ebXML Quality Review Group

Summary of Review of

ebXML Technical Architecture Risk Assessment v0.3.5

Release Date: **23rd March 2001**

Report prepared: 14th April 2001
Reviewers: Tim McGrath, Nagwa Abdelghfour, Jon Bosak, Stuart Campbell, Murray Maloney, Bob Glushko, Jim Werner, Ben Van De Walle

The Quality Review team reviewed the document "ebXML Technical Architecture Risk Assessment v0.3.5" as submitted by the Security team on March 23rd.

Firstly, we have no real concerns with the quality of this document. Under other circumstances this would be readily approved for public review.

However, at this stage we recommend some modifications be made prior to public review of this document.

Our concerns lie with the potential public reaction to some of this material (ie. the "spin" it gives to security risks).

As is clearly stated, this material has a primary audience of those parties involved in developing the ebXML technical specifications. For this audience, it is completely appropriate to identify gaps in the current ebXML specifications (eg line 311,325-327, 465-466, 611-617, etc.).

Unfortunately, this document has a wider audience in that it includes those parties implementing ebXML solutions (and also the analysts and consultants supporting any implementations). In its current style, this material paints a fairly bleak picture of the deficiencies in ebXML security mechanisms. This may create some unjustified impressions and unwarranted feedback that may distract from the primary function of this material.

We acknowledge that this is a matter of perspective. This document is, in one sense, a quality review of the security aspects across the ebXML specifications. It looks for (and finds) the holes in the work to date, and identifies future requirements.

We would like the Security team to create an 'executive overview' section at the start of the document to:

1. Describe the real security risks with any B2B application.

2. Point out the perspective taken by the team (ie looking for weaknesses not strengths).
3. The role of this material as a review of current specifications.
4. "Sell" the document to non-security experts.

At the same time as this matter is addressed we would like the Security team to consider some other (lesser) issues we have identified. These are:

Archiving (line 718-720)
The Quality Review team has asked the Requirements team to clarify this requirement, so it may no longer be an issue.

Registry and Repository Interface (line 788-789)
Is this out of scope for ebXML? ebXML does not dictate what information passes between a Registry and a Repository (if any).

Open Issues (line 692)
This section (13) may be more correctly entitled "Future Requirements".

Summary (line 782)
This section (14) may be more correctly entitled "Additional Requirements".

Alignment with other ebXML specifications
Line 278 – Shouldn't this read "The CPP *may be* stored in the ebXML *compliant* Registry and Repository"?
Line 166 – Is "Business Process Information Model" meant to be "Business Process and Information Model"?
Line 231 – Can the "Business Process Information Metamodel" also be in UML form?
Line 632-634 – Does this method support non-XML payloads?
Line 768-770 – Does this statement refer to any form of collaboration protocol agreement or a formal ebXML CPA (e.g. what about a verbal agreement)?

References
There are many documents referenced and not resolved in the Reference section. Examples of this appear throughout Figure 2 (line 217), and with references to "AS1" and "AS2" (line 744). This section should form part of the numbered sections and appear in the table of contents as per the ebXML template.

Editorial comments….

All ebXML submissions should be in PDF format to avoid problems with paper sizes and line number identification.
Footnote – "page of 2 of 2" (needs total number of pages)
Line 55 – Jenny needs an organisation.
Line 61-98 – remove redline editorial marks
Line 93-96 – Appendices should come after the Copyright statement

Line 130-133 – use the recommended abbreviations (see http://lists.ebxml.org/archives/ebxml-stc/200104/msg00001.html)
Line 140-146 – This paragraph is hard to follow and could be re-phrased. It should also try to avoid rhetorical statements without any supporting evidence.
Line 152-156 – This paragraph may be better after line 146
Line 164 – Figure 1 may be better before line 157 to keep it in context.
Line 246-248 – avoid referencing via attribute name only. These attributes should be described first.
Line 296 – Rather than reference the "BP" team this should state the specification involved.
Line 382, 478 – is "Trust Anchor" defined somewhere?
Line 447-448 – Is it feasible to illustrate what parts of these fragments are ebXML defined?
Line 538 – "Any" should not be in bold font.
Line 540 – There is missing text after "In " (may be "Appendix D"?).
Line 551 – Spelling of "currently".
Line 619-622 – This paragraph may be easier to follow if written as two sentences.
Line 658 – "vias" needs quote marks.
Line 659 – "actors" needs quote marks.
Line 678 – expand acronyms to full names and use specific document titles. (see http://lists.ebxml.org/archives/ebxml-stc/200104/msg00001.html).
Line
Line 703 – Figure 7 is hard to read in black and white print.
Line 707 – "xxx" spurious notation.
Line 847,970,1050 – These appendices need some introductory text.