Introduction

This document presents a collection of the most recent set of comments received from the QRT team regarding the ebXML Technical Architecture Risk Assessment document. These comments were made on base document version 3.5.

Reviewers

All comments listed in this document are attributed to their source by initials as indicated in the following list:

[QRT] Quality Review Team

Structural Comments

General

[QRT] 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.

Added new executive overview section as requested.

Specific

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.

Statement left until the requirement is restated.

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).

Since the title is changed to requirements and recommendations, this is left as a recommendation. This is a weak link. If left unaddressed it could cause security problems at the registry level.

Open Issues (line 692)

This section (13) may be more correctly entitled "Future Requirements".

Section changed.

Summary (line 782)

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

Section changed.

Alignment with other ebXML specifications

Line 278 – Shouldn't this read "The CPP *may be* stored in the ebXML *compliant* Registry and Repository"?

Change accepted.

Line 166 – Is "Business Process Information Model" meant to be "Business Process and Information Model"?

Change accepted.

Line 231 – Can the "Business Process Information Metamodel" also be in UML form?

Not for the purpose of this document. Text changed to indicate it must be changed from a UML form to an XML representation.

Line 632-634 – Does this method support non-XML payloads?

SOAP with attachments addresses non-XML payloads, and it is anticipated that the XML security specifications will align with all other W3C specs including SOAP with attachments

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)?

From a security perspective, an undocumented verbal agreement creates an opportunity for an agreement to be contested. It was the intent of the security team to identify this as a risk. If parties chose to work under verbal agreements, they must understand and accept this risk.

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.

TBD (partial completion)

Editorial comments….

All ebXML submissions should be in PDF format to avoid problems with paper sizes

and line number identification.

Change accepted.

Footnote – “page of 2 of 2” (needs total number of pages)

Line 55 – Jenny needs an organisation.

Name deleted (no response).

Line 61-98 – remove redline edit orial marks

Change accepted.

Line 93-96 – Appendices should come after the Copyright statement

Change accepted.

Line 130-133 – use the recommended abbreviations (see http://lists.ebxml.org/archives/ebxml-stc/200104/msg00001.html)

Changes accepted

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.

Changes accepted

Line 152-156 – This paragraph may be better after line 146

Changes accepted

Line 164 – Figure 1 may be better before line 157 to keep it in context.

Picture moved.

Line 246-248 – avoid referencing via attribute name only. These attributes should be described first.

Changes accepted

Line 296 – Rather than reference the “BP” team this should state the specification involved.

Changes accepted

Line 382, 478 – is “Trust Anchor” defined somewhere?

TBD

Line 447-448 – Is it feasible to illustrate what parts of these fragments are ebXML defined?

TBD

Line 538 – “Any” should not be in bold font.

Changes accepted

Line 540 – There is missing text after “In “ (may be “Appendix D”?).

New text supplied.

Line 551 – Spelling of “currently”.

Changes accepted

Line 619-622 – This paragraph may be easier to follow if written as two sentences.

TBD

Line 658 – “vias” needs quote marks.

Changes accepted

Line 659 – “actors” needs quote marks.

Changes accepted

Line 678 – expand acronyms to full names and use specific document titles. (see http://lists.ebxml.org/archives/ebxml-stc/200104/msg00001.html).

Changes accepted

Line 703 – Figure 7 is hard to read in black and white print.

TBD

Line 707 – “xxx” spurious notation.

Changes accepted

Line 847,970,1050 – These appendices need some introductory text.

TBD