OASIS ebXML Messaging Services 3.0 Conformance Profiles

Working Draft 08, 30 May 2007

Document identifier:

ebms-3.0_conformanceprofiles-wd-08

Location:

http://www.oasis-open.org/committees/documents.php?wg_abbrev=ebxml-msg

Technical Committee:

OASIS ebXML Messaging Services TC

Chair:

Ian Jones, British Telecom ian.c.jones@bt.com

Editors:

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

Contributors:

Pete Wenzel, Sun Microsystems pete.wenzel@sun.com
Ric Emery, AxWay <remery@cyclonecommerce.com>
Kazunori Iwasa, Fujitsu Limited <kiwasa@jp.fujitsu.com>
Dale Moberg, AxWay <dmoberg@cyclonecommerce.com>
Sacha Schlegel, HavanaWave sschlegel@cyclonecommerce.com
Hamid Ben Malek, Fujitsu Computer Systems hbenmalek@us.fujitsu.com

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 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 is a Working Draft, meaning that the TC has not necessarily reached consensus on any or all content, and all contents are subject to change.

Table of Contents

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. The document is non-normative in the sense that conformance profiles only refer to selected options and features that are already described in a normative way in the 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 exists 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 more recent, still in the last phases of standardization, 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 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 V23, excepts 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, 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.

The Gateway Conformance Profile

1.Purpose

The *Gateway* conformance profile (or G-CP) is to be considered 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 an already pervasive 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.Conformance Profile: Gateway RM V3

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" / 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, ineither Sender or Receiver role: • One-way / Push, • One-way / Pull, • Two-way / Sync (both Initiator and Responder roles)
Reliability	• 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	• 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, in particular authorization of the Pull signal for a particular MPC.
Error generation and reporting	• 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	• 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	**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

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 Profile 2.0 (BP2.0) [WSIBP20]
- Basic Security Profile (BSP) 1.1 [WSIBSP11]

Note: 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.

Processing Mode Parameters

Summary of P-Mode parameters that must be supported by an implementation conforming to this profile. Fore 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[]:** not 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)

3.Conformance Profile: Gateway RX V3

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" / 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.

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 Profile 2.0 (BP2.0) [WSIBP20]
- Basic Security Profile (BSP) 1.1 [WSIBSP11]
- Reliable and Secure Profile (RSP) 1.1 [WSIRSP11]

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.

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.

4.Conformance Profile: Gateway RM V2/3

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" / " V3 gateway" / 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): • 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: 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 J5. Sequence Numbers – Correct Sequence
V2 Security	Support for secure messaging, as required by UCC test profile under Test A , Test B and Test D: 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 required by UCC test profile under Test K: 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 K9. Out Of Sequence K10. MessageHeader format K11. Missing Payload
V2 Message Partition Channels	Not applicable.
V2 Message packaging	Support for the following packaging patterns, as required by UCC test profile under Test B, Test C and Test F: 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.

WS-I Conformance Requirements

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

Processing Mode Parameters

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

5.Conformance Profile: Gateway RX V2/3

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" / " V3 gateway" / 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)

WS-I Conformance Requirements

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

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.

Examples of Alternate Conformance Profiles

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.

2.Conformance Profile: Light Handler (LH-CP)

Feature Set

Conformance Profile: **LH-CP**	**Profile summary**: <"Sending+Receiving" / " light handler" / 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.Conformance Profile: Activity Monitor (AM-CP)

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

Appendix: 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:

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. Parameter	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: 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://www.oasis-open.org/committees/documents.php?wg_abbrev=ebxml-msg

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

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

[WSIBP20]: WS-I Basic Profile V2.0, Web-Services Interoperability consortium, 2007
<http://www.ws-i.org/deliverables/index.aspx>

[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>

[WSIRSP11]: WS-I Reliable, Secure Profile V1.1, Web-Services Interoperability consortium, 2007
<http://www.ws-i.org/deliverables/index.aspx>

Appendix: Notices

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's procedures with respect to rights in OASIS specifications can be found at 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 specification, can be obtained from the OASIS Executive Director.

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