.

1439

6.1 Persistent Storage and System Failure

1440 A MSH that supports Reliable Messaging MUST keep messages sent or received reliably in *persistent*
1441 *storage*. In this context *persistent storage* is a method of storing data that does not lose information after
1442 a system failure or interruption.

1443 This specification recognizes different degrees of resilience may be realized depending upon the
1444 technology used to store the data. However, at a minimum, persistent storage with the resilience
1445 characteristics of a hard disk (or equivalent) SHOULD be used. It is strongly RECOMMENDED that
1446 implementers of this specification use technology resilient to the failure of any single hardware or
1447 software component.

1448 After a system interruption or failure, a MSH MUST ensure that messages in persistent storage are
1449 processed as if the system failure or interruption had not occurred. How this is done is an implementation
1450 decision.

1451 In order to support the filtering of duplicate messages, a *Receiving MSH* MUST save the **MessageId** in
1452 *persistent storage*. It is also RECOMMENDED the following be kept in *persistent storage*:

- 1453 • the complete message, at least until the information in the message has been passed to the application or
1454 other process needing to process it,
- 1455 • the time the message was received, so the information can be used to generate the response to a *Message*
1456 *Status Request* (see section 7.1.1),
- 1457 • the complete response message.

1458

6.2 Methods of Implementing Reliable Messaging

1459 Support for Reliable Messaging is implemented in one of the following ways:

- 1460 • using the ebXML Reliable Messaging protocol,
- 1461 • using ebXML SOAP structures together with commercial software products that are designed to provide
1462 reliable delivery of messages using alternative protocols,
- 1463 • user application support for some features, especially duplicate elimination, or
- 1464 • some mixture of the above options on a per-feature basis.

1465 6.3 Reliable Messaging SOAP Header Extensions

1466 6.3.1 AckRequested Element

1467 The **AckRequested** element is an OPTIONAL extension to the SOAP **Header** used by the *Sending MSH*
 1468 to request a *Receiving MSH*, acting in the role of the actor URI identified in the SOAP **actor** attribute,
 1469 returns an *Acknowledgment Message*.

1470 The **AckRequested** element contains the following:

- 1471 • a **id** attribute (see section 2.3.7 for details)
- 1472 • a **version** attribute (see section 2.3.8 for details)
- 1473 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)
- 1474 • a SOAP **actor** attribute
- 1475 • a **signed** attribute

1476 This element is used to indicate to a *Receiving MSH*, acting in the role identified by the SOAP **actor**
 1477 attribute, whether an *Acknowledgment Message* is expected, and if so, whether the message should be
 1478 signed by the *Receiving MSH*.

1479 An *ebXML Message* MAY have zero, one, or two instances of an **AckRequested** element. A single MSH
 1480 node SHOULD only insert one **AckRequested** element. If there are two **AckRequested** elements
 1481 present, they MUST have different values for their respective SOAP **actor** attributes. At most one
 1482 **AckRequested** element can be targeted at the **actor** URI meaning *Next MSH* (see section 2.3.10) and at
 1483 most one **AckRequested** element can be targeted at the **actor** URI meaning *To Party MSH* (see section
 1484 2.3.11) for any given message.

1485 6.3.1.1 SOAP actor attribute

1486 The **AckRequested** element MUST be targeted at either the *Next MSH* or the *To Party MSH* (these are
 1487 equivalent for single-hop routing). This is accomplished by including a SOAP **actor** with a URN value
 1488 with one of the two ebXML **actor** URNs defined in sections 2.3.10 and 2.3.11 or by leaving this attribute
 1489 out. The default **actor** targets the *To Party MSH*.

1490 6.3.1.2 signed attribute

1491 The REQUIRED **signed** attribute is used by a *From Party* to indicate whether or not a message received
 1492 by the *To Party MSH* should result in the *To Party* returning a signed *Acknowledgment Message* –
 1493 containing a [XMLDSIG] **Signature** element as described in section 4.1. Valid values for **signed** are:

- 1494 • **true** - a signed *Acknowledgment Message* is requested, or
- 1495 • **false** - an unsigned *Acknowledgment Message* is requested.

1496 Before setting the value of the **signed** attribute in **AckRequested**, the *Sending MSH* SHOULD check if
 1497 the *Receiving MSH* supports *Acknowledgment Messages* of the type requested (see also [ebCPP]).

1498 When a *Receiving MSH* receives a message with **signed** attribute set to **true** or **false** then it should verify
 1499 it is able to support the type of *Acknowledgment Message* requested.

- 1500 • If the *Receiving MSH* can produce the *Acknowledgment Message* of the type requested, then it MUST
 1501 return to the *Sending MSH* a message containing an **Acknowledgment** element.
- 1502 • If the *Receiving MSH* cannot return an *Acknowledgment Message* as requested it MUST report the error to
 1503 the *Sending MSH* using an **errorCode** of **Inconsistent** and a **severity** of either **Error** if inconsistent with the
 1504 CPA, or **Warning** if not supported..

1505 6.3.1.3 AckRequested Sample

1506 In the following example, an *Acknowledgment Message* is requested of a MSH node acting in the role of
 1507 the *To Party* (see section 2.3.11). The **Acknowledgment** element generated MUST be targeted to the

1508 ebXML MSH node acting in the role of the *From Party* along the reverse message path (end-to-end
1509 acknowledgment).

```
1510 <eb:AckRequested SOAP:mustUnderstand="1" eb:version="2.0" eb:signed="false"/>
```

1511 6.3.1.4 AckRequested Element Interaction

1512 An **AckRequested** element MUST NOT be included on a message with only an **Acknowledgment**
1513 element (no payload). This restriction is imposed to avoid endless loops of *Acknowledgment Messages*.
1514 An *Error Message* MUST NOT contain an **AckRequested** element.

1515 6.3.2 Acknowledgment Element

1516 The **Acknowledgment** element is an OPTIONAL extension to the SOAP **Header** used by one Message
1517 Service Handler to indicate to another Message Service Handler that it has received a message. The
1518 **RefToMessageId** element in an **Acknowledgment** element is used to identify the message being
1519 acknowledged by its **MessageId**.

1520 The **Acknowledgment** element consists of the following elements and attributes:

- 1521 • an **id** attribute (see section 2.3.7 for details)
- 1522 • a **version** attribute (see section 2.3.8 for details)
- 1523 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)
- 1524 • a SOAP **actor** attribute
- 1525 • a **Timestamp** element
- 1526 • a **RefToMessageId** element
- 1527 • a **From** element
- 1528 • zero or more [XMLDSIG] **Reference** element(s)

1529 6.3.2.1 SOAP actor attribute

1530 The SOAP **actor** attribute of the **Acknowledgment** element SHALL have a value corresponding to the
1531 **AckRequested** element of the message being acknowledged. If there is no SOAP **actor** attribute
1532 present on an **Acknowledgment** element, the default target is the *To Party MSH* (see section for 10.1.3).

1533 6.3.2.2 Timestamp Element

1534 The REQUIRED **Timestamp** element is a value representing the time that the message being
1535 acknowledged was received by the *MSH* generating the acknowledgment message. It must conform to a
1536 dateTime [XMLSchema] and is expressed as UTC (section 3.1.6.2).

1537 6.3.2.3 RefToMessageId Element

1538 The REQUIRED **RefToMessageId** element contains the **MessageId** of the message whose delivery is
1539 being reported.

1540 6.3.2.4 From Element

1541 This is the same element as the **From** element within **MessageHeader** element (see section 3.1.1).
1542 However, when used in the context of an **Acknowledgment** element, it contains the identifier of the *Party*
1543 generating the *Acknowledgment Message*.

1544 If the **From** element is omitted then the *Party* sending the element is identified by the **From** element in
1545 the **MessageHeader** element.

1546 6.3.2.5 [XMLDSIG] Reference Element

1547 An *Acknowledgment Message* MAY be used to enable non-repudiation of receipt by a MSH by including
1548 one or more **Reference** elements, from the XML Signature [XMLDSIG] namespace, derived from the
1549 *message being acknowledged* (see section 4.1.3 for details). The **Reference** element(s) MUST be

1550 namespace qualified to the aforementioned namespace and MUST conform to the XML Signature
 1551 [XMLDSIG] specification. If the *message being acknowledged* contains an **AckRequested** element with
 1552 a **signed** attribute set to **true**, then the [XMLDSIG] **Reference** list is REQUIRED.

1553 Receipt of an *Acknowledgment Message*, indicates the original message reached its destination. Receipt
 1554 of a signed *Acknowledgment Message* validates the sender of the *Acknowledgment Message*. However,
 1555 a signed *Acknowledgment Message* does not indicate whether the message arrived intact. Including a
 1556 digest (see [XMLDSIG] section 4.3.3) of the original message in the *Acknowledgment Message* indicates
 1557 to the original sender what was received by the recipient of the message being acknowledged. The
 1558 digest contained in the *Acknowledgment Message* may be compared to a digest of the original message.
 1559 If the digests match, the message arrived intact. Such a digest already exists in the original message, if it
 1560 is signed, contained within the [XMLDSIG] **Signature / Reference** element(s).

1561 If the original message is signed, the [XMLDSIG] **Signature / Reference** element(s) of the original
 1562 message will be identical to the **Acknowledgment / [XMLDSIG] Reference** element(s) in the
 1563 *Acknowledgment Message*. If the original message is not signed, the [XMLDSIG] **Reference** element
 1564 must be derived from the original message (see section 4.1.3).

1565 Upon receipt of an end-to-end *Acknowledgment Message*, the *From Party MSH* MAY notify the
 1566 application of successful delivery for the referenced message. This MSH SHOULD ignore subsequent
 1567 *Error* or *Acknowledgment Messages* with the same **RefToMessageId** value.

1568 6.3.2.6 Acknowledgment Sample

1569 An example **Acknowledgment** element targeted at the *To Party MSH*:

```
1570 <eb:Acknowledgment SOAP:mustUnderstand="1" eb:version="2.0">
1571   <eb:Timestamp>2001-03-09T12:22:30</eb:Timestamp>
1572   <eb:RefToMessageId>323210:e52151ec74:7ffc@xtacy</eb:RefToMessageId>
1573   <eb:From> <eb:PartyId>uri:www.example.com</eb:PartyId> </eb:From>
1574 </eb:Acknowledgment>
```

1575 6.3.2.7 Sending an Acknowledgment Message by Itself

1576 If there are no errors in the message received and an *Acknowledgment Message* is being sent on its own,
 1577 not as a message containing payload data, then the **Service** and **Action** MUST be set as follows:

- 1578 • the **Service** element MUST be set to **urn:oasis:names:tc:ebxml-msg:service**
- 1579 • the **Action** element MUST be set to **Acknowledgment**

1580 6.3.2.8 Acknowledgment Element Interaction

1581 An **Acknowledgment** element MAY be present on any message, except as noted in section 6.3.1.4. An
 1582 *Acknowledgment Message* MUST NOT be returned for an *Error Message*.

1583 6.4 Reliable Messaging Parameters

1584 This section describes the parameters required to control reliable messaging. Many of these parameters
 1585 can be obtained from a CPA.

1586 6.4.1 DuplicateElimination

1587 The **DuplicateElimination** element MUST be used by the *From Party MSH* to indicate whether the
 1588 *Receiving MSH* MUST eliminate duplicates (see section 6.6 for Reliable Messaging behaviors). If the
 1589 value of **DuplicateElimination** in the CPA is **never**, **DuplicateElimination** MUST NOT be present.

- 1590 • If **DuplicateElimination** is present – The *To Party MSH* must persist messages in a persistent store so
 1591 duplicate messages will be presented to the *To Party Application At-Most-Once*, or
- 1592 • If **DuplicateElimination** is not present – The *To Party MSH* is not required to maintain the message in
 1593 persistent store and is not required to check for duplicates.

1594 If **DuplicateElimination** is present, the *To Party MSH* must adopt a reliable messaging behavior (see
 1595 section 6.6) causing duplicate messages to be ignored.

1596 If **DuplicateElimination** is not present, a *Receiving MSH* is not required to check for duplicate message
1597 delivery. Duplicate messages might be delivered to an application and persistent storage of messages is
1598 not required – although elimination of duplicates is still allowed.

1599 If the *To Party* is unable to support the requested functionality, or if the value of **duplicateElimination** in
1600 the CPA does not match the implied value of the element, the *To Party* SHOULD report the error to the
1601 *From Party* using an **errorCode** of **Inconsistent** and a **Severity** of **Error**.

1602 **6.4.2 AckRequested**

1603 The **AckRequested** parameter is used by the *Sending MSH* to request a *Receiving MSH*, acting in the
1604 role of the actor URI identified in the SOAP **actor** attribute, return an *Acknowledgment Message*
1605 containing an **Acknowledgment** element (see section 6.3.1).

1606 **6.4.3 Retries**

1607 The **Retries** parameter, from a CPA, is an integer value specifying the maximum number of times a
1608 *Sending MSH* SHOULD attempt to redeliver an unacknowledged *message* using the same
1609 communications protocol.

1610 **6.4.4 RetryInterval**

1611 The **RetryInterval** parameter, from a CPA, is a time value, expressed as a duration in accordance with
1612 the **duration** [XMLSchema] data type. This value specifies the minimum time a *Sending MSH* SHOULD
1613 wait between **Retries**, if an *Acknowledgment Message* is not received or if a communications error was
1614 detected during an attempt to send the message. **RetryInterval** applies to the time between sending of
1615 the original message and the first retry as well as the time between retries.

1616 **6.4.5 TimeToLive**

1617 **TimeToLive** is defined in section 3.1.6.4.

1618 For a reliably delivered message, **TimeToLive** MUST conform to:

1619
$$\mathbf{TimeToLive} > \mathbf{Timestamp} + ((\mathbf{Retries} + 1) * \mathbf{RetryInterval}).$$

1620 where **TimeStamp** comes from **MessageData**.

1621 **6.4.6 PersistDuration**

1622 The **PersistDuration** parameter, from a CPA, is the minimum length of time, expressed as a **duration**
1623 [XMLSchema], data from a reliably sent *Message*, is kept in *Persistent Storage* by a *Receiving MSH*.

1624 If the **PersistDuration** has passed since the message was first sent, a *Sending MSH* SHOULD NOT
1625 resend a message with the same **MessageId**.

1626 If a message cannot be sent successfully before **PersistDuration** has passed, then the *Sending MSH*
1627 should report a delivery failure (see section 6.5.7).

1628 **TimeStamp** for a reliably sent message (found in the message header), plus its **PersistDuration** (found
1629 in the CPA), must be greater than its **TimeToLive** (found in the message header).

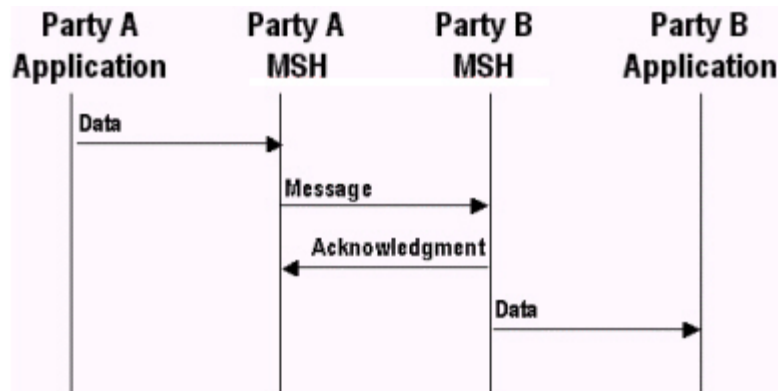
1630 **6.4.7 syncReplyMode**

1631 The **syncReplyMode** parameter from the CPA is used only if the data communications protocol is
1632 *synchronous* (e.g. HTTP). If the communications protocol is not *synchronous*, then the value of
1633 **syncReplyMode** is ignored. If the **syncReplyMode** attribute is not present, it is semantically equivalent
1634 to its presence with a value of **none**. If the **syncReplyMode** parameter is not **none**, a **SyncReply**
1635 element MUST be present and the MSH must return any response from the application or business
1636 process in the payload of the *synchronous* reply message, as specified in the CPA. Valid values of
1637 **syncReplyMode** are **mshSignalsOnly**, **signalsOnly**, **signalsAndResponse**, **responseOnly**, and **none**.
1638 See also the description of **syncReplyMode** in the CPPA [ebCPP] specification.

1639 If the value of *syncReplyMode* is *none* and a *SyncReply* element is present, the *Receiving MSH* should
 1640 issue an error with *errorCode* of *Inconsistent* and a *severity* of *Error* (see section 4.1.5).

1641 6.5 ebXML Reliable Messaging Protocol

1642 The ebXML Reliable Messaging Protocol is illustrated by the following figure.



1643
 1644 **Figure 6-1 Indicating a message has been received**

1645 The receipt of the *Acknowledgment Message* indicates the message being acknowledged has been
 1646 successfully received and either processed or persisted by the *Receiving MSH*.

1647 An *Acknowledgment Message* MUST contain an *Acknowledgment* element as described in section 6.3.1
 1648 with a *RefToMessageId* containing the same value as the *MessageId* element in the *message being*
 1649 *acknowledged*.

1650 6.5.1 Sending Message Behavior

1651 If a MSH is given data by an application needing to be sent reliably, the MSH MUST do the following:

- 1652 1. Create a message from components received from the application.
- 1653 2. Insert an *AckRequested* element as defined in section 6.3.1.
- 1654 3. Save the message in *persistent storage* (see section 6.1).
- 1655 4. Send the message to the *Receiving MSH*.
- 1656 5. Wait for the return of an *Acknowledgment Message* acknowledging receipt of this specific
 1657 message and, if it does not arrive before *RetryInterval* has elapsed, or if a communications
 1658 protocol error is encountered, then take the appropriate action as described in section 6.5.4.

1659 6.5.2 Receiving Message Behavior

1660 If this is an *Acknowledgment Message* as defined in section 6 then:

- 1661 1 Look for a message in *persistent storage* with a *MessageId* the same as the value of
 1662 *RefToMessageId* on the received Message.
- 1663 2 If a message is found in *persistent storage* then mark the persisted message as delivered.

1664 If the *Receiving MSH* is NOT the *To Party MSH* (as defined in section 2.3.10 and 2.3.11), then see
 1665 section 10.1.3 for the behavior of the *AckRequested* element.

1666 If an *AckRequested* element is present (not an *Acknowledgment Message*) then:

- 1667 1 If the message is a duplicate (i.e. there is a *MessageId* held in persistent storage containing the
 1668 same value as the *MessageId* in the received message), generate an *Acknowledgment Message*
 1669 (see section 6.5.3). Follow the procedure in section 6.5.5 for resending lost *Acknowledgment*

1670 *Messages*. The *Receiving MSH* MUST NOT deliver the message to the application interface.
 1671 Note: The check for duplicates is only performed when **DuplicateElimination** is present.

1672 2 If the message is not a duplicate or (there is no **MessageId** held in persistent storage
 1673 corresponding to the **MessageId** in the received message) then:

1674 a If there is a **DuplicateElimination** element, save the **MessageId** of the received message in
 1675 persistent storage. As an implementation decision, the whole message MAY be stored.

1676 b Generate an *Acknowledgment Message* in response (this may be as part of another
 1677 message). The *Receiving MSH* MUST NOT send an *Acknowledgment Message* until the
 1678 message has been safely stored in *persistent storage* or delivered to the application
 1679 interface. Delivery of an *Acknowledgment Message* constitutes an obligation by the
 1680 *Receiving MSH* to deliver the message to the application or forward to the next MSH in the
 1681 message path as appropriate.

1682 If there is no **AckRequested** element then do the following:

1683 1 If there is a **DuplicateElimination** element, and the message is a duplicate, then do nothing.

1684 2 Otherwise, deliver the message to the application interface

1685 If the *Receiving MSH* node is operating as an intermediary along the message's message path, then it
 1686 MAY use store-and-forward behavior. However, it MUST NOT filter out perceived duplicate messages
 1687 from their normal processing at that node.

1688 If an *Acknowledgment Message* is received unexpectedly, it should be ignored. No error should be sent.

1689 6.5.3 Generating an Acknowledgment Message

1690 An *Acknowledgment Message* MUST be generated whenever a message is received with an
 1691 **AckRequested** element having a SOAP **actor** URI targeting the *Receiving MSH* node.

1692 As a minimum, it MUST contain an **Acknowledgment** element with a **RefToMessageId** containing the
 1693 same value as the **MessageId** element in the message being acknowledged. This message MUST be
 1694 placed in persistent storage with the same **PersistDuration** as the original message.

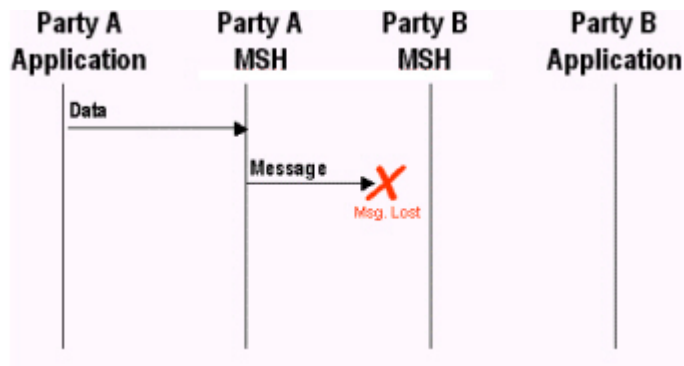
1695 The *Acknowledgment Message* can be sent at the same time as the response to the received message.
 1696 In this case, the values for the **MessageHeader** elements of the *Acknowledgment Message* are
 1697 determined by the **Service** and **Action** associated with the business response.

1698 If an *Acknowledgment Message* is being sent on its own, then the value of the **MessageHeader** elements
 1699 MUST be set as follows:

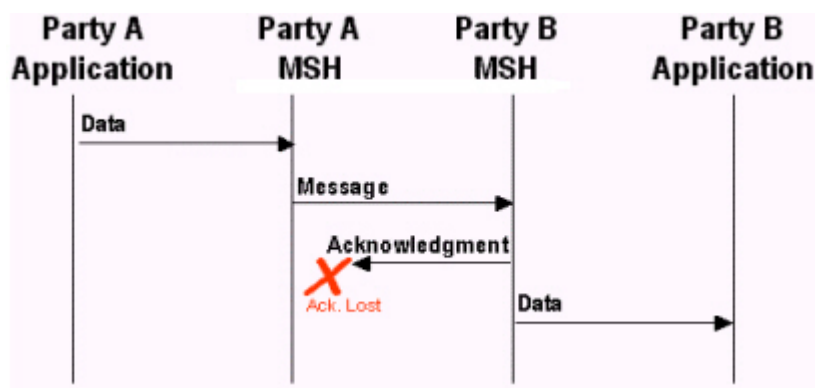
- 1700 • The **Service** element MUST be set to: **urn:oasis:names:tc:ebxml-msg:service**
- 1701 • The **Action** element MUST be set to **Acknowledgment**.
- 1702 • The **From** element MAY be populated with the **To** element extracted from the message received and all
 1703 child elements from the **To** element received SHOULD be included in this **From** element.
- 1704 • The **To** element MAY be populated with the **From** element extracted from the message received and all
 1705 child elements from the **From** element received SHOULD be included in this **To** element.
- 1706 • The **RefToMessageId** element MUST be set to the **MessageId** of the message received.

1707 6.5.4 Resending Lost Application Messages

1708 This section describes the behavior required by the sender and receiver of a message in order to handle
 1709 lost messages. A message is "lost" when a *Sending MSH* does not receive a positive acknowledgment to
 1710 a message. For example, it is possible a *message* was lost:



1711

1712 **Figure 6-2 Undelivered Message**1713 It is also possible the *Acknowledgment Message* was lost, for example:

1714

1715 **Figure 6-3 Lost Acknowledgment Message**1716 Note: *Acknowledgment Messages* are never acknowledged.1717 The rules applying to the non-receipt of an anticipated *Acknowledgment* due to the loss of either the
1718 application message or the *Acknowledgment Message* are as follows:

- 1719 • The *Sending MSH* MUST resend the original message if an *Acknowledgment Message* has been requested
1720 but has not been received and the following are true:
 - 1721 • At least the time specified in the **RetryInterval** parameter has passed since the message was last sent,
 - 1722 • The message has been resent less than the number of times specified in the **Retries** parameter.
- 1723 • If the *Sending MSH* does not receive an *Acknowledgment Message* after the maximum number of retries,
1724 the *Sending MSH* SHALL notify the application and/or system administrator function of the failure to receive
1725 an *Acknowledgment Message* (see also section 4.2.3.2.4 concerning treatment of errors).
- 1726 • If the *Sending MSH* detects a communications protocol error, the *Sending MSH* MUST resend the message
1727 using the same algorithm as if it has not received an *Acknowledgment Message*.

1728 **6.5.5 Resending Acknowledgments**1729 If the *Receiving MSH* receives a message it discovers to be a duplicate, it should resend the original
1730 *Acknowledgment Message* if the message is stored in *persistent store*. In this case, do the following:1731 Look in persistent storage for the first response to the received message (i.e. it contains a
1732 **RefToMessageId** that matches the **MessageId** of the received message).1733 If a response message was found in *persistent storage* then resend the persisted message back to the
1734 MSH that sent the received message. If no response message was found in *persistent storage*, then:

- 1735 (1) If **syncReplyMode** is not set to **none** and if the CPA indicates an application response is
1736 included, then it must be the case that the application has not finished processing the earlier

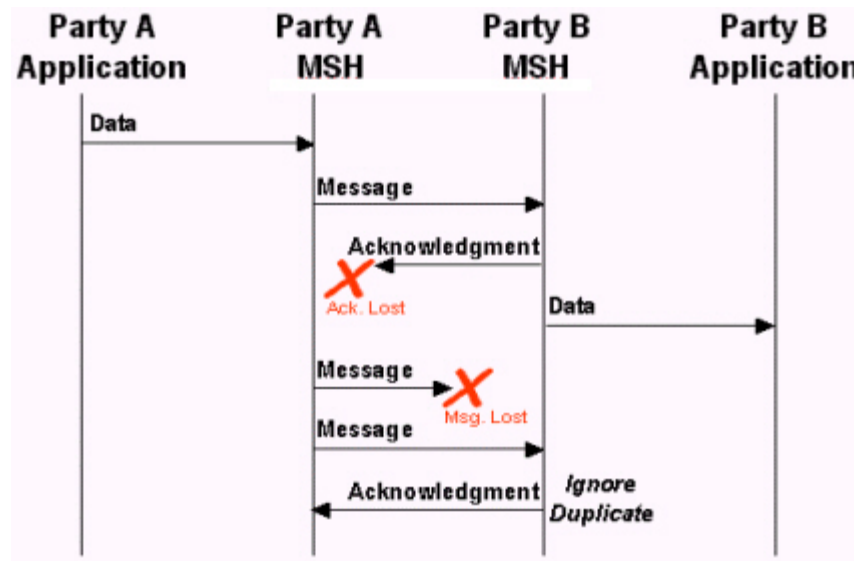
1737 copy of the same message. Therefore, wait for the response from the application and then
 1738 return that response synchronously over the same connection that was used for the
 1739 retransmission.

1740 (2) Otherwise, generate an *Acknowledgment Message*.

1741 6.5.6 Duplicate Message Handling

1742 In the context of this specification:

- 1743 • an "identical message" – a *message* containing the same ebXML SOAP **Header**, **Body** and ebXML Payload
 1744 Container(s) as the earlier sent *message*.
- 1745 • a "duplicate message" – a *message* containing the same **MessageId** as a previously received message.
- 1746 • the "first response message" – the message with the earliest **Timestamp** in the **MessageData** element
 1747 having the same **RefToMessageId** as the duplicate message.



1748

1749

Figure 6-4 Resending Unacknowledged Messages

1750 The diagram above shows the behavior to be followed by the *Sending* and *Receiving* MSH for messages
 1751 sent with an **AckRequested** element and a **DuplicateElimination** element. Specifically:

- 1752 1) The sender of the *message* (e.g. Party A MSH) MUST resend the "identical message" if no
 1753 *Acknowledgment Message* is received.
- 1754 2) When the recipient (Party B MSH) of the *message* receives a "duplicate message", it MUST resend to
 1755 the sender (Party A MSH) an *Acknowledgment Message* identical to the *first response message* sent
 1756 to the sender Party A MSH).
- 1757 3) The recipient of the *message* (Party B MSH) MUST NOT forward the message a second time to the
 1758 application/process.

1759 6.5.7 Failed Message Delivery

1760 If a message sent with an **AckRequested** element cannot be delivered, the MSH or process handling the
 1761 message (as in the case of a routing intermediary) SHALL send a delivery failure notification to the *From*
 1762 *Party*. The delivery failure notification message is an *Error Message* with **errorCode** of **DeliveryFailure**
 1763 and a **severity** of:

- 1764 • **Error** if the party who detected the problem could not transmit the message (e.g. the communications
 1765 transport was not available)
- 1766 • **Warning** if the message was transmitted, but an *Acknowledgment Message* was not received. This means
 1767 the message probably was not delivered.

1768 It is possible an error message with an **Error** element having an **errorCode** set to **DeliveryFailure**
 1769 cannot be delivered successfully for some reason. If this occurs, then the *From Party*, the ultimate
 1770 destination for the *Error Message*, MUST be informed of the problem by other means. How this is done is
 1771 outside the scope of this specification

1772 Note: If the *From Party MSH* receives an *Acknowledgment Message* from the *To Party MSH*, it should ignore all
 1773 other **DeliveryFailure** or *Acknowledgment Messages*.

1774 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

1775 [§]Duplicate Elimination is only performed at the To Party MSH, not at the Intermediate Level.

1776 7 Message Status Service

1777 The Message Status Request Service consists of the following:

- 1778 • A Message Status Request message containing details regarding a message previously sent is sent to a
 1779 Message Service Handler (MSH)
- 1780 • The Message Service Handler receiving the request responds with a Message Status Response message.

1781 A Message Service Handler SHOULD respond to Message Status Requests for messages that have
 1782 been sent reliably and the **MessageId** in the **RefToMessageId** is present in *persistent storage* (see
 1783 section 6.1).

1784 A Message Service Handler MAY respond to Message Status Requests for messages that have not been
 1785 sent reliably.

1786 A Message Service SHOULD NOT use the Message Status Request Service to implement Reliable
 1787 Messaging.

1788 If a *Receiving MSH* does not support the service requested, it SHOULD return an *Error Message* with an
 1789 **errorCode** of **NotSupported** and a **highestSeverity** attribute set to **Error**. Each service is described
 1790 below.

1791 7.1 Message Status Messages

1792 7.1.1 Message Status Request Message

1793 A Message Status Request message consists of an *ebXML Message* with no ebXML Payload Container
1794 and the following:

- 1795 • a **MessageHeader** element containing:
 - 1796 • a **From** element identifying the *Party* that created the Message Status Request message
 - 1797 • a **To** element identifying a *Party* who should receive the message.
 - 1798 • a **Service** element that contains: **urn:oasis:names:tc:ebxml-msg:service**
 - 1799 • an **Action** element that contains **StatusRequest**
 - 1800 • a **MessageData** element
- 1801 • a **StatusRequest** element containing:
 - 1802 • a **RefToMessageld** element in **StatusRequest** element containing the **Messageld** of the message
1803 whose status is being queried.
- 1804 • an [XMLDSIG] **Signature** element (see section 4.1 for more details)

1805 The message is then sent to the *To Party*.

1806 7.1.2 Message Status Response Message

1807 Once the *To Party* receives the Message Status Request message, they SHOULD generate a Message
1808 Status Response message with no ebXML Payload Container consisting of the following:

- 1809 • a **MessageHeader** element containing:
 - 1810 ▪ a **From** element that identifies the sender of the Message Status Response message
 - 1811 ▪ a **To** element set to the value of the **From** element in the Message Status Request message
 - 1812 ▪ a **Service** element that contains **urn:oasis:names:tc:ebxml-msg:service**
 - 1813 ▪ an **Action** element that contains **StatusResponse**
 - 1814 ▪ a **MessageData** element containing:
 - 1815 • a **RefToMessageld** that identifies the Message Status Request message.
- 1816 • **StatusResponse** element (see section 7.2.3)
- 1817 • an [XMLDSIG] **Signature** element (see section 4.1 for more details)

1818 The message is then sent to the *To Party*.

1819 7.1.3 Security Considerations

1820 Parties who receive a Message Status Request message SHOULD always respond to the message.
1821 However, they MAY ignore the message instead of responding with **messageStatus** set to
1822 **Unauthorized** if they consider the sender of the message to be unauthorized. The decision process
1823 resulting in this course of action is implementation dependent.

1824 7.2 StatusRequest Element

1825 The OPTIONAL **StatusRequest** element is an immediate child of a SOAP **Body** and is used to identify
1826 an earlier message whose status is being requested (see section 7.3.5).

1827 The **StatusRequest** element consists of the following:

- 1828 • an **id** attribute (see section 2.3.7 for details)
- 1829 • a **version** attribute (see section 2.3.8 for details)
- 1830 • a **RefToMessageld** element

1831 7.2.1 RefToMessageId Element

1832 A REQUIRED *RefToMessageId* element contains the *MessageId* of the message whose status is being
1833 requested.

1834 7.2.2 StatusRequest Sample

1835 An example of the *StatusRequest* element is given below:

```
1836 <eb:StatusRequest eb:version="2.0" >
1837   <eb:RefToMessageId>323210:e52151ec74:-7ffc@xtacy</eb:RefToMessageId>
1838 </eb:StatusRequest>
```

1839 7.2.3 StatusRequest Element Interaction

1840 A *StatusRequest* element MUST NOT be present with the following elements:

- 1841 • a *Manifest* element
- 1842 • a *StatusResponse* element
- 1843 • an *ErrorList* element

1844 7.3 StatusResponse Element

1845 The OPTIONAL *StatusResponse* element is an immediate child of a SOAP *Body* and is used by one
1846 MSH to describe the status of processing of a message.

1847 The *StatusResponse* element consists of the following elements and attributes:

- 1848 • an *id* attribute (see section 2.3.7 for details)
- 1849 • a *version* attribute (see section 2.3.8 for details)
- 1850 • a *RefToMessageId* element
- 1851 • a *Timestamp* element
- 1852 • a *messageStatus* attribute

1853 7.3.1 RefToMessageId Element

1854 A REQUIRED *RefToMessageId* element contains the *MessageId* of the message whose status is being
1855 reported. *RefToMessageId* element child of the *MessageData* element of a message containing a
1856 *StatusResponse* element SHALL have the *MessageId* of the message containing the *StatusRequest*
1857 element to which the *StatusResponse* element applies. The *RefToMessageId* child element of the
1858 *StatusRequest* or *StatusResponse* element SHALL contain the *MessageId* of the message whose
1859 status is being queried.

1860 7.3.2 Timestamp Element

1861 The *Timestamp* element contains the time the message, whose status is being reported, was received
1862 (section 3.1.6.2.). This MUST be omitted if the message, whose status is being reported, is
1863 *NotRecognized* or the request was *Unauthorized*.

1864 7.3.3 messageStatus attribute

1865 The REQUIRED *messageStatus* attribute identifies the status of the message identified by the
1866 *RefToMessageId* element. It SHALL be set to one of the following values:

- 1867 • *Unauthorized* – the Message Status Request is not authorized or accepted
- 1868 • *NotRecognized* – the message identified by the *RefToMessageId* element in the *StatusResponse*
1869 element is not recognized
- 1870 • *Received* – the message identified by the *RefToMessageId* element in the *StatusResponse* element has
1871 been received by the MSH
- 1872 • *Processed* – the message identified by the *RefToMessageId* element in the *StatusResponse* element has
1873 been processed by the MSH

- 1874 • **Forwarded** – the message identified by the **RefToMessageId** element in the **StatusResponse** element has
1875 been forwarded by the MSH to another MSH

1876 Note: if a Message Status Request is sent after the elapsed time indicated by **PersistDuration** has passed since the
1877 message being queried was sent, the Message Status Response may indicate the **MessageId** was **NotRecognized** –
1878 the **MessageId** is no longer in persistent storage.

1879 7.3.4 StatusResponse Sample

1880 An example of the **StatusResponse** element is given below:

```
1881 <eb:StatusResponse eb:version="2.0" eb:messageStatus="Received">
1882   <eb:RefToMessageId>323210:e52151ec74:-7ffc@xtacy</eb:RefToMessageId>
1883   <eb:Timestamp>2001-03-09T12:22:30</eb:Timestamp>
1884 </eb:StatusResponse>
```

1885 7.3.5 StatusResponse Element Interaction

1886 This element MUST NOT be present with the following elements:

- 1887 • a **Manifest** element
1888 • a **StatusRequest** element
1889 • an **ErrorList** element with a **highestSeverity** attribute set to **Error**

1890 8 Message Service Handler Ping Service

1891 The OPTIONAL Message Service Handler Ping Service enables one MSH to determine if another MSH is
1892 operating. It consists of:

- 1893 • one MSH sending a Message Service Handler Ping message to a MSH, and
1894 • another MSH, receiving the Ping, responding with a Message Service Handler Pong message.

1895 If a *Receiving MSH* does not support the service requested, it SHOULD return an *Error Message* with an
1896 **errorCode** of **NotSupported** and a **highestSeverity** attribute set to **Error**.

1897 8.1 Message Service Handler Ping Message

1898 A Message Service Handler Ping (MSH Ping) message consists of an *ebXML Message* containing no
1899 ebXML Payload Container and the following:

- 1900 • a **MessageHeader** element containing the following:
- 1901 • a **From** element identifying the *Party* creating the MSH Ping message
 - 1902 • a **To** element identifying the *Party* being sent the MSH Ping message
 - 1903 • a **CPAId** element
 - 1904 • a **ConversationId** element
 - 1905 • a **Service** element containing: **urn:oasis:names:tc:ebxml-msg:service**
 - 1906 • an **Action** element containing **Ping**
 - 1907 • a **MessageData** element
- 1908 • an [XMLDSIG] **Signature** element (see section 4.1 for details).

1909 The message is then sent to the *To Party*.

1910 An example Ping:

```
1911 . . .Transport Headers
1912 SOAPAction: "ebXML"
1913 Content-type: multipart/related; boundary="ebXMLBoundary"
1914
1915 --ebXMLBoundary
1916 Content-Type: text/xml
1917
```



```

1918 <?xml version="1.0" encoding="UTF-8"?>
1919 <SOAP:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1920   xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
1921   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
1922     http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
1923 <SOAP:Header xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
1924   xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
1925     http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
1926   <eb:MessageHeader version="2.0" SOAP:mustUnderstand="1"
1927     xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
1928     xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
1929       http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
1930     <eb:From> <eb:PartyId>urn:duns:123456789</eb:PartyId> </eb:From>
1931     <eb:To> <eb:PartyId>urn:duns:912345678</eb:PartyId> </eb:To>
1932     <eb:CPAId>20001209-133003-28572</eb:CPAId>
1933     <eb:ConversationId>20010215-111213-28572</eb:ConversationId>
1934     <eb:Service>urn:oasis:names:tc:ebxml-msg:service</eb:Service>
1935     <eb:Action>Ping</eb:Action>
1936     <eb:MessageData>
1937       <eb:MessageId>20010215-111212-28572@example.com</eb:MessageId>
1938       <eb:Timestamp>2001-02-15T11:12:12</eb:Timestamp>
1939     </eb:MessageData>
1940   </eb:MessageHeader>
1941 </SOAP:Header>
1942 <SOAP:Body/>
1943 </SOAP:Envelope>
1944
1945 --ebXMLBoundary--

```

1946 Note: The above example shows a Multipart/Related MIME structure with only one bodypart.

1947 8.2 Message Service Handler Pong Message

1948 Once the *To Party* receives the MSH Ping message, they MAY generate a Message Service Handler
 1949 Pong (MSH Pong) message consisting of an ebXML Message containing no ebXML Payload Container
 1950 and the following:

- 1951 • a **MessageHeader** element containing the following:
 - 1952 • a **From** element identifying the creator of the MSH Pong message
 - 1953 • a **To** element identifying a *Party* that generated the MSH Ping message
 - 1954 • a **CPAId** element
 - 1955 • a **ConversationId** element
 - 1956 • a **Service** element containing the value: *urn:oasis:names:tc:ebxml-msg:service*
 - 1957 • an **Action** element containing the value **Pong**
 - 1958 • a **MessageData** element containing:
 - 1959 • a **RefToMessageId** identifying the MSH Ping message.
- 1960 • an [XMLDSIG] **Signature** element (see section 4.1.1 for details).

1961 An example Pong:

```

1962 . . .Transport Headers
1963 SOAPAction: "ebXML"
1964 Content-Type: text/xml
1965
1966 <?xml version="1.0" encoding="UTF-8"?>
1967 <SOAP:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
1968   xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
1969   xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
1970     http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
1971 <SOAP:Header xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
1972   xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
1973     http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
1974   <eb:MessageHeader eb:version="2.0" SOAP:mustUnderstand="1">
1975     <eb:From> <eb:PartyId>urn:duns:912345678</eb:PartyId> </eb:From>
1976     <eb:To> <eb:PartyId>urn:duns:123456789</eb:PartyId> </eb:To>

```

```

1977 <eb:CPAId>20001209-133003-28572</eb:CPAId>
1978 <eb:ConversationId>20010215-111213-28572</eb:ConversationId>
1979 <eb:Service>urn:oasis:names:tc:ebxml-msg:service</eb:Service>
1980 <eb:Action>Pong</eb:Action>
1981 <eb:MessageData>
1982   <eb:MessageId>20010215-111213-395884@example2.com</eb:MessageId>
1983   <eb:Timestamp>2001-02-15T11:12:13</eb:Timestamp>
1984   <eb:RefToMessageId>20010215-111212-28572@example.com</eb:RefToMessageId>
1985 </eb:MessageData>
1986 </eb:MessageHeader>
1987 </SOAP:Header>
1988 <SOAP:Body/>
1989 </SOAP:Envelope>

```

1990 Note: This example shows a non-multipart MIME structure.

1991 8.3 Security Considerations

1992 Parties who receive a MSH Ping message SHOULD always respond to the message. However, there is
 1993 a risk some parties might use the MSH Ping message to determine the existence of a Message Service
 1994 Handler as part of a security attack on that MSH. Therefore, recipients of a MSH Ping MAY ignore the
 1995 message if they consider that the sender of the message received is unauthorized or part of some attack.
 1996 The decision process that results in this course of action is implementation dependent.

1997 9 MessageOrder Module

1998 The **MessageOrder** module allows messages to be presented to the *To Party* in a particular order. This
 1999 is accomplished through the use of the **MessageOrder** element. Reliable Messaging MUST be used
 2000 when a **MessageOrder** element is present.

2001 **MessageOrder** module MUST only be used in conjunction with the ebXML Reliable Messaging Module
 2002 (section 6) with a scheme of Once-And-Only-Once (sections 6.6). If a sequence is sent and one
 2003 message fails to arrive at the *To Party MSH*, all subsequent messages will also fail to be presented to the
 2004 *To Party Application* (see **status** attribute section 9.1.1).

2005 9.1 MessageOrder Element

2006 The **MessageOrder** element is an OPTIONAL extension to the SOAP **Header** requesting the
 2007 preservation of message order in this conversation.

2008 The **MessageOrder** element contains the following:

- 2009 • a **id** attribute (see section 2.3.7)
- 2010 • a **version** attribute (see section 2.3.8 for details)
- 2011 • a SOAP **mustUnderstand** attribute with a value of "1" (see section 2.3.9 for details)
- 2012 • a **SequenceNumber** element

2013 When the **MessageOrder** element is present, **DuplicateElimination** MUST also be present and
 2014 **SyncReply** MUST NOT be present.

2015 9.1.1 SequenceNumber Element

2016 The REQUIRED **SequenceNumber** element indicates the sequence a *Receiving MSH* MUST process
 2017 messages. The **SequenceNumber** is unique within the **ConversationId** and MSH. The *From Party MSH*
 2018 and the *To Party MSH* each set an independent **SequenceNumber** as the *Sending MSH* within the
 2019 **ConversationId**. It is set to zero on the first message from that MSH within a conversation and then
 2020 incremented by one for each subsequent message sent.

2021 A MSH that receives a message with a **SequenceNumber** element MUST NOT pass the message to an
 2022 application until all the messages with a lower **SequenceNumber** have been passed to the application.

2023 If the implementation defined limit for saved out-of-sequence messages is reached, then the *Receiving*
 2024 *MSH* MUST indicate a delivery failure to the *Sending MSH* with **errorCode** set to **DeliveryFailure** and
 2025 **severity** set to **Error** (see section 4.1.5).

2026 The **SequenceNumber** element is an integer value incremented by the *Sending MSH* (e.g. 0, 1, 2, 3, 4...)
 2027 for each application-prepared message sent by that MSH within the **ConversationId**. The next value after
 2028 99999999 in the increment is "0". The value of **SequenceNumber** consists of ASCII numerals in the
 2029 range 0-99999999. In following cases, **SequenceNumber** takes the value "0":

- 2030 1. First message from the *Sending MSH* within the conversation
- 2031 2. First message after resetting **SequenceNumber** information by the *Sending MSH*
- 2032 3. First message after wraparound (next value after 99999999)

2033 The **SequenceNumber** element has a single attribute, **status**. This attribute is an enumeration, which
 2034 SHALL have one of the following values:

- 2035 • **Reset** – the **SequenceNumber** is reset as shown in 1 or 2 above
- 2036 • **Continue** – the **SequenceNumber** continues sequentially (including 3 above)

2037 When the **SequenceNumber** is set to "0" because of 1 or 2 above, the *Sending MSH* MUST set the
 2038 **status** attribute of the message to **Reset**. In all other cases, including 3 above, the **status** attribute
 2039 MUST be set to **Continue**. The default value of the **status** attribute is **Continue**.

2040 A *Sending MSH* MUST wait before resetting the **SequenceNumber** of a conversation until it has received
 2041 confirmation of all the messages previously sent for the conversation. Only when all the sent Messages
 2042 are accounted for, can the *Sending MSH* reset the **SequenceNumber**.

2043 9.1.2 MessageOrder Sample

2044 An example of the **MessageOrder** element is given below:

```
2045 <eb:MessageOrder eb:version="2.0" SOAP:mustUnderstand="1">
2046   <eb:SequenceNumber>00000010</eb:SequenceNumber>
2047 </eb:MessageOrder>
```

2048 9.2 MessageOrder Element Interaction

2049 For this version of the ebXML Messaging Specification, the **MessageOrder** element MUST NOT be
 2050 present with the **SyncReply** element. If these two elements are received in the same message, the
 2051 *Receiving MSH* SHOULD report an error (see section 4.1.5) with **errorCode** set to **Inconsistent** and
 2052 **severity** set to **Error**.

2053 10 Multi-Hop Module

2054 Multi-hop is the process of passing the message through one or more intermediary nodes or MSH's. An
 2055 Intermediary is any node or MSH where the message is received, but is not the *Sending* or *Receiving*
 2056 *MSH*. This node is called an Intermediary.

2057 Intermediaries may be for the purpose of Store-and-Forward or may be involved in some processing
 2058 activity such as a trusted third-party timestamp service. For the purposes of this version of this
 2059 specification, Intermediaries are considered only as Store-and-Forward entities.

2060 Intermediaries MAY be involved in removing and adding SOAP extension elements or modules targeted
 2061 either to the **Next** SOAP node or the **NextMSH**. SOAP rules specify, the receiving node must remove
 2062 any element or module targeted to the **Next** SOAP node. If the element or module needs to continue to
 2063 appear on the SOAP message destined to the **Next** SOAP node, or in this specification the **NextMSH**, it
 2064 must be reapplied. This deleting and adding of elements or modules poses potential difficulties for signed
 2065 ebXML messages. Any Intermediary node or MSH MUST NOT change, format or in any way modify any
 2066 element not targeted to the Intermediary. Any such change may invalidate the signature.

2067 10.1 Multi-hop Reliable Messaging

2068 Multi-hop (hop-to-hop) Reliable Messaging is accomplished using the **AckRequested** element (section
2069 6.3.1) and an *Acknowledgment Message* containing an **Acknowledgment** element (section 6.3.1.4) each
2070 with a SOAP **actor** of **Next MSH** (section 2.3.10) between the *Sending MSH* and the *Receiving MSH*.
2071 This MAY be used in store-and-forward multi-hop situations.

2072 The use of the duplicate elimination is not required for Intermediate nodes. Since duplicate elimination by
2073 an intermediate MSH can interfere with End-to-End Reliable Messaging Retries, the intermediate MSH
2074 MUST know it is an intermediate and MUST NOT perform duplicate elimination tasks.

2075 At this time, the values of **Retry** and **RetryInterval** between Intermediate MSHs remains implementation
2076 specific. See section 6.4 for more detail on Reliable Messaging.

2077 10.1.1 AckRequested Sample

2078 An example of the **AckRequested** element targeted at the **NextMSH** is given below:

```
2079 <eb:AckRequested SOAP:mustUnderstand="1" eb:version="2.0" eb:signed="false"  
2080 SOAP:actor="urn:oasis:names:tc:ebxml-msg:actor:nextMSH" />
```

2081 In the preceding example, an *Acknowledgment Message* is requested of the next ebXML MSH node (see
2082 section 2.3.10) in the message. The **Acknowledgment** element generated MUST be targeted at the next
2083 ebXML MSH node along the reverse message path (the *Sending MSH*) using the SOAP **actor** with a
2084 value of **NextMSH** (section 2.3.10).

2085 Any Intermediary receiving an **AckRequested** with SOAP **actor** of **NextMSH** MUST remove the
2086 **AckRequested** element before forwarding to the next MSH. Any Intermediary MAY insert a single
2087 **AckRequested** element into the SOAP **Header** with a SOAP **actor** of **NextMSH**. There SHALL NOT be
2088 two **AckRequested** elements targeted at the next MSH.

2089 When the **SyncReply** element is present, an **AckRequested** element with SOAP **actor** of **NextMSH**
2090 MUST NOT be present. If the **SyncReply** element is not present, the Intermediary MAY return the
2091 Intermediate *Acknowledgment Message* synchronously with a synchronous transport protocol. If these
2092 two elements are received in the same message, the *Receiving MSH* SHOULD report an error (see
2093 section 4.1.5) with **errorCode** set to **Inconsistent** and **severity** set to **Error**.

2094 10.1.2 Acknowledgment Sample

2095 An example of the **Acknowledgment** element targeted at the **NextMSH** is given below:

```
2096 <eb:Acknowledgment SOAP:mustUnderstand="1" eb:version="2.0"  
2097 SOAP:actor="urn:oasis:names:tc:ebxml-msg:actor:nextMSH">  
2098 <eb:Timestamp>2001-03-09T12:22:30</eb:Timestamp>  
2099 <eb:RefToMessageId>323210:e52151ec74:-7ffc@xtacy</eb:RefToMessageId>  
2100 <eb:From> <eb:PartyId>uri:www.example.com</eb:PartyId> </eb:From>  
2101 </eb:Acknowledgment>
```

2102 10.1.3 Multi-Hop Acknowledgments

2103 There MAY be two **AckRequested** elements on the same message. An **Acknowledgment** MUST be
2104 sent for each **AckRequested** using an identical SOAP **actor** attribute as the **AckRequested** element.

2105 If the *Receiving MSH* is the *To Party MSH*, then see section 6.5.2. If the *Receiving MSH* is the *To Party*
2106 *MSH* and there is an **AckRequested** element targeting the Next MSH (the *To Party MSH* is acting in both
2107 roles), then perform both procedures (this section and section 6.5.2) for generating *Acknowledgment*
2108 *Messages*. This MAY require sending two **Acknowledgment** elements, possibly on the same message,
2109 one targeted for the *Next MSH* and one targeted for the *To Party MSH*.

2110 There MAY be multiple **Acknowledgements** elements, on the same message or on different messages,
2111 returning from either the Next MSH or from the *To Party MSH*. A MSH supporting Multi-hop MUST
2112 differentiate, based upon the **actor**, which **Acknowledgment** is being returned and act accordingly.

2113 If this is an *Acknowledgment Message* as defined in section 6 then:

- 2114 1 Look for a message in *persistent storage* with a **MessageId** the same as the value of
2115 **RefToMessageId** on the received Message.
- 2116 2 If a message is found in *persistent storage* then mark the persisted message as delivered.

2117 If an **AckRequested** element is present (not an *Acknowledgment Message*) then generate an
2118 *Acknowledgment Message* in response (this may be as part of another message). The *Receiving MSH*
2119 MUST NOT send an *Acknowledgment Message* until the message has been persisted or delivered to the
2120 *Next MSH*.

2121 **10.1.4 Signing Multi-Hop Acknowledgments**

2122 When a signed Intermediate *Acknowledgment Message* is requested (i.e. a signed *Acknowledgment*
2123 *Message* with a SOAP **actor** of **NextMSH**), it MUST be sent by itself and not bundled with any other
2124 message. The XML Signature [XMLDSIG] **Signature** element with **Transforms**, as described in section
2125 4.1.3, will exclude this **Acknowledgment** element. To send a signed *Acknowledgment Message* with
2126 SOAP **actor** of **NextMSH**, create a message with no payloads, including a single **Acknowledgment**
2127 element (see section 6.3.2.6), and a [XMLDSIG] **Signature** element with the following **Transforms**:

```
2128           <Transforms>
2129             <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
2130             <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
2131           </Transforms>
```

2132 **10.1.5 Multi-Hop Security Considerations**

2133 SOAP messaging allows intermediaries to add or remove elements targeted to the intermediary node.
2134 This has potential conflicts with end-to-end signatures since the slightest change in any character of the
2135 SOAP **Envelope** or to a payload will invalidate the **ds:Signature** by changing the calculated digest.
2136 Intermediaries MUST NOT add or remove elements unless they contain a SOAP **actor** of **next** or
2137 **nextMSH**. Intermediaries MUST NOT disturb white space – line terminators (CR/LF), tabs, spaces, etc. –
2138 outside those elements being added or removed.

2139 **10.2 Message Ordering and Multi-Hop**

2140 Intermediary MSH nodes MUST NOT participate in Message Order processing as specified in section 9.

2141

Part III. Normative Appendices

2142 Appendix A The ebXML SOAP Extension Elements Schema

2143 The OASIS ebXML Messaging Technical Committee has provided a version of the SOAP 1.1 envelope
2144 schema specified using the schema vocabulary that conforms to the W3C XML Schema
2145 Recommendation specification [XMLSchema].

2146 SOAP1.1- <http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd>

2147 It was necessary to craft a schema for the XLINK [XLINK] attribute vocabulary to conform to the W3C
2148 XML Schema Recommendation [XMLSchema]. This schema is referenced from the ebXML SOAP
2149 extension elements schema and is available from the following URL:

2150 Xlink - <http://www.oasis-open.org/committees/ebxml-msg/schema/xlink.xsd>

```

2151 <?xml version="1.0" encoding="UTF-8"?>
2152 <!-- Some parsers may require explicit declaration of xmlns:xml="http://www.w3.org/XML/1998/namespace".
2153      In that case, a copy of this schema augmented with the above declaration should be cached and used
2154      for the purpose of schema validation on ebXML messages. -->
2155 <schema targetNamespace="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2156       xmlns:tns="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2157       xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
2158       xmlns:xlink="http://www.w3.org/1999/xlink"
2159       xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
2160       xmlns="http://www.w3.org/2001/XMLSchema"
2161       elementFormDefault="qualified"
2162       attributeFormDefault="qualified"
2163       version="1.0">
2164   <import namespace="http://www.w3.org/2000/09/xmldsig#"
2165     schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd" />
2166   <import namespace="http://www.w3.org/1999/xlink"
2167     schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/xlink.xsd" />
2168   <import namespace="http://schemas.xmlsoap.org/soap/envelope/"
2169     schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd" />
2170   <import namespace="http://www.w3.org/XML/1998/namespace"
2171     schemaLocation="http://www.w3.org/2001/03/xml.xsd" />
2172   <!-- MANIFEST, for use in soap:Body element -->
2173   <element name="Manifest">
2174     <complexType>
2175       <sequence>
2176         <element ref="tns:Reference" maxOccurs="unbounded" />
2177         <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
2178       </sequence>
2179       <attributeGroup ref="tns:bodyExtension.grp" />
2180     </complexType>
2181   </element>
2182   <element name="Reference">
2183     <complexType>
2184       <sequence>
2185         <element ref="tns:Schema" minOccurs="0" maxOccurs="unbounded" />
2186         <element ref="tns:Description" minOccurs="0" maxOccurs="unbounded" />
2187         <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
2188       </sequence>
2189       <attribute ref="tns:id" />
2190       <attribute ref="xlink:type" fixed="simple" />
2191       <attribute ref="xlink:href" use="required" />
2192       <attribute ref="xlink:role" />
2193       <anyAttribute namespace="##other" processContents="lax" />
2194     </complexType>
2195   </element>
2196   <element name="Schema">
2197     <complexType>
2198       <attribute name="location" type="anyURI" use="required" />
2199       <attribute name="version" type="tns:non-empty-string" />
2200     </complexType>

```

```

2201 </element>
2202 <!-- MESSAGEHEADER, for use in soap:Header element -->
2203 <element name="MessageHeader">
2204   <complexType>
2205     <sequence>
2206       <element ref="tns:From"/>
2207       <element ref="tns:To"/>
2208       <element ref="tns:CPAId"/>
2209       <element ref="tns:ConversationId"/>
2210       <element ref="tns:Service"/>
2211       <element ref="tns:Action"/>
2212       <element ref="tns:MessageData"/>
2213       <element ref="tns:DuplicateElimination" minOccurs="0"/>
2214       <element ref="tns:Description" minOccurs="0" maxOccurs="unbounded"/>
2215       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2216     </sequence>
2217     <attributeGroup ref="tns:headerExtension.grp"/>
2218   </complexType>
2219 </element>
2220 <element name="CPAId" type="tns:non-empty-string"/>
2221 <element name="ConversationId" type="tns:non-empty-string"/>
2222 <element name="Service">
2223   <complexType>
2224     <simpleContent>
2225       <extension base="tns:non-empty-string">
2226         <attribute name="type" type="tns:non-empty-string"/>
2227       </extension>
2228     </simpleContent>
2229   </complexType>
2230 </element>
2231 <element name="Action" type="tns:non-empty-string"/>
2232 <element name="MessageData">
2233   <complexType>
2234     <sequence>
2235       <element ref="tns:MessageId"/>
2236       <element ref="tns:Timestamp"/>
2237       <element ref="tns:RefToMessageId" minOccurs="0"/>
2238       <element ref="tns:TimeToLive" minOccurs="0"/>
2239     </sequence>
2240   </complexType>
2241 </element>
2242 <element name="MessageId" type="tns:non-empty-string"/>
2243 <element name="TimeToLive" type="dateTime"/>
2244 <element name="DuplicateElimination">
2245 </element>
2246 <!-- SYNC REPLY, for use in soap:Header element -->
2247 <element name="SyncReply">
2248   <complexType>
2249     <sequence>
2250       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2251     </sequence>
2252     <attributeGroup ref="tns:headerExtension.grp"/>
2253     <attribute ref="soap:actor" use="required"/>
2254   </complexType>
2255 </element>
2256 <!-- MESSAGE ORDER, for use in soap:Header element -->
2257 <element name="MessageOrder">
2258   <complexType>
2259     <sequence>
2260       <element ref="tns:SequenceNumber"/>
2261       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
2262     </sequence>
2263     <attributeGroup ref="tns:headerExtension.grp"/>
2264   </complexType>
2265 </element>
2266 <element name="SequenceNumber" type="tns:sequenceNumber.type"/>
2267 <!-- ACK REQUESTED, for use in soap:Header element -->
2268 <element name="AckRequested">
2269   <complexType>
2270     <sequence>
2271       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

```

```

2272     </sequence>
2273     <attributeGroup ref="tns:headerExtension.grp" />
2274     <attribute ref="soap:actor" />
2275     <attribute name="signed" type="boolean" use="required" />
2276   </complexType>
2277 </element>
2278 <!-- ACKNOWLEDGMENT, for use in soap:Header element -->
2279 <element name="Acknowledgment">
2280   <complexType>
2281     <sequence>
2282       <element ref="tns:Timestamp" />
2283       <element ref="tns:RefToMessageId" />
2284       <element ref="tns:From" minOccurs="0" />
2285       <element ref="ds:Reference" minOccurs="0" maxOccurs="unbounded" />
2286       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
2287     </sequence>
2288     <attributeGroup ref="tns:headerExtension.grp" />
2289     <attribute ref="soap:actor" />
2290   </complexType>
2291 </element>
2292 <!-- ERROR LIST, for use in soap:Header element -->
2293 <element name="ErrorList">
2294   <complexType>
2295     <sequence>
2296       <element ref="tns:Error" maxOccurs="unbounded" />
2297       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
2298     </sequence>
2299     <attributeGroup ref="tns:headerExtension.grp" />
2300     <attribute name="highestSeverity" type="tns:severity.type" use="required" />
2301   </complexType>
2302 </element>
2303 <element name="Error">
2304   <complexType>
2305     <sequence>
2306       <element ref="tns:Description" minOccurs="0" />
2307       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
2308     </sequence>
2309     <attribute ref="tns:id" />
2310     <attribute name="codeContext" type="anyURI"
2311       default="urn:oasis:names:tc:ebxml-msg:service:errors" />
2312     <attribute name="errorCode" type="tns:non-empty-string" use="required" />
2313     <attribute name="severity" type="tns:severity.type" use="required" />
2314     <attribute name="location" type="tns:non-empty-string" />
2315     <anyAttribute namespace="##other" processContents="lax" />
2316   </complexType>
2317 </element>
2318 <!-- STATUS RESPONSE, for use in soap:Body element -->
2319 <element name="StatusResponse">
2320   <complexType>
2321     <sequence>
2322       <element ref="tns:RefToMessageId" />
2323       <element ref="tns:Timestamp" minOccurs="0" />
2324       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
2325     </sequence>
2326     <attributeGroup ref="tns:bodyExtension.grp" />
2327     <attribute name="messageStatus" type="tns:messageStatus.type" use="required" />
2328   </complexType>
2329 </element>
2330 <!-- STATUS REQUEST, for use in soap:Body element -->
2331 <element name="StatusRequest">
2332   <complexType>
2333     <sequence>
2334       <element ref="tns:RefToMessageId" />
2335       <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded" />
2336     </sequence>
2337     <attributeGroup ref="tns:bodyExtension.grp" />
2338   </complexType>
2339 </element>
2340 <!-- COMMON TYPES -->
2341 <complexType name="sequenceNumber.type">
2342   <simpleContent>

```



```

2343     <extension base="nonNegativeInteger">
2344         <attribute name="status" type="tns:status.type" default="Continue"/>
2345     </extension>
2346 </simpleContent>
2347 </complexType>
2348 <simpleType name="status.type">
2349     <restriction base="NMTOKEN">
2350         <enumeration value="Reset"/>
2351         <enumeration value="Continue"/>
2352     </restriction>
2353 </simpleType>
2354 <simpleType name="messageStatus.type">
2355     <restriction base="NMTOKEN">
2356         <enumeration value="Unauthorized"/>
2357         <enumeration value="NotRecognized"/>
2358         <enumeration value="Received"/>
2359         <enumeration value="Processed"/>
2360         <enumeration value="Forwarded"/>
2361     </restriction>
2362 </simpleType>
2363 <simpleType name="non-empty-string">
2364     <restriction base="string">
2365         <minLength value="1"/>
2366     </restriction>
2367 </simpleType>
2368 <simpleType name="severity.type">
2369     <restriction base="NMTOKEN">
2370         <enumeration value="Warning"/>
2371         <enumeration value="Error"/>
2372     </restriction>
2373 </simpleType>
2374 <!-- COMMON ATTRIBUTES and ATTRIBUTE GROUPS -->
2375 <attribute name="id" type="ID"/>
2376 <attribute name="version" type="tns:non-empty-string"/>
2377 <attributeGroup name="headerExtension.grp">
2378     <attribute ref="tns:id"/>
2379     <attribute ref="tns:version" use="required"/>
2380     <attribute ref="soap:mustUnderstand" use="required"/>
2381     <anyAttribute namespace="##other" processContents="lax"/>
2382 </attributeGroup>
2383 <attributeGroup name="bodyExtension.grp">
2384     <attribute ref="tns:id"/>
2385     <attribute ref="tns:version" use="required"/>
2386     <anyAttribute namespace="##other" processContents="lax"/>
2387 </attributeGroup>
2388 <!-- COMMON ELEMENTS -->
2389 <element name="PartyId">
2390     <complexType>
2391         <simpleContent>
2392             <extension base="tns:non-empty-string">
2393                 <attribute name="type" type="tns:non-empty-string"/>
2394             </extension>
2395         </simpleContent>
2396     </complexType>
2397 </element>
2398 <element name="To">
2399     <complexType>
2400         <sequence>
2401             <element ref="tns:PartyId" maxOccurs="unbounded"/>
2402             <element name="Role" type="tns:non-empty-string" minOccurs="0"/>
2403         </sequence>
2404     </complexType>
2405 </element>
2406 <element name="From">
2407     <complexType>
2408         <sequence>
2409             <element ref="tns:PartyId" maxOccurs="unbounded"/>
2410             <element name="Role" type="tns:non-empty-string" minOccurs="0"/>
2411         </sequence>
2412     </complexType>
2413 </element>

```

```
2414 <element name="Description">
2415   <complexType>
2416     <simpleContent>
2417       <extension base="tns:non-empty-string">
2418         <attribute ref="xml:lang" use="required" />
2419       </extension>
2420     </simpleContent>
2421   </complexType>
2422 </element>
2423 <element name="RefToMessageId" type="tns:non-empty-string" />
2424 <element name="Timestamp" type="dateTime" />
2425 </schema>
```

2426 Appendix B Communications Protocol Bindings

2427 B.1 Introduction

2428 One of the goals of this specification is to design a message handling service usable over a variety of
 2429 network and application level transport protocols. These protocols serve as the "carrier" of ebXML
 2430 Messages and provide the underlying services necessary to carry out a complete ebXML Message
 2431 exchange between two parties. HTTP, FTP, Java Message Service (JMS) and SMTP are examples of
 2432 application level transport protocols. TCP and SNA/LU6.2 are examples of network transport protocols.
 2433 Transport protocols vary in their support for data content, processing behavior and error handling and
 2434 reporting. For example, it is customary to send binary data in raw form over HTTP. However, in the case
 2435 of SMTP it is customary to "encode" binary data into a 7-bit representation. HTTP is equally capable of
 2436 carrying out *synchronous* or *asynchronous* message exchanges whereas it is likely that message
 2437 exchanges occurring over SMTP will be *asynchronous*. This section describes the technical details
 2438 needed to implement this abstract ebXML Message Handling Service over particular transport protocols.

2439 This section specifies communications protocol bindings and technical details for carrying *ebXML*
 2440 *Message Service* messages for the following communications protocols:

- 2441 • Hypertext Transfer Protocol [RFC2616], in both *asynchronous* and *synchronous* forms of transfer.
- 2442 • Simple Mail Transfer Protocol [RFC2821], in *asynchronous* form of transfer only.

2443 B.2 HTTP

2444 B.2.1 Minimum level of HTTP protocol

2445 Hypertext Transfer Protocol Version 1.1 [RFC2616] is the minimum level of protocol that **MUST** be used.

2446 B.2.2 Sending ebXML Service messages over HTTP

2447 Even though several HTTP request methods are available, this specification only defines the use of HTTP
 2448 POST requests for sending *ebXML Message Service* messages over HTTP. The identity of the ebXML
 2449 MSH (e.g. `ebxmlhandler`) may be part of the HTTP POST request:

2450 `POST /ebxmlhandler HTTP/1.1`

2451 Prior to sending over HTTP, an ebXML Message **MUST** be formatted according to ebXML Message
 2452 Service Specification. Additionally, the messages **MUST** conform to the HTTP specific MIME canonical
 2453 form constraints specified in section 19.4 of RFC 2616 [RFC2616] specification.

2454 HTTP protocol natively supports 8-bit and Binary data. Hence, transfer encoding is **OPTIONAL** for such
 2455 parts in an ebXML Service Message prior to sending over HTTP. However, content-transfer-encoding of
 2456 such parts (e.g. using base64 encoding scheme) is not precluded by this specification.

2457 The rules for forming an HTTP message containing an ebXML Service Message are as follows:

- 2458 • The **Content-Type: Multipart/Related** MIME header with the associated parameters, from the
 2459 ebXML Service Message Envelope **MUST** appear as an HTTP header.
- 2460 • All other MIME headers that constitute the ebXML Message Envelope **MUST** also become part of the HTTP
 2461 header.
- 2462 • The mandatory `SOAPAction` HTTP header field must also be included in the HTTP header and **MAY** have
 2463 a value of "ebXML"

2464 `SOAPAction: "ebXML"`

- 2465 • Other headers with semantics defined by MIME specifications, such as Content-Transfer-Encoding, **SHALL**
 2466 **NOT** appear as HTTP headers. Specifically, the "MIME-Version: 1.0" header **MUST NOT** appear as an
 2467 HTTP header. However, HTTP-specific MIME-like headers defined by HTTP 1.1 **MAY** be used with the
 2468 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:

```

2473 POST /servlet/ebXMLhandler HTTP/1.1
2474 Host: www.example2.com
2475 SOAPAction: "ebXML"
2476 Content-type: multipart/related; boundary="BoundaryY"; type="text/xml";
2477         start="<ebxmhheader111@example.com>"
2478
2479 --BoundaryY
2480 Content-ID: <ebxmhheader111@example.com>
2481 Content-Type: text/xml
2482
2483 <?xml version="1.0" encoding="UTF-8"?>
2484 <SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
2485     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
2486     xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
2487     xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2488     xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
2489         http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd
2490         http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
2491         http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
2492 <SOAP:Header>
2493   <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
2494     <eb:From>
2495       <eb:PartyId>urn:duns:123456789</eb:PartyId>
2496     </eb:From>
2497     <eb:To>
2498       <eb:PartyId>urn:duns:912345678</eb:PartyId>
2499     </eb:To>
2500     <eb:CPAId>20001209-133003-28572</eb:CPAId>
2501     <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
2502     <eb:Service>urn:services:SupplierOrderProcessing</eb:Service>
2503     <eb:Action>NewOrder</eb:Action>
2504     <eb:MessageData>
2505       <eb:MessageId>20001209-133003-28572@example.com</eb:MessageId>
2506       <eb:Timestamp>2001-02-15T11:12:12</eb:Timestamp>
2507     </eb:MessageData>
2508   </eb:MessageHeader>
2509 </SOAP:Header>
2510 <SOAP:Body>
2511   <eb:Manifest eb:version="2.0">
2512     <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
2513       xlink:role="XLinkRole" xlink:type="simple">
2514       <eb:Description xml:lang="en-US">Purchase Order 1</eb:Description>
2515     </eb:Reference>
2516   </eb:Manifest>
2517 </SOAP:Body>
2518 </SOAP:Envelope>
2519
2520 --BoundaryY--
2521 Content-ID: <ebxmlpayload111@example.com>
2522 Content-Type: text/xml
2523
2524 <?xml version="1.0" encoding="UTF-8"?>
2525 <purchase_order>
2526   <po_number>1</po_number>
2527   <part_number>123</part_number>
2528   <price currency="USD">500.00</price>
2529 </purchase_order>
2530
2531 --BoundaryY--

```

2532 B.2.3 HTTP Response Codes

2533 In general, semantics of communicating over HTTP as specified in the [RFC2616] MUST be followed, for
 2534 returning the HTTP level response codes. A 2xx code MUST be returned when the HTTP Posted

2535 message is successfully received by the receiving HTTP entity. However, see exception for SOAP error
2536 conditions below. Similarly, other HTTP codes in the 3xx, 4xx, 5xx range MAY be returned for conditions
2537 corresponding to them. However, error conditions encountered while processing an ebXML Service
2538 Message MUST be reported using the error mechanism defined by the ebXML Message Service
2539 Specification (see section 4.1.5).

2540 **B.2.4 SOAP Error conditions and Synchronous Exchanges**

2541 The SOAP 1.1 specification states:

2542 "*In case of a SOAP error while processing the request, the SOAP HTTP server MUST issue an HTTP*
2543 *500 "Internal Server Error" response and include a SOAP message in the response containing a SOAP*
2544 *Fault element indicating the SOAP processing error.*"

2545 However, the scope of the SOAP 1.1 specification is limited to *synchronous* mode of message exchange
2546 over HTTP, whereas the ebXML Message Service Specification specifies both *synchronous* and
2547 *asynchronous* modes of message exchange over HTTP. Hence, the SOAP 1.1 specification MUST be
2548 followed for *synchronous* mode of message exchange, where the SOAP Message containing a SOAP
2549 **Fault** element indicating the SOAP processing error MUST be returned in the HTTP response with a
2550 response code of "HTTP 500 Internal Server Error". When *asynchronous* mode of message exchange is
2551 being used, a HTTP response code in the range 2xx MUST be returned when the message is received
2552 successfully and any error conditions (including SOAP errors) must be returned via separate HTTP Post.

2553 **B.2.5 Synchronous vs. Asynchronous**

2554 When a synchronous transport is in use, the MSH response message(s) SHOULD be returned on the
2555 same HTTP connection as the inbound request, with an appropriate HTTP response code, as described
2556 above. When the **syncReplyMode** parameter is set to values other than **none**, the application response
2557 messages, if any, are also returned on the same HTTP connection as the inbound request, rather than
2558 using an independent HTTP Post request. If the **syncReplyMode** has a value of **none**, an HTTP
2559 response with a response code as defined in section B.2.3 above and with an empty HTTP body MUST
2560 be returned in response to the HTTP Post.

2561 **B.2.6 Access Control**

2562 Implementers MAY protect their ebXML Message Service Handlers from unauthorized access through the
2563 use of an access control mechanism. The HTTP access authentication process described in "HTTP
2564 Authentication: Basic and Digest Access Authentication" [RFC2617] defines the access control
2565 mechanisms allowed to protect an ebXML Message Service Handler from unauthorized access.

2566 Implementers MAY support all of the access control schemes defined in [RFC2617] including support of
2567 the Basic Authentication mechanism, as described in [RFC2617] section 2, when Access Control is used.

2568 Implementers that use basic authentication for access control SHOULD also use communications
2569 protocol level security, as specified in the section titled "Confidentiality and Transport Protocol Level
2570 Security" in this document.

2571 **B.2.7 Confidentiality and Transport Protocol Level Security**

2572 An ebXML Message Service Handler MAY use transport layer encryption to protect the confidentiality of
2573 ebXML Messages and HTTP transport headers. The IETF Transport Layer Security specification TLS
2574 [RFC2246] provides the specific technical details and list of allowable options, which may be used by
2575 ebXML Message Service Handlers. ebXML Message Service Handlers MUST be capable of operating in
2576 backwards compatibility mode with SSL [SSL3], as defined in Appendix E of TLS [RFC2246].

2577 ebXML Message Service Handlers MAY use any of the allowable encryption algorithms and key sizes
2578 specified within TLS [RFC2246]. At a minimum ebXML Message Service Handlers MUST support the key
2579 sizes and algorithms necessary for backward compatibility with [SSL3].

2580 The use of 40-bit encryption keys/algorithms is permitted, however it is RECOMMENDED that stronger
2581 encryption keys/algorithms SHOULD be used.

2582 Both TLS [RFC2246] and SSL [SSL3] require the use of server side digital certificates. Client side
2583 certificate based authentication is also permitted. All ebXML Message Service handlers MUST support
2584 hierarchical and peer-to-peer or direct-trust trust models.

2585 **B.3 SMTP**

2586 The Simple Mail Transfer Protocol (SMTP) [RFC2821] specification is commonly referred to as Internet
2587 Electronic Mail. This specifications has been augmented over the years by other specifications, which
2588 define additional functionality "layered on top" of this baseline specifications. These include:

2589 Multipurpose Internet Mail Extensions (MIME) [RFC2045], [RFC2046], [RFC2387]

2590 SMTP Service Extension for Authentication [RFC2554]

2591 SMTP Service Extension for Secure SMTP over TLS [RFC2487]

2592 Typically, Internet Electronic Mail Implementations consist of two "agent" types:

2593 Message Transfer Agent (MTA): Programs that send and receive mail messages with other MTA's on
2594 behalf of MUA's. Microsoft Exchange Server is an example of a MTA

2595 Mail User Agent (MUA): Electronic Mail programs are used to construct electronic mail messages and
2596 communicate with an MTA to send/retrieve mail messages. Microsoft Outlook is an example of a MUA.

2597 MTA's often serve as "mail hubs" and can typically service hundreds or more MUA's.

2598 MUA's are responsible for constructing electronic mail messages in accordance with the Internet
2599 Electronic Mail Specifications identified above. This section describes the "binding" of an ebXML
2600 compliant message for transport via eMail from the perspective of a MUA. No attempt is made to define
2601 the binding of an ebXML Message exchange over SMTP from the standpoint of a MTA.

2602 **B.3.1 Minimum Level of Supported Protocols**

2603 Simple Mail Transfer Protocol [RFC2821]

2604 MIME [RFC2045] and [RFC2046]

2605 Multipart/Related MIME [RFC2387]

2606 **B.3.2 Sending ebXML Messages over SMTP**

2607 Prior to sending messages over SMTP an ebXML Message MUST be formatted according to the ebXML
2608 Message Service Specification. Additionally the messages must also conform to the syntax, format and
2609 encoding rules specified by MIME [RFC2045], [RFC2046] and [RFC2387].

2610 Many types of data that a party might desire to transport via email are represented as 8bit characters or
2611 binary data. Such data cannot be transmitted over SMTP [RFC2821], which restricts mail messages to
2612 7bit US-ASCII data with lines no longer than 1000 characters including any trailing CRLF line separator. If
2613 a sending Message Service Handler knows that a receiving MTA, or ANY intermediary MTA's, are
2614 restricted to handling 7-bit data then any document part that uses 8 bit (or binary) representation must be
2615 "transformed" according to the encoding rules specified in section 6 of MIME [RFC2045]. In cases where
2616 a Message Service Handler knows that a receiving MTA and ALL intermediary MTA's are capable of
2617 handling 8-bit data then no transformation is needed on any part of the ebXML Message.

2618 The rules for forming an ebXML Message for transport via SMTP are as follows:

- 2619 • If using SMTP [RFC2821] restricted transport paths, apply transfer encoding to all 8-bit data that will be
2620 transported in an ebXML message, according to the encoding rules defined in section 6 of MIME
2621 [RFC2045]. The Content-Transfer-Encoding MIME header MUST be included in the MIME envelope portion
2622 of any body part that has been transformed (encoded).

- 2623 • The Content-Type: Multipart/Related MIME header with the associated parameters, from the
2624 ebXML Message Envelope MUST appear as an eMail MIME header.
- 2625 • All other MIME headers that constitute the ebXML Message Envelope MUST also become part of the eMail
2626 MIME header.
- 2627 • The SOAPAction MIME header field must also be included in the eMail MIME header and MAY have the
2628 value of ebXML:
2629 SOAPAction: "ebXML"
- 2630 • The "MIME-Version: 1.0" header must appear as an eMail MIME header.
- 2631 • The eMail header "To:" MUST contain the SMTP [RFC2821] compliant eMail address of the ebXML
2632 Message Service Handler.
- 2633 • The eMail header "From:" MUST contain the SMTP [RFC2821] compliant eMail address of the senders
2634 ebXML Message Service Handler.
- 2635 • Construct a "Date:" eMail header in accordance with SMTP [RFC2821]
- 2636 • Other headers MAY occur within the eMail message header in accordance with SMTP [RFC2821] and
2637 MIME [RFC2045], however ebXML Message Service Handlers MAY choose to ignore them.

2638 The example below shows a minimal example of an eMail message containing an ebXML Message:

```

2639 From: ebXMLhandler@example.com
2640 To: ebXMLhandler@example2.com
2641 Date: Thu, 08 Feb 2001 19:32:11 CST
2642 MIME-Version: 1.0
2643 SOAPAction: "ebXML"
2644 Content-type: multipart/related; boundary="Boundary"; type="text/xml";
2645 start="<ebxmhheader111@example.com>"
2646
2647 This is an ebXML SMTP Example
2648
2649 --Boundary
2650 Content-ID: <ebxmhheader111@example.com>
2651 Content-Type: text/xml
2652
2653 <?xml version="1.0" encoding="UTF-8"?>
2654 <SOAP:Envelope xmlns:xlink="http://www.w3.org/1999/xlink"
2655 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
2656 xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
2657 xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
2658 http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
2659 <SOAP:Header xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2660 xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
2661 http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
2662 <eb:MessageHeader SOAP:mustUnderstand="1" eb:version="2.0">
2663 <eb:From>
2664 <eb:PartyId>urn:duns:123456789</eb:PartyId>
2665 </eb:From>
2666 <eb:To>
2667 <eb:PartyId>urn:duns:912345678</eb:PartyId>
2668 </eb:To>
2669 <eb:CPAId>20001209-133003-28572</eb:CPAId>
2670 <eb:ConversationId>20001209-133003-28572</eb:ConversationId>
2671 <eb:Service>urn:services:SupplierOrderProcessing</eb:Service>
2672 <eb:Action>NewOrder</eb:Action>
2673 <eb:MessageData>
2674 <eb:MessageId>20001209-133003-28572@example.com</eb:MessageId>
2675 <eb:Timestamp>2001-02-15T11:12:12</eb:Timestamp>
2676 </eb:MessageData>
2677 <eb:DuplicateElimination/>
2678 </eb:MessageHeader>
2679 </SOAP:Header>
2680 <SOAP:Body xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
2681 xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
2682 http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
2683 <eb:Manifest eb:version="2.0">
2684 <eb:Reference xlink:href="cid:ebxmlpayload111@example.com"
2685 xlink:role="XLinkRole"
2686 xlink:type="simple">

```

```

2687     <eb:Description xml:lang="en-US">Purchase Order 1</eb:Description>
2688     </eb:Reference>
2689     </eb:Manifest>
2690 </SOAP:Body>
2691 </SOAP:Envelope>
2692
2693 --Boundary
2694 Content-ID: <ebxhmheader111@example.com>
2695 Content-Type: text/xml
2696
2697 <?xml version="1.0" encoding="UTF-8"?>
2698 <purchase_order>
2699     <po_number>1</po_number>
2700     <part_number>123</part_number>
2701     <price currency="USD">500.00</price>
2702 </purchase_order>
2703
2704 --Boundary--

```

2705 **B.3.3 Response Messages**

2706 All ebXML response messages, including errors and acknowledgments, are delivered *asynchronously*
 2707 between ebXML Message Service Handlers. Each response message **MUST** be constructed in
 2708 accordance with the rules specified in the section B.3.2.

2709 All ebXML Message Service Handlers **MUST** be capable of receiving a delivery failure notification
 2710 message sent by an MTA. A MSH that receives a delivery failure notification message **SHOULD** examine
 2711 the message to determine which ebXML message, sent by the MSH, resulted in a message delivery
 2712 failure. The MSH **SHOULD** attempt to identify the application responsible for sending the offending
 2713 message causing the failure. The MSH **SHOULD** attempt to notify the application that a message
 2714 delivery failure has occurred. If the MSH is unable to determine the source of the offending message the
 2715 MSH administrator should be notified.

2716 MSH's which cannot identify a received message as a valid ebXML message or a message delivery
 2717 failure **SHOULD** retain the unidentified message in a "dead letter" folder.

2718 A MSH **SHOULD** place an entry in an audit log indicating the disposition of each received message.

2719 **B.3.4 Access Control**

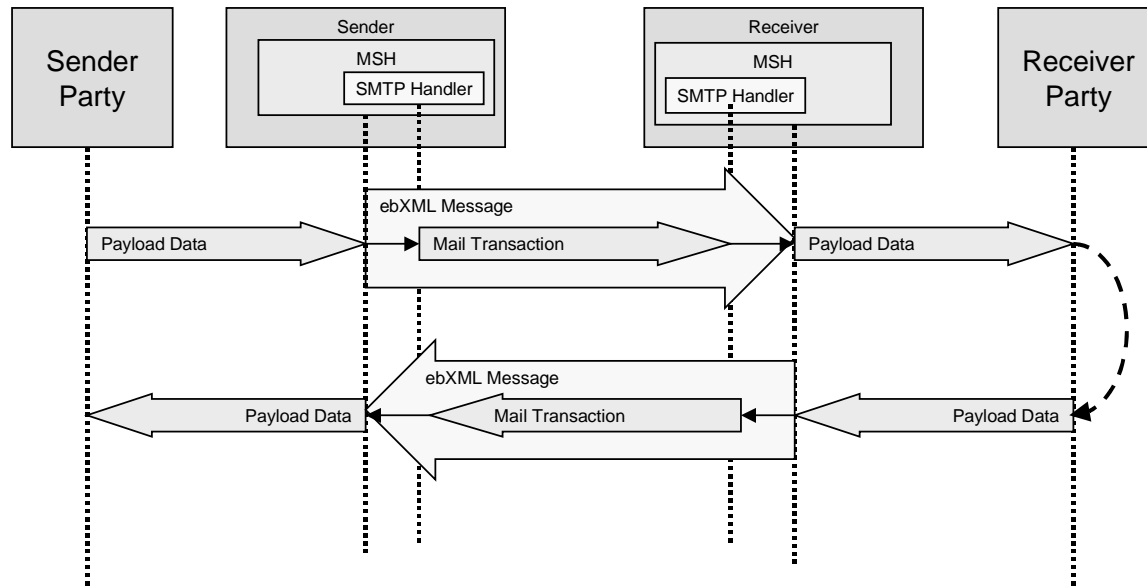
2720 Implementers **MAY** protect their ebXML Message Service Handlers from unauthorized access through the
 2721 use of an access control mechanism. The SMTP access authentication process described in "SMTP
 2722 Service Extension for Authentication" [RFC2554] defines the ebXML recommended access control
 2723 mechanism to protect a SMTP based ebXML Message Service Handler from unauthorized access.

2724 **B.3.5 Confidentiality and Transport Protocol Level Security**

2725 An ebXML Message Service Handler **MAY** use transport layer encryption to protect the confidentiality of
 2726 ebXML messages. The IETF "SMTP Service Extension for Secure SMTP over TLS" specification
 2727 [RFC2487] provides the specific technical details and list of allowable options, which may be used.

2728 **B.3.6 SMTP Model**

2729 All *ebXML Message Service* messages carried as mail in an SMTP [RFC2821] Mail Transaction as
 2730 shown in Figure B1.



2731

2732 **Figure B-1 SMTP Mail Depiction**

2733 **B.4 Communication Errors during Reliable Messaging**

2734 When the Sender or the Receiver detects a communications protocol level error (such as an HTTP,
 2735 SMTP or FTP error) and Reliable Messaging is being used then the appropriate transport recovery
 2736 handler will execute a recovery sequence. Only if the error is unrecoverable, does Reliable Messaging
 2737 recovery take place (see section 6).

2738 **Appendix C Supported Security Services**

2739 The general architecture of the ebXML Message Service Specification is intended to support all the
 2740 security services required for electronic business. The following table combines the security services of
 2741 the *Message Service Handler* into a set of security profiles. These profiles, or combinations of these
 2742 profiles, support the specific security policy of the ebXML user community. Due to the immature state of
 2743 XML security specifications, this version of the specification requires support for profiles 0 and 1 only.
 2744 This does not preclude users from employing additional security features to protect ebXML exchanges;
 2745 however, interoperability between parties using any profiles other than 0 and 1 cannot be guaranteed.

2746

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)

2747

2748 **References**2749 **Normative References**

- 2750 [\[RFC2119\]](#) Key Words for use in RFCs to Indicate Requirement Levels, Internet Engineering Task
2751 Force, March 1997
- 2752 [\[RFC2045\]](#) Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message
2753 Bodies, N Freed & N Borenstein, Published November 1996
- 2754 [\[RFC2046\]](#) Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. N. Freed, N.
2755 Borenstein. November 1996.
- 2756 [\[RFC2246\]](#) Dierks, T. and C. Allen, "The TLS Protocol", January 1999.
- 2757 [\[RFC2387\]](#) The MIME Multipart/Related Content-type. E. Levinson. August 1998.
- 2758 [\[RFC2392\]](#) Content-ID and Message-ID Uniform Resource Locators. E. Levinson, August 1998
- 2759 [\[RFC2396\]](#) Uniform Resource Identifiers (URI): Generic Syntax. T Berners-Lee, August 1998
- 2760 [\[RFC2402\]](#) IP Authentication Header. S. Kent, R. Atkinson. November 1998. RFC2406 IP
2761 Encapsulating Security Payload (ESP). S. Kent, R. Atkinson. November 1998.
- 2762 [\[RFC2487\]](#) SMTP Service Extension for Secure SMTP over TLS. P. Hoffman, January 1999.
- 2763 [\[RFC2554\]](#) SMTP Service Extension for Authentication. J. Myers. March 1999.
- 2764 [\[RFC2821\]](#) Simple Mail Transfer Protocol, J. Klensin, Editor, April 2001 Obsoletes RFC 821
- 2765 [\[RFC2616\]](#) Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee,
2766 "Hypertext Transfer Protocol, HTTP/1.1", June 1999.
- 2767 [\[RFC2617\]](#) Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., Sink,
2768 E. and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", June
2769 1999.
- 2770 [\[RFC2817\]](#) Khare, R. and S. Lawrence, "Upgrading to TLS Within HTTP/1.1", May 2000.
- 2771 [\[RFC2818\]](#) Rescorla, E., "HTTP Over TLS", May 2000 [SOAP] Simple Object Access Protocol
- 2772 [SOAP] W3C-Draft-Simple Object Access Protocol (SOAP) v1.1, Don Box, DevelopMentor; David
2773 Ehnebuske, IBM; Gopal Kakivaya, Andrew Layman, Henrik Frystyk Nielsen, Satish
2774 Thatte, Microsoft; Noah Mendelsohn, Lotus Development Corp.; Dave Winer, UserLand
2775 Software, Inc.; W3C Note 08 May 2000,
2776 <http://www.w3.org/TR/2000/NOTE-SOAP-20000508/>
- 2777 [SOAPAttach] SOAP Messages with Attachments, John J. Barton, Hewlett Packard Labs; Satish Thatte
2778 and Henrik Frystyk Nielsen, Microsoft, Published Oct 09 2000
2779 <http://www.w3.org/TR/2000/NOTE-SOAP-attachments-20001211>
- 2780 [SSL3] A. Frier, P. Karlton and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications
2781 Corp., Nov 18, 1996.
- 2782 [UTF-8] UTF-8 is an encoding that conforms to ISO/IEC 10646. See [XML] for usage conventions.
- 2783 [XLINK] W3C XML Linking Recommendation, <http://www.w3.org/TR/2001/REC-xlink-20010627/>
- 2784 [XML] W3C Recommendation: Extensible Markup Language (XML) 1.0 (Second Edition),
2785 October 2000, <http://www.w3.org/TR/2000/REC-xml-20001006>
- 2786 [XMLC14N] W3C Recommendation Canonical XML 1.0,
2787 <http://www.w3.org/TR/2001/REC-xml-c14n-20010315>

- 2788 [XMLNS] W3C Recommendation for Namespaces in XML, World Wide Web Consortium, 14
2789 January 1999, <http://www.w3.org/TR/1999/REC-xml-names-19990114/>
- 2790 [XMLDSIG] Joint W3C/IETF XML-Signature Syntax and Processing specification,
2791 <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/> **Error! Hyperlink reference**
2792 **not valid..**
- 2793 [XMLMedia] [RFC 3023](#), XML Media Types. M. Murata, S. St. Laurent, January 2001
- 2794 [XPointer] XML Pointer Language (XPointer) Version 1.0, W3C Candidate Recommendation 11
2795 September 2001, <http://www.w3.org/TR/2001/CR-xptr-20010911/>
- 2796

2797 **Non-Normative References**

- 2798 [ebCPP] ebXML Collaboration Protocol Profile and Agreement specification, Version 1.0,
2799 published 10 May, 2001, <http://www.ebxml.org/specs/ebCCP.doc>
- 2800 [ebBPSS] ebXML Business Process Specification Schema, version 1.0, published 27 April 2001,
2801 <http://www.ebxml.org/specs/ebBPSS.pdf>.
- 2802 [ebTA] ebXML Technical Architecture, version 1.04 published 16 February, 2001,
2803 <http://www.ebxml.org/specs/ebTA.doc>
- 2804 [ebRS] ebXML Registry Services Specification, version 2.0, published 6 December 2001
2805 <http://www.oasis-open.org/committees/regrep/documents/2.0/specs/ebrs.pdf>,
2806 published, 5 December 2001.
2807 <http://www.oasis-open.org/committees/regrep/documents/2.0/specs/ebrim.pdf>
- 2808 [ebREQ] ebXML Requirements Specification, <http://www.ebxml.org/specs/ebREQ.pdf>,
2809 published 8 May 2001.
- 2810 [ebGLOSS] ebXML Glossary, <http://www.ebxml.org/specs/ebGLOSS.doc>, published 11 May, 2001.
- 2811 [PGP/MIME] [RFC2015](#), "MIME Security with Pretty Good Privacy (PGP)", M. Elkins. October 1996.
- 2812 [SAML] Security Assertion Markup Language,
2813 <http://www.oasis-open.org/committees/security/docs/draft-sstc-use-strawman-03.html>
- 2814 [S/MIME] [RFC 2311](#), "S/MIME Version 2 Message Specification", S. Dusse, P. Hoffman, B.
2815 Ramsdell, L. Lundblade, L. Repka. March 1998.
- 2816 [S/MIMECH] [RFC 2312](#), "S/MIME Version 2 Certificate Handling", S. Dusse, P. Hoffman, B. Ramsdell,
2817 J. Weinstein. March 1998.
- 2818 [S/MIMEV3] [RFC 2633](#) S/MIME Version 3 Message Specification. B. Ramsdell, Ed June 1999.
- 2819 [secRISK] ebXML Technical Architecture Risk Assessment Technical Report, version 0.36
2820 published 20 April 2001
- 2821 [XMLSchema] W3C XML Schema Recommendation,
2822 <http://www.w3.org/TR/2001/REC-xmlschema-0-20010502/>
2823 <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>
2824 <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>
- 2825 [XMTP] XMTP - Extensible Mail Transport Protocol
2826 <http://www.openhealth.org/documents/xmtp.htm>

2827 **Contact Information**2828 **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

2829 **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

2830 **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

2831 **Acknowledgments**

2832 The OASIS ebXML-MS Technical Committee would like to thank the members of the original joint
2833 UN/CEFACT-OASIS ebXML Messaging Team for their work to produce v1.0 of this specification.

2834

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	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

2835 **Disclaimer**

2836 The views and specification expressed in this document are those of the authors and are not necessarily
2837 those of their employers. The authors and their employers specifically disclaim responsibility for any
2838 problems arising from correct or incorrect implementation or use of this design.

2839 **Copyright Statement**

2840 *Copyright (C) The Organization for the Advancement of Structured Information Standards [OASIS]*
2841 *January 2002. All Rights Reserved.*

2842 *This document and translations of it may be copied and furnished to others, and derivative works that*
2843 *comment on or otherwise explain it or assist in its implementation may be prepared, copied, published*
2844 *and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice*
2845 *and this paragraph are included on all such copies and derivative works. However, this document itself*
2846 *may not be modified in any way, such as by removing the copyright notice or references to OASIS,*
2847 *except as needed for the purpose of developing OASIS specifications, in which case the procedures for*
2848 *copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to*
2849 *translate it into languages other than English.*

2850 *The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors*
2851 *or assigns.*

2852 *This document and the information contained herein is provided on an "AS IS" basis and OASIS*
2853 *DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY*
2854 *WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR*
2855 *ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE."*