ND1618:2006/11

PROFILE FOR ebXML MESSAGING SERVICE 2.0 GATEWAYS

Issue 1

Network Interoperability Consultative Committee
Ofcom
Riverside House,
2a Southwark Bridge Road,
London SE1 9HA
UK
http://www.nicc.org.uk

Normative Information

Document history

Revision	Date	Notes
Draft 4	November 2006	Final Draft for Approval
Issue 1	24th November 2006	Issue for NICC Approval

Contents

Page

1. Introduction

This document provides recommendations on the usage of several configurable features available in ebXML ms 2.0 Message Service Handler (MSH) gateways **[2].** This is intended as a guide to communications providers using this standard for provider to provider eBusiness integration in the UK. This document is also a template for further refining and capturing specific information for a particular community.

The template itself is a semi completed version of the OASIS ebXML ms2.0 deployment profile template 1.0 **[1].**

Purpose

The ebXML Message Service Specification 2.0 **[2]** contains several optional and configurable features. Any use of ebMS within a community therefore requires an amount of standardization to achieve interoperability. Also, a community may want to further profile the content and format of some message elements, to match their business practices.

The purpose of this template deployment profile is to provide both a check list of the options and, where possible, make some recommendations as to their use within a community. This is based on the experience of BT Openreach in the use of ebXML ms2.0 for B2B integration with communications providers.

For a wider view of the options available it is suggested that one reads the committee drafts of the original ebXML ms 2.0 deployment profile template located on the OASIS ebXML IIC technical committee web site

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-iic

and in their document archive

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

Note, it is not possible to make recommendations in this document for all the items in the template as some are specific to the particular instance of a community.

Also note that this guide is not to be confused with the notion of a Collaboration Protocol Agreement (CPA), which focuses on the definition of how specific business processes are integrated between partners through gateways. Some elements of the Deployment Template will, however, map to a community's specific requirements on the use CPA and the features included in CPA.

A completed instance of the deployment profile template defines preferences as to how particular communities whish to configure and deploy ebXML ms2.0 gateways in an interoperable fashion. For information on wider ebXML ms2.0 interoperability, visit the following URL:

http://www.drummondgroup.com/html-v2/ebXML-companies.html

Audience

The document is intended for trading partner technical teams responsible for configuring Message Service Handlers (referred as MSH through out this document) to communicate with other such gateways within a community.

2. How to Use the Deployment Profile

There are three parts in the Deployment Profile:

- The section on the source specification modules (see section 3 below)
- The section on the profiling requirement details (see section 4 below)
- The section on operating conditions associated with the profile (see section 5 below)

Every feature from the source specification that is candidate for profiling is listed in a “profile requirement item” table of the form:

Specification Feature	<Description of the source specification item to be profiled. This is pre-filled in the Deployment Profile Template.>
Specification Reference	<Identifies the item in the source specification. This is pre-filled in the Deployment Profile Template >
Profiling	<how the item is profiled: option narrowing/selection, content formatting, narrowing structure of XML complex element, content integrity constraint. This reflects recommendations made and/or where further profiling is required for a particular community>
Alignment	<dependency / alignment with other data, e.g. binding, either with other item in this same specification, items from other ebXML specifications, or items specified in an external source, e.g. a domain-specific or industry-specific standard. >
Notes	<Profile-specific comments>

3. Modules of Message Service Specification (ebMS 2.0)

This section specifies which modules of the ebXML Message Service Specification are referred to in this template profile (i.e. modules that trading partners need to use or support in order to comply with the profile and communicate). For each used module, it is specified whether the module has been profiled or not. Each module is expanded in the sections to come.

3.1 Core Modules

Module Name and Reference	Core Extension Elements (section 4.1)
Profiling Status	Required and Profiled
Notes	

Module Name and Reference	Security Module (section 4.2)
Profiling Status	Required and Profiled
Notes	

Module Name and Reference	SyncReply Module (section 4.4)
Profiling Status	Never used in this profile
Notes	SyncReply is not generally supported by all commercial implementations of ebXML ms2.0. It is recommendation to avoid use of this feature if possible

3.2 Additional Modules

Module Name and Reference	Reliable Messaging Module (section 4.5)
Profiling Status	Required and Profiled
Notes	Reliable messaging is one of the key features of ebXML messaging. It recommended that implementations are configured to use reliable messaging

Module Name and Reference	Message Status Service (section 4.6)

Profiling Status	Required and Profiled
Notes	This service is not essential to achieve interoperability but if supported can be used as an aid to systems support. However there are potential issues with its use or abuse and it is suggested that the usage of this particular service be managed and monitored.

Module Name and Reference	Ping Service (section 4.7)
Profiling Status	Required and Profiled
Notes	This service is not essential to achieve interoperability but if supported can be used as an aid to systems support. However there are potential issues with its use or abuse and it is suggested that the usage of this particular service be managed and monitored.

Module Name and Reference	Multi-Hop (section 4.8)
Profiling Status	Never used in this profile
Notes	Multi-hop is rarely supported in commercial implementations of ebXML ms2.0 and there is no known real-world requirement to use it.

3.3 Communication Protocol Bindings

3.3.1 Profile Requirement Item: Transport Protocol

Specification Feature	Header elements:
Specification Reference	ebMS 2, Appendix B
Profiling (a)	Is HTTP a required or allowed transfer protocol? (See section B.2 of Message Service Specification for specifics of this protocol.) **No. HTTPS is the only preferred and allowed protocol**
Profiling (b)	Is HTTPS a required or allowed transfer protocol? (See section B.2 for specifics of this protocol.) **Yes**
Profiling (c)	Is (E)SMTP a required or allowed transfer protocol? (See section B.3 for specifics of this protocol.) **No. SMTP is not allowed as a transfer protocol.**
Profiling (d)	If SMTP, What is needed in addition to the ebMS minimum requirements for SMTP? **Not Applicable**
Profiling (e)	Are any transfer protocols other than HTTP and SMTP allowed or required? If so, describe the protocol binding to be used. **Not Applicable**
Alignment	
Notes	SMTP Support is not something generally available in commercially available ebXML ms2.0 gateways. It is recommended to opted for HTTPS as the generally used transport.

4. Profile Requirements Details

4.1 Module: Core Extension Elements

4.1.1 Profile Requirement Item: PartyId

Specification Feature	In message Header: /SOAP:Header/eb:MessageHeader/eb:From/eb:PartyId /SOAP:Header/eb:MessageHeader/eb:To/eb:PartyId Is a specific standard used for party identification? Provide details.
Specification Reference	ebMS 2, section 3.1.1.1 PartyId Element
Profiling (a)	Is a specific standard used for party identification? Provide details. Example - EAN•UCC Global Location Number. Ref.: ISO6523 - ICD0088. **PartyId should be based in D-U-N-S (Data Universal Numbering System)**
Profiling (b)	Should multiple PartyId elements be present in From and To elements? [See section 3.1.1.1 of Business-Level Requirements.] **No. If either the *From* or *To* elements contains multiple *PartyId* elements, all members of the list MUST identify the same organization.**
Profiling (c)	Is the type attribute needed for each PartyId, and if so, what must it contain? **PartyId attribute is required and it should have the following value:** *urn:oasis:names:tc:ebXML-cppa:partyid-type:duns*
Alignment	PartyId appears as PartyId element in CPA and the "type" attribute appears as PartyId/@type in CPA
Notes	PartyId is one of the keys to accessing entries in CPAs. It is recommended to standardized on the use of DUNS. However it is possible to use other designations.

4.1.2 Profile Requirement Item: Role

Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:From/eb:Role /SOAP:Header/eb:MessageHeader/eb:To/eb: Role
Specification Reference	ebMS 2, section 3.1.1.2 "Role Element"
Profiling	Are Roles defined for each party of each business process? List them, or provide a reference to the source of these values. **Yes. Roles should be defined for each party of each business process.** **They should be derived from the Business Process Specification for the relevant processes.**
Alignment	[Per-process; may reference Role values in BPSS [BPSS] definitions. Appears as Role/@name in CPA.]
Notes	In ebXML ms the role elements are regarded as optional. However when used in conjunction with CPAs these are mandatory as they are a key to gaining access to the content of the CPA. It is recommended the role names are taken directly from the published Business Process Specifications.

	For example: • WholesaleProvider • ServiceProvider • CommunicationsProvider Ideally role names should be independent of location of partners in the supply chain and should be neutral terms such as “Buyer” and “Seller”. However the terms above are prevalent in industry documentation and have stuck.

4.1.3 Profile Requirement Item: CPAId

Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:CPAId
Specification Reference	ebMS 2, section 3.1.2
Profiling	What identification scheme is used for the CPAId, and what form should it take? If a URI, how is it constructed? Does it reference a real CPA, or is it just a symbolic identifier? **No recommendation.**
Alignment	Appears as CollaborationProtocolAgreement/@cpaid in CPA.
Notes	It is recommended that the CPAId is based on community names of buyer and seller Example: *<CP1 Name>_<CP2 Name>_B2B_<ProductName>* The *CPAId* may reference an instance of a *CPA* as defined in the ebXML Collaboration Protocol Profile and Agreement Specification [ebCPP].

4.1.4 Profile Requirement Item: ConversationId

Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:ConversationId
Specification Reference	ebMS 2, section 3.1.3
Profiling (a)	What is the user definition of a Conversation? **Conversation should be an instance of a collaboration between two partners as specified in the Business Process Specification.** What is the business criterion used to correlate messages considered parts of the same conversation?

	The initiating role defines the ConversationId in the first message of a collaboration instance (a conversation). This ConversationId is used by all participants to correlate messages considered parts of the same collaboration instance.
Profiling (b)	In case the MSH implementation gives exposure of the ConversationId as it appears in the header, what identification scheme should be used for its value, and what format should it have? If a URI, how is it constructed? In case the ConversationId is not directly exposed, but only a handle that allows applications to associate messages to conversations, if the value of this handle is under control of the application, what format should it have? **A useful format to define unique conversation ids is.** *"C" + current timestamp in milliseconds (format "yyyyMMddHHmmssSSS") + "." new java.rmi.server.UID() + "@" + HostAddress.* *One has to be careful as to the host address exposed by this (ideally it should not be the address of a green side server as this may create a security weakness).*
Alignment	If BPSS is used, ConversationId typically maps to a business transaction. Is that the case? **No** Does it map instead to business collaboration? **ConversationIds are mapped to business collaborations but all current business collaborations support a single transaction only. This allows for the possibility of conversations spanning more than one transaction to be introduced in the future.**
Notes	It is recommended that Business Process Specifications define binary collaborations. An instance of one of these collaborations is taken to be a conversation. At the moment all such collaborations are defined to be one activity or transaction long.

4.1.5 Profile Requirement Item: MessageId

Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:MessageData/eb:MessageId
Specification Reference	ebMS 2, section 3.1.6.1
Profiling (a)	Although there is no requirement for an MSH to give control about MessageID to an application, some implementations may allow this. In this case, is there any requirement on the source of this ID? Any length and format restrictions if the ID is generated? **When sending a message to a trading partner using ebXML, a useful format to employ is:** *"G" + current timestamp in milliseconds (format "yyyyMMddHHmmssSSS") + "." new java.rmi.server.UID() + "@" + HostAddress*. *One has to be careful as to the host address exposed by this (ideally it should not be the address of a green side server as this may create a security*

	weakness).
Alignment	**Not Applicable**
Notes	The **MessageId** element is a globally unique identifier for each message conforming to MessageId.[Reference : RFC 2822].

4.1.6 Profile Requirement Item: Service

Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:Service /SOAP:Header/eb:MessageHeader/eb:Service/@type
Specification Reference	ebMS 2, section 3.1.4
Profiling (a)	Are Services (related groups of Actions) defined for each party of each business process? List them, or provide a reference to the source of these values. [Per-process; absent from BPSS definitions.] Is there a URI format scheme for this element? **Yes. Services are defined for each party of each business process. The service name should be same as the Collaboration name defined in the appropriate BPS.** **Example:** *<tp:Service tp:type="string">bcRequestOrder</tp:Service>*
Profiling (b)	Is there a defined "type" for Service elements? If so, what value must the type attribute contain? **Yes. A '*type*' attribute of Service Element should contain the data type of the Service Element value. The data type of the *'type'* attribute should be a valid string.**
Alignment	Appears as Service element in CPA Appears as Service/@type in CPA
Notes	It is recommended service names are strings taken from the name of a binary collaboration (e.g. bcRequestOrderv2). The version number suffix is used to allow multiple versions of the service to be address concurrently.

4.1.7 Profile Requirement Item: Action

Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:Action
Specification Reference	ebMS 2, section 3.1.5

Profiling	Are Actions defined for each party to each business process? List them, or provide a reference to the source of these values. [Per-process; may reference BusinessAction values in BPSS definitions. Example – within the EAN•UCC system, approved values are specified by the EAN•UCC Message Service Implementation Guide. <eb:Action>Confirmation</eb:Action> **Yes. Actions are defined for each party to each business process. Action names are same as that of the Requesting/Responding business activity names of business transaction activities within binary collaborations.** **Example:** • **rqRequestOrder (Requesting Business Activity)** • **rsConfirmOrder (Responding Business Activity)**
Alignment	Appears as ThisPartyActionBinding/@action in CPA.]
Notes	Because one needs to refer to both the requesting and responding activities via Action, the lowest level activity of a BPS is referred to. It is recommended the higher level business transaction activity is not referenced as a path to these two names. Therefore In multi transaction activity collaborations one needs to be careful not to have duplicate requesting and responding business activity names. In addition there are special action names for receipt and acceptance acknowledgements/exceptions.

4.1.8 Profile Requirement Item: Timestamp

Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:MessageData/eb:Timestamp /SOAP:Header/eb:MessageHeader/eb:Acknowledgment/eb:Timestamp
Specification Reference	ebMS 2, section 3.1.6.2, 6.3.2.2, 6.4.5, 7.3.2
Profiling	Must Timestamp include the 'Z' (UTC) identifier? **Yes**
Alignment	**Not Applicable**
Notes	It is recommended to use UTC for all ebXML ms related time elements.

4.1.9 Profile Requirement Item: Description

Specification Feature	Header elements: /SOAP:Header/eb:MessageHeader/eb:Description
Specification Reference	ebMS 2, section 3.1.8

Profiling	Are one or more Message Header Description elements required? **Not mandatory** In what language(s)? **If used, it will be in English (U.K)** Is there a convention for its contents? **It would be in plain text format and not case-sensitive**
Alignment	**Not Applicable**
Notes	The purpose of 'Description' element is to provide a human readable description of the purpose or intent of the message. The language of the description is defined by a required ***xml:lang*** attribute. The ***xml:lang*** attribute MUST comply with the rules for identifying languages specified in XML [XML]. Each occurrence SHOULD have a different value for ***xml:lang***. It is recommended not to use this description capability.

4.1.10 Profile Requirement Item: Manifest

Specification Feature	Header elements: /SOAP:Body/eb:Manifest
Specification Reference	ebMS 2, section 3.2.2
Profiling (a)	How many Manifest elements must be present, and what must they reference? **There is one Manifest element that references a single attached payload via xlink.** Does the order of Manifest elements have to match the order of the referenced MIME attachments? **Not Applicable**
Profiling (b)	Must a URI that cannot be resolved be reported as an error? **Yes**
Alignment	**Not Applicable**
Notes	**The purpose of the Manifest is:** • **to make it easier to directly extract a particular payload associated with this ebXML Message,** • **to allow an application to determine whether it can process the payload without having to parse it.**

4.1.11 Profile Requirement Item: Reference

Specification Feature	Header elements: /SOAP:Body/eb:Manifest/eb:Reference
Specification Reference	ebMS 2, section 3.2.1
Profiling (a)	Is the xlink:role attribute required? What is its value? **No**
Profiling (b)	Are any other namespace-qualified attributes required? **No**
Alignment	**Not Applicable**
Notes	

4.1.12 Profile Requirement Item: Reference/Schema

Specification Feature	Header elements: /SOAP:Body/eb:Manifest/eb:Reference/eb:Schema
Specification Reference	ebMS 2, section 3.2.1.1
Profiling	Are there any Schema elements required? If so, what are their location and version attributes? **No**
Alignment	**Not Applicable**
Notes	

4.1.13 Profile Requirement Item: Reference/Description

Specification Feature	Header elements: /SOAP:Body/eb:Manifest/eb:Reference/eb:Description
Specification Reference	ebMS 2, section 3.2.1.2
Profiling	Are any Description elements required? If so, what are their contents? **No Description elements required**
Alignment	**Not Applicable**

Notes	

4.2 Module: Security

4.2.1 Profile Requirement Item: Signature generation

Specification Feature	Header elements: /SOAP:Header/Signature
Specification Reference	ebMS 2, section 4.1.4.1
Profiling (a)	Must messages be digitally signed? **Yes**
Profiling (b)	Are additional Signature elements required, by whom, and what should they reference? **No**
Profiling (c)	What canonicalization method(s) must be applied to the data to be signed? **The recommended canonicalization method applied to the data to be signed is** *<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>*
Profiling (d)	What canonicalization method(s) must be applied to each payload object, if different from above? **Please refer profiling (c)**
Profiling (e)	What signature method(s) must be applied? **Signatures should use the SHA1 hashing algorithm. MD5 algorithms are not supported.**
Profiling (f)	What Certificate Authorities (issuers) are allowed or required for signing certificates? **The channel master for the community (e.g. the partner who all other partners trade with).**
Profiling (g)	Are direct-trusted (or self-signed) signing certificates allowed? **No.**
Alignment	(a) Appears as BusinessTransactionCharacteristics/@isAuthenticated=persistent and BusinessTransactionCharacteristics/@isTamperProof=persistent in CPA
Notes	The above is the recommended approach to signing and certificates. An example is to become a member of a BT Openreach community to enrol for a BT Openreach client Digital Certificate using the following web link:

	https://onsite.trustwise.com/services/BTGroupPlcB2BOpenreach/

4.2.2 Profile Requirement Item: Persistent Signed Receipt

Specification Feature	Header elements: /SOAP:Header/eb:Signature
Specification Reference	ebMS 2, section 4.1.4.2
Profiling (a)	Is a digitally signed Acknowledgment message required? **Yes**
Profiling (b)	If so, what is the Acknowledgment or Receipt schema? Standard ebXML ms delivery acknowledgement for ebXML ms delivery acknowledgement.
Alignment	Appears as BusinessTransactionCharacteristics/@isNonRepudiationReceiptRequired=persistent in CPA.
Notes	In addition it is recommended that messages are functionally acknowledged using receipt and acceptance acknowledgements/exceptions based on RNIF receipts. This is based on ebXML BPSS 1.05.

4.2.3 Profile Requirement Item: Non Persistent Authentication

Specification Feature	Header elements: /SOAP:Header/eb:Signature
Specification Reference	ebMS 2, section 4.1.4.3
Profiling	Are communication channel authentication methods required? [Yes, for Security Services Profiles 2-5.] **Yes** Which methods are allowed or required? **Client certificates**
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthenticated=transient in CPA.]
Notes	

4.2.4 Profile Requirement Item: Non Persistent Integrity

Specification Feature	Header elements: /SOAP:Header/eb:Signature
Specification Reference	ebMS 2, section 4.1.4.4.
Profiling	Are communication channel integrity methods required? **Not Applicable** Which methods are allowed or required? **Not Applicable**
Alignment	[Appears as BusinessTransactionCharacteristics/@isTamperproof=transient in CPA.]
Notes	

4.2.5 Profile Requirement Item: Persistent Confidentiality

Specification Feature	Header elements: /SOAP:Header/eb:Signature
Specification Reference	ebMS 2, section 4.1.4.5
Profiling (a)	Is selective confidentiality of elements within an ebXML Message SOAP Header required? If so, how is this to be accomplished? [Not addressed by Messaging Specification 2.0.] **No**
Profiling (b)	Is payload confidentiality (encryption) required? Which methods are allowed or required? **No. Payload encryption is not required.**
Alignment	(b) [Appears as BusinessTransactionCharacteristics/@isConfidential=persistent in CPA.]
Notes	It is recommended not to implement additional payload encryption for performance and interoperability reasons.

4.2.6 Profile Requirement Item: Non Persistent Confidentiality

Specification Feature	Header elements: /SOAP:Header/eb:Signature
Specification Reference	ebMS 2, section 4.1.4.6

Profiling	Are communication channel confidentiality methods required? [Yes, for Security Services Profiles 3, 6, 8, 11, 12.] **Yes** Which methods are allowed or required? **Https**
Alignment	[Appears as BusinessTransactionCharacteristics/@isConfidential=transient in CPA.]
Notes	**This relates to SSL which will provide confidentiality above the transport layer.**

4.2.7 Profile Requirement Item: Persistent Authorization

Specification Feature	Header elements: /SOAP:Header/eb:Signature
Specification Reference	ebMS 2, section 4.1.4.7
Profiling	Are persistent authorization methods required? Which methods are allowed or required? **No persistent authorization methods required.**
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthorizationRequired=persistent in CPA.]
Notes	

4.2.8 Profile Requirement Item: Non Persistent Authorization

Specification Feature	Header elements: /SOAP:Header/eb:Signature
Specification Reference	ebMS 2, section 4.1.4.8
Profiling	Are communication channel authorization methods required? **No** Which methods are allowed or required? **Not Applicable**
Alignment	[Appears as BusinessTransactionCharacteristics/@isAuthorizationRequired=transient in CPA.]
Notes	

4.2.9 Profile Requirement Item: Trusted Timestamp

Specification Feature	Header elements: /SOAP:Header/eb:Signature
Specification Reference	ebMS 2, section 4.1.4.9
Profiling	Is a trusted timestamp required? If so, provide details regarding its usage. **No**
Alignment	**Not Applicable**
Notes	

4.3 Module: Error Handling

4.3.1 Profile Requirement Item: Error

Specification Feature	Header elements: /SOAP:Header/eb:ErrorList/eb:Error /SOAP:Header/eb:ErrorList/ eb:Error/@codeContext /SOAP:Header/eb:ErrorList/ eb:Error/@errorCode
Specification Reference	ebMS 2, section 4.2.3.2.
Profiling (a)	Is an alternative codeContext used? If so, specify **No**
Profiling (b)	If an alternative codeContext is used, what is its errorCode list? **Not Applicable**
Profiling (c)	When errors should be reported to the sending application, how should this notification be performed (e.g. using a logging mechanism or a proactive callback)? **No recommendation.**
Alignment	**Not Applicable**
Notes	It is recommended ebXML messaging errors are logged. In addition application errors on messages sent can be notified back using receipt exceptions (which are also logged). The nature of such errors are such that anything that a partner requires immediate attention to requires a follow up phone call to the support desk.

4.4 Module : SyncReply

4.4.1 Profile Requirement Item: SyncReply

Specification Feature	Header elements: /SOAP:Header/eb:SyncReply/
Specification Reference	ebMS 2, section 4.3
Profiling (a)	Is SyncReply mode allowed, disallowed, or required, and under what circumstances? **Disallowed**
Profiling (b)	If SyncReply mode is used, are MSH signals, business messages or both expected synchronously? **Not Applicable**
Alignment	[Affects setting of 6.4.7 syncReplyMode element. Appears as MessagingCharacteristics/@syncReplyMode in CPA.]
Notes	SyncReply causes performance and interoperability issues and therefore is not often used.

4.5 Module: Reliable Messaging

4.5.1 Profile Requirement Item: SOAP Actor attribute

Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/
Specification Reference	ebMS 2, section 6.3.1.1
Profiling (a)	SOAP Actor attribute: Are point-to-point (nextMSH) MSH Acknowledgments to be requested? [Appears as MessagingCharacteristics/@ackRequested with @actor=nextMSH in CPA.] **Not Applicable. Point-to-Point MHS Acknowledgements not used**
Profiling (b)	Are end-to-end (toParty) MSH Acknowledgments to be requested? [Appears as MessagingCharacteristics/@ackRequested with @actor=toPartyMSH in CPA.] **Yes**
Notes	**The *AckRequested* element MUST be targeted at the *To Party MSH* (these are equivalent for single-hop routing).** **The default *actor* targets the *To Party MSH.***

4.5.2 Profile Requirement Item: Signed attribute

Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/

Specification Reference	ebMS 2, section 6.3.1.2
Profiling	Must MSH Acknowledgments be (requested to be) signed? **Yes**
Alignment	[Appears as MessagingCharacteristics/@ackSignatureRequested in CPA.]
Notes	

4.5.3 Profile Requirement Item: DuplicateElimination

Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/
Specification Reference	ebMS 2, section 6.4.1
Profiling (a)	Is elimination of duplicate messages required? **Yes**
Profiling (b)	What is the expected scope in time of duplicate elimination? In other words, how long should messages or message Ids be kept in persistent storage for this purpose? **1 day**
Alignment	Appears as MessagingCharacteristics/@duplicateElimination in CPA
Notes	**The *DuplicateElimination* element MUST be used by the *From Party MSH* to indicate whether the *Receiving MSH* MUST eliminate duplicates If the value of *duplicateElimination* in the CPA is *never*, *DuplicateElimination* MUST NOT be present.** **If *DuplicateElimination* is present – The *To Party MSH* must persist messages in a persistent store so duplicate messages will be presented to the *To Party* Application At-Most-Once** **If *DuplicateElimination* is not present – The *To Party MSH* is not required to maintain the message in persistent store and is not required to check for duplicates.**

4.5.4 Profile Requirement Item: Retries and RetryInterval

Specification Feature	Header elements: /SOAP:Header/eb:AckRequested/
Specification Reference	ebMS 2, section 6.4.3, 6.4.4

Profiling (a)	If reliable messaging is used, how many times must an MSH attempt to redeliver an unacknowledged message? **3**
Profiling (b)	What is the minimum time a Sending MSH should wait between retries of an unacknowledged message? **5 minutes**
Alignment	(a) [Appears as ReliableMessaging/Retries in CPA.] (b) [Appears as ReliableMessaging/RetryInterval in CPA.]
Notes	These parameters are configurable in CPA but the values above are recommended. The *Retries* parameter, from a CPA, is an integer value specifying the maximum number of times a *Sending MSH* SHOULD attempt to redeliver an unacknowledged *message* using the same communication protocol. It is not advisable to shorten the retry interval as most issues causing a retry need time to resolve themselves. Extending the number of retries and or the interval can sometimes be of benefit. However in large volume applications an issue arises as to the volume of retry traffic overwhelming an MSH.

4.5.5 Profile Requirement Item: PersistDuration

Specification Feature	Header elements:
Specification Reference	ebMS 2, section 6.4.6
Profiling	How long must data from a reliably sent message be kept in persistent storage by a receiving MSH, for the purpose of retransmission? **1 day**
Alignment	[Appears as ReliableMessaging/PersistDuration in CPA.]
Notes	**The *PersistDuration* parameter, from a CPA, is the minimum length of time, expressed as a, data from a reliably sent *Message*, is kept in *Persistent Storage* by a *Receiving MSH*.** **This needs to be consistent with the requirements for duplicate elimination and the likely duration of any retries employed.**

4.5.6 Profile Requirement Item: Reliability Protocol

Specification Feature	Header elements:
Specification Reference	ebMS 2, section 6.5.3, 6.5.7

Profiling (a)	Must a response to a received message be included with the acknowledgment of the received message, are they to be separate, or are both forms allowed? **No. They are to be separate.**
Profiling (b)	If a DeliveryFailure error message cannot be delivered successfully, how must the error message's destination party be informed of the problem? **No recommendation**
Alignment	**Not Applicable**
Notes	Partners will need to agree these.

4.6 Module: Message Status

4.6.1 Profile Requirement Item: Status Request message

Specification Feature	Header elements: Eb:MessageHeader/eb:StatusRequest
Specification Reference	ebMS 2, section 7.1.1
Profiling (a)	If used, must Message Status Request Messages be digitally signed? **Yes**
Profiling (b)	Must unauthorized Message Status Request messages be ignored, rather than responded to, due to security concerns? **Yes**
Alignment	**Not Applicable**
Notes	**It is recommended gateways support the Message Status service.**

4.6.2 Profile Requirement Item: Status Response message

Specification Feature	Header elements: Eb:MessageHeader/eb:StatusResponse
Specification Reference	ebMS 2, section 7.1.2
Profiling	If used, must Message Status Response Messages be digitally signed? **Yes**

Alignment	
Notes	**It is recommended gateways support the Message Status service.**

4.7 Module : Ping Service

4.7.1 Profile Requirement Item: Ping-Pong Security

Specification Feature	Header elements: Eb:MessageHeader/eb:Service Eb:MessageHeader/eb:Action
Specification Reference	ebMS 2, section 8.1, 8.2
Profiling (a)	If used, must Ping Messages be digitally signed? **Yes**
Profiling (b)	If used, must Pong Messages be digitally signed? **Yes**
Profiling (c)	Under what circumstances must a Pong Message not be sent? **A Pong should not be sent if Ping/Pong is not configured in the CPA or there is some other CPA violation like unknown sending party, security violation, etc.**
Profiling (d)	If not supported or unauthorized, must the MSH receiving a Ping respond with an error message, or ignore it due to security concerns? **Not Applicable**
Alignment	**Not Applicable**
Notes	

4.8 Module : Multi-Hop

4.8.1 Profile Requirement Item: Use of intermediaries

Specification Feature	Header elements:
Specification Reference	ebMS 2, section 10
Profiling (a)	Are any store-and-forward intermediary MSH nodes present in the message path? **Not Applicable**

Profiling (b)	What are the values of Retry and RetryInterval between intermediate MSH nodes? **Not Applicable**
Alignment	
Notes	It is recommended gateways do not support Multi-Hop

4.8.2 Profile Requirement Item: Acknowledgements

Specification Feature	Header elements: Eb:MessageHeader/
Specification Reference	ebMS 2, section 10.1.1, 10.1.3
Profiling (a)	Must each intermediary request acknowledgment from the next MSH? **Not Applicable**
Profiling (b)	Must each intermediary return an Intermediate Acknowledgment Message synchronously? **Not Applicable**
Profiling (c)	If both intermediary (multi-hop) and endpoint acknowledgments are requested of the To Party, must they both be sent in the same message? **Not Applicable**
Alignment	**Not Applicable**
Notes	It is recommended gateways do not support Multi-Hop

4.9 SOAP Extensions

4.9.1 Profile Requirement Item: #wildCard, Id

Specification Feature	Header elements:
Specification Reference	ebMS 2, section 2.3.6, 2.3.7, 2.3.8
Profiling	**(Section 2.3.6)** #wildcard Element Content: Are additional namespace-qualified extension elements required? If so, specify. **No. Additional namespace-qualified extension elements are not required** **(Section 2.3.7)** Is a unique “id” attribute required for each (or any) ebXML SOAP extension elements, for the purpose of referencing it alone in a digital signature?

	No **(Section 2.3.8)** Is a version other than "2.0" allowed or required for any extension elements? **No**
Alignment	**Not Applicable**
Notes	

4.10 MIME Header Container

4.10.1 Profile Requirement Item: charset

Specification Feature	MIME Header elements: Content-Type
Specification Reference	ebMS 2, section 2.1.3.2
Profiling	Is the "charset" parameter of Content-Type header necessary? If so, what is the (sub)set of allowed values? Example: Content-Type: text/xml; charset="UTF-8" **Not necessary**
Alignment	**Not Applicable**
Notes	

4.11 HTTP Binding

4.11.1 Profile Requirement Item: HTTP Headers

Specification Feature	Header elements, MIME parts
Specification Reference	ebMS 2, Appendix B.2.2.
Profiling (a)	Is a (non-identity) content-transfer-encoding required for any of the MIME multipart entities? **Yes**
Profiling (b)	If other than "ebXML" what must the SOAPAction HTTP header field contain? **Not Applicable as only ebXML is supported.**
Profiling (c)	What additional MIME-like headers must be included among the HTTP headers? **No additional MIME headers required other than**

	• **Content-Type** • **Transfer-Encoding**
Alignment	**Not Applicable**
Notes	

4.11.2 Profile Requirement Item: HTTP Response Codes

Specification Feature	Header elements, MIME parts
Specification Reference	ebMS 2, Appendix B.2.3.
Profiling	What client behaviours should result when 3xx, 4xx or 5xx HTTP error codes are received? No recommendation.
Alignment	**Not Applicable**
Notes	An example implementation is as follows: When Openreach is the sender, 3xx, 4xx, and 5xx error codes will result in the outbound message being marked in its gateway as rejected. One exception is error code 503 which will result in the Openreach http level Retry Handler kicking in. When Openreach is the receiver 3xx, 4xx and 5xx error codes should result in the sender terminating the POST. 503 returns from Openreach indicate that the gateway is busy. The sender may choose to retry the POST after a reasonable wait time. Suggestion would be to wait at minimum 30 seconds after a 503.

4.11.3 Profile Requirement Item: HTTP Access Control

Specification Feature	Header elements, MIME parts
Specification Reference	ebMS 2, Appendix B.2.6.
Profiling	Which HTTP access control mechanism(s) are required or allowed? [Basic, Digest, or client certificate (the latter only if transport-layer security is used), for example. Refer to item 4.1.4.8 in Security section. **Client certificate**
Alignment	Appears as AccessAuthentication elements in CPA
Notes	

4.11.4 Profile Requirement Item: HTTP Confidentiality and Security

Specification Feature	Header elements, MIME parts
Specification Reference	ebMS 2, Appendix B.2.7.
Profiling (a)	Is HTTP transport-layer encryption required? What protocol version(s)? **SSL v3 and TLS v1**
Profiling (b)	What encryption algorithm(s) and minimum key lengths are required? **No recommendation**
Profiling (c)	What Certificate Authorities are acceptable for server certificate authentication? **The suggestion is the channel master for the community (the partner with whom all other partners trade) be the certificate authority.**
Profiling (d)	Are direct-trust (self-signed) server certificates allowed? **No**
Profiling (e)	Is client-side certificate-based authentication allowed or required? **Client side authentication is not required for a particular trading partner, it only occurs when configuring a gateway client certificate for mutual authentication.** **Client side authentication takes place between servers. Mutual authentication should be setup for this.**
Profiling (f)	What client Certificate Authorities are acceptable? **For example, BT Openreach which will generate a private Certificate Authority and only certificates issued by that CA will be acceptable**
Alignment	**Not Applicable**
Notes	It is recommended that CPs sign messages using SHA1 hashing algorithm with 1024 bit key length. It is recommended not to support MD5 algorithms. CPs should act as certificate authorities for their communities.

4.12 SMTP Binding

4.12.1 Profile Requirement Item: MIME Headers

Specification Feature	Header elements, MIME parts
Specification Reference	ebMS 2, Appendix B.3.2.
Profiling (a)	Is any specific content-transfer-encoding required, for MIME body parts that must conform to a 7-bit data path? [Base64 or quoted-printable, for example.] **Not Applicable**
Profiling (b)	If other than "ebXML" what must the SOAPAction SMTP header field contain? **Not Applicable**
Profiling (c)	What additional MIME headers must be included among the SMTP headers? **Not Applicable**
Alignment	**Not Applicable**
Notes	**It is recommended that gateways do not support SMTP.**

4.12.2 Profile Requirement Item: SMTP Confidentiality and Security

Specification Feature	Header elements, MIME parts
Specification Reference	ebMS 2, Appendix B.3.4, B.3.5
Profiling (a)	What SMTP access control mechanisms are required? [Refer to item 4.1.4.8 in Security section.] **Not Applicable**
Profiling (b)	Is transport-layer security required for SMTP, and what are the specifics of its use? [Refer to item 4.1.4.6 in Security section.] **Not Applicable**
Alignment	**Not Applicable**
Notes	**It is recommended that gateways do not support SMTP.**

5. Operational Profile

This section defines the operational aspect of the profile: type of deployment that the above profile is supposed to be operated with, expected or required conditions of operations, usage context, etc.

5.1 Deployment and Processing requirements for CPAs

CPA Access	Profile requirements
Is a specific registry for storing CPAs required? If so, provide details.	**Not required.**
Is there a set of predefined CPA templates that can be used to create given Parties' CPAs?	**Where CPAs are used the channel master should produce and issue templates.**
Is there a particular format for file names of CPAs, in case that file name is different from CPAId value?	**File name should be the same as the value of CPAId.**
Others	

5.2 Security Profile

Security Profile	Profile requirements
Which security profile(s) are used, and under what circumstances (for which Business Processes)? [Refer to Appendix C of Message Service Specification. May be partially captured by BPSS isConfidential, isTamperproof, isAuthenticated definitions.]	**It is recommended to adopt persistent security at the application level, including:** • **Persistent digital signature** • **Persistent signed receipt** **[This corresponds to Security Profile 7. Refer "Supported Security Services" in ebMS 2.0 specification]**
(section 4.1.5) Are any recommendations given, with respect to protection or proper handling of MIME headers within an ebXML Message?	**SSL encrypts the application data which includes the SOAP message.**
Are any specific third-party security packages approved or required?	**No**
What security and management policies and practices are recommended?	**BS7799**
Any particular procedure for doing HTTP authentication, e.g. if exchanging name and password, how?	**Authentication is done using digital signatures**
Others	

5.3 Reliability Profile

Reliability Profile	Profile requirements

If reliable messaging is required, by which method(s) may it be implemented? [The ebXML Reliable Messaging protocol, or an alternative reliable messaging or transfer protocol.]	**Reliable messaging is required and it must be implemented in ebXML Reliable Messaging protocol**
Which Reliable Messaging feature combinations are required? [Refer to Section 6.6 of Message Service Specification.]	**DuplicateElimination + AckRequestedToPartyMSH (Once-And-Only-Once Reliable Message at the End-To-End level only based upon end-to-end retransmission)**
Others	

5.4 Error Handling Profile

Error Reporting	Profile requirements
(Section 4.2.4.2) Should errors be reported to a URI that is different from that identified within the From element? What are the requirements for the error reporting URI and the policy for defining it?	**No**
What is the policy for error reporting? In case an error message cannot be delivered, what other means are used to notify the party, if any?	**This should be defined as part of operational procedures for the community.**
(Appendix B.4) What communication protocol-level error recovery is required, before deferring to Reliable Messaging recovery? [For example, how many retries should occur in the case of failures in DNS, TCP connection, server errors, timeouts; and at what interval?]	**HTTP retries should be implemented. The number of retries would be decided by the trading partner.**
Others	

5.5 Message Payload and Flow Profile

Message Quantitative Aspects	Profile requirements
What are typical and maximum message payload sizes that must be handled? (maximum, average)	**The typical average message size is around 3 KB. But, this is a calculated payload size and nothing that system restricts.** **Also note that no compression techniques should be used for the message payloads.**
(Section 2.1.4) How many Payload Containers must be present?	**Only one.**
What is the structure and content of each container? [List MIME Content-Types and other process-specific requirements.] Are there restrictions on the MIME types allowed for attachments?	*Content-ID: _Part_0_23833428.1134129301506* *Content-Type: application/xml* *Content-Transfer-Encoding: binary* *<AddOrder>* *<OrderLines>*

	----- *</OrderLines>* *</AddOrder>*
How is each container distinguished from the others? [By a fixed ordering of containers, a fixed Manifest ordering, or specific Content-ID values.]. Any expected relative order of attachments of various types?	**Not applicable as there would be only one payload container.**
Others	

5.6 Additional Messaging Features beyond ebMS Specification

Additional Features	Profile requirements
Are there additional features out of specification scope that are part of this messaging profile, as an extension to the ebMS profiling?	**No**

5.7 Additional Deployment or Operational Requirements

Operational or Deployment Conditions	Profile requirements
Operational or deployment aspects that are object to further requirements or recommendations.	**Trading partner should supply single IP address that other partners use to receive requests from and a single address to send requests to.**

References

Ref No	Title	Version	Author	Date
01	OASIS ebXML ms2.0 deployment profile template 1.0 http://www.oasis-open.org/committees/download.php/1713/ebMS_Deployment_Guide_Template_10.doc	Version 1.0		March 2003
02	OASIS ebXML Message Service Specification (ebMS)	Version2.0		01/04/2002

- End -