OASIS ebXML Messaging Services 3.0 Conformance Profiles

Committee Draft 03

12 August 2008

Specification URIs:

This Version:

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/ebms3-confprofiles-cd-03.pdf

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/ebms3-confprofiles-cd-03.html

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/ebms3-confprofiles-cd-03.odt

Previous Version:

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/ebms3-confprofiles-cd-02.pdf

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/ebms3-confprofiles-cd-02.html

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/ebms3-confprofiles-cd-02.odt

Latest Version:

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/ebms3-confprofiles.pdf

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/ebms3-confprofiles.html

http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/200707/ebms3-confprofiles.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/ns/ebms/v3.0/profiles/200707

Abstract:

This document is a supplement to the ebMS-3 specification [ebMS3]. It defines some conformance profiles that support specific messaging styles or context of use. Future releases of this document are likely to be augmented with additional conformance profiles that reflect the choices or needs of user communities. As a pre-condition to interoperability it is necessary for two implementations to agree on which common conformance profile, or which compatible conformance profiles, they will comply with. This document and its future releases is intended as a medium to publish conformance profiles that users and products will claim compliance with.

Status:

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

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

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

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

Notices

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

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

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

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

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

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

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

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

Table of Contents

1 Introduction

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

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

Future releases of the present document are likely to be augmented with additional conformance profiles that reflect the choices or needs of user communities. This document intends to serve as a medium for publishing such conformance profiles. Conformance profiles only refer to selected options and features that are already described in a normative way in the ebMS-3 specification: it is possible to conform to the core ebMS-3 specification without conforming to one of its profiles, but conforming to one of the profiles described here implies conformance to the core ebMS-3 specification.

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

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

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

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

- **Gateway RM V2/3:** supporting both ebMS V2 and V3, using WS-Reliability1.1 (produced by the WSRM OASIS TC) as reliable messaging specification.

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

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

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

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

1.1 Terminology

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

1.2 Normative References

[ebMS2] *OASIS ebXML Message Service Specification Version 2.0*, April 1, 2002. http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0.pdf

[ebMS3] *OASIS ebXML Messaging Services, Version 3.0: Part 1, Core Features*, 2007. http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.pdf

[RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt

[UCC-MS2] *UCC/EAN Basic Reliable ebXML Messaging v2.0 Interoperability Testing*, 2002.

[WSIAP10] *WS-I Attachment Profile V1.0*, Web-Services Interoperability Consortium, 2007. http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile

[WSIBP12] *WS-I Basic Profile V1.2 (draft)*, Web-Services Interoperability Consortium, 2007. http://www.ws-i.org/deliverables/workinggroup.aspx?wg=basicprofile

[WSIBSP11] Abbie Barbir, et al, eds, *Basic Security Profile Version 1.1*, Web-Services Interoperability Consortium, 2006. http://www.wsi.org/Profiles/BasicSecurityProfile-1.1.html

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

1.3 Non-normative References

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

2 The Gateway Conformance Profile

2.1 Purpose

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

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

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

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

2.2 Conformance Profile: Gateway RM V3

The Gateway RM V3 is identified by the URI:

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

This section identifies the requirements for conforming to this profile.

2.2.1 Feature Set

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

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	The implementation MUST support all ebMS simple MEPs, in either Sender or Receiver role: • One-way / Push,

	• One-way / Pull, • Two-way / Sync (both Initiator and Responder roles) Regardless of which MEP is used, the sending of an eb:Receipt message MUST be supported: • 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. The sender of the User message MUST accept (i.e. must not Fault and must process as expected) 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 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. Use of the ebbpsig:NonRepudiationInformation element (as defined in **[ebBP-SIG]**) MUST be supported as content for the eb:Receipt message, both by sender and receiver.
Reliability	The following message reliability features MUST be supported: • Sender and Receiver MSH MUST support the following QoS features for pushed or pulled ebMS messages: at-least-once, at-most-once, exactly-once. • Receiver MSH MUST be able to acknowledge pulled messages (AtLeastOnce.Contract.AckResponse=”true”). • Receiver MSH MUST supports Acknowledgments on delivery (supports P-Mode with Reliability.AtLeastOnce.Contract.AckOnDelivery=”true”) • Sender and Receiver MSH MUST support the following reply patterns for acknowledgments (P-Mode AtLeastOnce.ReplyPattern): either “response”, or “callback” (no support for polling required)
Security	The following message security features MUST be supported: • Sender and Receiver MSH MUST support username / password token, digital signatures and encryption. • Sender and Receiver MSH MUST support content-only transforms. • Sender and Receiver MSH MUST support security of attachments as required. • Sender and Receiver MSH MUST support 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.

	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”
Error generation and reporting	The following error handling features MUST be supported: • 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 MUST 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 is REQUIRED, so that selective pulling by a partner MSH is possible.
Message packaging	The following message packaging features MUST be supported: • Support for attachments is REQUIRED. • Support for MessageProperties is REQUIRED. • Ability to process messages that contain both a signal message unit (eb:SignalMessage) and a user message unit (eb:UserMessage) is REQUIRED.
Interoperability Parameters	**Transport:** HTTP 1.1 **SOAP version:** 1.2 **Reliability Specification:** WS-Reliability 1.1. Only “Response” or “Callback” ReplyPattern values are required to be supported. **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

2.2.2 WS-I Conformance Requirements

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

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

Notes:

– Compliance with AP1.0 would normally require compliance with BP1.1, which in turn requires the absence of SOAP Envelope in the HTTP response of a One-Way (R2714). However, recent BP versions such as BP1.2 [WSIBP12] override this requirement. Consequently, the Gateway conformance profile does not require conformance to these deprecated requirements inherited from BP1.1 (R2714, R1143) regarding the use of HTTP.

– The above WS-I profiles must be complied with within the scope of features exhibited by the Gateway RM V3 ebMS conformance profile. For example, since only SOAP 1.2 is required by Gateway RM V3, the requirements from BSP 1.1 that depend on SOAP 1.1 would not apply. Similarly, none of the requirements for DESCRIPTION (WSDL) or REGDATA (UDDI) apply here, as these are not used.

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

- Basic Profile 2.0 (BP2.0)iui

2.2.3 Processing Mode Parameters

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

– full support is required: an implementation is supposed to support the possible options for this parameter.

– Support for a subset of values is required.

– No support is required: an implementation is not required to support the features controlled by this parameter, and therefore not required to understand this parameter.

0. General PMode parameters:

- **(PMode.ID:** support not required)
- **(PMode.Agreement:** support not required)

- **PMode.MEP:** support for**:** http://www.oasis-open.org/committees/ebxml-msg/{one-way, two-way}
- **PMode.MEPbinding:** support for**:** http://www.oasis-open.org/committees/ebxml-msg/{ push, pull, sync}
- **PMode.**Initiator.Party: support required**.**
- **PMode.Initiator.Role:** support required**.**
- **PMode.**Initiator.Authorization.username and **PMode.**Initiator.Authorization.password: support for: wsse:UsernameToken.
- **PMode.**Responder.Party: support required**.**
- **PMode.Responder.Role:** support required**.**
- **PMode.**Responder.Authorization.username and **PMode.**Responder.Authorization.password: support for: wsse:UsernameToken.

1. PMode[1].Protocol:

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

2.PMode[1].BusinessInfo:

- **PMode[1].BusinessInfo**.Service: support required**.**
- **PMode[1].BusinessInfo**.Action: support required**.**
- **PMode[1].BusinessInfo.Properties[]:** support required.
- **(PMode[1].BusinessInfo**.PayloadProfile[]:not required**)**
- **(PMode[1].BusinessInfo**.PayloadProfile.maxSize: not required**)**
- **PMode[1].BusinessInfo.MPC:** support required**.**

3. PMode[1].ErrorHandling:

- **(PMode[1].**ErrorHandling.Report.SenderErrorsTo: support not required**)**
- **PMode[1].**ErrorHandling.Report.ReceiverErrorsTo: support required (for address of the MSH sending the message in error or for third-party).
- **PMode[1].**ErrorHandling.Report.AsResponse: support required (true/false).
- **(PMode[1].**ErrorHandling.Report.ProcessErrorNotifyConsumer support not required**)**
- **PMode[1].**ErrorHandling.Report.ProcessErrorNotifyProducer: support required (true/false)

- **PMode[1].**ErrorHandling.Report.DeliveryFailuresNotifyProducer: support required (true/false)

4. PMode[1].Reliability:

- **PMode[1].**Reliability.AtLeastOnce.Contract: support required (true/false)
- **PMode[1].**Reliability.AtLeastOnce.Contract.AckOnDelivery: true/false
- **PMode[1].**Reliability.AtLeastOnce.Contract.AcksTo: support required.
- **PMode[1].**Reliability.AtLeastOnce.Contract.AckResponse: support required (true/false)
- **PMode[1].**Reliability.AtLeastOnce.ReplyPattern: support required for: {Response, Callback}.
- **PMode[1].**Reliability.AtMostOnce.Contract: support required (true/false)
- **(PMode[1].**Reliability.InOrder.Contract: support not required**)**
- **(PMode[1].**Reliability.StartGroup: support not required**)**
- **(PMode[1].**Reliability.Correlation: support not required**)**
- **(PMode[1].**Reliability.TerminateGroup: support not required**)**

5. PMode[1].Security:

- **PMode[1].**Security.WSSVersion: support required for: {1.0 , 1.1 }
- **PMode[1].**Security.**X509.**Sign: support required.
- **PMode[1].**Security.**X509.**Signature.Certificate: support required.
- **PMode[1].**Security.**X509.**Signature.HashFunction: support required.
- **PMode[1].**Security.**X509.**Signature.Algorithm: support required.
- **PMode[1].**Security. **X509.**Encryption.Encrypt: support required.
- **PMode[1].**Security.**X509.**Encryption.Certificate: support required.
- **PMode[1].**Security.**X509.**Encryption.Algorithm: support required.
- **(PMode[1].**Security.**X509.**Encryption.MinimumStrength: support not required**)**
- **PMode[1].**Security.UsernameToken.username: support required.
- **PMode[1].**Security.UsernameToken.password: support required.
- **PMode[1].Security.UsernameToken.Digest:** support required (true/false)
- **(PMode[1].Security.UsernameToken.Nonce:** not required**)**
- **PMode[1].Security.UsernameToken.Created:** support required.
- **PMode[1].**Security.PModeAuthorize: support required (true/false)

- **PMode[1].**Security.SendReceipt: support required (true/false)
- **Pmode[1].**Security.SendReceipt.ReplyPattern: support required (both "response" and "callback"))

2.3 Conformance Profile: Gateway RX V3

The Gateway RX V3 is identified by the URI:

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

This section identifies the requirements for conforming to this profile.

2.3.1 Feature Set

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

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

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:] • 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	**Transport:** HTTP 1.1 **SOAP version:** 1.2 **Reliability Specification:** WS-ReliableMessaging 1.1. Only "Response" or "Callback" ReplyPattern values are required to be supported. **Security Specification:** WSS1.0 and WSS 1.1.

2.3.2 WS-I Conformance Requirements

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

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

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

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

- Basic Profile 2.0
- Reliable and Secure Profile (RSP) 1.1

2.3.3 Processing Mode Parameters

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

- **PMode[1].**Reliability.AtLeastOnce.Contract.AckOnDelivery: "false" only needs be supported.

2.4 Conformance Profile: Gateway RM V2/3

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

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

This section identifies the requirements for conforming to this profile.

2.4.1 Feature Set

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

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

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

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

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 the following MEPs (in either Sender or Receiver role) is REQUIRED: • One-way / Push, defined as exchanges controlled by SyncReplyMode values: “mshSignalsOnly", "signalsOnly" or “none”.
V2 Reliability	Support for reliable messaging, as specified in UCC test profile under Test E and Test J, is REQUIRED: Test E Acknowledgments E1. Unsigned Data/Unsigned Ack E2. Unsigned Data/Signed Ack E3. Signed Data/Unsigned Ack E4. Signed Data/Signed Ack E5. Signed Data/Signed Ack Secure Channel Test J Single-Hop Reliable Messaging J1. Once and Only Once Profile – Successful Retries, RetryInterval J2. Duplicate Detection - Original Acknowledgement to Duplicate Request J3. Delivery Failure Notification J4. Long Running Conversation
V2 Security	Support for secure messaging, as specified by UCC test profile under Test A , Test B and Test D, is REQUIRED: Test A Certificate Exchange A1. Personal Certificate Test B Simple Data Transfer B2. HTTP/S Data Transfer Test D Data Security

	D1. Signed Data D2. Signed Data Secure Channel (HTTP/S) D3. Client Authentication - Signed Data Secure Channel (HTTP/S)
V2 Error generation and reporting	Support for error handling, as specified by UCC test profile under Test K, is REQUIRED: Test K Error Handling K1. SOAP:Fault K2. ValueNotRecognized K3. NotSupported K4. Inconsistent Sync K5. Inconsistent Signature K6. Inconsistent Acknowledgment Signature K7. SecurityFailure K8. TimeToLiveExpired K10. MessageHeader format K11. Missing Payload
V2 Message Partition Channels	Not applicable.
V2 Message packaging	Support for the following packaging patterns, as specified by UCC test profile under Test B, Test C and Test F, is REQUIRED: Test B Simple Data Transfer B1. HTTP Data Transfer Test C Large File Transfer C1. HTTP Large File Send Test F Multiple Payload Handling F1. Multiple Payload Transfer – two payloads F2. Multiple Payload Transfer – five payloads F3. Multiple Payload Signed – two payloads F4. Multiple Payload Signed with Signed Acknowledgment – five payloads – secure channel
V2 Interoperability Parameters	**Transport:** HTTP 1.1 and HTTP/S

V2 processing mode	**Processing mode representation**: CPPA 2.0 or CPPA 1.0

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

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

2.4.2 WS-I Conformance Requirements

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

2.4.3 Processing Mode Parameters

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

2.5 Conformance Profile: Gateway RX V2/3

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

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

This section identifies the requirements for conforming to this profile.

2.5.1 Feature Set

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

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

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	**Profile Feature Set**

Aspects	
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)

2.5.2 WS-I Conformance Requirements

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

2.5.3 Processing Mode Parameters

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

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

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

but such profile is not defined here.

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

3.2.2 WS-I Conformance Requirements

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

- Basic Profile 1.2 [WSIBP12]

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

3.3 Conformance Profile: Activity Monitor (AM-CP)

The Activity Monitor CP is identified by the URI:

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

3.3.1 Feature Set

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

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

3.3.2 WS-I Conformance Requirements

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

- Basic Profile 1.2 [WSIBP12]

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

4 Conformance Clauses

4.1 Gateway RM V3 Conformance Clause

In order to conform to the **Gateway RM V3** Profile, an implementation must comply with all normative statements and requirements in Section 2.2.

In particular, it must:

- implement the set if features as required in the Feature Set table of Section 2.2.1.

- comply with WS-I requirements listed in Section 2.2.2.

- support the required PMode parameters described in Section 2.2.3.

4.2 Gateway RX V3 Conformance Clause

In order to conform to the **Gateway RX V3** Profile, an implementation must comply with all normative statements and requirements in Section 2.3.

In particular, it must:

- implement the set if features as required in the Feature Set table of Section 2.3.1.

- comply with WS-I requirements listed in Section 2.3.2.

- support the required PMode parameters described in Section 2.3.3.

4.3 Gateway RM V2/3 Conformance Clause

In order to conform to the **Gateway RM V2/3** Profile, an implementation must comply with all normative statements and requirements in Section 2.4.

In particular, it must:

- implement the set if features as required in the Feature Set table of Section 2.4.1.

- comply with WS-I requirements listed in Section 2.4.2.

- support the required PMode parameters described in Section 2.4.3.

4.4 Gateway RX V2/3 Conformance Clause

In order to conform to the **Gateway RX V2/3** Profile, an implementation must comply with all normative statements and requirements in Section 2.5.

In particular, it must:

- implement the set if features as required in the Feature Set table of Section 2.5.1.

- comply with WS-I requirements listed in Section 2.5.2.

- support the required PMode parameters described in Section 2.5.3.

Appendix A Conformance Profile Template and Terminology

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

In each entry of this table (column 2) specify which features are REQUIRED or RECOMMENDED by this profile (this applies also to the absence of features).

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	

Terminology:

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.

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

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

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:

1. "*resource-constrained handler*". This characterizes an implementation that generally is not always connected, may not be directly addressable, may have no static IP address, has limited persistent capability, and is not subject to high-volume traffic.

2. "B2B or G2G *gateway*". This characterizes an implementation that generally is acting as the gateway for an enterprise or government agency. It has a fixed address; it may have connectivity restrictions due to security; and it must support various types of connectivity with diverse partners.

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

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

1. The transport protocol supported, for which a non-exhaustive list of values is: HTTP, SMTP, HTTPS.

2. SOAP version: either SOAP 1.1 or SOAP 1.2.

3. The reliability specification supported, either WS-Reliability or WS-ReliableMessaging.

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

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

Message Exchage Patterns, Error Reporting, Reliability, Security, Message Partition Flows, Message Packaging, Transport.

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

Appendix B Acknowledgments

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

Participants:

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

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

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

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

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

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

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

Sacha Schlegel, Individual <sacha@schlegel.li>

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

Appendix C Revision History

Rev	Date	By Whom	What
CD 02	25 Jul 2007	J. Durand	Candidate draft for CD
CD 03	28 Oct 2008	J. Durand	Missing subsection 2.2.1, more specific profiling of eb:Receipt, more specific message authorization requirements.