1 – VERSION HISTORY

1.0b1 1/23/2004

[beta DRAFT: This is the first draft version of the initial release of the Retail Gas/Electric Quadrant-Specific Electronic Delivery Mechanism standard (RXQEDM)]

Style Definition: NAESB Section Title: Level 2

Style Definition: NAESB Para Title: None

Style Definition: NAESB Tab Title: Level 1, Space Before: 0 pt, After: 0 pt, Widow/Orphan control

Deleted: 2

Inserted: 2.0

Deleted: 12/31/2003

Deleted: Internet Electronic Transport (ET)

Inserted: Internet Electronic Transport (ET) standard

Deleted: ¶
¶

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

2 – INTRODUCTION

The North American Energy Standards Board (NAESB) is a voluntary non-profit organization comprised of members from all aspects of the greater gas and electric industries. The NAESB mission is to take the lead in developing and implementing standards across the industry to simplify and expand electronic communication, and to streamline business practices. The vision of NAESB is a seamless North American marketplace for energy, as recognized by its customers, the business community, industry participants and regulatory bodies.

NAESB Electronic Delivery Mechanism standards for the Retail Gas and Electric Quadrants are used by the Retail Electric Quadrant (REQ), and the Retail Gas Quadrant (RGQ) for electronic delivery of transactions and other information between trading partners.

Deleted: Internet Electronic Transport Standards

Deleted: Wholesale Gas Quadrant (WGQ),

Deleted: ,

Deleted: the electronic transport of

Deleted: payloads

NAESB recognizes that as the energy industry evolves and uses NAESB standards, additional and amended NAESB standards will be necessary. Any industry participant seeking additional or amended standards (including principles, definitions, standards, data elements, process descriptions, technical implementation instructions) should submit a request detailing the change to the NAESB office so that the appropriate process may take place to amend the standards.

TAB 1 Version Notes

Contains notes about this version, and, if appropriate, a brief summary of changes from the immediately preceding version.

TAB 2 Introduction

Provides a background statement about NAESB's Mission and the underlying concepts behind the design and use of this guide.

TAB 3 Executive Summary

Provides a brief outline of the industry business situation which is the basis for development of this guide.

TAB 4 Business Process & Practices

Provides a brief overview of the business process and the NAESB-approved principles, definitions and standards related to the business process covered by this guide.

TAB 5 Related Standards

Provides a reference to any related standards.

TAB 6 Technical Implementations

EDI/EDM and Batch FF/EDM

Provides an overview of the business process for Internet EDI/EDM and Batch FF/EDM.

INTERACTIVE FF/EDM

Provides an overview of the business process for Interactive FF/EDM.

TAB 7 Testing Guidelines

Formatted: Indent: Before: 0", First line: 0.5"

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

Provides guidelines for testing the EDM RXQEDMstandards.

Deleted:

TAB 8 Appendices

RXQEDMAppendix A – Reference Guide

Deleted: Table 1 –

Deleted: Error Codes¶

Appendix B – RXQ EDM FAQ

Appendix C – Sample RXQEDM Technical Exchange Worksheet (QTEW)

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

3 – EXECUTIVE SUMMARY

The North American Energy Standards Board (NAESB) Retail Electric Quadrant (REQ), and Retail Gas Quadrant (RGQ) have developed standards for electronic commerce over the Internet. The RGQ/REQ Electronic Delivery Mechanism (RXQEDM) standards enable the rapid, reliable, and safe transportation of electronic information between NAESB trading partners.

This document is a high-level guide to implementing various technologies necessary to communicate transactions and other electronic data using standard protocols. As such, this guide is not intended to be a comprehensive, in-depth manual. Where possible, this guide points to more in-depth material. The Reference section provides locations on the Internet to obtain more information as well as recommended books and periodicals.

Deleted: Wholesale Gas Quadrant (WGQ),

Deleted: Internet Electronic Transport

Comment:

BUSINESS REASONS FOR USING RGQ AND REQ ELECTRONIC DELIVERY MECHANISM

Energy companies need to exchange information and data with other energy companies. RXQEDM enables this with the following advantages:

RXQEDMStandardized Process. RXQEDM standardizes how packages are exchange, regardless of the business process, the trading partner, or the energy quadrant.

Deleted: Security.

Deleted: incorporates the PAIN security principles of Privacy, Authenticity, Integrity and Non-repudiation. ¶

Audit Trail. RXQEDM gives both Sender and Receiver a detailed audit trail, enabling better controls and less errors.

Error Notification. RXQEDM prescribes how errors are to be handled, and provides a foundation for efficient and quick resolution to errors.

Minimum technology requirements. RXQEDM is built on low-cost technology and readily-available Web browser and open source technology.

Interactive and Batch Capabilities. RXQEDM provides mechanisms for both fully-automated and manual-assisted business processes.

Any Payloads. RXQEDM can deliver any kind of payload, whether it is EDI, flat-files, XML, documents, etc.

Software Standards. The RXQEDM standards increase the likelihood that software vendors will provide Commercial Off-The-Shelf (COTS) software packages.

OVERVIEW OF ELECTRONIC TRANSPORT LIFE CYCLE

In the RXQEDM life-cycle, the party sending data, the “Sender”, creates an electronic package by encrypting the data payload and applying appropriate header ‘envelope’ information such as ‘to’ and ‘from’. This electronic package is submitted to the trading partner’s SSL Web server as an HTTP Request using the POST method.

The receiving party, the “Receiver”, receives and decrypts the package, then forwards the payload data to back-office processes. A Receipt is sent from the Receiver to the Sender with timestamps and any error notices. The Receiver back-office systems process the data

Deleted: receipt

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

according to NAESB Quadrant-specific Electronic Delivery Mechanisms (QEDM), Trading Partner Agreements, and related documents. If the Receiver decrypts in a separate process, the Receiver may send an Error Notification package to the Sender to identify errors found during decryption.

Trading partners can be either the Sender or Receiver depending on what information and data needs to be exchanged.

The RXQEDM standards focus on the transport of the electronic package and not the contents of the package. Each business process may define different contents, and the RXQEDM is designed to work with any type of contents (e.g. EDI, flat files, etc).

The following are RXQEDM life-cycle scenarios:

1. **Success**. The Successful scenario is when the electronic package was delivered with no errors, and the Sender has received a Receipt from the Receiver.
2. **Invalid Package Response**. The Invalid Package Response scenario is when the Receiver was unable to disassemble the electronic package, and has sent an HTTP Response to the Sender notifying them of package errors.
3. **Invalid Package Error Notification**. The Invalid Package Error Notification scenario is when a Receiver detects an error in the package AFTER the Response is sent. This scenario exists when a Receiver has implemented processes where the decryption occurs after the Response is sent. Decryption errors are communicated to the Sender via an HTTP Request using the RXQEDM Error Notification format.

Errors detected after successful decryption (e.g. format errors, EDI errors, etc) are beyond the scope of the RXQEDM, and can be found in the QEDM standards.

Parties implementing RXQEDM should become familiar with the following components of the RXQEDM:

- RXQEDM Network and Communications Requirements ??GB changed some headers
- Sending RXQEDM Electronic Packages
- Receiving RXQEDM Electronic Packages
- Security

[??LS Waiting on final EC disposition of AS2 issues.

Deleted: Protocols

Deleted: Secure

Deleted: Secure

Formatted: Bullets and Numbering

Deleted: ; refer to EC;

Inserted: ; refer to EC;

KEY ASSUMPTIONS

This document makes the following assumptions:

- **Platform Independence.** An RXQEDM implementation can communicate with all trading partners in the energy industry, regardless what hardware, operating system and programming languages trading partners use.
- **Open Standards.** NAESB has adopted open standard technologies to provide flexibility and scalability.
- **Importance of the Technical Exchange Worksheet (TEW)**. RXQEDM relies on the exchange of technical information between trading partners to establish and maintain

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

reliable RXQEDM production. Additional requirements and information may be required. The information in the RXQEDM TEW complements the information contained in the Internet ET TEW. A sample TEW is included in Appendix C??. The TEW may be a part of a Trading Partner Agreement (TPA).

- **Testing With RXQEDM Trading Partners.** Since the RXQEDM is not platform-specific, testing with other trading partners on a variety of platforms is very important in ensuring that each RXQEDM application is compatible with a range of platforms used by various trading partners.
- **Lack of Internet Quality of Service (QoS).** Implementers of RXQEDM should be aware that the Internet lacks QoS. High-priority RXQEDM package transfers such as Bill-Ready Usage and Invoices have no priority over low-priority transfers such as music MP3 files. Business processes that have firm or tight transfer timing requirements should be constructed to properly mitigate the risk associated with this lack of guaranteed QoS on the Internet. QoS may be improved by using a private network in lieu of the Internet.

Further Information

[Is it current?do we need this?]Please see the NAESB home page at http://www.naesb.org/ for additional useful information on the implementation of RXQEDM.

Deleted: This worksheet is intended to establish communications between two parties.

Deleted: Refer to your quadrant-specific EDM (QEDM).

Deleted: Testing should ensure receipt of the package, proper decryption, and appropriate receipts were sent.

Deleted: Internet

Deleted: of

Deleted: files

Deleted: (e.g.

Deleted: song

Deleted: '

Deleted:) have equal access to Internet bandwidth as high-priority files (e.g. Nominations)

Deleted: RXQEDM

Deleted: e

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

4 – BUSINESS PROCESS AND PRACTICES

A. OVERVIEW

Role of EDM in NAESB REQ, and RGQ Quadrants

Many business processes defined by the retail NAESB Quadrants (RGQ, REQ) require the exchange of transactions and transaction data. The RXQEDM, in concert with the Internet ET, enables NAESB parties to securely and reliably exchange transactions over the Internet. RXQEDM electronic 'packages' are created using the standards defined in this document.

Version 1.0 of the RXQEDM standard incorporates many of the EDM standards found in the NAESB WGQ EDM v1.7.

Roles in RXQEDM

In the RXQEDM life-cycle, one party sends a package, and the other party receives the package. The party sending the package is also referred to as the Client, and the party receiving the package is also referred to as the Server.

NAESB business processes often require that parties act in both the Sender and Receiver roles. For example, once the Receiver of a payload file of Bill-ready Usage has successfully processed the payload, they switch to the Sender role to send Invoices back to the original Sender. RXQEDM implementations need to implement both Sender and Receiver capabilities.

The standards adopted for RXQEDM should be adhered to by the trading parties as minimum standards. A trading party may offer additional functions or features as options but should not require their use. Such additional features or functions are termed "mutually agreed to". If both trading partners agree on the inclusion, the additional feature requirements will be met. If either trading party does not agree to the inclusion of additional features, then the partners must allow for transmission and receipt of data using the minimum standards.

To establish an RXQEDM trading partnership with another company, a company needs to exchange technical information about their RXQEDM implementation. This may include:

- Contact information
- Common Code Identifiers (e.g. DUNS number)

This may be exchanged using a Technical Exchange Worksheet (TEW). A sample TEW is in Appendix C??. In some cases, this information may be exchanged with a Trading Partner Agreement.

Implementation Approaches

The NAESB RXQEDM can be constructed using any IT deployment model, including the use of in-house development, consulting/development help from a third-party, Commercial Off-The-Shelf (COTS) software, or an outsourced solution with a third-party. The best solution for each organization must be determined based on the assessment of specific needs and the resources available to that organization.

All parties should fully investigate the ramifications of implementing electronic commerce using the Internet. This includes ensuring that all customer data, internal data, and applications are

Deleted: Internet Electronic Transport (ET) in

Deleted: WGQ.

Deleted: B

Deleted: Quadrant-specific Electronic Delivery Mechanisms (QEDMs)

Deleted: all technical specifications of the NAESB WGQ EDM Version 1.6, including mutually-agreeable business practices to protect the sender of a document with non-repudiation and with digitally-signed Error Notifications.

Deleted: sender

Deleted: receiver as the

Deleted: Nominations

Deleted: an

Deleted: acknowledgement

Deleted: may

Deleted: c

Deleted: <#>public keys, including key exchange and update policies¶ <#>test URLs¶ <#>production URLs, including alternative paths if available¶

Deleted: <#>Use of 'time-c-qualifier' if in REQ or RGQ¶

Deleted: using

Deleted: using

Deleted: using

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

secured from intruders or other unauthorized parties.

Deleted: not authorized for access

Deleted:

Participation in electronic commerce over the Internet involves hardware, software, and technical expertise. Hardware requirements may include a server to receive incoming RXQEDM packages and a firewall to block intruder access. Software includes operating software for the servers, including the firewall, programming languages which support Internet technologies, and encryption/decryption software to provide security during the transfer. Technical expertise may be involved in the development and maintenance of server applications to process incoming files as well as applications to initiate communication with the server of your trading partner.

Third-party providers offer a variety of services from a full "turn key" solution to assistance where you require it, including programming, system configuration, system administration and private communication links. Criteria for selecting an outsourced RXQEDM service provider should consider their ability and experience with RXQEDM standards for HTTP Request and Response validation and processing.

Formatted: NAESB Para Title, Space Before: 0 pt

Internet ET Communications

The default electronic transport and communications protocol for exchanging electronic information is the NAESB Internet ET.

Deleted: Secure

Sending RXQEDM Packages

??translators

Receiving RXQEDM Packages

??Translators

??Acknowledgements/997

-

B. GENERAL STANDARDS

Principles:

0.1.1 An entity is a person or organization with sufficient legal standing to enter into a contract or arrangement with another such person or organization (as such legal standing may be determined by those parties) for the purpose of conducting and/or coordinating energy transactions.

0.1.2 There should be a unique entity common code for each entity name and there should be a unique entity name for each entity common code.

Standards:

0.3.1 Entity common codes should be "legal entities", that is, Ultimate Location, Headquarters Location, and/or Single Location (in Dun & Bradstreet Corporation ("D&B") terms). However, in the following situations, a Branch Location (in D&B terms) can also be an entity common code:

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

1. when contracting party provides a D-U-N-S®[1] Number at the Branch Location level;

OR

2. to accommodate accounting for an entity that is identified at the Branch Location level.

Deleted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Inserted: 2/25/2004

Deleted: 1/23/2004

1 D-U-N-S® is a registered trademark of Dun & Bradstreet, Inc.

C. QUADRANT ELECTRONIC DELIVERY MECHANISM RELATED STANDARDS

Principles:

[11].1.1 The RXQEDM does not pick winners, rather it should create an environment where the marketplace can dictate a winner or winners (4.1.2)

[11].1.2 The solutions should be cost effective, simple and economical (4.1.3)

[11].1.3 The solutions should provide for a seamless marketplace for energy (4.1.4).

[11].1.4 Parties should interface with third-party vendors according to RXQEDM standards (4.1.6).

[11].1.5 Electronic communications between parties to the transaction should be done on a non-discriminatory basis, whether through an agent or directly with any party to the transaction (4.1.7).

[11].1.6 Protocols and tools that parties elect to support should be "Internet-compatible" (4.1.12).

[11].1.7 The industry should use standard policies and guidelines for testing (4.1.14).

[11].1.10 Trading Partners should mutually select and use a version of the NAESB RXQEDM standards under which to operate, unless specified otherwise by government agencies. Trading Partners should also mutually agree to adopt later versions of RXQEDM standards as needed, unless specified otherwise by government agencies (4.1.39).

B2,B3:[11].1.x9 Service providers should post clear and precise business processing rules at the designated site, or in writing, upon request.

B2/3: [11].1.x10 There should be at least one standard computer-to-computer exchange of transactional data for each defined transaction data exchange format.

B2/3:[11].1.34 For RXQEDM FF/EDM, the content and usage of flat files should reasonably correspond to the RXQEDM data sets used for RXQEDM EDI/EDM.

B2/3:[11].1.35 If RXQEDM FF/EDM is implemented, flat files should be exchanged via the RXQEDM EDI/EDM.

Definitions:

[11].2.1 "RXQEDM Testing". Testing electronic delivery between trading partners includes testing of: A) Connectivity; B) Encryption/Decryption; and C) Digital signatures where appropriate (4.2.20).

[11].2.3 "Trading Partner" is a party that enters into an agreement with another party to transact business electronically using the RXQEDM standard (4.2.22x).

[11].2.4 "Originating party" is any party originating/creating an RXQEDM package. This could be a third-party (4.2.23x).

[11].2.5 "Third-Party" is any organization that a trading party uses to provide services to comply

Deleted: INTERNET

Deleted: TRANSPORT

Deleted: Internet Electronic Transport (ET)

Deleted: NAESB

Deleted: [11].1.8 The NAESB RXQEDM should not set standards for site-level security. Individual organization security standards should be relied upon (4.1.15).¶

[11].1.9 Trading partners should maintain redundant connections to the public Internet for NAESB RXQEDM Web sites. These redundant connections should be topographically diverse (duality of) paths to minimize the probability of a single point of failure (4.1.36).¶

Deleted: RXQEDM

Deleted: the NAESB

Deleted: ,

Formatted

Formatted: NAESB Para Default, Indent: Before: 0", Hanging: 0.63"

Formatted

Formatted

Deleted: ¶

Deleted: packages

Deleted: [11].2.2 "Fail-over" defines a prescribed process executed when a NAESB RXQEDM Client fails to establish a connection to the target NAESB RXQEDM Server. (4.2.21x)¶

Deleted: the

Deleted: also include

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

with the required elements of the RXQEDM (4.2.24x).

[11].2.6 "Receiving Party" is any party that hosts (either in-house or outsourced) an RXQEDM compliant server capable of receiving RXQEDM packages (4.2.25x).

[11].2.6 "Translator" is a program or set of programs that processes the contents of an RXQEDM package. The Translator is responsible for ??.

[11].2.7 "Trading Partner Agreement", or "TPA" is a legal agreement between trading parties. The TPA often dictates service level agreements and problem remediation processes. The TPA may include technical exchange information such as URLs, etc. (4.2.26x)

[11].2.11 "COTS". Commercial Off-The-Shelf; software that can be purchased and that requires little or no customization.

[11].2.12 "Electronic Package". A data stream sent using the NAESB Internet ET protocols.

[11].2.13 "??Error Notification". RXQEDMError Notification is a package sent from the Receiver of the original data to the Sender when errors are trapped after the RXQEDM Receipt is sent. This is normally used for decryption errors detected after the RXQEDM Receipt has been sent.

[11].2.17 "IETF". Internet Engineering Task Force; a body of technical experts that set standards, known as Requests for Comments (RFC) for the Internet.

[11].2.19 "Internet EDM". The GISB and NAESB WGQ standards up to and including Version 1.7. The "RXQEDM" and "QEDM" standards were derived from these EDM standards.

[11].2.20 "RXQEDM" is the Electric Delivery Mechanism standards for the Retail NAESB Quadrants RGQ and REQ.

[11].2.21 "Payload Files". The data contents inside of an Internet ET electronic package.

[11].2.22 "Protocol Failure". A protocol failure occurs any time a sending party's NAESB RXQEDM server cannot connect to the receiving party's NAESB RXQEDM server. For example, if a server tries to connect to a server and fails, or tries to post a file and fails, this is a protocol failure.

[11].2.23 "Exchange Failure". An exchange failure is when a sending party's NAESB RXQEDM server has had continual protocol failures over a thirty-minute period. Each party is required to try at least 3 times over the thirty-minute minimum/two-hour maximum period before flagging an exchange failure.

[11].2.24 "QEDM". Quadrant-specific Electronic Delivery Mechanism; the set of standards for each NAESB quadrant that define the EDM standards for EDI, flat-files, electronic bulletin boards, and other technologies. The QEDM excludes electronic transport practices and standards. The QEDMs were derived from the GISB and NAESB WGQ Internet EDM standards.

[11].2.25 "??Receipt". The HTTP Response sent from the Receiver to the Sender that includes the 'gisb-acknowledge-receipt' section with a timestamp and OK/error status.??Should this be 'ET Receipt' to differentiate from other receipts?

[11].2.26 "Receiver". The party that receives an RXQEDM Electronic Package.

[11].2.27 "Sender". The party that sends an RXQEDM Electronic Package.

[11].2.28 "QoS". Quality of Service; term used to define what level of network bandwidth is guaranteed or assured. The Internet does not offer guaranteed quality of service.

Deleted: Receiving Program

Deleted: HTTP Requests from a Sender.

Deleted: Receiving Program

Deleted: generating the "gisb-acknowledge-receipt", which includes any party that hosts (either in-house or outsourced) an RXQEDM compliant server capable of receiving RXQEDM packages (4.2.25x).

Deleted: [11].2.8 "Batch Browser". A Browser that can be run with little or no manual operation or intervention. See "Browser".¶

Deleted: [11].2.9 "Browser". A software program capable of generating HTTP Requests, including HTTP POST requests.¶

Deleted: [11].2.10 "Client". The computer hardware and software used by the Sender to transmit an Electronic Package to the Receiver's Server. A Client can be fully-automated or manual.¶

Deleted: via HTTP POST that contains envelope header information and Payload File(s). The Payload Files are encrypted using defined RXQEDM encryption techniques.

Deleted: [11].2.14 "HTTP Request". The stream of data sent from the Client to the Server that includes header information and payload data.¶

[11].2.15 "HTTP Response". The stream of data sent from the Server to the Client in response to an HTTP Request, and includes the Receipt.¶

[11].2.16 "HTTP Server". The computer hardware and softwa ... [1]

Deleted: [11].2.18 "Interactive Browser". A Browser that requ ... [2]

Deleted: or "

Deleted: Internet Electronic Transport"RXQEDM. The NAE ... [3]

Deleted: NAESB RXQEDM is content-independent.

Deleted: RXQEDM

Deleted: e

Deleted: p

Inserted: 2/25/2004

Formatted ... [4]

Deleted: 2/25/2004

Deleted: 1/23/2004

[11].2.29 "Technical Exchange Worksheet" or "TEW". A document or worksheet used to communicate important information related to the technical implementation of RXQEDM; includes information such as ??ISA/GS, etc

B2/3/4:[11].2.x11 "EDI/EDM" is the term used to describe ANSI ASC X12 computer-to-computer electronic data interchange of information in files as mapped from the x.4.z RXQ standards in the NAESB RXQ Implementation Guides and communicated between trading partners over the Internet using the NAESB Internet ET.

B2/3/4:[11].2.x12 "FF/EDM" is the term used to describe a standardized flat-file electronic data interchange of information in files as mapped from the x.4.z RXQ standards. FF/EDM is communicated between trading partners over the Internet using the NAESB Internet ET.

B2/3/4:[11].2.x18 "Batch Flat File" is the term used within the FF/EDM to describe the automated computer-to-computer transfer of flat files.

B2/3/4:[11].2.x19 "Interactive Flat File" is the term used within the FF/EDM to describe the transfer of flat files using an interactive browser.

B2/3/4:[11].2.x20 Testing data sets between trading partners includes testing of:

1. intended business results,
2. proposed electronic delivery mechanisms, and
3. related EDI/EDM and, where supported, FF/EDM implementation issues.

Testing should include enveloping, security, data validity, and standards compliance (e.g. ANSI X12 and NAESB RXQ Related Standards).

Standards:

[11].3.1 All parties sending and receiving data should accept a TCP/IP connection (4.3.1x).

[11].3.x2 On time stamping, data leaves control of the originator by the same time (deadline), regardless of mechanism (3rd party service provider time stamp is acceptable) and 15 minutes of communication time should be available to allow accumulation of all transactions to the pipeline. A standard network protocol (TCP/IP) should be in service for direct connect to the pipeline designated site.

[11].3.2 Trading partners should retain audit trail data for at least 24 months. This data retention requirement does not otherwise modify statutory, regulatory, or contractual record retention requirements (4.3.4).

[11].3.5 The Internet ET timestamp in the "gisb-acknowledgement-receipt" designates the time a file is received at the Receiver's designated site. The timestamp consists of the "time-c" data element, and in some cases the "time-c-qualifier" data element.

[11].3.x RGQ and REQ require the use of the "time-c-qualifier" data element to identify the time-zone of the Receiver's timestamp. (4.3.9)

[11].3.6 The Receiver generates a timestamp upon the successful receipt of a complete file. The timestamp should be generated by the Receiving Program immediately, prior to further processing by the Receiving Program.

Deleted: URLs, contacts and Public Key policies.

Deleted: [11].2.30 "TCP". Transmission Control Protocol; IETF RFCs 793, 1122, 1323¶

See "http://www.itprc.com/tcpipfaq/default.htm"¶

[11].2.31 "RSA". A mathematical algorithm for encryption developed by Rivest/Shamir/Adleman. See http://world.std.com/~franl/crypto/rsa-guts.html.¶

[11].2.32 "SSL". Secure Sockets Layer; a privacy technique that uses encryption to hide information from electronic observers on the Internet.¶

See "http://developer.netscape.com/docs/manuals/security/sslin/contents.htm"¶

[11].2.33 "PGP". Pretty Good Privacy; software used to create Public and Private Keys for privacy and digital signature applications; see http://www.uk.pgp.net/pgpnet/pgp-faq/¶

[11].2.34 "Private Key". The sequence of digits known as a 'key' that is kept private by the owner of a digital certificate, and is used by the certificate owner in encryption and decryption algorithms.¶

[11].2.35 "Public Key". The sequence of digits known as a 'key' that an owner of a digital certificate shares with trading partners. T ... [5]

Formatted: Bullets and Numbering

Deleted: [11].3.3 At a minimum, the designated RXQEDM Server/Receiver site should be accessible via the public Internet. This specifically does not precl ... [6]

Deleted: [11].3.4 The minimum acceptable protocol should be HTTP. All sending and receiving parties should be capable of sending and receiving the HTTP versions ... [7]

Deleted: A

Deleted: Refer to QEDM standards for use of the

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

[11].3.7 After timestamp generation, the Receiver and sends an immediate HTTP Response to the Sender. The "gisb-acknowledgement-receipt", which includes the timestamp data element(s), is the primary part of the HTTP Response. (4.3.9)

[11].3.8 The Server clock generating the timestamp should be synchronized with the National Institute of Standards and Technology (NIST) time in order to mitigate discrepancies between the clocks of the Sender and Receiver. Computer clocks should be synchronized as necessary to ensure at minimum +/- 20 second synchronization with an atomic clock. Specific business processes may have tighter synchronization requirements. (4.3.10x).

[11].3.12 A failure to complete a unit of work is a protocol failure.

[11].3.13 Three protocol failures within a 30-minute timeframe is an exchange failure.

[11].3.x RXQEDM relies on the NAESB Internet ET to enforce the privacy, authentication, integrity, and non-repudation (PAIN) security principles.

[11].3.19 Internet protocols should be used for accessing all industry business functions. (4.3.36)

[11].3.x45 NAESB RGQ/REQ standard code value descriptions should be displayed for code values where appropriate. (4.3.45)

[11].3.x47 Where they exist for the same business function, flat-files, EDI and web pages should use the same nomenclature for data set names, data element names, code values and/or code value descriptions, abbreviations and message text. (4.3.47)

[11].3.21 Trading partners should use common codes for legal entities for RXQEDM envelope data elements. (4.3.56x)

[11].3.67 A Party that desires to provide services that do not exist using existing transaction sets should, prior to implementation, submit a request for standardization to NAESB RXQEDM, including applicable descriptions of the EDI/EDM and FF/EDM implementation. (4.3.67)

[11].3.80 FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means:
Rows are separated by a carriage return/line feed (CRLF).
Fields are separated by commas.
When a field contains a comma, the field should be enclosed by double-quotes.
Double-quotes should not be used within any data field.
When numeric data is negative, the minus sign should precede the number.
When numeric data contains decimal precision, the decimal point should be included within the field.
When numeric data contains one or more significant leading zeros, these zeros should be preserved in the flat file.
Date fields should be formatted as YYYYMMDD.
Time fields should be specified in a 24 hour format, formatted as HH:MM or HH:MM:SS, as applicable.

Deleted: .

Deleted: [11].3.9 The HTTP Response should be sent to the Internet Protocol (IP) address of the HTTP Request (4.3.11x).¶

Deleted: [11].3.10 At a minimum, one designated site for receipt should be identified for each trading partner. That site should be identified by a specific Uniform Resource Locator (URL). This does not preclude multiple designated sites being mutually agreed to between trading partners (4.3.12).¶

Deleted: [11].3.11 The Sender should make three attempts to complete a unit of work. A unit of work consists of one complete HTTP POST transaction as defined in the technical specification of the HTTP protocol (IETF RFC 1945). (4.3.13).¶

Deleted: [11].3.14 The RXQEDM roles for Sender and Receiver are defined in the following table. The entire table defines a unit of work:

Deleted: Client (Sender) ... [8]

Deleted: [11].3.15 Trading partners should implement all security features (privacy, secure authentication, integrity, and non-repudiation) using a file-based approach via a commercially-available implementation of PGP 6.5 or greater (or compatible with PGP 6.5) or, on a mutually agreed basis, an OpenPGP compatible product. (4.3.15)¶

Deleted: [11].3.16 Trading partners should implement basic authentication.¶

[11].3.17 Encryption keys should be self-certified. The exchange of ... [9]

Deleted: [11].3.20 Batch and Interactive Browsers should use Internet-compatible common l ... [10]

Deleted: the

Deleted: "to" and "from"

Deleted: ¶

Deleted: [11].3.22 Private network connections to NAESB RXQEDM servers, which include all NAE ... [11]

Inserted: 2/25/2004

Formatted ... [12]

Deleted: 2/25/2004

Deleted: 1/23/2004

Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one NAESB REQ/RGQ data element. Note that there should be exactly one space between the day (DD) and the hour (HH).

The maximum amount of data to be placed in a field should be limited to 256 characters.

When a field contains no data, the empty field should result in two delimiters next to each other. Note that there should be no blank spaces between the delimiters.

(WGQ EDM Cross reference 4.3.80)

[11].3.x81 The first row of an FF/EDM flat-file should be the standard abbreviations for RXQ data elements in the order the corresponding data appears in subsequent rows. The data element order is at the option of the sender. If a data element abbreviation is not recognized, the entire flat-file should be rejected. (WGQ EDM cross-reference 4.3.81)

[11].3.x82 For FF/EDM flat-files, each transaction (e.g. Enrollment) should be contained in a single row. (WGQ EDM cross-reference 4.3.82)

[11].3.x83 ??when Internet ET is not used, For Interactive Flat File EDM, 128-bit Secure Sockets Layer (SSL) encryption should be used. (WGQ EDM cross-reference 4.3.83)

[11].3.86 To the extent that multiple electronic delivery mechanisms are used (e.g. EDI or flat-files), the same business result should occur. (WGQ EDM cross-reference 4.3.86)

[11].3.87 When a party changes the business rule(s) it will apply to documents, it should notify its trading partners at least two weeks in advance of the change(s). The notification should include identification of the data element(s) that are changing, the intended business result of such change(s) in the business rule(s), and the effective date of such change(s). For the purposes of this standard, a business rule change is any change in: A) the presence and/or the acceptable content of a data element sent by the changing party, B) a new business response to an accepted data element received by the changing party; C) a new business response to the acceptable content of a data element received by the changing party; D) a new intended business result. (WGQ EDM cross-reference 4.3.87)

[11].3.x Absent mutual agreement between the affected trading partners to the contrary, trading partners notifying their sending or receiving trading partners of a change(s) under Standard [11].3.87 should provide the means to test such change(s) during at least a two week time period prior to the effective date of the change(s). (WGQ EDM cross-reference 4.3.87)

[11].3.x Trading partners receiving notice of change(s) from a trading partner should be prepared not to implement such change(s) even after testing has been completed, as the notifying trading partner is permitted to cancel or postpone such change(s). Notifying trading partners canceling or postponing the effective date of change(s) should provide affected trading partners with notice of cancellation or postponement at least one business day prior to the applicable effective date. (WGQ EDM cross-reference 4.3.87)

Formatted: GISB Default Para Indent, Indent: Before: 0", Hanging: 0.63"

Formatted: Normal

Formatted: Indent: Before: 0", Hanging: 0.63"

Formatted: Normal

Formatted: GISB Default Para Indent, Indent: Before: 0", Hanging: 0.63"

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

D. INTERPRETATIONS

NAESB has no interpretations of standards that relate to RXQEDM implementation.

Deleted: [11].3.25 RXQEDM128-bit Secure Socket Layer (SSL) encryption should be used for RXQEDM. (4.3.88)¶

Formatted: NAESB Section Title

Deleted: ¶

Formatted: NAESB Para Default

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

5 – RELATED STANDARDS

COMMON CODES

RXQEDM uses the D-U-N-S® Number as the common company identifier for the HTTP Request and Response data dictionary 'to' and 'from' HTTP header elements. The D-U-N-S® Number is a 9-digit number assigned to companies by the Dun & Bradstreet Corporation (D&B). The D-U-N-S+4® Number is a 10- to 13-digit number, where characters 10 through 13 are arbitrarily assigned by the owner of the D-U-N-S® Number.

For RXQEDM Common Code purposes, an entity will use one and only one D-U-N-S® Number. Entity common codes should be "legal entities," that is, Ultimate Location, Headquarters Location, and/or Single Location (in D&B terms). However, in the following situations, a Branch Location (in D&B terms) can also be an entity common code:

1. When the contracting party provides a D-U-N-S® Number at the Branch Location level.
2. To accommodate accounting for an entity that is identified at the Branch Location level.

Since D&B offers customers the option of carrying more than one D-U-N-S® Number per entity, please refer to NAESB's Web Page at www.naesb.org for directions on determining the one and only one D-U-N-S® Number constituting the NAESB RXQEDM Entity Common Code.

Common Codes

For NAESB REQ/RGQ Common Code purposes, an entity will use one and only one D-U-N-S® Number. Entity common codes should be "legal entities," that is, Ultimate Location, Headquarters Location, and/or Single Location (in Dun & Bradstreet Corporation ("D&B") terms). However, in the following situations, a Branch Location (in D&B terms) can also be an entity common code: 1. When the contracting party provides a D-U-N-S® Number at the Branch Location level; or 2. to accommodate accounting for an entity that is identified at the Branch Location level. Since D&B offers customers the option of carrying more than one D-U-N-S® Number per entity, please refer to NAESB's Web Page at www.naesb.org for directions on determining the one and only one D-U-N-S® Number constituting the NAESB WGQ Entity Common Code.

In the datasets, an asterisk by a data element means that it is a "common code," so the field will reflect the industry-supported common code for location or company.

INTERNET ELECTRONIC TRANSPORT (ET)

In NAESB business processes, the RXQEDM standards are used in conjunction with the Internet ET standards. ??more?

PARTY ROLES

Various types of parties are involved in NAESB business processes and the use of RXQEDM, including distribution companies, end-users, regulatory entities, service providers, and suppliers.

Formatted: NAESB Section Title

Deleted: ¶

Formatted: NAESB Section Title

Formatted: Normal

Formatted: NAESB Section Title

Deleted: I

Deleted: all of the transaction sets, there are multiple parties that may be involved in the transaction

Deleted: . There are

Deleted: (OPEN ISSUE 022)

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

NAESB REQ/RGQ ELECTRONIC DATA INTERCHANGE TRADING PARTNER AGREEMENT

Formatted: NAESB Section Title

In 1998, GISB adopted Standard 6.3.3, the NAESB WGQ Electronic Data Interchange Trading Partner Agreement (TPA) for exchange of data within the gas industry. The NAESB WGQ TPA defines the relationship of the sender and receiver of NAESB WGQ Standard ASC X12 documents. This agreement represents a complete set of balanced terms which a company should accept whether it is sender or receiver of electronic documents. It has established all the data items necessary to exchange electronic documents in a step by step, fill in the blank model form. The use of the TPA minimizes preparation, negotiation and review time. This will allow more time for implementation of electronic commerce. Copies of this agreement may be obtained from the NAESB office or may be downloaded from the NAESB home page at www.naesb.org.

Party Roles

In all of the transaction sets, there are multiple parties that may be involved in the transaction. There are the Transportation Service Provider (a.k.a. Pipeline or Transporter), the Service Requester (a.k.a. Shipper), Service Requester Agent (a.k.a. Shipper's Agent) and Third Party Service Provider (a.k.a. Third Party Agent). It is important to distinguish between the role of the Service Requester Agent and the Third Party Service Provider.

The Service Requester Agent is the party contractually authorized by the Service Requester to submit business transactions to the Transportation Service Provider on behalf of the Service Requester for a service requester contract. Once the Service Requester Agent is contractually authorized, the agent becomes the Service Requester for subsequent business transactions unless and until the agency relationship is terminated.

The Third Party Service Provider is the communications agent that the Service Requester or Service Requester Agent may subscribe to in order to send and receive transactions with the Transportation Service Provider.

It is possible that a single entity may, at times, provide the role of a Service Requester Agent for one party while providing the role of Third Party Service Provider for another party. Likewise, a single entity could be both Service Requester Agent and Third Party Service Provider for a single party.

In EDI implementation, the party that is authorized to send and receive transactions will be the party identified in the transmission envelope (ISA Header Segment). If the sending party is a Service Requester, Service Requester Agent or Third Party Service Provider, their appropriate identifiers will appear here. In all cases, the Transportation Service Provider, Service Requester and Service Requester Agent (if applicable) will be identified in the body of the transaction (N1 Name Segment).

HYPERTEXT TRANSFER PROTOCOL (HTTP)

Formatted: NAESB Section Title

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

The Hypertext Transfer Protocol (HTTP) is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. It is a generic, stateless, object-oriented protocol which can be used for many tasks, such as name servers and distributed object management systems, through extension of its request methods

(commands). A feature of HTTP is the typing of data representation, allowing systems to be built independently of the data being transferred.

HTTP has been in use by the World-Wide Web global information initiative since 1990. Appendix A?? of the Electronic Delivery Mechanism Related Standards manual contains a listing of the HTTP version(s) supported by NAESB WGQ.

Formatted: NAESB Para Title

HTTP transaction-set Code Values

The following table contains a list of code values to be used with the transaction-set data element, which is a mutually agreeable (MA) data element in the HTTP Request.

HTTP transaction-set Code Values	NAESB RxQ Standard Number	Transaction Set Description

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

6 – TECHNICAL IMPLEMENTATION - RXQEDM

EDI/EDM

The EDI/EDM uses the following technologies and components to securely and reliably transport electronic packages to trading partners:

- X12??

Deleted: NAESB RXQEDM

Deleted: <#>TCP/IP and HTTP POST. RXQEDM uses a specifically-structured HTTP POST to transport payload data from one trading partner to the other.¶
<#>Mime multi-part encoding. RXQEDM package structure requires that each section of the package be encoded. ¶
<#>A "Browser", running at the Sender's site as Client software. This software is referred to in this document as "Client".¶
<#>A "Server" running at the Receiver's site, usually on a dedicated computer. This is a Web or HTTP server, and is referred to in this document as "Server".¶

Formatted: NAESB Para Title

ANSI ASC X12 Standards

The NAESB WGQ standards reflect industry use of the American National Standards Institute (ANSI) ASC X12 standards maintained by the Data Interchange Standards Association, Inc. (DISA). The technical implementation documents included in this manual reflect the NAESB WGQ subset of the ANSI ASC X12 standards versions. It is recommended that any industry participant who wishes to utilize the ANSI ASC X12 standards should also have a copy of the ANSI ASC X12 Standards Reference document for a full understanding of the X12 requirements. NAESB members may purchase an ANSI reference document through NAESB by contacting the NAESB office. Non-NAESB industry participants may purchase the reference document by contacting:

Manager of Publications
DISA
333 John Carlyle Street, Suite 600
Alexandria, VA 22314
Voice: 703-548-7005
Fax: 703-548-5738
www.disa.org

As a member of ANSI, NAESB WGQ will utilize the ANSI ASC X12 standards and remain in full compliance. In all standards, occasions arise where the standard does not fully meet a need. NAESB WGQ recognizes this and will add interim usages and code values when required. When NAESB WGQ utilizes an interim solution, NAESB WGQ will apply to ANSI and the appropriate ANSI organizations for acceptance of the interim solution. ANSI's final solution may provide a usage or code value different than the interim solution. NAESB WGQ standards will be updated to reflect the final solution.

The architecture of ASC X12 is designed for end to end communications. The translator that generates the ASC X12 file and envelope will assign control numbers and counts that will appear within the ISA/IEA segments of the transaction and within the GS/GE segments of the transaction. These numbers and counts allow the translator to ensure that all of the segments in an envelope and all of the data elements in an envelope have been received and that the transmission was complete.

ISA contents

The ISA segment marks the beginning of an X12 document. It can be equated to an envelope that a paper document would come in via the mail. The envelope may contain one or more functional groups (defined by the GS segment) and one or more transaction sets.

The ISA is the interchange control segment to be utilized on all NAESB WGQ X12 standards. The segment identifies the sender and receiver of the document. The Interchange Sender

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

ID/Interchange Receiver ID is published by both the sender and receiver for other parties to use as the sender/receiver ID to route data to them. The sender must always code the sender's ID in the sender element and the designated receiver's ID in the receiver ID. Trading partners utilizing a password for their documents will use the Security Information element. The receiver of the document identifies a password for the sender to include in this element. This sender and receiver information is specified in the NAESB WGQ Electronic Data Interchange Trading Partner Agreement.

There are additional elements in the ISA segment. These elements are traditionally assigned by the sending party's translator. These elements inform the receiver of the date/time that the envelope was generated, the X12 version number being utilized, whether the transmission is for test or production purposes, and what characters were used to designate the end of a sub element, element or segment. Different characters must be chosen for the sub element, element and segment delimiters. These delimiting characters must never appear in the data.

For more information on the ISA segment and the possible values for its elements, contact DISA at the above address or consult the appropriate version of the ANSI ASC X12 Standards Reference document corresponding to the NAESB WGQ transaction set being sent/received. Information about control segments (including the ISA and IEA) can be found in the Overview/Introduction and Control Standards sections of the reference document. Specific information about the ISA and IEA segments and corresponding elements can be found in the Segment Directory and Data Element Dictionary sections.

GS contents

The GS segment indicates the beginning of a functional group and provides control information for the data that follows it. A functional group can be defined as a group of transactions related to one business application. Within a mailing envelope, there may be a bundle of information relating to imbalances and a bundle of information relating to measurement information. Each of these 'bundles' is sent within its own (or a separate) GS Functional Group Header and a GE Functional Group Trailer in the X12 environment. The sender of a transmission provides the Application Sender's Code that the receiver of the transmission will reflect back on acknowledging documents. The receiver of a transmission provides the Application Receiver's Code that the sender will include in the transmission for the receiver to utilize in routing to internal applications. Group Control Numbers are originated and maintained by the sender of the document.

For more information on the GS segment and the possible values for its elements, contact DISA at the above address or consult the appropriate version of the ANSI ASC X12 Standards Reference document corresponding to the NAESB WGQ transaction set being sent/received. Information about control segments (including the GS and GE) can be found in the Overview/Introduction and Control Standards sections of the reference document. Specific information about the GS and GE segments and corresponding elements can be found in the Segment Directory and Data Element Dictionary sections.

997 Usage

The 997 Functional Acknowledgment is used to indicate the results of the syntactical analysis of the X12 documents. The documents include the transaction sets and functional groups with an ISA/IEA envelope. This standard covers all of the X12 and NAESB WGQ standard criteria that the receiver of the document has incorporated into the receiver's translator. The translator may be set to accept all information into the receiver's application processing, it may be set to accept

Deleted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Inserted: 2/25/2004

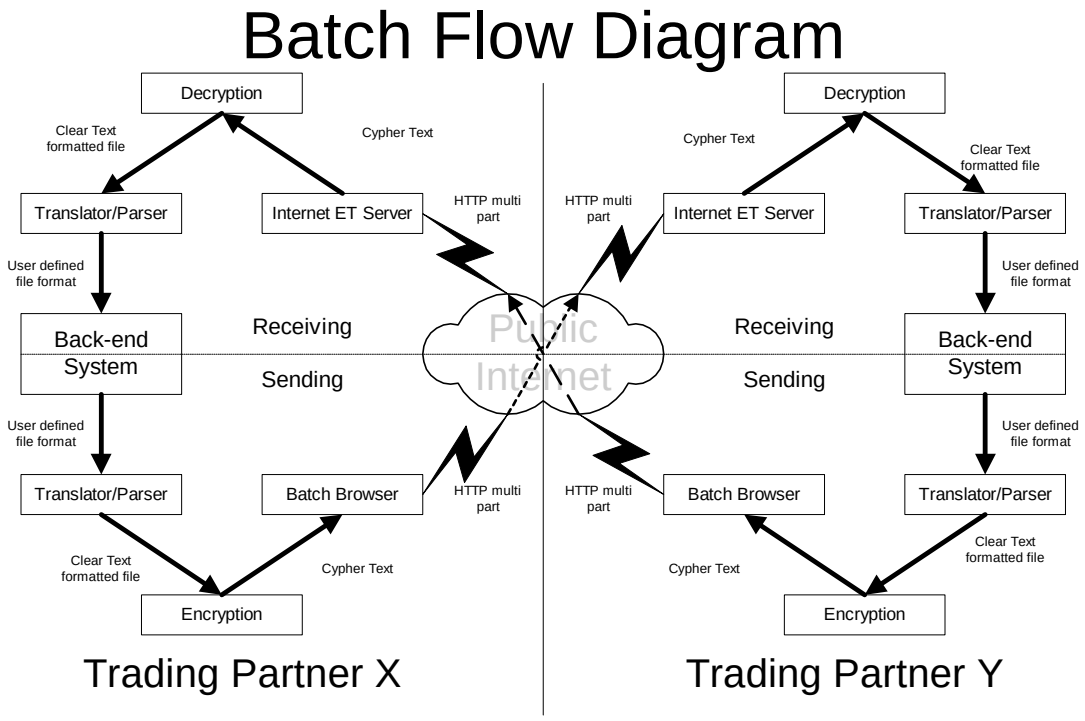
Deleted: 1/23/2004

only ANSI ASC X12 compliant information into the receiver's application processing, or it may be set to accept only ANSI ASC X12 and NAESB WGQ compliant information into the receiver's application processing. Compliance checking, in a translator, may be set to any of several levels. NAESB WGQ recommends that compliance checking be set to the element level in the Functional Acknowledgement.

The 997 informs the originator of the transaction whether the translator accepted the file, accepted it with errors, or rejected it. When errors occur, the 997 identifies the location and type of error that was encountered. Once a transaction passes the translator, the 997 is sent to the originator of the transaction and the data (if accepted) is passed on to the receiver's business application for processing.

Batch Flow Diagram

The flow of data to and from trading partners in an automated environment is diagrammed below.



Creating An Outbound RXQEDM Payload

The following is an example of the steps necessary to send an RXQEDM package:

[??overhaul]

1. Open HTTP connection
2. Check connection status. If in error, re-queue package according to RXQEDM

Deleted: ¶

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

standards. This check should be performed here and throughout the following processes.
3. Post, including a) Authentication, b) Send multipart form, c) Receive HTTP Response data
4. Check connection status. If in error re-queue package according to RXQEDM standards
5. Check HTTP status code (200 is good, less than 300 may be acceptable). If status is not successful re-queue package according to RXQEDM standards
6. Close connection - wait for other end to close in a reasonable time
7. Parse HTTP Response data elements
8. If request-status ok, then log success
9. If request-status error, then log error
10. If no valid request-status re-queue package according to RXQEDM standards
11. Remove package from sending queue when successful or when failed completely

The important characteristics of EDI payload are:

Using an X12 Translator EDI/EDM

??

Processing Inbound RXQEDM Payloads

[??overhaul]

The following is an example of the steps necessary to receive an RXQEDM package:
1. Parse multi-part form
2. Validate HTTP Request data elements
3. If HTTP Request data elements in error, return appropriate RXQEDM standard error code in the HTTP Response data elements
4. Save data
5. Create "gisb-acknowledgement-receipt"
6. If using signed receipts, produce a digital signature over the "gisb-acknowledgement-receipt" created in step 5.
7. Encapsulate the "gisb-acknowledgement-receipt" and digital signature body parts in a "Content-Type" of "multipart/signed envelope"
8. Return HTTP Response with the "gisb-acknowledgement-receipt" object back to Client
9. Close connection
10. Log final results
11. Route data file to the next process based upon "input-format"

Acknowledgement Receipt: "gisb-acknowledgement-receipt"

??official timestamp for exchanges

Deleted:

Formatted: NAESB Section Title

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

INTERACTIVE FF/EDM

[??PASTED FROM wgq edm]

Formatted: NAESB Para Title

Industry Goals/ Purpose

NAESB WGQ defined two ways in which flat files could be used to send transactions and transaction responses: interactive and batch. This section covers implementation considerations for the use of interactive flat files.

In general, interactive flat file communication has similarity with EBB/EDM. For example, both involve human interaction and both use a Web browser to accomplish their purpose. Interactive flat files differ from EBB/EDM in how the transaction data is prepared. EBB/EDM allows for direct Web page entry of the data elements of the transaction, while flat files are prepared as part of a separate process "off-line".

A variety of tools could be used to prepare flat files. However, what NAESB WGQ had in mind was to facilitate the preparation by creating standards that are consistent with how spreadsheets can save files. Further, the standards were devised to avoid the need for programming (e.g., using spreadsheet macros) in order to create the file. The flexibility for the sender to order the data elements does imply programming to interpret the received file on the part of the recipient.

An interactive flat file process may choose different mechanisms to respond to the uploaded file. While NAESB WGQ has set no standards as to how this should be accomplished, an example is the response may be an HTML screen which highlights any errors found or it may be a file response. As another example, the response could be part of the same Web connection (HTTP round trip) or via an asynchronous mechanism (the user is either notified when the result is available or can go look for the result on a Web page).

This portion of the guide assumes an HTTP multipart form file upload. Other implementations (e.g., custom JAVA applet) are not described; however, some of the same considerations described below are applicable.

Applicable Standards

HTTP Post with mult-part forms (RFC 1867)

Secure Sockets Layer (SSL) – HTTPS

Minimum Technical Characteristics of the Client Workstation

see Appendix C

Inserted: 2/25/2004

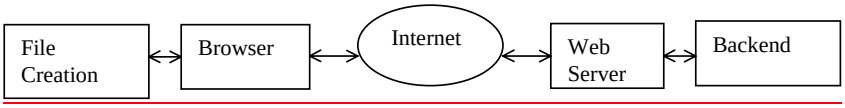
Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

Flow Diagram

This paragraph and the following diagram depict a possible flat file upload process with the user doing the upload on the left side. A spreadsheet can be used for file creation. The Web browser and Web server cooperate to ensure encryption of the upload file and the response. The Web server will also cause the browser to prompt for a logon id and password. The Web server may perform a certain amount of pre-validation before sending the file to the TSP's backend system for further processing. When the backend completes its processing, the Web server program gathers the results which may be kept in a database table. It then formats those results, possibly as a file or an HTML response, and sends them back to the browser. The browser then offers the file save dialogue or displays the results as appropriate. If errors are reported in these results, the user would correct them in the spreadsheet, resave the input to a flat file and again upload the file. This process would continue until no errors are returned.



Specification

The Parts of a Page

General

While NAESB WGQ did not either suggest the use of a Web page or determine the design of a Web page for flat file uploads, this section makes suggestions as to how a flat file could be transmitted.

Header Area`

Left side

The top left side of the Web page can provide navigation to the Customer Activities home page and/ or directly to some of its major menu items. That is, it can look exactly like the Header section for EBB/EDM.

Right side

The top right side of the Web page can provide for invocation of page functions as it does for EBB/EDM. Since uploading a flat file does not have need for most of the EBB/EDM functions, this portion of the page may be limited to such things as the "Submit" function.

Forms Area

The Forms Area will be uncomplicated for Interactive Flat File uploads. Its exact look will depend on how interactivity is implemented and whether optional response types are made available. At minimum, it needs to have a text box to specify the file to be uploaded. This text box will be accompanied by a "Browse" button to allow a graphical selection of the file versus having to type its full path and name. This button is provided automatically by the browser. It is also necessary to include a "Submit" button near

Deleted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Inserted: 2/25/2004

Deleted: 1/23/2004

(e.g., immediately below) the text box for the file name. This button is necessary as part of a multipart form. The "Submit" function mentioned above in the right side of the Functions Area could be made to programmatically (e.g., using Javascript) "click" this "Submit" button. If alternative response types (see Intro above) are provided, such choices could be made available with a drop-down list box. It may make sense to provide this ahead of (e.g., above) the text box which provides entry of the file name. Two other possible controls include a dropdown from which to choose the TSP being nominated and a text box to indicate the DUNS number of the nominator. These would simulate the "to" and "from" fields in the batch EDM process. An example of what this may look like is provided in a subsequent section. As it is unlikely that this collection of user interface controls will require much screen real estate, it may make sense to allow a larger portion of the screen for response information if it is an HTML screen response.

Matrix Area

The matrix area could be used for an HTML response if that alternative is made available. If so, it is also desirable that it be as consistent as possible with the look and feel of the response resulting from EBB/EDM (assuming it is implemented on the site along with Interactive Flat file capability).

Page Functions

As was stated above, there might not be many functions besides the "Submit" function. The Submit function will have the effect of uploading the flat file for processing by the back end system. Depending upon the specific implementation, it may generate an acknowledgement of the receipt of the uploaded file, errors encountered in the prevalidation (if any) and/or the actual results of the backend processing (e.g., Quick Response info).

Page Format

To accomplish a file upload, the Forms Area must include a multi-part form which requires a special HTML values for the Form tag which are ENCTYPE="multipart/form-data", ACTION="scriptname" and METHOD="POST" where scriptname is the script or program which processes the upload file on the Web server. The form will also contain a tag specifying a file as a type of input such as the following: <input type="file" size="30" name="input-data">. It is this tag which causes the browser to create a text box and a button for browsing to a specific file. The NAESB WGQ-specified browser release (i.e., version 4 or better) ensures that mulitpart forms are supported.

File Creation

As was mentioned in the Industry Goals section, it is envisioned that the creation of the required flat file format be possible without programming. Specifically, what the designers had in mind was the use of a spreadsheet to accomplish this. The user would first type a "heading" row which contains the names of the data elements being uploaded (see NAESB WGQ Standard 4.3.81). Then the user would type appropriate data values in subsequent rows of the spreadsheet (note NAESB WGQ Standard 4.3.82). When all data is entered, the user would choose a file save menu and choose a file type of "comma separated values". The user must carefully note where this file is saved so that it can be chosen in the browser Forms area as described above.

To facilitate the repeated use of this spreadsheet, it would make sense to save a spreadsheet in its native format including the heading information, thus allowing reuse of this as a template for subsequent nominations. If this is done, the user must be careful not to choose this native

Deleted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Inserted: 2/25/2004

Deleted: 1/23/2004

format file (e.g., for Excel this would be the .xls file) as the file to be uploaded, as it will not be of the proper file type (it is a binary file and not the one with the necessary text layout). Other spreadsheet features may be employed to avoid having to repeatedly enter data (e.g., the contract identifier) which does not change from row to row.

While the vision includes no programming, it does not preclude the use of macros or other "front ends" to make it easier for the user to create the proper file format. For example, a special program with a customized form for data entry could be written which facilitates easier data entry or integration with an existing system. This program would have the responsibility of taking the form data and arranging into a format compliant with the standard (see NAESB WGQ Standard 4.3.80).

Uploading Mechanism

If both EBB/EDM and Interactive FF/EDM are available, it may be useful to have submenus for each under the appropriate NAESB WGQ standard menu. Once this menu is chosen, the user can be presented a Web page as described above under the Parts of a Page and Page Format sections.

Receipt Programming

Interpreting a multipart form upload

A multipart form is sent to the Web server using a layout described in the applicable Internet Request For Comment (RFC), currently RFC 1867. This RFC describes how a multipart form allows the uploading of a variety of MIME types from a single form, one of which is a File type. As part of the upload, an HTTP header is sent indicating the string of characters which acts as a delimiter for each part of the upload form. If the form is processed by a traditional Common Gateway Interface (CGI) program (e.g., using C/C++ or Perl or others), it will have to parse the data using the RFC as a specification of data format.

Using a commercial component to assist

For some Web servers it may be possible to obtain a commercially available component which reduces the task of receiving an uploaded file to simple object method and property syntax.

Assigning data element values (parsing the uploaded file)

Once the file has been successfully received by the Web server, it may be useful to pre-validate it as much as possible. For this to be done, the individual elements of the file need to be parsed and, presumably, saved to an array or data base table. Assigning the data elements to the proper storage area is facilitated by the first row which provides standardized abbreviations (see NAESB WGQ Standard 4.3.81) for each position in the delimited file's records (or rows).

Pre-validations

At this stage it may be possible to reject the uploaded file for various reasons, thus avoiding sending "garbage data" to the backend system. This could be the result of an unrecognized header row data element name. It may also be due to the discovery that the file is binary, indicating a probable mistake by the sending party (e.g., upload of the spreadsheet's native format or another unexpected format). In any case, the goal here is to avoid unnecessarily burdening the backend and providing the quickest possible response to the user.

Synchronous Vs Asynchronous

As was mentioned in the Industry Goals section, a variety of implementations are possible for

Formatted: Indent: Before: 0"

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

Interactive Flat Files. One type of implementation could be characterized as "synchronous" where the user waits for the reply from the backend validations as part of the same HTTP round trip. In other words, after pressing the Submit button, the system returns a response confirming the receipt of the uploaded file followed by the completely validated response to the browser which is waiting for that response.

A different implementation may only acknowledge receipt of the uploaded file and will make the results of the backend validation available some time later. The user may or may not be notified of the availability of the full validation response. If not, they may periodically check a particular Web link for a list of available responses. NAESB WGQ was intentionally silent as regards how the EBB/EDM or Interactive FF/EDM accomplish showing validation results.

Yet other implementations may be possible.

Interface to backend system

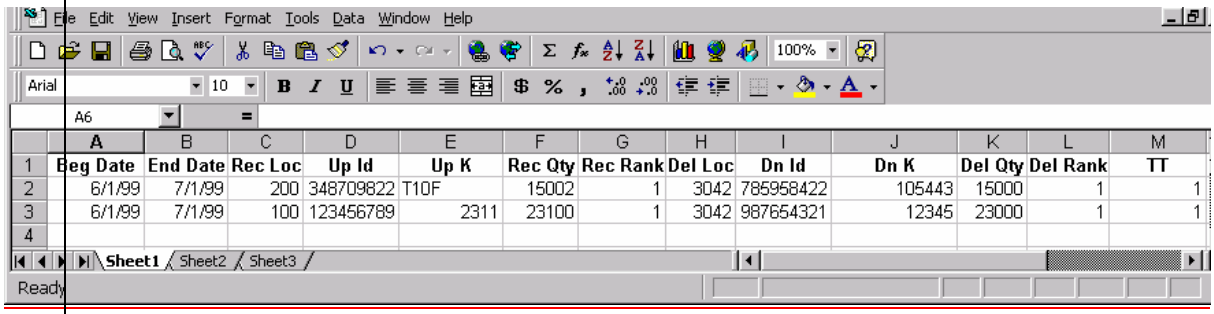
NAESB WGQ standards make no attempt to specify backend mechanisms, so this is completely up to the individual providers. Typical implementations may include two-tier (traditional client/server applications), two-tier with data base stored procedures or three-tier. Again, other implementations are possible, and this guide makes no attempt to be complete.

Formatting the response

As mentioned above, the response can be presented in an HTML screen or in a flat file. This may be based on an option provided to the sender on the upload form. If it is a flat file response, it must conform to the NAESB WGQ standards which include flexibility in the order of data elements within a record (or row). It may be more "user friendly" to have a well-defined (presumably published on the provider's Web site) sequence so as to avoid making the user incur programming time and expense otherwise necessary to handle a variable sequence.

Examples

Sample spreadsheet



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Beg Date	End Date	Rec Loc	Up Id	Up K	Rec Qty	Rec Rank	Del Loc	Dn Id	Dn K	Del Qty	Del Rank	TT
2	6/1/99	7/1/99	200	348709822	T10F	15002	1	3042	785958422	105443	15000	1	1
3	6/1/99	7/1/99	100	123456789	2311	23100	1	3042	987654321	12345	23000	1	1
4													

Flat file saved from the spreadsheet

Beg Date,End Date,Rec Loc,Up ID,Up K,Rec Qty,Rec Rank,Del Loc,Dn ID,Dn K,Del Qty,Del Rank,TT
19990601,19990701,28476,420824973,Q10C,1000,1,30948,293841234,W02R,970,1,01
19990601,19990701,34521,009712345,0200,25309,999,6111,087654765,P109,24500,999,01

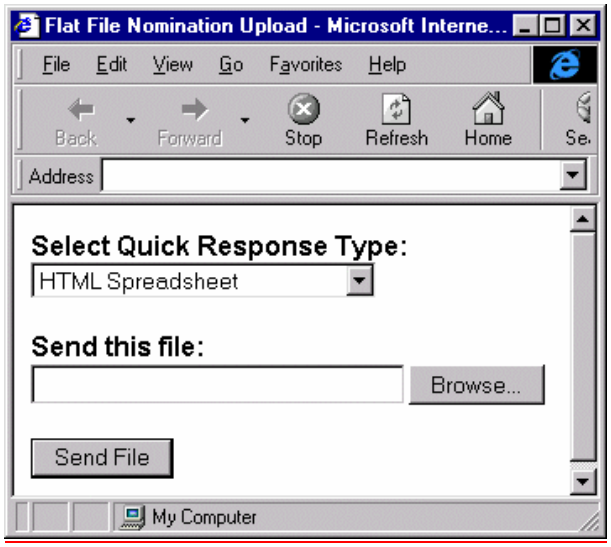
Sample HTML upload form

Deleted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Inserted: 2/25/2004

Deleted: 1/23/2004



Deleted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Inserted: 2/25/2004

Deleted: 1/23/2004

HTML for Sample Form

The following is the HTML for the above (note the user of multipart form and the post method):

```
<html>
<head>
<title>Flat File Nomination Upload</title>
</head>
        <form ENCTYPE="multipart/form-data" ACTION="ProcessUpload.asp" METHOD="POST">
                <p><strong>Select Quick Response Type: </strong><br>
                <select name="QRType" size="1">
                        <option value="Spreadsheet">HTML Spreadsheet</option>
                        <option value="Echo">HTML Echo of Input with Errors</option>
                        <option value="Tab">Tab Delimited Flat File</option>
                        <option value="Comma">Comma Delimited Flat File</option>
                        <option value="Fixed">Fixed Format Flat File</option>
                </select></p>
                <p><strong>Send this file:<br></strong>
                <input type="file" size="30" name="input-data"></p>
                <p><strong><input type="submit" value="Send File"></strong></p>
        </form>
</body>
</html>
```

Security

Formatted: Indent: Before: 0"

Authentication

NAESB Internet ET Standard 4.3.84 calls for use of Basic Authentication. This is a standard part of the HTTP specification. Without use of encryption, this would be a clear text transmission of user id and password. To avoid this, merely protect the page from which the logon is invoked with Secure Sockets Layer encryption as described below. Note that where the user id and password information is maintained, it is different for different Web environments. You may want to consider providing the ability for users to change their password.

Encryption

NAESB WGQ Standard 4.3.83 calls for the use of 128-bit encryption using Secure Socket Layer (SSL) technology. SSL is accomplished by obtaining a certificate from providers and using Web servers capable of using these certificates to accomplish SSL. The browsers specified in the Standard Client Configuration standard are known to be able to handle SSL mechanisms. Any pages to be protected with SSL need to be invoked with the HTTPS protocol by using "https" versus "http" as part of the hyperlink (HREF) name. Note that this means using a Fully Qualified versus Relative link name. This, in turn, causes a new DNS lookup from the browser. When the hostname is provided by more than one machine, this may result in the request being sent to a different machine. This would only cause problems where necessary state information is being maintained in the memory of the Web server's machine.

Formatted: Font: (Default) Arial, 11 pt, Font color: Auto

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

7 – TESTING GUIDELINES

Formatted: NAESB Tab Title

Formatted: NAESB Section Title

NAESB RXQEDM TEST GUIDELINES

[??testing section needs complete overhaul]

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

8 –APPENDICES

[??appendices needs complete overhaul]

Formatted: Normal

APPENDIX A - Reference Guide

NAESB

NAESB Web Site: (www.naesb.org) Primary reference for energy industry standards.

Time Synchronization

Time synchronization is required to assure that all trading partners' transaction times are accurate. Testing has shown that the clocks on all computer systems drift. Time accuracy is dependent on how much a system's clock drifts, how frequently it is resynchronized and the accuracy of the source used for synchronization.

Each NAESB business process may have unique time-synchronization requirements. Refer to the QEDM for time-synchronization standards for target markets. Servers need to be time-synchronized according to the standards needed for the most-restrictive target market, that is the one with the smallest drift allowance.

Authoritative time synchronization is now being provided by governmental agencies around the world based on a synchronized network of atomic clocks. In the United States this includes the U. S. Naval Observatory and the National Institute of Standards and Technology.

An easy way to obtain the current time is from the U. S. Naval Observatory's Web site at tycho.usno.navy.mil/cgi-bin/timer.pl. The output from this page can easily be edited and reformatted to set a local system's time. Commercial, shareware and public domain packages are also available to synchronize system times, including IETF NTP, Internet daytime, nisttime / usnotime.

Further information on time synchronization may be found at the following Web sites:

- http://tycho.usno.navy.mil/ntp.html
- www.ccd.bnl.gov/xntp

Inserted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Deleted: 2/25/2004

Deleted: 1/23/2004

APPENDIX B – FREQUENTLY ASKED QUESTIONS

[??FAQ needs complete overhaul]

Q: Use of "time-c-qualifier" across quadrants. We understand that the retail quadrants require the "time-c-qualifier" for "gisb-acknowledgement-receipt", while the WGQ does not require this data element. If we participate in multiple quadrants, which standard do we use?

A: You are required to follow the standards dictated by the quadrant that governs the transaction or business process. For example, if you are executing a WGQ nomination, then you should adhere to WGQ standards, which do not require the "time-c-qualifier". If you are executing an REQ enrollment, you need to adhere to the REQ standards, which require "time-c-qualifier". Of course, all parties can mutually-agree to use the "time-c-qualifier" or not.

Q: Atomic Clock Synchronization. How often do we need to synchronize our system clocks with an atomic clock?

A: ??+/- 20 seconds; Refer to your QEDM for time-synchronization standards for the business processes you are executing.

Deleted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Inserted: 2/25/2004

Deleted: 1/23/2004

APPENDIX C – SAMPLE TECHNICAL EXCHANGE WORKSHEET (TEW)

??assume appended to Internet ET TEW

EDM Specifications	Test	Production
DUNS/DUNS+4 Number		
EDI/EDM Segment Terminator (character 4 in ISA)		
EDI/EDM Data Element Terminator (character 128?? in ISA)		
EDI/EDM ISA08/GS08		
Using 'time-c-qualifier' in Receipt? (Y/N)	Y (required by RXQ)	Y (required by RXQ)

Deleted: 2/25/2004

Formatted: Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Inserted: 2/25/2004

Deleted: 1/23/2004

Page 11: [1] Deleted **George M. Behr** **1/23/2004 11:05 PM**

[11].2.14 "HTTP Request". The stream of data sent from the Client to the Server that includes header information and payload data.

[11].2.15 "HTTP Response". The stream of data sent from the Server to the Client in response to an HTTP Request, and includes the Receipt.

[11].2.16 "HTTP Server". The computer hardware and software used by the Receiver to receive HTTP Requests from the Sender's Client, and to send HTTP Responses to the Sender's Client. The Server is an HTTP/Web Server.

Page 11: [2] Deleted **George M. Behr** **1/23/2004 11:05 PM**

[11].2.18 "Interactive Browser". A Browser that requires manual operation or intervention. See "Browser".

Page 11: [3] Deleted **George M. Behr** **1/23/2004 11:05 PM**

Internet Electronic Transport"RXQEDM. The NAESB standards developed after Version 1.7 for the secure transport of electronic information between trading partners.

Page 1: [4] Formatted **George M. Behr** **11/18/2003 4:08 PM**

Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around

Page 12: [5] Deleted **George M. Behr** **1/23/2004 11:08 PM**

[11].2.30 "TCP". Transmission Control Protocol; IETF RFCs 793, 1122, 1323
See "http://www.itprc.com/tcpipfaq/default.htm"

[11].2.31 "RSA". A mathematical algorithm for encryption developed by Rivest/Shamir/Adleman. See http://world.std.com/~franl/crypto/rsa-guts.html.

[11].2.32 "SSL". Secure Sockets Layer; a privacy technique that uses encryption to hide information from electronic observers on the Internet.
See "http://developer.netscape.com/docs/manuals/security/sslin/contents.htm"

[11].2.33 "PGP". Pretty Good Privacy; software used to create Public and Private Keys for privacy and digital signature applications; see http://www.uk.pgp.net/pgpnet/pgp-faq/

[11].2.34 "Private Key". The sequence of digits known as a 'key' that is kept private by the owner of a digital certificate, and is used by the certificate owner in encryption and decryption algorithms.

[11].2.35 "Public Key". The sequence of digits known as a 'key' that an owner of a digital certificate shares with trading partners. The trading partners use the public key in encryption and decryption algorithms in electronic transactions with the certificate owner.

[11].2.36 "HTTP". Hypertext transport protocol; Assumes version HTTP/1.1; IETF RFCs 2616, 2069. See "http://www.w3.org/Protocols/Specs.html"

RXQEDM[11].2.37 "MIME". Multipurpose Internet Mail Extensions; IETF RFCs 2045, 2046, 2047, 2048, 2049; See http://www.faqs.org/rfcs/rfc2045.html.

Page 12: [6] Deleted **George M. Behr** **1/23/2004 11:43 PM**

[11].3.3 At a minimum, the designated RXQEDM Server/Receiver site should be accessible via the public Internet. This specifically does not preclude location of the designated site on a private intranet as long as the designated site is accessible via the public Internet (4.3.7).

Page 12: [7] Deleted **George M. Behr** **1/23/2004 11:43 PM**

[11].3.4 The minimum acceptable protocol should be HTTP. All sending and receiving parties should be capable of sending and receiving the HTTP versions supported by NAESB RXQEDM (4.3.8).

Page 13: [8] Deleted **George M. Behr** **1/23/2004 11:47 PM**

Client (Sender)	Server (Receiver)	Receiving Program (Receiver)
	Listen for Connect	
Connect	Accept Connection	
Write HTTP Request	Read HTTP Request	Start of Receipt
Write HTTP Request	Read HTTP Request	
EOF (send)	Read HTTP Request	End of Receipt
Read HTTP Response	Write HTTP Response	
Received		
EOF HTTP Response		

(Cross Reference 4.3.14).

Page 13: [9] Deleted **George M. Behr** **1/23/2004 11:48 PM**

[11].3.16 Trading partners should implement basic authentication.

[11].3.17 Encryption keys should be self-certified. The exchange of keys should be done in a secure manner such as via postal mail. Key policies, including key exchange policies should be communicated to trading partners.

[11].3.18 Encryption keys should have a limited lifetime whose duration is determined by the key's owner. A key's end of life is expressed in the expiration date field contained in each Public Key. A lifetime of one year or less is recommended.

Page 13: [10] Deleted **George M. Behr** **1/23/2004 11:48 PM**

[11].3.20 Batch and Interactive Browsers should use Internet-compatible common browser software. (4.3.37)

Page 13: [11] Deleted **George M. Behr** **1/23/2004 11:49 PM**

[11].3.22 Private network connections to NAESB RXQEDM servers, which include all NAESB RXQEDM standardized Internet communication, may be at any point on a party's firewall boundary at the party's discretion on a non-discriminatory access basis. The specific type and speed of these connections should be mutually agreed. It is at the discretion of each party on how multiple private network connections should be managed, so long as such management is done on a non-discriminatory access basis. (4.3.64)

[11].3.23 Parties should be limited to the NAESB RXQEDM approved list of available TCP ports for RXQEDM implementations. (4.3.70x)

[11].3.24 RXQEDM implementations should not require any inbound ports to be opened on the Sender's firewall. (4.3.71, 4.1.37)

Page 1: [12] Formatted **George M. Behr** **11/18/2003 4:08 PM**

Position: Horizontal: Center, Relative to: Margin, Vertical: 0", Relative to: Paragraph, Wrap Around