Produced on behalf of the Combined Gas & Electricity IT Working Group

Draft for industry consultation

White Paper

Part B - 'Technical'

Version 0.3
IT WG
10/10/2000

Table of Contents

1. XML STANDARDS PROFILE

1.1. STANDARDS AND THE INTERNET

It is generally accepted that XML and the Internet will be the strategic technologies to facilitate the wider uptake of business-to-business (B2B) electronic data interchange (EDI) communications into the future. This statement is supported by a wide variety of white papers from various sources (see Appendix 5.3). The previous recommendations, in this document, to adopt XML and the Internet reflect this wider industry consensus.

XML allows definition of the content of business transactions and the Internet provides the ubiquitous mechanism to move the transactions between parties.

Whilst XML is a very young technology, the associated standards are rapidly being formulated with vendors already providing significant levels of product support (see appendix 5.5). Little needs to be said about the acceptance of the Internet transport protocols.

It is less certain, however, what will be the generally accepted mechanism and standards to co-ordinate the exchange between parties of business transactions across the Internet.

Acceptance of a particular mechanism has important implications for the direction of product development and the use of XML in a broader business sense, not just for energy transactions.

1.1.1. Analysis

There are multiple bodies such as the World Wide Web Consortium (W3C www.w3.org), the Internet Engineering Task Force (IETF www.ietf.org) and UN/OASIS (www.ebxml.org/geninfo.htm#about) producing complementary and competing standards for XML based EDI.

In turn, these have been combined into XML frameworks by selection of a compatible subset of standards. The major frameworks relevant to the energy industry are listed below. Appendix … provides more detail on the frameworks mentioned above.

1) BizTalk (www.BizTalk.org) – a Microsoft initiative
2) ebXML (www.ebXML.org) – a UN/EDIFACT and OASIS initiative
3) GISB EDM (www.gisb.org) – an Gas Industry Standards Board (GISB - US) initiative
4) EDIINT AS1/2 (www.ietf.org) – an IETF initiative for EDI on the Internet

Proponents of the frameworks are actively seeking support to encourage the market in their direction, and hence the adoption of their set of standards. Activities include soliciting vendor support and collection of compliant transaction sets from customers and interest groups.

A review of the history of the frameworks and associated standards (see Appendix 1), however, highlights the immaturity of much of this work. Many of the standards are still in working draft and have only appeared in the first half of 2000. There is thus considerable risk in early adoption of a particular framework.

1.1.2. Recommendations

Whilst subsequent sections look in detail at the standards available and make recommendations in some areas, the general recommendations of this paper are that

1) … an interim solution be sought in the short term which allows participants to progress the development of full retail contestability (FRC) systems, but delays selection of standards in areas of uncertainty.

2) … the final decision on the framework and Internet standards to be used for business-to-business transactions in the Australian energy industry be reached by the January 2001 timeframe, pending further market movement either towards a dominant B2B framework, or increased inter-operability between B2B frameworks.

3) … the implementation of the final framework occur by the July 2001 timeframe.

1.2. XML "STACK"

There are a number of levels or layers at which standards must be employed to ensure an orderly exchange of XML transactions across the Internet. The diagram below summarises the purpose of each layer.

Use of the term "stack" is by analogy with communication systems, with each layer utilising the output of the previous layer.

LAYER	PURPOSE	COMMENTS	POSTAL EXAMPLES
ENCODING	Define language of business transactions XML selected	Whilst XML has been mandated, decisions are still needed in terms of how the XML standards are used - naming conventions, documentation standards etc	English
TRANSACTION	Implement business process Specify nature of acknowledgment and response	Outcomes are 1. a dictionary of data elements to be exchanged 2. the transactions that constitute the individual processes 3. the general conventions for transaction exchange.	Letter
SECURITY	Authentication Integrity Non-repudiation	Exchanges are occurring across a public network.	Signature Seal Witness Signature
	Compression		Shorthand
	Privacy		Locked satchel
ENVELOPE	Attach transfer information to content eg. 1. Addresses 2. Priority 3. Delivery 4. Manifests 5. Security	Transactions need to be placed in a container that is understood by the systems that will transport the transactions across the Internet. Much of the incompatibility between frameworks arises as a result of the envelope they select, and the knowledge the TRANSPORT layer must have of the envelope.	Envelope Address List of contents Seal
NETWORK	Specify path to recipients	Depending on the architecture used to pass documents between participants in a business process, the envelope may travel directly to the intended recipient, or may be routed through a common point, often referred to as a portal. The portal, in turn, manages delivery to the intended recipient.	Sorting centre Personal delivery
TRANSPORT	Next hop in path	Much of the leverage gained by using the Internet comes as a result of its accepted transport mechanisms.	Mailvan Courier
INTERNET ACCESS	Access the transport system	This is largely a participant issue.	Walk to the postbox

1.2.1. Analysis

Appendix 3 examines in detail the standards available at each layer.

1.2.2. Recommendations

The recommendations of Appendix 3 are listed below.

1.2.2.1.ENCODING

4) … that the acronym "aseXML" be adopted to identify the XML based transaction set of the Australian Energy Industry.

5) … that the data dictionary and transaction set be expressed in the language of XML schemas.

1.2.2.2.TRANSACTION

6) … that all available free and open transaction flows and data dictionaries be reviewed to determine those closest to Australian requirements, and a subset be used as the basis for development of the Australian XML Energy standard.

7) … that the necessary mechanisms to prioritize and ratify adoption of transaction areas to local market conditions be established.

1.2.2.3.SECURITY

8) … that S/MIME be the preferred standard for provision of security services due to its wide acceptance and compliance with X.509v3 certificates.

9) … that public keys be initially exchanged as part of the legal/financial framework established between parties in the energy market.

10) … that participant systems support a migration to X509.v3 certificates, certificate authorities and revocation lists in the longer term to support a migration to X509.v3 certificates for public key distribution.

1.2.2.4.ENVELOPE

11) … that preference be given to frameworks employing MIME based packaging given the stability of MIME standards and their widespread implementation.

1.2.2.5.NETWORK

12) … that the industry initially adopt a peer-to-peer network architecture allowing participants to "opt" in, with a portal remaining an option in the longer term to provide a lower barrier to entry.

13) … that any use of XML should be contingent on compliance in full to the local standard for the relevant XML transactions.

14) … that peer-to-peer exchanges separate the making of requests and the retrieval of the response into separate exchanges to allow migration to a portal architecture.

1.2.2.6.TRANSPORT

15) … that preference be given to HTTP as the transport protocol to be used in the final standard.

16) … that preference be given to use of the HTTP POST method for delivery of transaction requests and responses.

17) … that use of the response portion of an HTTP POST to contain the transaction response be prohibited to allow future migration to a portal architecture.

1.2.2.7.INTERNET ACCESS

18) … that, where a peer-to-peer architecture is adopted, participants maintain dedicated links to the Internet in order to minimise the issues associated with availability.

19) … that participants review their Internet infrastructure in light of the operational requirements resulting from the use of business-to-business electronic data interchange in the energy market.

1.3. INTERIM ARRANGEMENTS

Whilst this paper recommends delaying the final decision on a set of standards, it recognises the need for participants to prototype systems and develop infrastructure in preparation for full retail contestability.

The aim of the interim arrangements is thus to minimise the establishment overhead whilst offering an environment as close as possible the final solution. Two approaches are proposed.

The first approach utilises an FTP server accessed via NEMNet for the exchange of transactions between participants, assuming early implementers already have NEMNet connections.

The second approach is to utilise the Internet and adopt the preferred recommendations, recognising that rework may be required.

1.3.1. Analysis

The table below compares the two approaches.

	ADVANTAGES	**DISADVANTAGES**
NEMMCO FTP	• Secure network • Participant familiarity • Mechanism already used for NEM • No need for additional Internet infrastructure • Simple shared server configuration • No envelope needed	• Possible impact on production NEMNet • Possible firewall reconfiguration implications • Not preferred transport • Overhead of shared server • Needs procedures to avoid processing of incomplete transactions
Internet HTTP	• Closest to preferred solution • No involvement of NEMNet	• Key management issues • Infrastructure requirements • Security risks • Forces decisions in areas of uncertainty

The first approach avoids envelope, security and key management issues but is contingent on approval and support by NEMMCO. It allows participants to gain familiarity with the transaction set and its integration into their existing legacy systems. In order to negate any impacts on the production market systems, there are likely to be conditions in terms of volume, availability and tail capacities.

The second approach avoids the need for a migration from FTP to HTTP but by its nature, mandates the need for decisions to be made in areas where the standards are not clear.

1.3.2. Recommendations

Given a desire to minimise establishment overheads, it is recommended that

20) … a common server accessed by NEMNet using FTP be used as an interim framework to facilitate participant familiarity with XML and development of their Full Retail Contestability infrastructure.

1.4. WAY FORWARD

The table below summarises the areas in which decisions will be made under the interim, final and future recommendations.

LAYER	INTERIM	FINAL	FUTURE
ENCODING	√	X	X
TRANSACTION	√	X	X
SECURITY	X	√ (Manual key exchange)	√ (X.509v3 Certificates)
ENVELOPE	X	√	X
NETWORK	X	√ (peer-to-peer)	√ (portal)
TRANSPORT	√ (FTP)	√ (?HTTP)	X
ACCESS	√ (NEMNet)	√ (Internet)	X

In conclusion, the recommendations discussed previously suggest the actions below.

- Short-term focus on encoding and transaction standards to codify the data dictionary and transactions to be used, given that the business processes required are well known.

- Selection and implementation of an interim solution to facilitate participant familiarity with XML and development of their Full Retail Contestability infrastructure.

Watching brief to be maintained on standards development with a final recommendation no later than January 2001 for implementation by July 2001.

APPENDICES

1. HISTORY OF THE DEVELOPMENT OF INTERNET BASED STANDARDS FOR BUSINESS-TO-BUSINESS COMMUNICATIONS

In order to understand the level of maturity of the available Internet standards applicable to business-to-business communications, it is useful first to look at the history of the development of these standards.

Four areas are addressed below. The first section deals with the standards traditionally associated with Electronic Data Interchange – that of the ANSI X12 standard.

The second details the XML standards whilst the third describes the efforts, mostly by the US utility industry, to document sets of transaction interchanges. There is a mixture of X12 and XML based sets.

Finally, the fourth area looks at the recent development of XML based frameworks for B2B communications.

1.1. Electronic Data Interchange (EDI)

1979
- ANSI X12 Committee formed to address EDI

1983
- First X12 standards appeared

1994-98
- Utility Interest Group (UIG) (www.uig.org) develops X12 subsets for the US Utility Sector

1995
- RFC 1767 – MIME Encapsulation of EDI objects (www.ietf.org/rfc/rfc1767.txt)
- RFC 1867 – Form-based File Upload in HTML (www.ietf.org/rfc/rfc1867.txt)

1996
- Gas Industry Standards Board (GISB) (www.gisb.org) develops Electronic Delivery Mechanism (EDM) for EDI over Internet via RFC 1867 (HTTP based)
- RFC 2015 - MIME Security with Pretty Good Privacy (PGP)

1997
- GISB EDM standard largely implemented by US Gas Industry (X12 content)

1998

- Automobile Industry Action Group adopts GISB EDM

1999

- Pennsylvania Electric Companies adopt GISB EDM for B2B
- RFC 2633 - S/MIME Version 3 Message Specification (www.ietf.org/rfc/rfc2633.txt)
- EDIINT AS1 "MIME based Secure EDI" released (SMTP based) (www.ietf.org/internet-drafts/draft-ietf-ediint-as1-11.txt)
- IETF EDI Group + GISB EDM produce IETF EDIINT AS2 "HTTP Transport for Secure EDI" (www.ietf.org/internet-drafts/draft-ietf-ediint-as2-07.txt)
- GISB AS2 Profile – migration of EDM to EDIINT AS2

A couple of points to note are that

- GISB EDM and EDIINT AS1/2 can carry any format payload, not just X12.
- GISB EDM and EDIINT AS1/2 leverage all the work done by the IETF in the security area via use of S/MIME and PGP/MIME.

The conclusions to be drawn are that

- the use of GISB EDM for live transactions shows the Internet to be a viable communications environment for the utility industry
- convergence of GISB EDM and EDIINT AS1 via EDIINT AS2 could provide a proven, secure option for secure document exchange with an available product set via those supporting GISB EDM and EDIINT AS1.

1.2. XML

Feb 1998

- XML 1.0 recommendation released (www.w3.org/TR/REC-xml)

Jan 1999

- XML namespace recommendation released (www.w3.org/TR/REC-xml-names)

Apr 2000

- XML schema working drafts released (www.w3.org/TR/xmlschema-0)

May 2000

- Simple Object Access Protocol (SOAP) note released (www.w3.org/TR/SOAP)

July 2000

- XML Digital Signature working draft released (www.w3.org/TR/xmldsig-core)

The conclusions to be drawn are that

- XML is a young technology
- whilst the basic standards are in place, it will be some months before a sufficient core of specifications are officially approved
- product offerings have focused largely on tools to manipulate XML documents rather than exchange them
- the rate of development is indicative of the commitment to - XML within the marketplace and bodes well for its longevity as a technology

1.3. Utility Transaction Sets

1994-98

- UIG X12 subsets for the US

1998

- UK Data Transfer Catalogue (DTC) (X12 based)

1999

- XML-PIPE Transaction set from XMLPIPE.ORG (www.xmlpipe.org) (XML based)

2000

- (Jan) US Coalition For Uniform Business Rules (CUBR) (www.cubr.org) Standard Electronic Transactions (SET) for retail electricity and gas markets (X12 based)
- (May) Ontario Energy Board (OEB) Transaction Set (www.oeb.gov.on.ca) (XML based)

The conclusions to be drawn are that

- a number of published transaction sets for the utility industry are available for reference
- there is considerable terminology overlap amongst the transaction sets with each building on the work of earlier standards
- the work of CUBR and Ontario Energy Board represents the latest overseas experience.

1.4. XML B2B Frameworks

2000

- (Feb) BizTalk 1.0 draft released
- (June) BizTalk 2.0 draft released
- (July) ebXML Transport Routing and Packaging working drafts released

The conclusions to be drawn are that

- XML B2B frameworks are in their infancy
- no clear market preference is yet discernible
- for point-to-point exchanges, use of more established mechanisms such as EDIINT AS2 may offer lower risk in the short term.

2. FRAMEWORKS FOR B2B ON THE INTERNET

The Gas Industry Standards Board (www.gisb.org) in the US was one of the first organisations to recognise the benefits of using the Internet for EDI (see Appendix 1.1 for the chronology involved). They created the GISB Electronic Data Mechanism (EDM) that uses HTTP to transport X12 based documents in a peer-to-peer architecture. It is widely used in the US Gas Industry and is being considered for use in the deregulated electricity markets by a number of US states. Whilst initially using X12, the use of MIME in EDM allows the carriage of any content type including XML.

The Internet Engineering Task Force (IETF) (www.ietf.org), the group responsible for many of the Internet infrastructure standards, also recognised the value of the net to EDI. They have an EDI working group which produced a standard for EDI via mail, referred to as EDIINT AS1. Being a later standard, EDI adopted much of the more recent security work but still deals with point to point exchanges.

In recognition that GISB and EDIINT AS1 both had different strengths, an effort was undertaken to merge the standards resulting in a draft standard called EDIINT AS2. Both EDIINT AS1 and EDIINT AS2 allow the carriage of arbitrary content via the use of MIME.

With the rise of XML as a technology capable of solving many of the problems associated with B2B EDI, two major groups have sought to provide more complete frameworks for EDI using XML. BizTalk (www.BizTalk.org) is a Microsoft initiative while ebXML (www.ebXML.org) is a collaborative effort of the UN EDIFACT group and the Organisation for the Advancement of Structured Information Standards (www.oasis-open.org).

These later frameworks intend to support multi-party transactions, and thus provide more extensive standardisation of the carriage of ancillary information with the transaction payload.

2.1. Analysis

The table below summarises some of the key features of each framework. For further information, see Appendix ….

	NETWORK	ENVELOPE	SECURITY	HEADER	TRANSPORT
GISB	Peer-to-peer	MIME	PGP/MIME	Security	HTTP
EDIINT AS1	Peer-to-peer	MIME	S/MIME	Security	SMTP
EDIINT AS2	Peer-to-peer	MIME	PGP or S/MIME	Security	SMTP/HTTP
EbXML	Multi-party	MIME	S/MIME or PGP/MIME	Addressing Manifests Security Delivery Priority	HTTP
BizTalk	Multi-party	XML/MIME	S/MIME	Addressing Manifests Security Delivery	HTTP

3. STANDARDS REVIEW

The diagram below is an expanded version of that appearing in section? It shows the major standards, options or issues at each layer, a description of which appear below.

<table>
<tr><td></td><td colspan="5">BUSINESS PROCESS/TRANSACTIONS
|
|
V</td></tr>
<tr><td>ENCODING</td><td colspan="5">DTD vs schemas, namespaces, file organisation, naming, versioning, style guides</td></tr>
<tr><td>TRANSACTION</td><td colspan="5">XML-PIPE, OEB, DTC, CUBR, US-UIG</td></tr>
<tr><td>SECURITY</td><td colspan="5">S/MIME, PGP/MIME, SSL, Certificates</td></tr>
<tr><td>ENVELOPE</td><td colspan="5">ebXML, EDIINT AS1/2, SOAP, BizTalk</td></tr>
<tr><td>NETWORK</td><td colspan="5">Peer-to-Peer, Portal</td></tr>
<tr><td rowspan="3">TRANSPORT</td><td>MIME
(ebXML)
(BizTalk)
(EDIINT AS1/2)</td><td>XML
(SOAP)</td><td rowspan="2">FTP
File
Shares</td><td rowspan="2">JMS</td><td rowspan="2">Proprietary</td></tr>
<tr><td colspan="2">HTTP/SMTP</td></tr>
<tr><td colspan="3">Point-to-Point</td><td colspan="2">Messaging
Middleware</td></tr>
<tr><td>INTERNET ACCESS</td><td colspan="5">Dial-up vs dedicated links
Dedicated vs shared gateways
Firewall considerations</td></tr>
</table>

3.1. ENCODING

The section highlights a number of areas where decisions need to be made in order to establish an environment where XML transactions may be formulated by separate groups but easily combined into a single standard.

3.1.1. Acronym for Standards and Development Process

It is useful to have an acronym to describe the encoding standards and the transactions. Some suggestions are given below.

aesXML – "(A)ustralian (E)nergy (S)tandard for XML Transactions"
aseXML – "(A)ustralian (S) tandard for (E)nergy Transactions in XML"
esaXML – "XML (E)nergy (S)tandard for (A)ustralia"
ETML – "(E)nergy (T)ransactions (M)arkup (L)anguage"
eXML – "(E)nergy Industry Transaction (M)arkup (L)anguage"

3.1.2. Recommendations

4) … that the acronym "aseXML" be adopted to identify the XML based transaction set of the Australian Energy Industry.

3.1.3. DTD vs Schemas?

Whilst Document Type Definitions (DTD) are part of the XML 1.0 standard (www.w3.org/TR/REC-xml), there is a trend towards the use of XML Schemas on the Internet, even though the relevant standards are still working drafts (www.w3.org/TR/xmlschema-0). As an example, the Ontario Energy Board transaction set is defined in terms of XML schemas.

3.1.4. Recommendations

5) … that the data dictionary and transaction set be expressed in the language of XML schemas.

3.1.5. XML Schemas

Details of the use of XML schemas within aseXML are contained in Part 3 of the White Paper – Guidelines for Development of the Australian Standard for Energy Transactions in XML (aseXML).

3.2. TRANSACTION

3.2.1. Options for XML Transaction Set Specification

The process for arriving at a suitable transaction set for the industry is, in essence, a variant of the package vs. in-house system argument faced by most organisations.

In this case, the package solutions consist of pre-defined sets of transactions developed by consortia, member sponsored groups or individual industry players – ie use of an "Existing" solution. The in-house approach is to examine the set of locally required transactions and develop a standard that exactly meets these, but incurs considerable commitment of resources along the way – ie "Build as you go".

An intermediate approach is to take an existing transaction set and modify it to meet Australian market conditions, thus creating a local industry standard – ie use of customised version of an existing solution, eg "Existing + Build as you go". Where the "goodness of fit" to requirements is sufficient, an option is to become involved in the creation of the existing standard and have local requirements incorporated into it.

Table 1 over-the-page compares these three approaches. Values are normalised such that more stars imply a more desirable option.

Table 1 – Comparison of 3 Options (normalised)

ISSUE	BUILD AS YOU GO	EXISTING	EXISTING + BUILD AS YOU GO
Requirements Match [1]	*****	*	*****
Initial Development			
Timeframe	*	*****	***
Resource level	*	*****	***
Specification / Arbitration [2]	****	**	***
Licensing / Copyright [3]	*****	***(**)	***(**)
Ongoing Development			
Resource level	*	*****	** [4]
Product adoption [5]	*	***	*
Lock-in [6]	*	*****	***

Notes to Table 1

1. A match to local conditions must be considered a high priority issue. Given the uniqueness of the local market, the possibility of an exact match to a pre-existing standard is unlikely.
2. Specification is the process involved in deriving the transaction set. Arbitration is the process by which a decision is reached where the interested parties cannot agree. These issues may be considered a two-edged sword. On one hand, an existing standard will have these mechanisms in place thus putting less onus on the participants. On the other hand, the development is locked in to the timeframe of the existing processes. The scores assume the latter case.
3. Existing transaction sets may or may not place restrictions on their use/modification.
4. This option does allow adoption where applicable of developments in the existing standard.
5. The standard continues to be enhanced by other members. There is thus the likelihood that a new transaction requirement has already been addressed by the standard.
6. Where the local variant is sufficiently different to the base standard, a migration path is less likely to exist should a move to a new standard be required.

3.2.2. Analysis

In an ideal world, the table above indicates that adoption of a pre-existing standard offers the best solution in terms of the overheads associated with creation and maintenance of the standard.

The reality is that an exact match to a pre-existing transaction set does not exist (see next section), and thus some degree of customisation will be necessary. Where possible, leverage should be obtained from the work of others provided there are no issues attached such as copyright.

It is reasonable to assume that B2B products in the energy sector will adopt whatever standard transaction sets are in use by the market. Thus to minimise any product rework by vendors necessary to meet local conditions, efforts should be made to keep the local standard as close to the pre-existing standards as possible.

3.2.3. Recommendations

6) … that all available free and open transaction flows and data dictionaries be reviewed to determine those closest to Australian requirements, and a subset be used as the basis for development of the Australian XML Energy standard.

3.2.4. Existing XML Transaction Sets

Research by a number of participants indicates there to be only one, publicly available, energy related XML transaction set and accompanying data dictionary. This set, called XML-PIPE (www.xml-pipe.com), is the result of a member-sponsored organisation consisting of Keane, PriceWaterhouseCoopers and Excelergy. It is made available on the Internet at no cost and with no restrictions on its use or modification.

A variant of this is available from the Ontario Energy Board (www.oeb.gov.on.ca/), who have used XML-PIPE as a basis for their deregulated market.

In addition to being used in Ontario, XML-PIPE has been adopted by PJM (Pennsylvania, New Jersey, Maryland) in the US as part of its FRC and is actively being considered by a number of other US states.

Additional information on XML-Pipe.ORG may be found in Appendix …, or alternatively in References Appendix.

A number of data dictionaries and transaction sets also exist that utilise the X12 standard. Whilst not being in the XML format, these standards provide a good source of starting material for the local transaction set.

The first of these is the Utility Industy Group (www.uig.org) X12 subsets, which have for many years formed the basis for much of the EDI in the utility industry in the US. A draft XML data dictionary has recently be released (www.uig.org/upload/Articles/data dictionary draft 060400.pdf). More recently the deregulation of the UK markets has led to the development of the Data Transfer Catalogue (DTC). Finally, as a result of the deregulation activity in the US, the Coalition for Uniform Business Rules (www.cubr.org) has released an extensive document cataloguing proposed data flows and entities for the retail gas and electricity markets. This document is particularly helpful as the transaction flows are presented diagrammatically.

Appendix … shows the chronology of the development of the transaction sets mentioned above.

3.2.5. Industry Perspective

Excelergy and PriceWaterhouseCoopers are currently working with PowerCor to adapt the XML-PIPE standard to meet Australian requirements in the Customer Transfer area. Discussions with Excelergy and PriceWaterhouseCoopers representatives indicate that of the 14 transactions now identified, 6 will be modifications of existing XML-PIPE transactions whilst the remaining 8 are new. In general, Excelergy have found that a 3:5 ratio of modify to new to be common when considering adoption of XML-PIPE to a new circumstance. In terms of the data dictionary, however, less change is required. Ballpark figures given by Excelergy for specification of a complete set of transactions were 4 weeks for entity analysis and 3 months for transaction review.

3.2.6. Analysis

It is clear from the above figures that considerable work is still to be done to create a set of transactions covering all aspects of the Australian energy market. A prioritisation process will be required between the broad transaction groups such as

- NMI Data Processes
- CATS7
- Service Orders
- Customer Information
- Billing
- Meter Data Management, Meter Data
- Fault Management / Trouble Orders

3.2.7. Recommendations

7) … that the necessary mechanisms to prioritize and ratify adoption of transaction areas to local market conditions be established.

3.3. SECURITY

Standards at this layer address five main areas -

- Authentication – parties know the identities of those with whom they are communicating
- Integrity – exchanges can not be tampered with on-route
- Non-repudiation – parties cannot deny involvement in exchanges.
- Compression – improves the effectiveness of the cryptographic algorithm
- Privacy – only the parties involved know the contents of any exchange

The first three issues are usually applied to a payload first via the use of a message digest. The digest includes a signed (authentication) version of the results of a hash function (integrity) across the payload and a timestamp (non-repudiation). This data is typically kept with the payload until processed by the final application, especially where financial transactions are concerned.

Whilst not strictly a security issue, compression is typically applied as the next security step prior to payload encryption since compression relies on redundancy and encryption algorithms try to generate data with no redundancy. Were the order of the two to be reversed, the compression would be of no value.

Compression is likely to be of significant value with XML documents due to the highly redundant nature of its tag structure.

Encryption of the payload (which now includes the message digest) is optional depending on whether the transport mechanism provides privacy or not. In the general case of multiple transport hops, end to end privacy mandates the use of encryption of the payload prior to its delivery to the transport system.

There are two standards commonly employed on the Internet for provision of the security services on the content of exchanged information

- S/MIME – Secure Multipurpose Internet Multimedia Extensions.
- PGP/MIME – Pretty Good Privacy Multipurpose Internet Multimedia Extensions.

As indicated by the names, both apply to the securing of information encoded in MIME format. Both rely on public key cryptography and hence require the exchange of public keys.

Public keys are tied to a particular person or organisation via a Digital Certificate and it is in the area of certificates that the two differ significantly.

More recently, a working draft standard has been released by W3C on XML encoding of digital signatures. Because of the recent release of this draft (see Appendix…), no framework has yet adopted it.

Security can also be applied at the transport layer, the most well known example being the secure sockets layer (SSL). This standard provides a private pipe over which confidential information such as passwords may be passed without further encryption.

SSL is used to provide secure point-to-point HTTP (HTTPS) sessions and more recently secure FTP (S/FTP) sessions.

For more complete background information on security issues, refer to the "Data Transport Alternatives for Electronic Business Transactions" white paper from UIG.

3.3.1. Industry experience

The use of the standards in the frameworks discussed previously is presented below.

	GISB	EDIINT AS1	EDIINT AS2	ebXML	BizTalk
S/MIME	X	√	√	√	√
PGP/MIME	√	X	√	√	X
SSL	√	X	√	√	?

EDIINT AS2, being an attempt to merge GISB and EDIINT AS1, allows selection of either MIME standard.

ebXML draws from EDIINT AS2 and thus also allows either MIME standard. Work on the application of security to ebXML is just commencing.

The BizTalk framework version 2.0 mentions its intention to use S/MIME but defers implementation details to a subsequent release.

The Ontario Energy Board has mandated the use of S/MIME with triple DES and the SHA message digest algorithm.

3.3.2. Analysis

The widespread use of PGP in mail systems has lead to it becoming a stable standard with multiple implementations. It uses its own certificate format and relies on the concept of a "web of trust" for their distribution. The idea is that A trusts B who trusts C etc. Thus A accepts C's certificate because it was provided by B.

S/MIME adopts the ISO X509v3 standard for digital certificates. This standard uses the concept of certificate authorities for certificate

distribution. In this architecture, a signature is accepted because a trusted organisation digitally countersigns it. The latest version of PGP has some support for X.509v3 certificates. The table above shows S/MIME to have the broadest adoption within the available frameworks.

Whilst certificates and certificate authorities are needed in the context of the Internet, the other legal/financial arrangements of the energy markets require considerable exchange of information prior to any business transaction being conducted. Exchange of public keys could be included as part of this information negating the need for the complexity of digital certificates. In addition, there is some concern about the interoperability of software using X509v3 certificates.

In the longer term, businesses may require certificates in other areas of electronic business, at which point their use could be incorporated into the energy market.

Were a trusted portal (see section…) to be implemented, an alternative to S/MIME and PGP/MIME would be the use of HTTPS with usernames and passwords.

3.3.3. Recommendations

8) … that S/MIME be the preferred standard for provision of security services due to its wide acceptance and compliance with X.509v3 certificates.

9) … that public keys be initially exchanged as part of the legal/financial framework established between parties in the energy market.

10) … that participant systems support a migration to X509.v3 certificates, certificate authorities and revocation lists in the longer term to support a migration to X509.v3 certificates for public key distribution.

3.4. ENVELOPE

The purpose of an envelope is to attach the temporal information needed to exchange transactions to their information content. The temporal information includes

- Addressing (sender, recipient(s)).
- Transaction manifest (list of contents and attachments).
- Security information (digital signatures etc).

The information above is usually carried in the envelope header, whilst the transaction content is carried in the envelope payload.

Envelope standards specify both the format of the header, and the way in which the envelope, header and payload will be packaged.

3.4.1. Industry Perspective

The table below shows the packaging standards adopted by the various frameworks.

	GISB	EDIINT AS1	EDIINT AS2	ebXML	BizTalk
MIME	√	√	√	√	√
XML	X	X	X	X	√

The more recent frameworks have considered XML as an alternative packaging format. ebXML selected MIME because of the stability of the standards and the minimal changes needed to established infrastructure. BizTalk uses XML for single documents (via the Simple Object Access Protocol (SOAP) standard) but extends this to use MIME where other attachments are required.

In terms of header formats, GISB and EDIINT assume a point-to-point architecture and rely on the structure of MIME to carry the header information.

The more recent frameworks provide greater structure to the header as a separate entity, with both ebXML and BizTalk using XML to express the header content.

3.4.2. Analysis

MIME is normally selected as the packaging standard given that the associated standards are long established and provide for a rich environment.

It is interesting to note the inconsistency of the BizTalk approach and it is perhaps only a matter of time before the use of XML for single documents is incorporated into the multi-document format.

The packaging standard adopted has implications for the transport used. Both HTTP and SMTP use MIME to encode data transfers and frameworks must specific how to map their envelope structures onto those used by the transport layers.

Selection of an envelope standard is thus part of the larger question of selecting a B2B XML framework. Both XML frameworks are in their infancy and it is difficult to predict which why the market will go.

3.4.3. Recommendations

11) … that preference be given to frameworks employing MIME based packaging given the stability of MIME standards and their widespread implementation.

3.5. NETWORK

Two broad categories of network architecture are available. In peer to peer, each entity manages the connection to each other entity. In the portal approach, all transactions pass through a single point.

The table below compares these categories, more stars implying a preferable option.

ISSUE	PEER TO PEER	INDUSTRY PORTAL
Maintenance of interfaces[2]	** [1]	*****
Trust	*****	**
Cost allocation	*****	** [3]
Transitional reliability[4]	***	*****
Long-term reliability[5]	*****	**
Capability[6]	***	*****
Complexity[7]	*	*****
Availability[10]	**	*****
Compliance/Certification[8]	**	*****
Transition arrangements[9]	**	*****

More stars preferable.

1. An industry portal isolates the idiosyncrasies of communications with each participant to the portal.
2. Peer-to-peer avoids the complexities of cost distribution for a shared resource.
3. In the initial phase where systems are being accepted, a portal would provide a more stable test environment and isolate players from each other
4. The nature of a peer-to-peer topology makes it more tolerate to failure than a star style topology.
5. A portal allows participants to provide different levels of transaction capability in terms of transaction formats, with the portal filling in the gaps and providing translation services.
6. In peer-to-peer, each participant must manage the interface to each other participant.
7. In peer-to-peer, each participant must verify the operation of its interface with each other participant. There may also be a critical mass of certified participants needed to ensure the integrity of the market, as was the case in the UK.
8. Since a portal can provide translation services, participants wishing to move to XML can do so without requiring others to move from existing formats eg. flat file. In a peer-to-peer approach, participants wishing to move to XML would have to implement the translation themselves, or ensure all their communicants had also moved to XML.
9. A portal offers an exchange point that is always available, peer-to-peer requires simultaneous availability of communicating parties

3.5.1. Industry Experience

Both the UK DTC and the Ontario models utilise a portal approach.

Experience, provided by Excelergy and PriceWaterhouseCoopers representatives, of the Pennsylvania/New Jersey/Maryland (PJM) FRC indicates that a portal approach is preferable where adherance to the transaction standard can not be enforced, especially where the number of participants is large. In this case, there were seven distributors and 70 retailers. Whilst the regulator called for a single standard for data exchange, there were no cost penalties for non-compliance. Variations resulted from the implementation of the transaction set by each participant depending on the legacy systems involved. The net result was a peer-to-peer network where each participant had to certify themselves against 76 others.

3.5.2. Analysis

The table above suggests that a portal approach is the best solution in an ideal world, especially in light of the US and UK experience. Such an approach, however, requires agreement by participants on the body to host the portal and its associated costing issues.

Given the desire of the industry to move quickly in order to prepare for the 1/1/2001 deadline, a peer-to-peer approach provides more flexibility for those wishing to embrace XML early in the development process. The need for consensus is thus reduced in the short term but a migration path is needed should the complexity of interactions exceed an acceptable level.

The danger in initially adopting a peer-to-peer approach, as seen in the case of PJM, is the possibility for a proliferation of slightly different transaction sets between peers. It is thus important that any XML exchange adhere fully to a single transaction set standard.

In order to allow a migration to a portal approach in the future, it is recommended that requests and responses be treated as separate exchanges, ie. the response should NOT be included in the acknowledgment of the request. Whilst incurring additional overhead, this approach allows the insertion of a portal between the parties and may be required in any event due to latencies in transaction processing.

3.5.3. Recommendations

12) … that the industry initially adopt a peer-to-peer network architecture allowing participants to "opt" in, with a portal remaining an option in the longer term to provide a lower barrier to entry.

13) … that any use of XML should be contingent on compliance in full to the local standard for the relevant XML transactions.

14) … that peer-to-peer exchanges separate the making of requests and the retrieval of the response into separate exchanges to allow migration to a portal architecture.

3.6. TRANSPORT

The aim at this level is to leverage existing communication mechanisms, particularly those provided by the Internet. These mechanisms fall into two broad categories, messaging middleware and point-to-point.

Messaging middleware has tended to be used for internal connection of disparate systems within organisations but has not seen widespread adoption on the Internet due to the proprietary nature of many of the interfaces and architectures. JMS (Java Messaging Service) is an attempt to standardise the interface to messaging middleware in order to allow applications to be written without reference to the underlying middleware implementation. Appendix 4 provides more details on middleware and its use with the Internet.

Point-to-point protocols fall into two groups, those (HTTP/SMTP) for which an encapsulation of the data is required to achieve delivery, and those for which the mechanism itself implies the destination (FTP, file shares).

FTP is an efficient file transfer mechanism but suffers from a poor security architecture, where passwords appear in clear-text. It is also presents some difficulties when firewalls are employed.

SMTP provides the backbone for mail transport and thus is as ubiquitous as the Internet itself. It is also most susceptible to deal of service attacks such as 'spamming'.

HTTP is a recent, simple protocol that is easy to use with firewalls.

3.6.1. Industry Experience

The table below shows the transport protocols adopted by each of the frameworks. A question mark indicates that use is possible but not standardised.

	GISB	EDIINT AS1	EDIINT AS2	ebXML	BizTalk
HTTP	√	X	√	√	√
SMTP	X	√	√	?	?
FTP	X	X	X	?	?

3.6.2. Analysis

The merging of the GISB and EDIINT AS1 standards is partially recognition of the advantages of HTTP as a transport.

Adoption of HTTP and its POST method as the first binding to be specified for both ebXML and BizTalk reinforces HTTP as the transport of choice.

3.6.3. Recommendations

15) … that preference be given to HTTP as the transport protocol to be used in the final standard.

16) … that preference be given to use of the HTTP POST method for delivery of transaction requests and responses.

17) … that use of the response portion of an HTTP POST to contain the transaction response be prohibited to allow future migration to a portal architecture.

3.7. INTERNET ACCESS

Whilst it is not the intention of this paper to mandate the nature of participant's access to the Internet, the issues below need to be considered.

- dial-up vs dedicated lines
- line sizing
- dedicated vs shared infrastructure
- firewall design

3.7.1. Analysis

The availability requirement necessary in a peer-to-peer network architecture essentially precludes the use of dial-up links. The problem of availability increases when multi-party transactions are considered. It is anticipated that most participants already have permanent Internet connections.

The decision to separate or combine Internet infrastructure for general business and participation in the energy market will generally be driven by cost, reliability and scalability issues. Participants will need to consider the possibility of malicious attacks such as spamming and denial of service as well as the impact of failures of non-essential functions during normal operation. An example of the latter might be a shared SMTP/HTTP gateway running out of disk space due to the proliferation of large mail attachments at Christmas.

Finally, participant firewalls will need to be reviewed. The aim of B2B is to more closely link back-end systems. This may necessitate the opening up of firewalls to allow B2B transaction exchanges.

3.7.2. Recommendations

18) … that, where a peer-to-peer architecture is adopted, participants maintain dedicated links to the Internet in order to minimise the issues associated with availability.

19) … that participants review their Internet infrastructure in light of the operational requirements resulting from the use of business-to-business electronic data interchange in the energy market.

4. USE OF MIDDLEWARE IN THE ENERGY INDUSTRY (FRC Infrastructure)

4.1. Introduction

This paper examines the potential contribution of alternative middleware solutions to the infrastructure for the Energy Industry FRC. This examination is necessarily brief and in broad outline only, given that:

(a) the FRC infrastructure must support participation by both large energy enterprises as well as small to medium-size players,
(b) most middleware solutions currently available in the market require substantial implementation costs, and therefore
(c) middleware solutions in the context of the FRC infrastructure will be regarded as a potential barrier to market entry by smaller participants, and must therefore be treated as a non-essential and optional component.

4.2. Definition of Middleware

Middleware is a technological framework that allows the diverse and distributed applications and systems of an organisation to communicate and interact with each other seamlessly in or near to real time. A well-designed middleware framework should:

- allow information to flow quickly and seamlessly to and from each application.
- enable new "best of breed" applications to be easily integrated into the enterprise "federation" of member applications and systems.
- provide a standard communication protocol to enable communication between all types of applications (mission-critical back-end systems, front-end customer interfaces, B2B gateway applications), regardless of whether they are from different vendors with different protocols.
- enable workflow management and automation of business processes across multiple applications.
- allow transformation of data between member applications with different data models and world-views.
- ideally use an event-driven model that employs a "publish on subject / subscribe to subject" approach to messaging that minimises network traffic, instead of the traditional request/reply model.
- contain a common repository for storing metadata definitions of each application's data model.

4.3. Middleware and Full Retail Contestability

In the context of the Energy Industry FRC, the potential contribution of middleware use can be examined under two different scenarios:

Scenario 1: Use of Middleware purely as an internal solution within an individual market participant
Scenario 2: Use of Middleware to enable a Energy Industry market participant's internal FRC applications to interact seamlessly with the FRC applications of other market participants

4.3.1. Scenario 1: Use of Middleware purely as an internal solution within an individual market participant

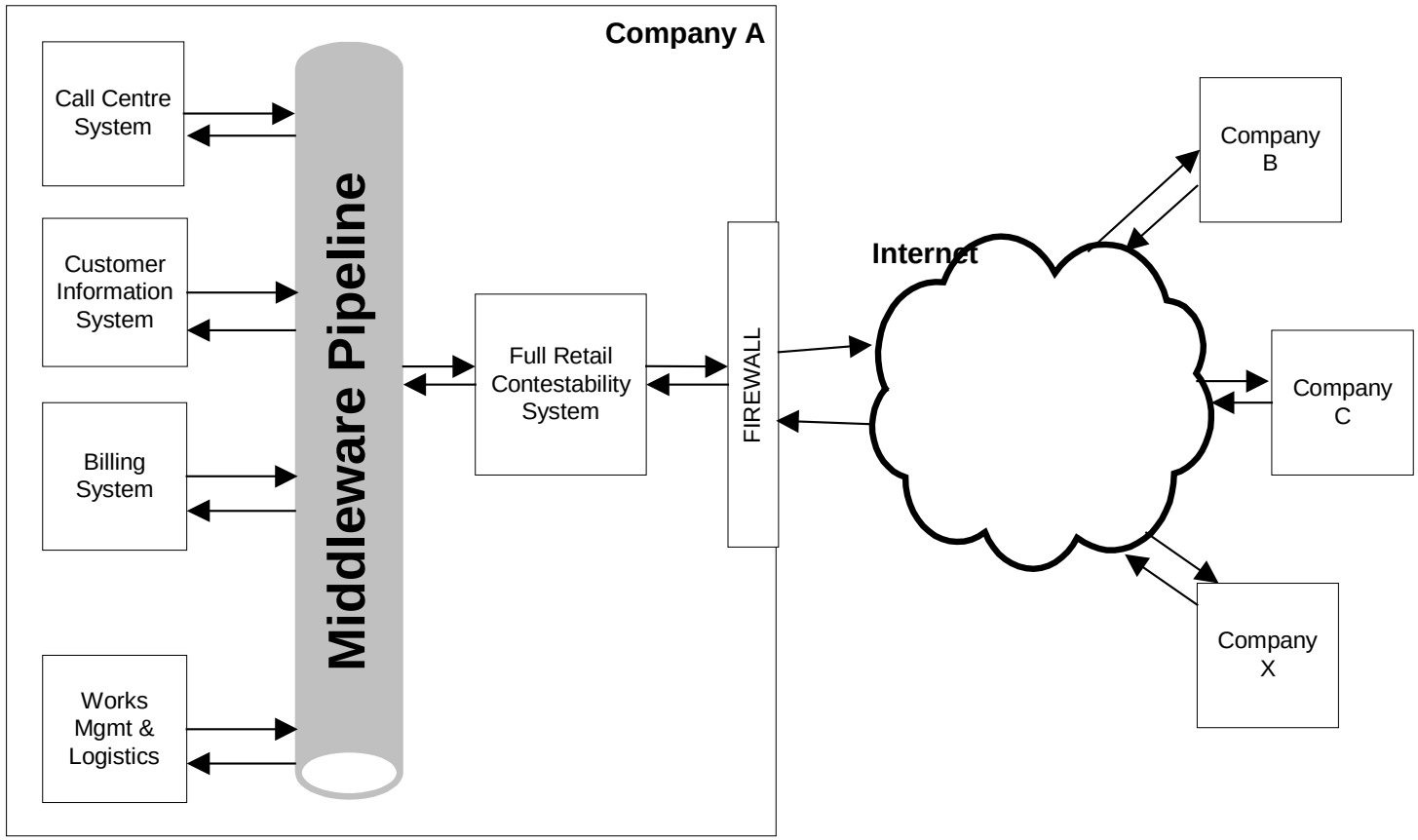
In this scenario (see Figure 1 over the page), company A uses a middleware platform to integrate its internal applications. As an example, suppose company A gains a new customer from company B. A's Call Centre system would capture the new customer's details and initiate a business process workflow that first publishes a "customer_acquisition" message to all subscribing applications. The Full Retail Contestability (FRC) application subscribes to this message, which triggers the creation of an XML document which it sends out using HTTP, HTTPS or other protocol to the appropriate URLs (Company B, the Market Operator/Portal, and other nominated market participants or business partners). Note that the FRC application referred to here is an abstraction; for any given participant the FRC functions may be distributed among the enterprise's call centre, CIS and other systems.

When company B or other parties returns an acknowledgment and/or acceptance of the customer acquisition notification, the incoming message comes through the firewall and is subscribed by the FRC application listening for such messages. The FRC application logs audit and non-repudiation information for the received message, then publishes a message internally within A that continues the original business process workflow to, for example,

- update the Customer Information System,
- notify the Works Management & Logistics system to perform any required field work and services at the new customer's premises, and
- inform the Billing system to put the new customer on a billing cycle).

The communications between A's internal applications are channelled through its Middleware information pipeline.

Figure 1: Use of Middleware as an internal solution within a market participant



4.3.2. Scenario 2: Use of Middleware to enable a Energy Industry market participant's internal FRC applications to interact seamlessly with the FRC applications of other market participants

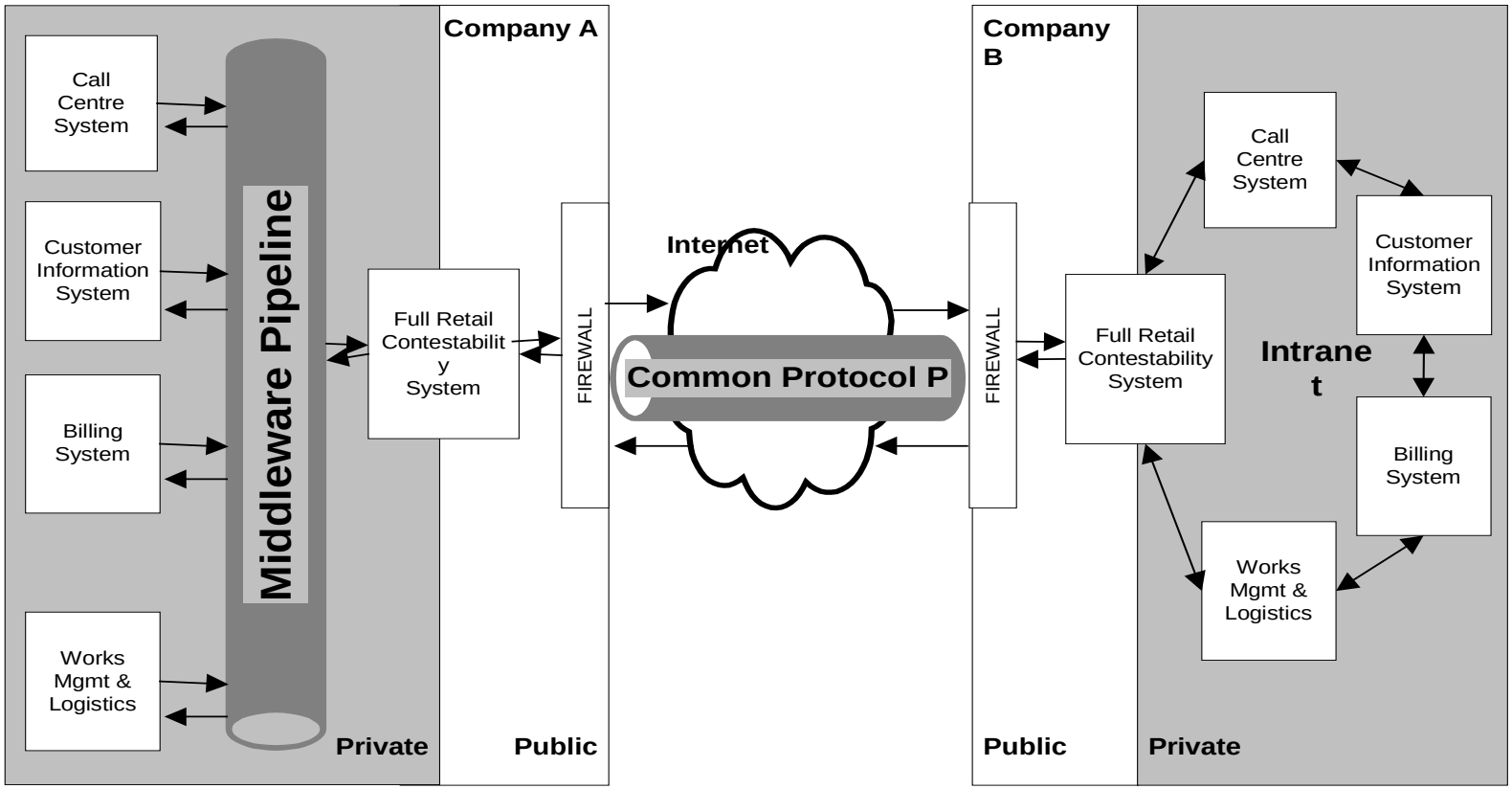
This scenario (see Figure 2) is an extension of the middleware framework across enterprises, effectively creating business-to-business integration. The objective is to move from mere integration of different applications within one organisation to a seamless flow of information across multiple business enterprises. This will require the participating enterprises to:

- share a common Middleware framework and infrastructure
- use a common Middleware communications protocol (eg. MQSeries, TIB/Rendezvous, etc),
- use the same Internet protocols (HTTP, HTTPS, SMTP etc),
- share a common security infrastructure (PKI, certificates, signature verification, etc)
- use XML and a common set of DTD or XML schema definitions (this is already being addressed by the IT WG),
- use a common set of business processes for the exchange of data and messages (also being addressed),

In Figure 2:

- Company A uses Middleware suite M with communication protocol P to integrate its internal private operations. P is also used to publicly communicate with company B and possibly other market participants and business partners.
- Company B uses protocol P to communicate publicly with company A and possibly other business partners. It may or may not use Middleware suite M to integrate its own applications.
- Protocol P is sued to handle the public communication exchanges between companies A and B, in addition to the internal applications integration of company A.

Figure 2: Use of Middleware to enable a market participant's internal systems to communicate seamlessly with the FRC systems of other market participants



5. REFERENCES

5.1. XML GENERAL INFORMAITON

- www.w3c.org
- www.xml.org
- www.oasis-open.org

5.2. XML TUTORIALS

- www.xml.com

5.3. XML WHITE PAPERS

- www.uig.org/upload/Articles/XML White Paper FINAL10.pdf
- www.gegxs.com/geiscom/downloads/xmlwhitepaper.pdf
- www.sun.com/forte/fusion/whitepapers/xml.pdf
- www.excelergy.com/deregedi/form.html
- www.8760.com/gci.pdf

5.4. FRAMEWORKS

- www.BizTalk.org
- www.ebXML.org
- www.gisb.org
- www.ietf.org

5.5. CURRENT SUPPORT FOR XML IN COMMERICAL PRODUCTS

5.5.1. INTEL

- www.intel.com/network/solutions/xml.htm
- www.intel.com/network/tech_bulletins/7210_xml_award.htm

5.5.2. ORACLE

- Using XML and Relational Databases for Internet Applications
- XML Support in Oracle8i and Beyond
- Oracle's XML-Enabled Internet Platform for Business-to-Business E-Commerce

Using XML in Oracle Database Applications

Part2: About Oracle XML Products
Part3: Customizing Data Presentation
Part4: Exchanging Business Data Among Applications

5.5.3. SYBASE

- Using XML with the Sybase Adaptive Server SQL Databases

5.5.4. IBM

- Visual XML Tools: Bridging business applications with XML

5.5.5. SUN

- PORTABLE DATA/PORTABLE CODE: XML & JAVA TECHNOLOGIES

5.5.6. MICROSOFT

- Expanded XML Support in Internet Explorer 5
- Internet Explorer 5 and XML
- My XML, Your Browser

5.5.7. PEOPLESOFT

- PeopleSoft Launches PeopleSoft 8 today

5.5.8. SAP

- XML-Based Web Collaboration Technologies Enhance Flexibility, Openness of mySAP.com