



OASIS ebXML Messaging Services 3.0 Conformance Profiles

Committee Draft 04

28 October 2008

Specification URIs:

This Version:

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd02/ebms-3.0-confprofiles-cd-02.pdf>

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd02/ebms-3.0-confprofiles-cd-02.html>

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd02/ebms-3.0-confprofiles-cd-02.odt>

Previous Version:

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd01/ebms-3.0-confprofiles-cd-01.pdf>

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd01/ebms-3.0-confprofiles-cd-01.html>

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/cd01/ebms-3.0-confprofiles-cd-01.odt>

Latest Version:

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/ebms-3.0-confprofiles-cd-01.pdf>

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/ebms-3.0-confprofiles-cd-01.html>

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/prof/ebms-3.0-confprofiles-cd-01.odt>

Technical Committee:

OASIS ebXML Messaging Services TC

Chair:

Ian Jones, British Telecommunications plc <ian.c.jones@bt.com>

Editor:

Jacques Durand, Fujitsu Computer Systems <jdurand@us.fujitsu.com>

Related Work:

This specification is related to:

- OASIS ebXML Messaging Services Version 3.0: Part 1, Core Specification

Declared XML Namespace:

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/>

Abstract:

This document is a non-normative supplement to the ebMS-3 specification [ebMS3]. It defines some conformance profiles that support specific messaging styles or context of use. Future

33 releases of this document are likely to be augmented with additional conformance profiles that
34 reflect the choices or needs of user communities. As a pre-condition to interoperability it is
35 necessary for two implementations to agree on which common conformance profile, or which
36 compatible conformance profiles, they will comply with. This document and its future releases is
37 intended as a medium to publish conformance profiles that users and products will claim
38 compliance with.

39 **Status:**

40 This document was last revised or approved by the ebXML Messaging Services Committee on
41 the above date. The level of approval is also listed above. Check the "Latest Version" or "Latest
42 Approved Version" location noted above for possible later revisions of this document.

43 Technical Committee members should send comments on this specification to the Technical
44 Committee's email list. Others should send comments to the Technical Committee by using the
45 "Send A Comment" button on the Technical Committee's web page at
46 <http://www.oasis-open.org/committees/ebxml-msg/>

47 For information on whether any patents have been disclosed that may be essential to
48 implementing this specification, and any offers of patent licensing terms, please refer to the
49 Intellectual Property Rights section of the Technical Committee web page at
50 <http://www.oasis-open.org/committees/ebxml-msg/ipr.php>

51 The non-normative errata page for this specification is located at
52 <http://www.oasis-open.org/committees/ebxml-msg/>

Notices

53

54 Copyright © OASIS® 2007. All Rights Reserved.

55 All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual
56 Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

57 This document and translations of it may be copied and furnished to others, and derivative works that
58 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published,
59 and distributed, in whole or in part, without restriction of any kind, provided that the above copyright
60 notice and this section are included on all such copies and derivative works. However, this document
61 itself may not be modified in any way, including by removing the copyright notice or references to OASIS,
62 except as needed for the purpose of developing any document or deliverable produced by an OASIS
63 Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR
64 Policy, must be followed) or as required to translate it into languages other than English.

65 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
66 or assigns.

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

72 OASIS requests that any OASIS Party or any other party that believes it has patent claims that would
73 necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard,
74 to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to
75 such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that
76 produced this specification.

77 OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of
78 any patent claims that would necessarily be infringed by implementations of this specification by a patent
79 holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR
80 Mode of the OASIS Technical Committee that produced this specification. OASIS may include such
81 claims on its website, but disclaims any obligation to do so.

82 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
83 might be claimed to pertain to the implementation or use of the technology described in this document or
84 the extent to which any license under such rights might or might not be available; neither does it
85 represent that it has made any effort to identify any such rights. Information on OASIS' procedures with
86 respect to rights in any document or deliverable produced by an OASIS Technical Committee can be
87 found on the OASIS website. Copies of claims of rights made available for publication and any
88 assurances of licenses to be made available, or the result of an attempt made to obtain a general license
89 or permission for the use of such proprietary rights by implementers or users of this OASIS Committee
90 Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no
91 representation that any information or list of intellectual property rights will at any time be complete, or
92 that any claims in such list are, in fact, Essential Claims.

93 The names "OASIS", ebXML, ebXML Messaging Services, ebMS are trademarks of [OASIS](http://www.oasis-open.org), the owner
94 and developer of this specification, and should be used only to refer to the organization and its official
95 outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving
96 the right to enforce its marks against misleading uses. Please see
97 <http://www.oasis-open.org/who/trademark.php> for above guidance.

98

Table of Contents

99	1 Introduction.....	5
100	1.1 Terminology.....	6
101	1.2 Normative References.....	6
102	1.3 Non-normative References.....	7
103	2 The Gateway Conformance Profile.....	8
104	2.1 Purpose.....	8
105	2.2 Conformance Profile: Gateway RM V3.....	8
106	2.2.1 Feature Set.....	8
107	2.2.2 WS-I Conformance Requirements.....	10
108	2.2.3 Processing Mode Parameters.....	11
109	2.3 Conformance Profile: Gateway RX V3.....	14
110	2.3.1 Feature Set.....	14
111	2.3.2 WS-I Conformance Requirements.....	14
112	2.3.3 Processing Mode Parameters.....	15
113	2.4 Conformance Profile: Gateway RM V2/3.....	15
114	2.4.1 Feature Set.....	15
115	2.4.2 WS-I Conformance Requirements.....	18
116	2.4.3 Processing Mode Parameters.....	18
117	2.5 Conformance Profile: Gateway RX V2/3.....	18
118	2.5.1 Feature Set.....	18
119	2.5.2 WS-I Conformance Requirements.....	19
120	2.5.3 Processing Mode Parameters.....	19
121	3 Examples of Alternate Conformance Profiles.....	20
122	3.1 Purpose.....	20
123	3.2 Conformance Profile: Light Handler (LH-RM CP).....	20
124	3.2.1 Feature Set.....	20
125	3.2.2 WS-I Conformance Requirements.....	21
126	3.3 Conformance Profile: Activity Monitor (AM-CP).....	21
127	3.3.1 Feature Set.....	21
128	3.3.2 WS-I Conformance Requirements.....	22
129	Appendix A Conformance Profile Template and Terminology.....	23
130	Appendix B Acknowledgments.....	25
131	Appendix C Revision History.....	26
132		

133

1 Introduction

134

135 The intent of the core ebMS-3 specification [ebMS3] is to provide a stable, normative framework for
136 developers to work with, but is not sufficient for guaranteeing “out-of-the-box” interoperability between
137 conforming implementations. The specification contains options and makes use of third-party
138 specifications for which more than one alternative may exist (e.g. SOAP 1.1 vs SOAP 1.2).
139 Implementations of ebMS-3 must generally settle on some of these options in order to interoperate. The
140 main specification intentionally does not prescribe which ones should be used by an implementation: it is
141 the role of conformance profiles to do so. The notion of conformance profile used here has been defined
142 in [QAFrameW].

143 Different user communities may elect to use different conformance profiles, reflecting different sets of
144 options. Or, they may decide to use different versions of referred third-party specifications that are still in
145 transition at the time the core specification is written (e.g. SOAP, and WSS). These elections – which
146 may evolve over time and are more dependent on usage patterns than the core specification - are
147 captured by conformance profiles. Because conformance profiles are dependent on the needs and
148 choices of user communities, and because they may evolve faster than the underlying core specification
149 (here ebMS-3) - i.e. some profiles will get deprecated, or new ones will appear - it is preferable that they
150 are not defined in the core specification which is expected to remain a stable reference. Instead,
151 conformance profiles are specified in a separate document that is not part of the standard and is easier to
152 update.

153 Future releases of the present document are likely to be augmented with additional conformance profiles
154 that reflect the choices or needs of user communities. This document intends to serve as a medium for
155 publishing such conformance profiles. The document is non-normative in the sense that conformance
156 profiles only refer to selected options and features that are already described in a normative way in the
157 ebMS-3 specification.

158 Section 2 introduces a conformance profile – the “Gateway profile” that lists the features expected of a
159 Message Service Handler (MSH) acting as e-Business or e-Government gateway to back-end systems.

160 Although wide-scale interoperability is best served by having all users adopt a single profile, at the time
161 this document is written there are two transitional aspects that call for temporary definitions of some
162 variants of the Gateway profile:

- 163 ● There is today a significant user base for ebMS V2. Given the disruptive leap from V2 to V3
164 (largely due to convergence with Web services protocols), there is a need for a multi-version
165 profile supporting both (V2+V3). Conforming implementations will be able to interact both with
166 partners using V2 and partners using V3.
- 167 ● There exist two largely equivalent specifications for reliable messaging: (a) WS-Reliability 1.1 and
168 (b) WS-ReliableMessaging. (a) has been an OASIS standard for several years, has been tested
169 and implemented by communities of users, notably in Asia. (b) is a more recent standard, still
170 awaiting for WS-I interoperability guidance, but enjoying a broad support among US-based
171 companies.

172 These transitional aspects are likely to vanish in the long run, but they call for supportive conformance
173 profiles for the time being. As a result, the following variants of the gateway profile are defined here:

174

- 175 ● **Gateway RM V2/3:** supporting both ebMS V2 and V3, using WS-Reliability1.1 (produced by the
176 WSRM OASIS TC) as reliable messaging specification.
- 177 ● **Gateway RM V3:** supporting ebMS V3 exactly in the same way as the previous RM V2/3 profile,
178 but not requiring support for V2. Conformance to Gateway RM V2/3 implies conformance to
179 Gateway RM V3.

- 180 ● **Gateway RX V2/3:** supporting both ebMS V2 and V3 with same features as Gateway RM V2/3,
181 excepts that it uses WS-ReliableMessaging (produced by the WS-RX OASIS TC) as reliable
182 messaging specification.
- 183 ● **Gateway RX V3:** supporting ebMS V3 exactly in the same way as the previous RX V2/3 profile,
184 but not requiring support for V2. Conformance to Gateway RX V2/3 implies conformance to
185 Gateway RX V3.

186

187 *NOTE: It is certainly possible for an implementation or product to support all these conformance profiles*
188 *simultaneously. As already mentioned, a product conforming to Gateway RM V2/3 or RX V2/3 will*
189 *automatically conform respectively to Gateway RM V3 or RX V3. In addition, an MSH implementation*
190 *can conform to both Gateway RM V2/3 and Gateway RX V2/3, by simply alternating at run-time*
191 *between the two reliability modules used for RM and RX. This run-time assignment may be*
192 *implemented in various ways, e.g. by using a different URL, or by associating a particular reliability*
193 *processing with specific user data (e.g. originating party ID). The P-Mode would be the place where to*
194 *specify which reliability mode is to be associated with a particular message content.*

195 Prior experience in diverse communication sectors (e.g. TVs, cell phones and messaging middleware)
196 has shown that adoption is best promoted by facilitating local or “regional” interoperability first – i.e. by
197 recognizing that different communities of users may have different requirements and therefore adoption
198 paths. These would be served by different conformance profiles. Then in a second phase, global
199 interoperability needs will push for some consolidation, meaning convergence toward a core conformance
200 profile elected by all.

201 In addition to defining an e-Business / e-Government Gateway profile and its transitional variants, the
202 role of this document is to provide some framework and notation for defining additional profiles, a couple
203 of which are provided as examples.

204 1.1 Terminology

205 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
206 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as
207 described in IETF RFC 2119.

208 1.2 Normative References

- 209 **[ebMS2]** OASIS ebXML Message Service Specification Version 2.0, April 1, 2002. [http://](http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf)
210 www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf
- 211 **[ebMS3]** OASIS ebXML Messaging Services, Version 3.0: Part 1, Core Features, 2007.
212 http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.pdf
- 213 **[RFC 2119]** S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. IETF
214 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>
- 215 **[UCC-MS2]** UCC/EAN Basic Reliable ebXML Messaging v2.0 Interoperability Testing, 2002.
- 216 **[WSIAP10]** WS-I Attachment Profile V1.0, Web-Services Interoperability Consortium, 2007.
217 <http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile>
- 218 **[WSIBP12]** WS-I Basic Profile V1.2 (draft), Web-Services Interoperability Consortium,
219 2007. <http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile>
- 220 **[WSIBSP11]** Abbie Barbir, et al, eds, Basic Security Profile Version 1.1, Web-Services
221 Interoperability Consortium, 2006.
222 <http://www.wsi.org/Profiles/BasicSecurityProfile-1.1.html>

223 **[ebBP-SIG]** OASIS ebXML Business Process TC, *ebXML Business Signals Schema*,
224 2006. <<http://docs.oasis-open.org/ebxml-bp/ebbp-signals-2.0>>
225

226 **1.3 Non-normative References**

227 **[QAFrameW]** Karl Dubost, et al, eds, *QA Framework: Specification Guidelines*, 2005.
228 <http://www.w3.org/TR/qaframe-spec/>
229

230

2 The Gateway Conformance Profile

231

2.1 Purpose

232 The *Gateway* conformance profile (or G-CP) is to be considered the baseline for conducting electronic
233 business. G-CP addresses the messaging requirements of most enterprise e-Business or e-Government
234 gateways.

235 It is expected that user communities will generate variants of the G-CP profile that differ by their
236 interoperability parameters, e.g. a variant that uses a transport other than HTTP. Also, the Gateway
237 messaging function may evolve over time to reflect an evolution of the enterprise gateway requirements
238 among the user community. A line of evolution is along the versions of the underlying specifications used
239 by ebMS V3.0, in particular SOAP and WSS. After careful consideration at the time the ebMS V3.0
240 specification is finalized, the following versions have been selected for G-CP:

- 241 • SOAP 1.2 has been selected because of an already pervasive support by most SOAP stacks
242 (most of these stacks also support SOAP 1.1).
- 243 • Both WSS 1.0 and WSS 1.1. Although 1.1 is too recent to be broadly supported by
244 implementers, this version supports security of attachments. While G-CP mandates support for
245 both, the version to be used for a particular exchange or with a particular partner can still be
246 specified in the processing mode (P-Mode). This makes it possible for a partially conforming
247 implementation to interoperate with others.

248 As mentioned in the introduction, G-CP comes in four variants, called here transitional variants. The first
249 one to be described here is Gateway RM V3, based on the WS-Reliability1.1 standard for reliable
250 messaging.

2.2 Conformance Profile: Gateway RM V3

252 The Gateway RM V3 is identified by the URI:

253 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/gateway-rmv3>

2.2.1 Feature Set

255 Gateway RM V3 is defined as follows, using the table template and terminology provided in Appendix F
256 (“Conformance”) of the core ebXML Messaging Services V3.0 specification [ebMS3].

257

Conformance Profile: Gateway RM V3	Profile summary: <“Sending+Receiving” / “ gateway-rmv3” / Level 1 / HTTP1.1 + SOAP 1.2 + WSS1.1 + WS-Reliability 1.1 >
Functional Aspects	Profile Feature Set
ebMS MEP	Support for all ebMS simple MEPs, in either Sender or Receiver role: <ul style="list-style-type: none"> • One-way / Push, • One-way / Pull,

	<ul style="list-style-type: none"> • Two-way / Sync (both Initiator and Responder roles) <p>Regardless of which MEP is used, the sending of an eb:Receipt message must be supported:</p> <ul style="list-style-type: none"> – For the One-way / Push, both “response” and “callback” reply patterns must be supported. – For the One-way / Pull, the “callback” pattern is the only viable option, and the User message sender MUST be ready to accept an eb:Receipt either piggybacked on a PullRequest, or sent separately. The User message receiver MUST be able to send an eb:Receipt separately from the PullRequest. – For the Two-way / Sync, both “response” and “callback” reply patterns must be supported for the first leg. The “callback” pattern is the only viable option for the second leg. The reply sender MUST be ready to accept an eb:Receipt either piggybacked on another User message, or sent separately. The reply receiver MUST be able to send an eb:Receipt separately. <p>Use of the ebbpsig:NonRepudiationInformation element (as defined in [ebBP-SIG]) MUST be supported as content for the eb:Receipt message.</p>
Reliability	<ul style="list-style-type: none"> • Support for the following QoS features for pushed or pulled ebMS messages: at-least-once, at-most-once, exactly-once. • Ability to acknowledge pulled messages (AtLeastOnce.Contract.AckResponse="true"). • Supports Acknowledgments on delivery (supports P-Mode with Reliability.AtLeastOnce.Contract.AckOnDelivery="true") • Supports the following reply patterns for acknowledgments (P-Mode AtLeastOnce.ReplyPattern): either “response”, or “callback” (no support for polling required)
Security	<ul style="list-style-type: none"> • Support for username / password token, digital signatures • and encryption. • Support for content-only transforms. • Support for security of attachments required. • Support for message authorization at P-Mode level (see 7.10 in [ebMS3]) using wsse:UsernameToken profile. Authorization of the Pull signal - for a particular MPC - must be supported at minimum. <p>NOTE on XMLDsig: XMLDsig allows arbitrary XSLT Transformations when constructing the plaintext over which a signature or reference is created. Conforming applications that allow use of XSLT transformations when verifying either signatures or references are encouraged to maintain lists of “safe” transformations for a given partner, service, action and role combination. Static analysis of XSLT expressions with a human user audit is encouraged for trusting a given expression as “safe”</p>

Error generation and reporting	<ul style="list-style-type: none"> • Capability of the Receiving MSH to report errors from message processing, either as ebMS error messages or as Faults to the Sending MSH. The following modes of reporting to Sending MSH are supported: (a) sending error as a separate request (ErrorHandling.Report.ReceiverErrorsTo=<URL of Sending MSH>), (b) sending error on the back channel of underlying protocol (ErrorHandling.Report.AsResponse="true"). • Capability to report to a third-party address (ErrorHandling.Report.ReceiverErrorsTo=<other address>). • Capability of Sending MSH to report generated errors as notifications to the message producer (support for Report.ProcessErrorNotifyProducer="true") (e.g. delivery failure). • Generated errors: All specified errors to be generated when applicable, except for EBMS:0010: On Receiving MSH, no requirement to generate error EBMS:0010 for discrepancies between message header and the following P-Mode features: P-Mode.reliability and P-Mode.security, but requirement to generate such error for other discrepancies.
Message Partition Channels	Support for additional message channels beside the default, so that selective pulling by a partner MSH is possible.
Message packaging	<ul style="list-style-type: none"> • Support for attachments required. • Support for MessageProperties required. • Support for processing messages that contain both a signal message unit (eb:SignalMessage) and a user message unit (eb:UserMessage).
Interoperability Parameters	<p>Transport: HTTP 1.1</p> <p>SOAP version: 1.2</p> <p>Reliability Specification: WS-Reliability 1.1. Only "Response" or "Callback" ReplyPattern values are required to be supported.</p> <p>Security Specification: WSS1.0 and WSS 1.1. When using the One-way / Pull MEP or the Two-way / Sync MEP, the response message must use by default the same WSS version as the request message. Otherwise, the version to be applied to a message is specified in the P-Mode.security</p>

258

259 2.2.2 WS-I Conformance Requirements

260 The Web-Services Interoperability consortium has defined guidelines for interoperability
 261 of SOAP messaging implementations. In order to ensure maximal interoperability across
 262 different SOAP stacks, MIME and HTTP implementations, this conformance profile requires
 263 compliance with the following WS-I profiles:

- 264 ● Basic Security Profile (BSP) 1.1 [WSIBSP11]
- 265 ● Attachment Profile (AP) 1.0, [WSIAP10] with regard to the use of MIME and SwA.

266 Notes:

- 267 – Compliance with AP1.0 would normally require compliance with BP1.1, which in turn
268 requires the absence of SOAP Envelope in the HTTP response of a One-Way (R2714).
269 However, recent BP versions such as BP1.2 [WSIBP12] override this requirement.
270 Consequently, the Gateway conformance profile does not require conformance to
271 these deprecated requirements inherited from BP1.1 (R2714, R1143) regarding the
272 use of HTTP.
- 273 – The above WS-I profiles must be complied with within the scope of features exhibited
274 by the Gateway RM V3 ebMS conformance profile. For example, since only SOAP 1.2 is
275 required by Gateway RM V3, the requirements from BSP 1.1 that depend on SOAP 1.1
276 would not apply. Similarly, none of the requirements for DESCRIPTION (WSDL) or
277 REGDATA (UDDI) apply here, as these are not used.

278 This conformance profile may be refined in a future version to require conformance to the
279 following WS-I profiles, once approved and published by WS-I:

- 280 ● Basic Profile 2.0 (BP2.0) iui

281

282 2.2.3 Processing Mode Parameters

283 Summary of P-Mode parameters that must be supported by an implementation conforming to this profile.
284 For each parameter, either:

- 285 – full support is required: an implementation is supposed to support the possible options for this
286 parameter.
- 287 – Support for a subset of values is required.
- 288 – No support is required: an implementation is not required to support the features controlled by this
289 parameter, and therefore not required to understand this parameter.

290

291 0. General PMode parameters:

- 292 • **(PMode.ID:** support not required)
- 293 • **(PMode.Agreement:** support not required)
- 294 • **PMode.MEP:** support for: [http://www.oasis-open.org/committees/ebxml-](http://www.oasis-open.org/committees/ebxml-msg/)
295 [msg/{one-way, two-way}](http://www.oasis-open.org/committees/ebxml-msg/)
- 296 • **PMode.MEPbinding:** support for: <http://www.oasis-open.org/committees/ebxml->
297 [msg/{ push, pull, sync}](http://www.oasis-open.org/committees/ebxml-)
- 298 • **PMode.Initiator.Party:** support required.
- 299 • **PMode.Initiator.Role:** support required.

- 300 • **PMode.Initiator.Authorization.username** and
- 301 **PMode.Initiator.Authorization.password**: support for: wsse:UsernameToken.
- 302 • **PMode.Responder.Party**: support required.
- 303 • **PMode.Responder.Role**: support required.
- 304 • **PMode.Responder.Authorization.username** and
- 305 **PMode.Responder.Authorization.password**: support for: wsse:UsernameToken.

306

307 **1. PMode[1].Protocol:**

- 308 • **PMode[1].Protocol.Address**: support for "http" scheme.
- 309 • **PMode[1].Protocol.SOAPVersion**: support for SOAP 1.2.

310

311 **2.PMode[1].BusinessInfo:**

- 312 • **PMode[1].BusinessInfo.Service**: support required.
- 313 • **PMode[1].BusinessInfo.Action**: support required.
- 314 • **PMode[1].BusinessInfo.Properties[]**: support required.
- 315 • **(PMode[1].BusinessInfo.PayloadProfile[]: not required)**
- 316 • **(PMode[1].BusinessInfo.PayloadProfile.maxSize: not required)**
- 317 • **PMode[1].BusinessInfo.MPC**: support required.

318

319 **3. PMode[1].ErrorHandling:**

- 320 • **(PMode[1].ErrorHandling.Report.SenderErrorsTo**: support not required)
- 321 • **PMode[1].ErrorHandling.Report.ReceiverErrorsTo**: support required (for address of
- 322 the MSH sending the message in error or for third-party).
- 323 • **PMode[1].ErrorHandling.Report.AsResponse**: support required (true/false).
- 324 • **(PMode[1].ErrorHandling.Report.ProcessErrorNotifyConsumer** support not
- 325 **required)**
- 326 • **PMode[1].ErrorHandling.Report.ProcessErrorNotifyProducer**: support required
- 327 (true/false)
- 328 • **PMode[1].ErrorHandling.Report.DeliveryFailuresNotifyProducer**: support required
- 329 (true/false)

330

331 **4. PMode[1].Reliability:**

- 332 • **PMode[1].Reliability.AtLeastOnce.Contract**: support required (true/false)
- 333 • **PMode[1].Reliability.AtLeastOnce.Contract.AckOnDelivery**: true/false

- 334 • **PMode[1].Reliability.AtLeastOnce.Contract.AcksTo**: support required.
- 335 • **PMode[1].Reliability.AtLeastOnce.Contract.AckResponse**: support required
- 336 (true/false)
- 337 • **PMode[1].Reliability.AtLeastOnce.ReplyPattern**: support required for: {Response,
- 338 Callback}.
- 339 • **PMode[1].Reliability.AtMostOnce.Contract**: support required (true/false)
- 340 • **(PMode[1].Reliability.InOrder.Contract**: support not required)
- 341 • **(PMode[1].Reliability.StartGroup**: support not required)
- 342 • **(PMode[1].Reliability.Correlation**: support not required)
- 343 • **(PMode[1].Reliability.TerminateGroup**: support not required)

344

345 **5. PMode[1].Security:**

- 346 • **PMode[1].Security.WSSVersion**: support required for: {1.0 , 1.1 }
- 347 • **PMode[1].Security.X509.Sign**: support required.
- 348 • **PMode[1].Security.X509.Signature.Certificate**: support required.
- 349 • **PMode[1].Security.X509.Signature.HashFunction**: support required.
- 350 • **PMode[1].Security.X509.Signature.Algorithm**: support required.
- 351 • **PMode[1].Security.X509.Encryption.Encrypt**: support required.
- 352 • **PMode[1].Security.X509.Encryption.Certificate**: support required.
- 353 • **PMode[1].Security.X509.Encryption.Algorithm**: support required.
- 354 • **(PMode[1].Security.X509.Encryption.MinimumStrength**: support not required)
- 355 • **PMode[1].Security.UsernameToken.username**: support required.
- 356 • **PMode[1].Security.UsernameToken.password**: support required.
- 357 • **PMode[1].Security.UsernameToken.Digest**: support required (true/false)
- 358 • **(PMode[1].Security.UsernameToken.Nonce**: not required)
- 359 • **PMode[1].Security.UsernameToken.Created**: support required.
- 360 • **PMode[1].Security.PModeAuthorize**: support required (true/false)
- 361 • **PMode[1].Security.SendReceipt**: support required (true/false)
- 362 • **Pmode[1].Security.SendReceipt.ReplyPattern**: support required (both "response"
- 363 and "callback"))

364

365 **2.3 Conformance Profile: Gateway RX V3**

366 The Gateway RX V3 is identified by the URI:

367 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/gateway-rxv3>

368 **2.3.1 Feature Set**

369 Gateway RX V3 is equivalent to the RM V3 conformance profile feature-wise.

370 The only difference is about the way messaging reliability is ensured. This profile relies on WS-
371 ReliableMessaging1.1 instead of WS-Reliability1.1.

372 The feature set is therefor the same as in RM V3 except for the last table row:

Conformance Profile: Gateway RX V3	Profile summary: <“Sending+Receiving” / “ gateway-rxv3” / Level 1 / HTTP1.1 + SOAP 1.2 + WSS1.1 + WS-ReliableMessaging1.1 >
Functional Aspects	Profile Feature Set
ebMS MEP	[same as in Gateway RM V3]
Reliability	[same as in Gateway RM V3, except for the following feature:] <ul style="list-style-type: none"> No support required for Acknowledgments on delivery (supports P-Mode with Reliability.AtLeastOnce.Contract.AckOnDelivery=”false”)
Security	[same as in Gateway RM V3]
Error generation and reporting	[same as in Gateway RM V3]
Message Partition Channels	[same as in Gateway RM V3]
Message packaging	[same as in Gateway RM V3]
Interoperability Parameters	<p>Transport: HTTP 1.1</p> <p>SOAP version: 1.2</p> <p>Reliability Specification: WS-ReliableMessaging 1.1. Only “Response” or “Callback” ReplyPattern values are required to be supported.</p> <p>Security Specification: WSS1.0 and WSS 1.1.</p>

373 **2.3.2 WS-I Conformance Requirements**

374 The Web-Services Interoperability consortium has defined guidelines for interoperability
375 of SOAP messaging implementations. In order to ensure interoperability across different SOAP
376 stacks, MIME and HTTP implementations, this conformance profile requires compliance with the following
377 WS-I profiles.

- 378 • Basic Security Profile (BSP) 1.1 [WSIBSP11]
- 379 • Attachment Profile (AP) 1.0, [WSIAP10] with regard to the use of MIME and SwA.

380 Note: the above WS-I profiles must be complied with within the scope of features exhibited by the
 381 Gateway RX V3 ebMS conformance profile. For example, since only SOAP 1.2 is required by Gateway
 382 RX V3, the requirements from BSP 1.1 that depend on SOAP 1.1 would not apply. Also, same
 383 observations apply to compliance to AP1.0, regarding inherited BP1.1 requirements (R2714, R1143), as
 384 in Gateway RM V3.

385 The Gateway RX V3 may be refined in a future version to require conformance to the following WS-I
 386 profiles, once approved and published by WS-I:

- 387 • Basic Profile 2.0
- 388 • Reliable and Secure Profile (RSP) 1.1

389 2.3.3 Processing Mode Parameters

390 The P-Mode parameters to be supported are same as in Gateway RM V3, except for the following:

- 391 • **PMode[1].Reliability.AtLeastOnce.Contract.AckOnDelivery**: “false” only needs be supported.

392 2.4 Conformance Profile: Gateway RM V2/3

393 The Gateway RM V2/3 is identified by the URI:

394 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/gateway-rmv2v3>

395 2.4.1 Feature Set

396 Gateway RM V2/3 is defined as an extension of RM V3. As far as V3 is concerned, the features to be
 397 supported by this conformance profile are exactly the same as in RM V3.

398 Regarding ebMS V2, the features to be supported for RM V2/3 are those required in the test profile:
 399 **“UCC/EAN Basic Reliable ebXML Messaging v2.0”** defined in “UCC Global Interoperability
 400 Program for ebXML MS” [UCC-MS2]. RM V2/3 requires the following restrictions – or tolerates the
 401 following relaxations – on the UCC test profile:

- 402 • Only the HTTP1.1 + HTTP/S protocols must be used – SMTP is not part of RM V2/3.
- 403 • The value “signalsAndResponse” as well “responseOnly” do not need be supported for
 404 SyncReplyMode. This means that “synchronous” request-responses do not need be supported.
- 405 • The Message Services (Ping, Status) tests H as defined in the above UCC test profile, do not
 406 need be supported.
- 407 • The following capabilities, already optional in the UCC test profile, do not need be supported:
 408 Encrypted File Transfer (Test G), Other Languages (Test I).

409 NOTE: An additional row has been added to the table: “portability parameters”, which associates a
 410 particular processing mode (P-Mode in V3) representation with the profile so that implementations
 411 supporting this profile can process the same processing mode representation.

412

Conformance Profile: Gateway RM V2/3	Profile summary: <“Sending+Receiving” / “gateway-rmv2v3” / Level 1 / HTTP1.1 + SOAP 1.2 + WSS1.1 + WS-Reliability 1.1 > + < “Sending+Receiving” / UCC-EAN V2 handler / Level 1 / HTTP1.1 >
---	--

Functional Aspects	Profile Feature Set for ebMS V2 (to add to those for V3 in RM V3)
EbMS V2 MEP	Support for (in either Sender or Receiver role): <ul style="list-style-type: none"> • One-way / Push, defined as exchanges controlled by SyncReplyMode values: "mshSignalsOnly", "signalsOnly" or "none".
V2 Reliability	Support for reliable messaging, as required by UCC test profile under Test E and Test J: <p>Test E Acknowledgments</p> <p>E1. Unsigned Data/Unsigned Ack</p> <p>E2. Unsigned Data/Signed Ack</p> <p>E3. Signed Data/Unsigned Ack</p> <p>E4. Signed Data/Signed Ack</p> <p>E5. Signed Data/Signed Ack Secure Channel</p> <p>Test J Single-Hop Reliable Messaging</p> <p>J1. Once and Only Once Profile - Successful Retries, RetryInterval</p> <p>J2. Duplicate Detection - Original Acknowledgement to Duplicate Request</p> <p>J3. Delivery Failure Notification</p> <p>J4. Long Running Conversation</p>
V2 Security	Support for secure messaging, as required by UCC test profile under Test A , Test B and Test D: <p>Test A Certificate Exchange</p> <p>A1. Personal Certificate</p> <p>Test B Simple Data Transfer</p> <p>B2. HTTP/S Data Transfer</p> <p>Test D Data Security</p> <p>D1. Signed Data</p> <p>D2. Signed Data Secure Channel (HTTP/S)</p> <p>D3. Client Authentication - Signed Data Secure Channel (HTTP/S)</p>
V2 Error generation and reporting	Support for error handling, as required by UCC test profile under Test K: <p>Test K Error Handling</p>

	<p>K1. SOAP:Fault</p> <p>K2. ValueNotRecognized</p> <p>K3. NotSupported</p> <p>K4. Inconsistent Sync</p> <p>K5. Inconsistent Signature</p> <p>K6. Inconsistent Acknowledgment Signature</p> <p>K7. SecurityFailure</p> <p>K8. TimeToLiveExpired</p> <p>K10. MessageHeader format</p> <p>K11. Missing Payload</p>
V2 Message Partition Channels	Not applicable.
V2 Message packaging	<p>Support for the following packaging patterns, as required by UCC test profile under Test B, Test C and Test F:</p> <p>Test B Simple Data Transfer</p> <p>B1. HTTP Data Transfer</p> <p>Test C Large File Transfer</p> <p>C1. HTTP Large File Send</p> <p>Test F Multiple Payload Handling</p> <p>F1. Multiple Payload Transfer - two payloads</p> <p>F2. Multiple Payload Transfer - five payloads</p> <p>F3. Multiple Payload Signed - two payloads</p> <p>F4. Multiple Payload Signed with Signed Acknowledgment - five payloads - secure channel</p>
V2 Interoperability Parameters	Transport: HTTP 1.1 and HTTP/S
V2 processing mode	Processing mode representation: CPPA 2.0 or CPPA 1.0

413

414 This conformance profile combines ebMS V2 and V3 in the following way:

- 415
- 416
- 417
- Each one of the two messaging versions is operating separately as within two separate message handlers, without any requirement for each handler to be aware of the other handler.

- 418 • The P-Mode is a notion that has been defined only for V3. This conformance profile
419 does not define the equivalent for V2 and there is no requirement in this profile to
420 extend it to V2.
- 421 • This conformance profile does not extend the notion of MEP as defined in V3. No
422 MEP is defined or supported that makes use of both V2 and V3 messages.
- 423 • Message Ids must however be unique across V2 and V3.
- 424 • Although common header elements may be used to correlate V2 messages and V3
425 messages – e.g. ConversationID, RefToMessageId – this conformance profile does
426 not require a handler to support any correlation semantics across V2 and V3. A V3
427 message referencing a V2 message cannot be considered as part of a V3 MEP as
428 defined in the V3 specification.

429 2.4.2 WS-I Conformance Requirements

430 The same compliance rules as for RM V3 apply. Only ebMS V3 messages are concerned with these
431 rules.

432 2.4.3 Processing Mode Parameters

433 The P-Mode parameters to be supported for the V3 capability are same as in Gateway RM V3.

434 2.5 Conformance Profile: Gateway RX V2/3

435 The Gateway RX V2/3 is identified by the URI:

436 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/gateway-rxv2v3>

437 2.5.1 Feature Set

438 Gateway RX V2/3 is equivalent to the RX V3 conformance profile feature-wise.

439 The only difference is about the way messaging reliability is ensured. This profile relies on WS-
440 ReliableMessaging1.1 instead of WS-Reliability1.1. The same difference in V3 feature set table between
441 RM V3 and RX V3, applies here. The feature set for the V2 part is the same as in RM V2/3.

442

Conformance Profile: Gateway RX V2/3	Profile summary: <"Sending+Receiving" / " gateway-rxv2v3" / Level 1 / HTTP1.1 + SOAP 1.2 + WSS1.1 + WS-ReliableMessaging 1.1 > + < "Sending+Receiving" / UCC-EAN V2 handler / Level 1 / HTTP1.1>
Functional Aspects	Profile Feature Set
V2 Functional Aspects (same as in RM V2/3)	(same as in RM V2/3)
V3 Functional Aspects (same as in RX V3)	(same as in RX V3)

443

444 **2.5.2 WS-I Conformance Requirements**

445 The same compliance rules as for RX V3 apply. Only ebMS V3 messages are concerned with these
446 rules.

447 **2.5.3 Processing Mode Parameters**

448 The P-Mode parameters to be supported for the V3 capability are same as in Gateway RM V2/3, except
449 for the following:

- 450 • **PMode[1].Reliability.AtLeastOnce.Contract.AckOnDelivery:** “false” only needs be supported.

451

3 Examples of Alternate Conformance Profiles

3.1 Purpose

Some MSH implementations may have to operate under conditions where the full capabilities of the above Gateway conformance profile (G-CP) are not only unnecessary, but also not appropriate due to limited resources. In such cases, specific conformance profiles may need be defined as an alternate baseline for interoperability. Examples of such profiles (LH-CP and AM-CP) are given below.

The conformance profile below is intended to apply to messaging devices that do not have the ability to receive incoming requests (e.g. HTTP requests), due to a lack of static IP address or firewall restrictions. These message handlers also are supposed to be limited in storage capability. It is named LH-CP, meaning Light Handler.

3.2 Conformance Profile: Light Handler (LH-RM CP)

The Light Handler CP is identified by the URI:

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/lighthandler-rm>

NOTE: For consistency with the notations used in the previous Gateway conformance profiles, an alternative light handler profile using WS-ReliableMessaging instead of WS-Reliability would be named:

<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/lighthandler-rx>

3.2.1 Feature Set

Conformance Profile: LHRM-CP	Profile summary: <“Sending+Receiving” / “ lighthandler-rm” / Level 1 / HTTP1.1 + SOAP 1.1 + WS-Reliability 1.1>
Functional Aspects	Profile Feature Set
ebMS MEP	Support for One-way / Push (as initiator), and One-way / Pull (as initiator).
Reliability	Support for guaranteed delivery only: must be able to receive reliability acks on the SOAP response to the Push, and to resend a pushed message. Must be able to resend a non-acknowledged Pull signal. No requirement to acknowledge a pulled message.
Security	Support for username / password token
Error reporting	Support for error notification to the local message producer (e.g. reported failure to deliver pushed messages). Ability to report message processing errors for pulled messages to the remote party via Error messages (such an error may be bundled with another pushed message or a Pull signal.).
Message Partition Channels	Sending on default message partition flow channel (no support for additional message partitions required.)
Message packaging	No support for attachments required – i.e. the payload will use the SOAP body-, no support for MessageProperties required.

Interop Parameters	Transport: HTTP 1.1 SOAP version: 1.1 WSS: none Reliability Specification: WS-Reliability 1.1
--------------------	--

470

471 3.2.2 WS-I Conformance Requirements

472 This conformance profile will require compliance with the following WS-I profile, once formally approved
473 by WS-I (currently in Board approval draft status):

- 474 • Basic Profile 1.2 [WSIBP12]

475 Note: the above WS-I profile must be complied with within the scope of features exhibited by the Light
476 Handler ebMS conformance profile.

477 3.3 Conformance Profile: Activity Monitor (AM-CP)

478 The Activity Monitor CP is identified by the URI:

479 <http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/cprofiles/200707/activity-monitor>

480 3.3.1 Feature Set

481 The following conformance profile is even more restricted in capability. It is intended to match the
482 capability of a monitoring component that is supposed to only send messages (Sending role only), e.g.
483 for some type of business activity monitoring where reliability is not required as the loss of one of some
484 messages can be offset by subsequent messages.

485

Conformance Profile: AM-CP	Profile summary: <“Sending” / “activity-monitor” / Level 1 / HTTP1.1 + SOAP 1.1 >
Functional Aspects	Profile Feature Set
ebMS MEP	Support for One-way / Push (initiator)
Reliability	None.
Security	none
Error reporting	Support for generating errors associated with sending user messages, and notifying remote party via messages. Support for error reporting by notifying its own party (e.g. inability to open a connection).
Message Partition Channels	default message partition channel.
Message packaging	No support for attachments required, no support for MessageProperties required.
Interop Parameters	Transport: HTTP 1.1 SOAP version: 1.1

	WSS: none
	Reliability Specification: none

486

487 **3.3.2 WS-I Conformance Requirements**

488 This conformance profile requires compliance with the following WS-I profiles.

- 489 • Basic Profile 1.2 [WSIBP12]

490 Note: the above WS-I profile must be complied with within the scope of features exhibited by the Activity
491 Monitor conformance profile.

492
493

Appendix A Conformance Profile Template and Terminology

494
495

In order to facilitate the definition and comparison of conformance profiles, it is recommended to use the following template for describing a conformance profile:

Conformance Profile: <name>		Profile summary: [list of:] < ebMS Role(s) / DeploymentType / Level / InteroperabilityParameters >
Functional Aspects		Profile Feature Set
ebMS MEP		
Reliability		
Security		
Error reporting		
Message Partition Channels		
Message packaging		
Interop. Parameters	Transport and version	
	SOAP version	
	Reliability specification and version	
	Security specification and version	

496

497 Terminology:

498
499
500

A conformance profile is primarily associated with a common type of deployment or usage of an MSH implementation. It identifies a set of features that must be implemented in order for an MSH to support this type of deployment.

501

A conformance profile for ebMS is expressed using the following terms:

502
503

Role: This property refers to any possible role a message handler could take (see Section 2 in [ebMS3], which defines Sending and Receiving.)

504
505
506

Deployment Type: A deployment type characterizes a context in which the implementation operates and the expected functional use for this implementation. For example, the following deployment types are expected to be among the most common, nonexclusive from others:

- 507 1. "*resource-constrained handler*". This characterizes an implementation that generally is not
508 always connected, may not be directly addressable, may have no static IP address, has limited
509 persistent capability, and is not subject to high-volume traffic.
- 510 2. "*B2B or G2G gateway*". This characterizes an implementation that generally is acting as the
511 gateway for an enterprise or government agency. It has a fixed address; it may have connectivity
512 restrictions due to security; and it must support various types of connectivity with diverse
513 partners.

514 **Level:** This property represents a level of capability for this conformance profile, expressed as a positive
515 integer (starting from 1). All other properties being equal, an implementation that is conforming to a
516 profile at level N (with N>1) is also conforming to the same profile at level N-1.

517 **Interoperability parameters:** This property is a composed property. It is a vector of parameters that
518 must (in general) be similar pairwise between two implementations in order for them to interoperate.
519 Three parameters are identified here, not exclusive from others. Some are only relevant to ebMS V3:

- 520 1. The transport protocol supported, for which a non-exhaustive list of values is: HTTP, SMTP,
521 HTTPS.
- 522 2. SOAP version: either SOAP 1.1 or SOAP 1.2.
- 523 3. The reliability specification supported, either WS-Reliability or WS-ReliableMessaging.

524 **Conformance Profile:** A conformance profile is then fully identified by one or more quadruples of the
525 form: < Role / DeploymentType / Level / InteropParameters>, or <R / D / L / P>, which is called the
526 *profile summary*.

527 **Functional Aspect:** A conformance profile will impose specific requirements on different aspects of the
528 specification, that are called here functional aspects. A set of (non-exhaustive) functional aspects is:

529 Message Exchange Patterns, Error Reporting, Reliability, Security, Message Partition Flows, Message
530 Packaging, Transport.

531 **Profile Feature Set:** The set of specification requirements associated with a conformance profile. This
532 set is partitioned using the functional aspects listed for the specification: it can be expressed as a list of
533 functional aspects, annotated with the required features of each aspect.

534

535

Appendix B Acknowledgments

536
537

The following individuals have participated in the creation of this specification and are gratefully acknowledged.

538

Participants:

539

Hamid Ben Malek, Fujitsu Software <hbenmalek@us.fujitsu.com>

540

Jacques Durand, Fujitsu Software <jdurand@us.fujitsu.com>

541

Ric Emery, Axway Inc. <remery@us.axway.com>

542

Kazunori Iwasa, Fujitsu Limited <kiwasa@jp.fujitsu.com>

543

Ian Jones, British Telecommunications plc <ian.c.jones@bt.com>

544

Rajashekar Kailar, Centers for Disease Control and Prevention <kailar@bnetal.com>

545

Dale Moberg, Axway Inc. <dmoberg@us.axway.com>

546

Sacha Schlegel, Individual <sacha@schlegel.li>

547

Pete Wenzel, Sun Microsystems <pete.wenzel@sun.com>

548

549

Appendix C Revision History

550

Rev	Date	By Whom	What
CD 02	25 Jul 2007		

551