Deployment Guide Template
Version 1.0
for ebXML Message Service 2.0

OASIS ebXML Implementation, Interoperability and Conformance Technical Committee

24 February, 2003

Change Log

Version	Date	Description
0.1	26 June, 2002	Initial draft by P. Wenzel.
0.2	16 September, 2002	Reformatted document, published with notes by J. Durand.
0.3	3 October, 2002	Rearranged into user-targeted sections, incorporated comments by J. Durand, M. Martin, E. van LydeGraf.
1.0	27 January, 2003	Additional text, cleanup and CPA references by P. Wenzel; non-normative EAN•UCC examples by T.Bikeev; comments by J. Durand.
1.0	24 February, 2003	Incorporated comments by J. Durand.

Unresolved Issues/Comments

J. Durand: We should add the level of requirement in the spec for each of these optional features: "OPTIONAL", "RECOMMENDED", "STRONGLY RECOMMENDED").

Introduction

The ebXML Message Service Specification 2.0 (ebMS), found at <http://www.oasis-open.org/committees/ebxml-msg/documents/ebMS_v2_0rev_c.pdf>, contains a plethora of configurable features and options. Any use of ebMS requires a certain amount of standardization within a trading community, and due to the degree of optionality allowed by the specification, these communities must also document exactly which parts of it must be deployed and how, in order to foster interoperability on multiple levels between participants. Such information may be collected and published as a Deployment Guide for a community. It also represents an agreed-upon convention for the use of the ebXML message handler within the community, the capabilities that are expected from an implementation, and the deployment details. This is not to be confused with the notion of Collaboration Protocol Agreement (CPA), which focuses on the runtime collaboration mode between partners, for a particular business process. Some elements of the Deployment Template will, however, map to a community's specific requirements of applicable CPA elements.

This Template document, upon being fully populated with specific requirements, thus becomes a Deployment Guide Instance Document. It is the intention of the OASIS ebXML IIC Technical Committee to collect and archive examples of Deployment Guides created from this Template, as an aid to user communities whose standardization efforts involve the ebXML Message Service. By publishing Deployment Guides for different communities using the same Template format, it will be easier for a user community to consult the configuration setups, as well as conventions used by other user communities with which they may want to interoperate. This will help them to assess whether these two communities will be able to interoperate, or under what conditions.

How to Use the Template

The Template is divided into two user-targeted sections—Business-Level Requirements and Technical-Level Requirements—which correspond roughly to the Business Operational View and Functional Service View, respectively, as described by the ebXML Technical Architecture Specification <http://www.ebxml.org/specs/ebTA.pdf>

The numbering and titles of the items is intended to match the section numbering and titles of the corresponding requirements or options in the Messaging specification document. This makes it easier to cross-reference these requirements to the original specification, for further details on the use and implications of the choices that can be made.

In many cases, the Technical-Level Requirements are a direct consequence of choices made in the Business-Level Requirements section. Where items appear to be duplicated between the two sections, the Technical-Level items are meant to provide more explicit details necessary for implementation of the business requirements, such as precise data formatting specifications.

Two classes of users would be expected to collaborate in the completion of this Template to produce a Deployment Guide:

1. Business Process Designers would detail the business-process specific requirements of the Message Service.
2. Standards Community Technical Architects would make the technical decisions necessary to implement the business processes most effectively.

Consumers of a Deployment Guide include:

1. Business process implementers (IT departments), to deploy a Message Service solution according to the requirements of specific trading communities.
2. Software solution vendors, to identify all areas in which business process specification bodies require software flexibility, and what specific configurations are necessary to support such standards.

Examples shown in the "Value" column are non-normative, having been provided by EAN•UCC based upon that organization's experience using this template, and should be replaced with text appropriate to the Deployment Guide developer's organization.

When populating the Template, it is possible that a deployment requirement can have more than one answer. For example, when a requirement maps to a CPA element, users may want to specify several authorized values, as this community may want to allow more than one choice, to be further described by specific CPAs. In that case, and if CPAs are already defined, it is recommended to annotate each value with the CPA identification it will relate to. By doing so, the resulting Deployment Guide will give an overview of all the possible uses for a particular MSH feature (e.g. Security). This will help to quickly assess the deployment requirements for this particular feature. An alternative would be to provide pointers to existing CPAs, which the Template also allows. However, these CPAs may change in time (updates, additions). It is the role of the Deployment Guide to precisely show what capabilities are expected from a deployed implementation within a community. CPA designers will use it as a reference, so that new CPAs remain within these capabilities.

For items that are not relevant to the community, "Not Applicable" should be specified. Likewise, "No Recommendation Given" will indicate that there is no modification or preference for an item notated as such. The Deployment Guide developer may also choose to note "Recommendation Pending" for items that are likely to be specified in future versions of the Guide.

Business-Level Requirements

[The items in this section are intended to be answered by a business process designer, and are either specific to the use cases and Business Processes being deployed, or are a matter of general policy.]

3.1.1.1 PartyId Element

Specification	Value
Is a specific standard used for party identification? Provide details.	Example - EAN•UCC Global Location Number. Ref.: ISO6523 - ICD0088.

3.1.2 CPA Access

Specification	Value
Is a specific registry for storing CPAs required? If so, provide details.	
Is there a set of predefined CPA templates that can be used to create given Parties' CPAs?	

3.1.4 Service Element

Specification	Value
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.]	

3.1.5 Action Element

Specification	Value
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 Action values in BPSS definitions.]	Example – within EAN•UCC system approved values are specified by [EAN•UCC MS Impl.-G]. `<eb:Action>Confirmation</eb:Action>`

3.1.1.2 Role Element

Specification	Value
Are Roles defined for each party of each business process? List them, or provide a reference to the source of these values. [Per-process; may reference Role values in BPSS definitions. Appears as Role element of CPA.]	Example – within EAN•UCC system approved values are specified by [EAN•UCC MS Implementation Guide]. `<eb:Role>http:/www.ean-ucc.org/roles/seller</eb:Role>`

Appendix C: Supported Security Services

Specification	Value
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.]	Example - within EAN•UCC it is recommended to adopt persistent security at the application level, including: • Persistent digital signature • Persistent signed receipt • Persistent confidentiality • Persistent authorization [This corresponds to Security Profile 21.]
Are any specific third-party security packages approved or required?	

4.1.2 Security and Management

Specification	Value
What security and management policies and practices are recommended?	

6.6 Reliable Messaging Combinations

Specification	Value
Which Reliable Messaging feature combinations are required? [Refer to Section 6.6 of Message Service Specification.]	

Technical-Level Requirements

This section requires an in-depth knowledge of the ebXML Message Service and all its constituent standards and technologies, and their application to the specific use cases and Business Processes of the user community being addressed.

2 ebXML with SOAP

2.1 Packaging Specification

2.1.1 SOAP Structural Conformance

2.1.2 Message Package

Specification	Value
Is a Content-ID MIME header necessary? If so, how is it to be constructed?	
Is the start parameter of the Content-Type header necessary?	

2.1.3 Header Container

2.1.3.1 Content-Type

Specification	Value
Is a Content-ID MIME header necessary? If so, how is it to be constructed?	

2.1.3.2 charset attribute

Specification	Value
Is the "charset" parameter of Content-Type header necessary? If so, what is the (sub)set of allowed values?	

2.1.4 Payload Container

Specification	Value
How many Payload Containers must be present? What is the structure and content of the container? [List MIME types and other process-specific requirements.]	

2.1.5 Additional MIME Parameters

Specification	Value
Are any additional MIME parameters needed?	

2.2 XML Prolog

2.2.1 XML Declaration

Specification	Value
Is an XML declaration required in the SOAP Message?	
What XML version(s) are allowed?	

2.2.2 Encoding Declaration

Specification	Value
Is the encoding declaration of the SOAP Message necessary? [If so, allowed values must be the same as for MIME Content-Type "charset" parameter.]	

2.3 ebXML SOAP Envelope extensions

2.3.6 #wildcard Element Content

Specification	Value
Are additional namespace-qualified extension elements required? If so, specify.	

2.3.7 id attribute

Specification	Value
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?	

2.3.8 version attribute

Specification	Value
Is a version other than "2.0" allowed or required for any extension elements?	

3 Core Extension Elements

3.1 MessageHeader Element

3.1.1 From and To Elements

3.1.1.1 PartyId Element

Specification	Value
Should multiple PartyId elements be present in From and To elements? [See section 3.1.1.1 of Business-Level Requirements. Appears as PartyId element in CPA.]	
Is the type attribute needed for each PartyId, and if so, what must it contain? [Appears as PartyId/@type in CPA.]	`<eb:PartyId eb:type="http:/www.iso.int/schemas/eanucc/gln">1234567890128</eb:PartyId>`

3.1.2 CPAId Element

Specification	Value

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? See section 3.1.2 of Business-Level Requirements for repository information. Appears as CollaborationProtocolAgreement/@cpaid in CPA.]	Example – within EAN•UCC system the value of the CPAId is the concatenation of the Sender and Receiver GLNs followed by a four digit serial number.
	`1234567890128 - GLN Party A`
	`3456789012340 - GLN Party B`
	`0001 - CPA Number between parties A and B`

3.1.3 ConversationId Element

Specification	Value
Is a specific conversation identification scheme recommended?	

3.1.4 Service Element

Specification	Value
Is there a defined "type" for Service elements? If so, what value must the type attribute contain? [Appears as Service/@type in CPA.]	
If not provided in Business-Level Requirements above, what is the set of possible values for the Service element? Is there a URI format scheme for this element? [Appears as Service element in CPA.]	

3.1.6 MessageData Element
3.1.6.2 Timestamp Element

Specification	Value
Must Timestamp include the 'Z' (UTC) identifier? [Also for Timestamp elements described in ebMS sections 6.3.2.2, 6.4.5, 7.3.2.]	

3.1.8 Description Element

Specification	Value
Are one or more Message Header Description elements required? In what language(s)? Is there a convention for its contents?	

3.2 Manifest Element
3.2.2 Manifest Validation

Specification	Value
How many Manifest elements must be present, and what must they reference?	
Must a URI that cannot be resolved be reported as an error?	

3.2.1 Reference Element

Specification	Value
Is the xlink:role attribute required? What is its value?	
Are any other namespace-qualified attributes required?	

3.2.1.1 Schema Element

Specification	Value
Are any Schema elements required? If so, what are their location and version attributes?	

3.2.1.2 Description Element

Specification	Value
Are any Description elements required? If so, what are their contents?	

4.1 Security Module

4.1.5 Security Considerations

Specification	Value
Are any recommendations given, with respect to protection or proper handling of MIME headers within an ebXML Message?	

4.1.4.1 Persistent Digital Signature

Specification	Value
Must messages be digitally signed? [Yes, for Security Services Profiles 1, 6-21. Appears as BusinessTransactionCharacteristics/@isAuthenticated=persistent and BusinessTransactionCharacteristics @isTamperProof=persistent in CPA]	

4.1.1 Signature Element

Specification	Value
Are additional Signature elements required, by whom, and what should they reference?	

4.1.3 Signature Generation

Specification	Value
What canonicalization method(s) must be applied to the data to be signed? [Recommended method is "http://www.w3.org/TR/2001/REC-xml-c14n-20010315".]	
What canonicalization method(s) must be applied to each payload object, if different from above?	
What signature method(s) must be applied?	
What Certificate Authorities (issuers) are allowed or required for signing certificates?	
Are direct-trusted (or self-signed) signing certificates allowed?	
What certificate verification policies and procedures must be followed?	

4.1.4.2 Persistent Signed Receipt

Specification	Value
Is a digitally signed Acknowledgment message required? [Yes, for Security Services Profiles 7, 8, 10, 12, 14, 15, 17, 19-21. See the items beginning with Section 4.1.4.1 for specific Signature requirements. Appears as BusinessTransactionCharacteristics/@isNonRepudiationReceiptRequired=persistent in CPA.]	
If so, what is the Acknowledgment or Receipt schema?	

4.1.4.3 Non-persistent Authentication

Specification	Value
Are communication channel authentication methods required? [Yes, for Security Services Profiles 2-5.] Which methods are allowed or required? [Appears as BusinessTransactionCharacteristics/@isAuthenticated=transient in CPA.]	

4.1.4.4 Non-persistent Integrity

Specification	Value
Are communication channel integrity methods required? [Yes, for Security Services Profile 4.] Which methods are allowed or required? [Appears as BusinessTransactionCharacteristics/@isTamperproof=transient in CPA.]	

4.1.4.5 Persistent Confidentiality

Specification	Value
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.]	
Is payload confidentiality (encryption) required? [Yes, for Security Services Profiles 13, 14, 16, 17, 21, 22.] Which methods are allowed or required? [Appears as BusinessTransactionCharacteristics/@isConfidential =persistent in CPA.]	

4.1.4.6 Non-persistent Confidentiality

Specification	Value
Are communication channel confidentiality methods required? [Yes, for Security Services Profiles 3, 6, 8, 11, 12.] Which methods are allowed or required? [Appears as BusinessTransactionCharacteristics/@isConfidential =transient in CPA.]	

4.1.4.7 Persistent Authorization

Specification	Value
Are persistent authorization methods required? [Yes, for Security Services Profiles 18-21.] Which methods are allowed or required? [Appears as BusinessTransactionCharacteristics/@isAuthorizatio nRequired=persistent in CPA.]	

4.1.4.8 Non-persistent Authorization

Specification	Value
Are communication channel authorization methods required? [Yes, for Security Services Profile 2.] Which methods are allowed or required? [Appears as BusinessTransactionCharacteristics/@isAuthorizatio nRequired=transient in CPA.]	

4.1.4.9 Trusted Timestamp

Specification	Value
Is a trusted timestamp required? [Yes, for Security Services Profiles 9-12, 15-17, 20, 21.] If so, provide details regarding its usage.	

4.2 Error Handling Module

4.2.3 ErrorList Element

4.2.3.2 Error Element

4.2.3.2.2 codeContext attribute

Specification	Value
Is an alternative codeContext used? If so, specify.	

4.2.3.2.3 errorCode attribute

Specification	Value
If an alternative codeContext is used, what is its errorCode list?	
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)?	

4.2.4 Implementing Error Reporting and Handling

4.2.4.1 When to Generate Error Messages

4.2.4.1.1 Security Considerations

Specification	Value
Under what conditions should errors NOT be reported to the sending MSH, for security reasons?	

4.2.4.2 Identifying the Error Reporting Location

Specification	Value
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?	
What is the policy for error reporting?	

4.3 SyncReply Module

Specification	Value
Is SyncReply mode allowed, disallowed, or required, and under what circumstances? [May be process-specific.]	
If SyncReply mode is used, are MSH signals, business messages or both expected synchronously? [Affects setting of 6.4.7 syncReplyMode element. Appears as MessagingCharacteristics/@syncReplyMode in CPA.]	

6 Reliable Messaging Module

6.2 Methods of Implementing Reliable Messaging

Specification	Value
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.]	

6.3 Reliable Messaging SOAP Header Extensions

6.3.1 AckRequested Element

6.3.1.1 SOAP actor attribute

Specification	Value
Are point-to-point (nextMSH) MSH Acknowledgments to be requested? [Yes, for RM Combinations 1, 3, 5, 7; refer to ebMS section 6.6. Appears as MessagingCharacteristics/@ackRequested with @actor=nextMSH in CPA.]	
Are end-to-end (toParty) MSH Acknowledgments to be requested? [Yes, for RM Combinations 1, 2, 5, 6. Appears as MessagingCharacteristics/@ackRequested with @actor=toPartyMSH in CPA.]	

6.3.1.2 signed attribute

Specification	Value
Must MSH Acknowledgments be (requested to be) signed? [Appears as MessagingCharacteristics/@ackSignatureRequested in CPA.]	

6.4 Reliable Messaging Parameters

6.4.1 DuplicateElimination

Specification	Value
Is elimination of duplicate messages required? [Yes, for RM Combinations 1-4. Appears as MessagingCharacteristics/@duplicateElimination in CPA.]	
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?	

6.4.3 Retries

Specification	Value
If reliable messaging is used, how many times must an MSH attempt to redeliver an unacknowledged message? [Appears as ReliableMessaging/Retries in CPA.]	

6.4.4 RetryInterval

Specification	Value
What is the minimum time a Sending MSH should wait between retries of an unacknowledged message? [Appears as ReliableMessaging/RetryInterval in CPA.]	

6.4.6 PersistDuration

Specification	Value
How long must data from a reliably sent message be kept in persistent storage by a receiving MSH, for the purpose of retransmission? [Appears as ReliableMessaging/PersistDuration in CPA.]	

6.5 ebXML Reliable Messaging Protocol

6.5.3 Generating an Acknowledgment Message

Specification	Value
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?	

6.5.7 Failed Message Delivery

Specification	Value
If a DeliveryFailure error message cannot be delivered successfully, how must the error message's destination party be informed of the problem?	

7 Message Status Service

Specification	Value
Is the Message Status Service required for reliable and/or best-effort messaging?	

7.1 Message Status Messages

7.1.1 Message Status Request Message

Specification	Value
If used, must Message Status Request Messages be digitally signed?	

7.1.2 Message Status Response Message

Specification	Value
If used, must Message Status Response Messages be digitally signed?	

7.1.3 Security Considerations

Specification	Value
Must unauthorized Message Status Request messages be ignored, rather than responded to, due to security concerns?	

8 Message Service Handler Ping Service

Specification	Value
Is the Ping Service required?	

8.1 Message Service Handler Ping Message

Specification	Value
If used, must Ping Messages be digitally signed?	

8.2 Message Service Handler Pong Message

Specification	Value
If used, must Pong Messages be digitally signed?	
Under what circumstances must a Pong Message not be sent?	

8.3 Security Considerations

Specification	Value
If not supported or unauthorized, must the MSH receiving a Ping respond with an error message, or ignore it due to security concerns?	

9 MessageOrder Module

Specification	Value
Is message ordering (within a Conversation) required? [If so, a once-and-only-once Reliable Messaging scheme must also be selected.]	

10 Multi-Hop Module

Specification	Value
Are any store-and-forward intermediary MSH nodes present in the message path?	

10.1 Multi-hop Reliable Messaging

Specification	Value
What are the values of Retry and RetryInterval between intermediate MSH nodes?	

10.1.1 AckRequested Sample

Specification	Value
Must each intermediary request acknowledgment from the next MSH?	
Must each intermediary return an Intermediate Acknowledgment Message synchronously?	

10.1.3 Multi-Hop Acknowledgments

Specification	Value
If both intermediary (multi-hop) and endpoint acknowledgments are requested of the To Party, must they both be sent in the same message?	

Appendix B Communications Protocol Bindings

B.1 Introduction

Specification	Value
Is HTTP a required or allowed transfer protocol? (See section B.2 for specifics of this protocol.)	
Is HTTPS a required or allowed transfer protocol? (See section B.2 for specifics of this protocol.)	
Is (E)SMTP a required or allowed transfer protocol? (See section B.3 for specifics of this protocol.)	
Are any transfer protocols other than HTTP and SMTP allowed or required? If so, describe the protocol binding to be used.	

B.2 HTTP

B.2.2 Sending ebXML Service messages over HTTP

Specification	Value
Is a (non-identity) content-transfer-encoding required for any of the MIME multipart entities?	
If other than "ebXML" what must the SOAPAction HTTP header field contain?	
What additional MIME-like headers must be included among the HTTP headers?	

B.2.3 HTTP Response Codes

Specification	Value
What client behaviors should result when 3xx, 4xx or 5xx HTTP error codes are received?	

B.2.6 Access Control

Specification	Value
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. Appears as AccessAuthentication elements in CPA.]	

B.2.7 Confidentiality and Transport Protocol Level Security

Specification	Value
Is HTTP transport-layer encryption required? What protocol version(s)? [SSLv3, TLSv1, for example. Refer to item 4.1.4.6 in Security section.]	
What encryption algorithm(s) and minimum key lengths are required?	
What Certificate Authorities are acceptable for server certificate authentication?	
Are direct-trust (self-signed) server certificates allowed?	
Is client-side certificate-based authentication allowed or required?	
What client Certificate Authorities are acceptable?	
What certificate verification policies and procedures must be followed?	

B.3 SMTP

B.3.1 Minimum Level of Supported Protocols

Specification	Value
What is needed in addition to the ebMS minimum requirements for SMTP?	

B.3.2 Sending ebXML Messages over SMTP

Specification	Value
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.]	
If other than "ebXML" what must the SOAPAction SMTP header field contain?	
What additional MIME headers must be included among the SMTP headers?	

B.3.4 Access Control

Specification	Value
What SMTP access control mechanisms are required? [Refer to item 4.1.4.8 in Security section.]	

B.3.5 Confidentiality and Transport Protocol Level Security

Specification	Value
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.]	

B.4 Communication Errors during Reliable Messaging

Specification	Value
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?]	

Other Infrastructure Guidelines

The following infrastructure requirements fall outside the scope of the Messaging Specification, but may be important to specify in a Deployment Guide.

Specification	Value
What are typical and maximum message payload sizes that must be handled?	
What are typical communication bandwidth and processing capabilities of an MSH for these Services?	