CHANGE LOG

Tab 2, Introduction

Section/ Paragraph	Area to Change/Comment	Suggested Change
Header	Replace WGQ with REQ	REQ for WGQ
17	Greater gas industry	Replaced with greater gas and electric industries
[all]	Most, but not all, references to WGQ	Replaced most instances of WGQ with REQ.
17	Marketplace for natural gas	Replaced by matketplace for energy
[all]	Most references to Internet EDI/EDM and BATCH FF	Replaced with Electronic Delivery Mechanism (EDM)
18	TAB 7, TAB 8, TAB 9 and TAB 10	Replaced with TAB 7 Testing Guidelines and TAB 8 Appendix
18	Appendix C and Appendix D	Eliminated, and renamed Appendix E to Appendix C

CHANGE LOG

Tab 3, Executive Summary

Section/ Paragraph	Area to Change/Comment	Suggested Change
Header	Replace WGQ with REQ	REQ for WGQ
19	Added sentence introducing the concept of NAESB, as should be present in all Exec Summaries.	Selected sentence off NAESB website explaining NAESB.
[all]	Most, but not all, references to WGQ	Replaced most instances of WGQ with REQ.
[all]	Numerous references to Batch FF/EDM	Removed references to Batch FF/EDM, following lead of Tab 6.
19,20	Spelled out all acronyms the first time they appeared, as should be the case with an Exec Summary	NAESB, all 4 quadrants, EDM, EDI, FTTF
19	Identified who benefits from standards	Added Gas and Electric utilities, changed the word 'bank' to 'financial institution.
20	More precise wording on who will require consensus	Added 'international community'.
20	Identify testing partners	Changed Gas to Electric
21	Concerns about reliability	Updated wording to more accurately describe the current state of affairs with the Internet

BUSINESS PROCESS AND PRACTICES

[Editor's Notes – to be deleted after review]

Section/ Paragraph	Area to Change/Comment	Suggested Change
[all]	"Transportation Service Provider" and "TSP"; these sound like natural gas terms. Regardless, I think it needs to be changed due to the ambiguity.	No action taken. What term will we use in REQ? Once we decide, we will need to go through the entire document and replace.
[all]	"Natural Gas" or "Gas"	"Energy"
[all]	"GISB" or "Gas Industry Standards Board"	"NAESB/GISB"
[all]	"3rd party"	"third-party"
[all]	"shippers"	"parties"
[all]	Name of REQ EDM? I used "EDM-REQ" to differentiate from NAESB WGQ EDM	Used EDM-REQ to differentiate REQ implementation from WGQ; can easily be globally replaced later.
[all]	General editing	Tightened up language using standard techniques (e.g. "utilize" becomes "use")
A	"Gas Industry"	"Electric Industry", even better "Energy Industry"
A, para 1	Language about EBB and FF does not apply	Delete language about EBB and FF
A, para 1	Need language regarding the reasons for an EDM for REQ; includes: need for future collaboration w/ WGQ; scope of initial EDM-REQ;	Added language "Role of EDM-REQ in NAESB
A, para 1	Need REQ-specific language for the role of the Internet EDM in REQ, including: large volumes, large transactions; existing implementations of EDM; ebXML; AS2; of EDI; of XML	Added language
A, para 1	XML: my understanding is that we need to address this in the standard.	Included some language; needs to be expanded and made consistent throughout document
A, para 2	Language about EBB and FF does not apply	Delete down to "separated flat files".
A, para 2	"Protect from non-repudiation" is worded incorrectly	Maybe "with non-repudiation"
A, para 3	Language about EBB	Delete entire paragraph
A, para 4	Questions in front can be removed; instead simply state value statement.	Deleted
A, para 28	"Pipeline"	Replaced with "Energy"
A, para 30	Need language about OpenPGP	Language added by Dick B

C, 4.1	Principles; deleted a bunch of them; should we renumber?	No action taken.
C, 4.1.1, 8, 11, 13, 16–35, 38	Language about EBB, IPs, and/or FF	Deleted relevant language or bullet
C, 4.2	Definitions; deleted a bunch, adding some: should we renumber?	No action taken
C, 4.2	Should we add a list of REQ entity types (LDC, TDSP, EDC, CR, ESP, ESCO, etc)	Added some then stopped. Are these needed?
C, 4.2.1-10, 12-20	Language about EBB, IPs, and/or FF	Deleted relevant language or bullet
C, 4.2.21	Need language describing Failover scenario/process	Added language
C, 4.2.29	We reference 'trading partner agreement' and should have a definition. Will there be an REQ standard?	Added language re: trading partner agreement
C, 4.3	Standards: deleted a bunch; will be adding some; should we renumber	No action taken
C, 4.3.2	Language about 'pipeline'	Deleted language.
C, 4.3.3	Language about 15-minute window: does this apply to REQ and EDI/EDM?	No action taken
C, 4.3.4	Data retention requirements	Language modified by Dick B
C, 4.3.15	Need Open PGP language	Modified to include Open PGP language
C, 4.3.16	Appears to be related to IP or EBB mechanisms	Deleted
C, 4.3.5-7, 9, 17-35, 37-52, 54-63, 65-69, 72-73, 75-76, 78-86	Language about EBB, IPs, and/or FF	Deleted relevant language or bullet
C, 4.3.87	Language talks about changing business rules	Deleted
C, 4.3.88	Need 128-bit language	Added by Dick B
D, 7.3.24	Not relevant to REQ	Deleted
D, 7.3.35	Not relevant to REQ	Deleted

Location	Details of Change	Comments
Pargraph 1 & 2	Deleted – dealt with history of DRN common codes and Gas Transaction Points	
Paragraph 3	Modified - EBB working group 5 to REQ-TEIS, deleted reference to FERC order 563, and changed GISB to NAESB while removing references to Capacity Release and Nominations	
Paragraph 4	Changed WGQ to REQ, two places	
Paragraph 5	Deleted – deals with flagging CommonCode fields with *.	
NAESB WGO Electronic Data Interchange Trading Partner Agreement	Deleted entire section – see comments.	I doubt we want to use the WGQ EDI TPA as it stands but we do need a standard document for exchange of technical information. Possibly the Texas model would work, just a thought. Here is the URL for the document discussed in the original paragraph. http://www.naesb.org/protected/tpa980820.doc
Party section	Deleted most of this because it deals with W. G. entities only.	Made a feable attempt at describing Retail Electric Party or Entitiy roles. I am not a word smith so feel free to add/delete/re-write. I think it would be helpful to have a section defining all the entities involved.
ANSI ASC X12 Standards	changed WGQ to REQ	
ISA contents paragraph 2	changed WGQ to REQ & deleted last sentence.	Last sentence can be added back once we decide what to do about a standard document to trade technical information.
ISA contents paragraph 4	changed WGQ to REQ	
GS Contents	change WGQ to REQ	
997 Usage	change WGQ to REQ	
Hypertext Transfer	change WGQ to REQ	

Protocol (HTTP)		
HTTP Trnasaction-set Codes	Deleted entire table since it is Gas transaction names only.	I feel the tranasction set table needs to be a State by State list, should we just put a reference to each state's documentation or a note of future reference once the standard documents are Identified.

CHANGE LOG

Tab 6

Section/ Paragraph	Area to Change/Comment	Suggested Change
[all]	Numerous references to WGQ.	Replaced WGQ with REQ
[all]	Numerous references to Batch FF/EDM	Removed references to Batch FF/EDM
Page 51	Extraneous "to"	Removed
Page 52	Common Code Identifier fromat	Tagged as OPEN ISSUE
[all]	Numerous references to gisb-acknowledgment-receipt	Tagged as OPEN ISSUE
Page 52	Description of input-format data element incorrect for REQ use	Removed reference to FF, added XML
[all]	Numerous references to CDI/script	Removed references to CGI/script
Page 52	request-status	Removed reference to decryption process
Page 53	time-c data element lacks time-zone indicator	Added time-zone indicator
Page 53	Transaction-set data element requires enhancement to remove gas industry specific references	Changed transaction-set to 16 character free form text field
Page 54	Diagram	Added EDM Server and simplified
Page 58	Reference to pipeline under Throughput Considerations	Removed pipeline reference
Page 58	HTTP Request Data Elements	Brief description added
Page 59	Incorrect description of transaction-set for REQ purposes	Provided new description for transaction-set, and tagged 8-character names as an OPEN ISSUE
Page 59	Writing a Batch Browser	Removed reference to NAESB home page
Page 59	Description of content type line	Rephrased to indicate that this referred to the specific example on page 59
Page 60	Description of content length	Rephrased to indicate that this referred to the specific example earlier on page 59
[all]	Several references to version 1.4	Changed to 1.6
Page 65	Reference to multipart POST	Tagged implementation as an OPEN ISSUE
Page 67	References to Central time zone	Removed restriction to use Central time
Page 67	Synchronization of client	Added reference to clock accessible via the Internet
Page 67	References to gas nominations	Removed references to gas

		nominations
Page 67	Brief description of HTTP Request	Moved the description to page 58
Page 68	Using a Web Server	Added reference to the POST method as the only supported HTTP method
Page 68	Timestamp time-c references lack timezone indicator	Added identifier for time zone
Page 68	Text incorrectly indicates that SSL or S-HHTP are optional	Removed references to SSL being optional and all references to S-HTTP
Page 68	The CGI Process	Changed to The Receive Process
Page 68	Text specific to pipelines and gas industry	Replaced with more generic text
Page 69	Reference to C program	Removed
Page 69	Reference to BGI programming	Removed
Page 69	Writing the CGI Process	Changed to Developing the Receive Process
Page 69	Reference to GET operation	Removed
[all]	References to CGI process	Changed to receiving program
Page 69	Reference to standard input	Changed to input stream
Page 71	Reference to standard output	Changed to sending program
Page 71	URL/CGI Implementation Guidelines	Changed to Receive Process URL Implementation Guidelines
Page 71	References to WGQ standard 4.3.12	Tagged as OPEN ISSUE
Page 71	A separate URL for nominations	Replaced by a separate URL may be used for customized processing
Page 72	Text specific to gas industry regarding capacity release	Replaced with more generic text
Page 72	References to Central Time zone	Removed
Page 72	References to nomination deadline	Removed
Page 74	time-c data element has no time zone indicator	Added time zone indicator and provided description of its use
Numerous Examples	examples of gisb-acknowledgement-receipt containing time-c missing time zone indicator	Updated all examples of time-c to include time zone indicator

CHANGE LOG

Appendix

Section/ Paragraph	Area to Change/Comment	Suggested Change
[all]	References to WGQ	Replaced with REQ
Page 104	"natural gas industry" reference under definition of NAESB	Replaced "natural gas industry" with "energy industry"
Page 104	Missing reference to PGP Corporation	Added reference to PGP Corporation
Page 108-112	Appendix C and D not applicable to REQ at this time	Removed pages 108-112
Page 113	Reference to WGQ Customer Activities Web Site	Removed reference.

CHANGE LOG

Tab 2, Introduction

Section/ Paragraph	Area to Change/Comment	Suggested Change
Header	Replace WGQ with REQ	REQ for WGQ
17	Greater gas industry	Replaced with greater gas and electric industries
[all]	Most, but not all, references to WGQ	Replaced most instances of WGQ with REQ.
17	Marketplace for natural gas	Replaced by matketplace for energy
[all]	Most references to Internet EDI/EDM and BATCH FF	Replaced with Electronic Delivery Mechanism (EDM)
18	TAB 7, TAB 8, TAB 9 and TAB 10	Replaced with TAB 7 Testing Guidelines and TAB 8 Appendix
18	Appendix C and Appendix D	Eliminated, and renamed Appendix E to Appendix C

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. NAESB Retail Electric Quadrant (REQ) Standards are a product of the North American Energy Standards Board. 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. This will lead to a seamless North American marketplace for energy, as recognized by its customers, the business community, industry participants and regulatory bodies.

The standards are written as 'minimums,' which industry participants are encouraged to exceed (if they are not doing so already) through provision of value-added services and customized arrangements. NAESB defines 'exceed the minimum standard' to mean surpassing the standards without negative impact on contracting and non-contracting parties.

All of the standards have been adopted in the realization that as the industry evolves and uses the 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 to the NAESB office, detailing the change, 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 REQ 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 Implementation - Electronic Delivery Mechanism (EDM)

Provides an overview of the business process for EDM.

Data Dictionary

Provides definition of the standard data elements and the usage requirements for each element.

Batch Flow Diagram

Sending Transactions

Provides instructions to develop mechanisms for sending of NAESB REQ standard format data files.

Receiving Transactions

Provides instructions to develop mechanisms for receiving of NAESB REQ standard format data files.

Security

Provides guidelines for data privacy, data integrity, authentication and non-repudiation of inbound and outbound transactions.

Other Considerations

Provides information regarding error notification and testing. Includes a reference guide and examples for repudiation and validation.

TAB 7 Testing Guidelines

TAB 8 Appendix

Appendix A - Reference Guide
Appendix B - Repudiation and Validation Examples
Appendix C - Minimum Technical Characteristics for an EDM Server+

CHANGE LOG

Tab 3, Executive Summary

Section/ Paragraph	Area to Change/Comment	Suggested Change
Header	Replace WGQ with REQ	REQ for WGQ
19	Added sentence introducing the concept of NAESB, as should be present in all Exec Summaries.	Selected sentence off NAESB website explaining NAESB.
[all]	Most, but not all, references to WGQ	Replaced most instances of WGQ with REQ.
[all]	Numerous references to Batch FF/EDM	Removed references to Batch FF/EDM, following lead of Tab 6.
19,20	Spelled out all acronyms the first time they appeared, as should be the case with an Exec Summary	NAESB, all 4 quadrants, EDM, EDI, FTTF
19	Identified who benefits from standards	Added Gas and Electric utilities, changed the word 'bank' to 'financial institution.
20	More precise wording on who will require consensus	Added 'international community'.
20	Identify testing partners	Changed Gas to Electric
21	Concerns about reliability	Updated wording to more accurately describe the current state of affairs with the Internet

EXECUTIVE SUMMARY

The North American Energy Standards Board Retail Electric Quadrant ~~Whole Gas Quadran~~t (NAESB REQ~~WGQ~~) has developed standards for accomplishing electronic commerce over the Internet. ~~using ANSI ASC X12 (EDI/EDM~~ flat files (FF/EDM), and Customer Activities Web site ~~presentations (EBB/EDM).~~ Technologies necessary for all Internet Electronic Delivery Mechanisms (EDM) to rapidly, reliably and safely move data across the Internet have been determined. For data ~~EDI and flat files, once~~ received from a trading partner via the Internet, the data is decrypted and moved through a translator or other appropriate processor for NAESB ~~WG~~REQ standard file formats and forwarded to a back-end processing application. However, file format translation and back-end processing are outside the Internet EDM scope. ~~For NAESB WGQ Customer Activities and Informational Posting Web sites, requirements for data presentation, navigation and session security have been determined~~.

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

Open Standards

There are several major topic areas related to Internet Electronic Delivery Mechanism covered in this manual. When looking to implement Internet EDM, one should become familiar with the following components of the implementation:

Communications Protocols

Sending of Transactions

Receipt of Transactions

Security

HTTP Transport for Secure EDI (a.k.a. IETF EDIINT AS2)

The "open" standard technologies selected by NAESB ~~WG~~REQ to address these areas are designed to provide flexibility and scalability. There are business benefits gained from adherence to "HTTP Transport for Secure EDI" such as:

Allows potential to more readily, electronically trade with others (e.g., ~~electric~~ gas utilities, financial institutions~~banks~~, suppliers, retail customers)

Makes it more likely that packages can be purchased to replace custom written applications~~s~~ currently in place to support NAESB ~~WGQ~~ REQ EDM

Strengthens the surety of receipt and error notification

HTTP Transport for Secure EDI (AS2) is an emerging standard, largely based on the original

NAESB WGQ EDM, that is being developed by the Internet Engineering Task Force, the Internet standards body. Adherence with a formal, international Internet standard, such as AS2 ensures that the specification will not change without due process and any changes that do occur will be the result of a broad consensus in the international community. Individual companies and entire industries are free to use as much or as little of AS2 as they see fit, providing the maximum flexibility to meet business needs. The specific implementation of the standards is dependent upon what fits the trading partner's needs and available resources. A brief delineation of these components is covered at a high level in the Business Process and Practices (Major functions of Internet EDM covered by the Standards) section and in more detail in later sections.

Same Application Implementation For All Trading Partners

The basic assumption in designing and implementing the Internet EDM application is that it is not platform-specific. What is meant by this is that an organization's Internet EDM application serves the role of communicating with all trading partners in the electric ~~gas~~ industry no matter what hardware, operating system and programming languages they use at their site. For this reason, testing with other trading partners with a variety of platforms is very important in ensuring that each ~~your~~ EDM application is compatible with a range of platforms used by various trading partners.

Testing With Electric ~~Gas~~ Industry Internet EDM Participants

(THIS SECTION NEEDS TO BE REWRITTEN REFERRING TO OUR GUIDELINES (1 16 03)

To provide a way for parties interested in Internet EDM testing to initiate testing relationships, the NAESB home page will have a list of organizations willing to act as testing partners and their respective test coordinator. – The Future Technology Task Force (FTTF) meets on an intermittent basis be scheduled teleconference or in-person meetings to discuss issues, problems, further refinement of the standards. These discussions will provide a means to benchmark results and provide feedback to each other on possible enhancements to the participants' implementations. The FTTF realized that the technology being implemented is relatively new and all organizations can benefit from the sharing of research and technical information and the resolution of gas business issues integrated with the new technologies.

Importance of the Trading Partner Agreement When Using EDM

The expectations of who will perform what function and how it will be accomplished in Internet EDM should, at some level, be laid out in the trading partner agreement. This clarification in the agreement would help to expedite a smoother communication between the trading partners when first setting up their Internet EDM relationship. The newness of the Internet EDM standards and the various implementations of the applications between trading partners bring to the forefront a quandary of issues related to establishing the business rules associated with these standards. The specifications in the trading partner agreement should be tested before production implementation to formulate a solution to any problems revealed during testing well before reliance on the implementation.

Concerns About Future Reliability of the Public Internet

The Internet has proven its viability as a business communication method in many different

industries, but ~~Continued~~ monitoring of the Internet's viability as a communications medium~~n infrastructure~~ will continue to take place. Increased traffic and potential lack of sufficient transmission capacity on the Internet is difficult to predict and quantify at this time. Concerns may be resolved by new Internet service providers and new communications technologies to compensate for the rapid growth of the Internet.

Further Information

Please see the NAESB home page at http://www.naesb.org/ for additional useful information on the implementation of Internet EDM.

BUSINESS PROCESS AND PRACTICES

[Editor's Notes – to be deleted after review]

Section/ Paragraph	Area to Change/Comment	Suggested Change
[all]	"Transportation Service Provider" and "TSP"; these sound like natural gas terms. Regardless, I think it needs to be changed due to the ambiguity.	No action taken. What term will we use in REQ? Once we decide, we will need to go through the entire document and replace.
[all]	"Natural Gas" or "Gas"	"Energy"
[all]	"GISB" or "Gas Industry Standards Board"	"NAESB/GISB"
[all]	"3rd party"	"third-party"
[all]	"shippers"	"parties"
[all]	Name of REQ EDM? I used "EDM-REQ" to differentiate from NAESB WGQ EDM	Used EDM-REQ to differentiate REQ implementation from WGQ; can easily be globally replaced later.
[all]	General editing	Tightened up language using standard techniques (e.g. "utilize" becomes "use")
A	"Gas Industry"	"Electric Industry", even better "Energy Industry"
A, para 1	Language about EBB and FF does not apply	Delete language about EBB and FF
A, para 1	Need language regarding the reasons for an EDM for REQ; includes: need for future collaboration w/ WGQ; scope of initial EDM-REQ;	Added language "Role of EDM-REQ in NAESB
A, para 1	Need REQ-specific language for the role of the Internet EDM in REQ, including: large volumes, large transactions; existing implementations of EDM; ebXML; AS2; of EDI; of XML	Added language
A, para 1	XML: my understanding is that we need to address this in the standard.	Included some language; needs to be expanded and made consistent throughout document
A, para 2	Language about EBB and FF does not apply	Delete down to "separated flat files".
A, para 2	"Protect from non-repudiation" is worded incorrectly	Maybe "with non-repudiation"
A, para 3	Language about EBB	Delete entire paragraph
A, para 4	Questions in front can be removed; instead simply state value statement.	Deleted
A, para 28	"Pipeline"	Replaced with "Energy"
A, para 30	Need language about OpenPGP	Language added by Dick B
C, 4.1	Principles; deleted a bunch of them; should we renumber?	No action taken.
C, 4.1.1, 8,	Language about EBB, IPs, and/or FF	Deleted relevant language or bullet

11, 13, 16–35, 38		
C, 4.2	Definitions; deleted a bunch, adding some: should we renumber?	No action taken
C, 4.2	Should we add a list of REQ entity types (LDC, TDSP, EDC, CR, ESP, ESCO, etc)	Added some then stopped. Are these needed?
C, 4.2.1-10, 12-20	Language about EBB, IPs, and/or FF	Deleted relevant language or bullet
C, 4.2.21	Need language describing Failover scenario/process	Added language
C, 4.2.29	We reference 'trading partner agreement' and should have a definition. Will there be an REQ standard?	Added language re: trading partner agreement
C, 4.3	Standards: deleted a bunch; will be adding some; should we renumber	No action taken
C, 4.3.2	Language about 'pipeline'	Deleted language.
C, 4.3.3	Language about 15-minute window: does this apply to REQ and EDI/EDM?	No action taken
C, 4.3.4	Data retention requirements	Language modified by Dick B
C, 4.3.15	Need Open PGP language	Modified to include Open PGP language
C, 4.3.16	Appears to be related to IP or EBB mechanisms	Deleted
C, 4.3.5-7, 9, 17-35, 37-52, 54-63, 65-69, 72-73, 75-76, 78-86	Language about EBB, IPs, and/or FF	Deleted relevant language or bullet
C, 4.3.87	Language talks about changing business rules	Deleted
C, 4.3.88	Need 128-bit language	Added by Dick B
D, 7.3.24	Not relevant to REQ	Deleted
D, 7.3.35	Not relevant to REQ	Deleted

A. Overview

Role of REQ Internet EDM in NAESB~~Where Internet EDM Fits in Gas Industry Commerce~~

The Retail Electric Quadrant (REQ) of NAESB commissioned the development of an Electronic Delivery Mechanism (EDM-REQ) that addressed the specific needs and requirements of the REQ.

In 2002 the existing GISB EDM was modified to reflect the change to NAESB and the creation of the Wholesale Gas Quadrant (WGQ) roots. Most of the changes that went into the new NAESB WGQ EDM (EDM-REQ) were cosmetic. Yet these changes underscored the ownership of this standard by the WGQ, and the lack of ownership by the REQ.

The REQ believes that NAESB should have one EDM, collaboratively established by the four quadrants. 2002-03 REQ and NAESB goals and timelines do not allow the time required to collaborate with the WGQ and other NAESB quadrants on a NAESB-wide EDM. The REQ EDM initiative is focused on action under the control of REQ: establishing an Internet EDM standard for use by the REQ. The current plan is to collaborate with the other quadrants towards a common NAESB EDM later in 2003. Leaders of the EDM-REQ initiative are intimate and engaged with the EDM-WGQ efforts and are optimistic that in the future there will be a single NAESB EDM standard.

There are many areas of overlap in the EDM-REQ and EDM-WGQ. These areas should be consolidated into a single section of the future NAESB-wide EDM, eliminating unnecessary repetition and potential conflicts. For example, some narrative later in this section describing how solutions can be deployed applies generically to any NAESB EDM solution.

The EDM-REQ extends the base EDM-WGQ to establish a standard for future REQ implementations. REQ has established this EDM-REQ standard now to meet REQ annual plan timelines. It is the intention of the REQ to collaborate in the future with other NAESB quadrants towards the goal of a common NAESB-wide EDM standard.

The initial scope of the EDM-REQ is focused on the EDI/EDM and XML/EDM components necessary to facilitate continent-wide REQ e-business. FF/EDM, IP/EDM and EBB/EDM were intentionally removed from the EDM-REQ with the intention of addressing these requirements at a later date.

~~The EDM~~ Role of Internet EDM in the REQ

REQ electronic commerce requires the exchange of large volumes of transactions and transaction data. The EDM-REQ enables REQ parties to securely and reliably exchange these transactions over the Internet. These transactions include:

- ~~is to address electronic commerce over the Internet using Customer Activities Web site presentations (EBB/EDM), flat files (FF/EDM), and~~ ANSI ASC X12 (EDI/EDM) transactions used in DE, MA, MD, NJ, NY, PA, TX, VA,

- XML transactions used in Ontario.

Retail electric marketplaces including DE, MD, NJ, NY, PA, and TX have used the EDM-WGQ with some extensions to support retail ebusiness since 1999. In 2002, the Ontario marketplace implemented the ebXML Messaging EDM standard. The MA marketplace currently has the EDIINT AS2 EDM standard slated for 2003 implementation. All of these implementations share common architectural technologies thanks to involvement from NAESB technical architects.

The successful deployment of future REQ marketplaces requires an Internet EDM standard. Deploying and maintaining multiple standards is not cost-effective for regional and national REQ parties.

~~between trading partners.~~

~~EDI/EDM has been a part of the GISB standards since their inception. GISB has set standards for transmitting ANSI ASC X12 transactions over the Internet and they have been in place since GISB Version 1.0. In Version 1.4 of the GISB Standards, two new methods of data communication have been added. The first, EBB/EDM is to be used to replace proprietary electronic bulletin boards (EBBs) as described below. The second, FF/EDM is the communication of comma separated flat files. In~~ Version 1~~0.5~~ of the EDM-REQ standard incorporates all technical specifications of the NAESB/GISB WGQ EDM Version 1.6, including:

- EDI/EDM compliance with method of the broader "HTTP Transport for Secure EDI" standard being developed by the Internet Engineering Task force (IETF).
- Mutually-agreeable business practices to protect the sender of a document with non-repudiation and with digitally-signed Error Notifications.

~~EDI/EDM method of communication have been modified to comply with the broader "HTTP Transport for Secure EDI" standard being developed by the Internet Engineering Task force (IETF). These technical changes do not impact the underlying required business practices established by GISB. In addition, the security features of the EDI/EDM and batch FF/EDM communication method now includes mutually agreeable business practices to protect the sender of a document from non-repudiation and to digitally sign Error Notifications.~~

~~In Order No. 587-G, the Federal Energy Regulatory Commission (the Commission) required pipelines to conduct all business transactions using Internet communications to solve the difficulties created by the proprietary EBBs and to provide shippers with a standardized method for doing business. In Order No. 587-I, the Commission recognized that "While shippers and pipelines did not object to the requirement that pipelines support the use of EDI, they contend that EDI should not be the exclusive means of communication and that some form of interactive approach is also necessary." The EBB/EDM approach was developed to satisfy two main concerns: (1) EDI/EDM may only be cost-effective for those doing high volume transactions and (2) shippers did not want to lose the interactive functionality provided by EBBs. Even shippers that are employing EDI may not do so for every transportation service provider with which they do business or for every type of transaction conducted because the level of business does not always justify the expenditure. Further, the Commission stated in Order No. 587-I, that "[it] continues to favor an approach to communication in which shippers can~~

~~either transact business using computer-to-computer file transfers or conduct business online in an interactive fashion, whichever approach best fits their needs."~~

Business Reasons for Using EDI/EDM [and XML/EDM??]

~~The question may be asked, what are the advantages of using Internet EDM to communicate our business transactions in GISB EDI standard data formats as opposed to using Value-added Networks (VANs). As an even broader question, why use EDI standard data formats for transactions at all?~~ With EDI, data already existing in your own computer applications can be used to build ~~nominations and other~~ energy ~~gas~~ industry transactions. Information from a trading partner ~~service provider such as scheduling, allocation, invoicing,~~ can be mapped to a common format. This common format ~~eliminates the need for the following~~ reduces ~~as these additional steps leave room for~~ errors, unnecessary intervention and complications in processing by eliminating or reducing:

- The transfer of data from a paper document to an application format input file at each trading partner site;
- The ~~if electronic files are used,~~ mapping between various application data formats for each and every trading partner.

A company that relies on computerized systems to conduct business and exchanges transactions with several trading partners can communicate those transactions more efficiently with EDI standard data formats and with Internet EDM as the communications mechanism. EDI employs standard data formats for all trading partners.

Using the Internet for communications, ~~By using the public Internet~~ a trading party needs to support only ~~for transmission,~~ a single connection to its trading partners. This can eliminate ~~is required, eliminating~~ the complexity of different connection methods for different trading partners.

Exchanging transactions over a ~~EDI using a~~ Value-Added Network (VAN) has the following disadvantages:

- VAN's have ~~(Value-added Network) can~~ proven ~~rapidly become~~ expensive in REQ marketplaces where large volumes of transactions (e.g. residential customer usage) and large transactions (e.g. interval usage) are commonplace.
- ~~if a significant volume of data is exchanged.~~ VAN's may impose charges based on number of transactions or number of characters sent, whereas, the ~~public~~ Internet does not impose transactions charges.
- ~~In a~~ VAN ~~environment,~~ transmission of transactions sent to trading partners who use a different VAN may be considerably delayed because of data transfer schedules between the VAN's. The Internet EDM solution eliminates this delay because the transaction is sent directly to the trading partner's designated receipt site.
- Most VAN's do not support XML-formatted transactions.

Roles in Electronic Commerce

In all electronic commerce, one party initiates, or sends, a transaction and the other

party receives the transfer. In the Internet environment, the sender is referred to as the client and the receiver is referred to as the server. You should expect to act in both the client role and the server role during the electronic commerce process. Once a transaction set is successfully received for processing, the original receiving party switches to the client role to send a confirmation transaction back to the original sender's server. Therefore, it is essential that both the sending and receiving aspects of electronic commerce are addressed in your implementation.

The standards adopted for Internet EDM, as with all NAESB/GISB standards, 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" in that if both trading partners agree on the inclusion, the additional feature requirements will be met. However, 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.

The Trading Partner Agreement is a key reference in electronic commerce. It will define the "designated site" for each partner (see the Business Practices Subcommittee documentation), values used for variable parameters, and optional features that will be used by the partners.

Assess Your Capabilities

Internet EDM can be constructed and deployed with internal resources, with consulting/development help from a third-party, or as an outsourced solution with a third-party. ~~There are many questions that readers of this narrative may want answered to clarify the standards or at least provide options for their organization's implementation of NAESB/GISB Internet EDM standards. However, t~~The best solution for each ~~a particular~~ organization must be determined based on the assessment of specific needs and the resources available to that organization.

With ~~Depending on your situation, you may implement the complete solution with internal resources. Given the existence of~~ in-house Internet systems expertise, it ~~is should be~~ possible to implement Internet EDM ~~the technologies in this guide~~ with little to no ~~, if any,~~ assistance. ~~On the other~~ Other ~~hand, smaller~~ organizations may view COTS Internet EDM or Internet EDM outsourcing as the most strategic use of their time and money.~~want to use this guide to identify services that they will obtain from a third party.~~

Where possible, ~~As much as possible, the~~ NAESB Internet EDM has adopted technologies ~~chosen~~ that can be acquired ~~for most of the programs needed to implement Internet EDM could be acquired as "shrink-wrapped" software~~ at low cost. Sample code is provided where readily-available commercial quality products ~~that can just be "plugged in"~~ do not exist~~, sample code has been identified~~. This sample code is not supported but rather ~~has the drawback of being unsupported. It~~ is intended for companies that have technical expertise but need ~~just~~ some starter code from which to build their own versions~~A mixture of internal expertise and third-party services will be the likely approach of several organizations. To determine where you may require the services of a third party, you should assess your present capabilities. For example, a company may have experience with X12 translators, but little experience with Internet technology at this time.~~

In-house Implementation

This document is extremely pertinent ~~i~~f you ~~are choosing~~ choose to implement most or all of the required functionality with internal resources~~ly, this document is particularly pertinent~~. The pilot test report posted on NAESB/GISB's home page captures "lessons learned" from those companies that participated in the pilot project.

The pilot test ~~It was~~ demonstrated ~~throughout the pilot test~~ that electronic commerce using the Internet can work. However, ~~it is strongly encouraged that~~ all parties are strongly encouraged to fully investigate the ramifications of introducing electronic commerce using the Internet. This includes ensuring that all customer data, internal data, and applications are secure from intruders or other parties not authorized for access.

Participation in electronic commerce over the Internet will involve hardware, software, and technical expertise. Hardware requirements may include a server to receive incoming EDI files, a firewall processor to block intruder access. Software will include 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.

The NAESB/GISB home page contains the text of the pilot test report and reference materials that parties may ~~utilize~~use in evaluating and choosing hardware and software.

Using a Third-Party

As with any technology solution, a company must choose between building in-house, buying off-the-shelf software, or outsourcing, and any combination of the above. ~~There are many questions that readers of this narrative may want answered to clarify the standards or at least provide options for their organization's implementation of NAESB/GISB Internet EDM standards. However, t~~The best solution for a particular organization must be determined based on the assessment of specific needs and the resources available to that organization.

~~It is expected that~~ Third-party providers ~~will~~ offer a variety of services from a full "turn key" solution to assistance only where you require it. Such assistance might include programming, system configuration and system administration as well as private communication links.

EDM-REQ Network Connections

Trading partners should maintain redundant connections to the public Internet for EDM-REQ sites. These redundant connections should be topographically diverse paths to minimize the probability of a single point of failure. Three possible approaches to redundant connections are:

1) Maintain multiple ISPs and multiple points of connectivity, each of which was identified by the same URL making the process of redundancy transparent to the sender.

2) Maintain different Internet connectivity URLs (presumably on topographically different ISPs). For this to result in communication redundancy, the sender should know of the existence of the secondary URL and have programming in place that will automatically switch batch-browser transmissions to the secondary URL when the primary URL is unavailable.

3) Maintain multiple connections to the same ISP. This involves only one URL but the presumption would be that the ISP would provide alternate diverse paths for the URL.

Receivers may maintain multiple URLs and, if such have been disclosed, the sender should attempt to use these during primary URL outages. The redundant public Internet connections can be through a single ISP or multiple ISPs. If multiple URLs are provided for EDM-REQ access, the following conditions should be met:

- The information provided by each URL should be exactly the same, although trans-ids can be different.
- The trading partners should be informed of both URLs and their availability by system wide notice or by Trading Partner Agreement.
- The URLs should be identified as primary and secondary if either:
- There is a TSP connection speed difference between the URLs (The faster connection listed as primary)

or

- One URL is only available when the other is down (primary URL being the most available)
- The URLs should be listed as primary and alternate if:
- The URLs have the same TSP connection speed

and

- The URLs are customarily available simultaneously

Note: A URL is considered available (in the context of communication redundancy) if all the IP facilities are properly functioning up to and including the HTTP service. This would include any TSP provided facilities including firewalls, DNS servers, routers, hubs, LANs, etc. that are between the TSP's HTTP server and the ISP's point of presence.

Note: In this context redundancy refers to normal operations redundancy (as opposed to disaster recovery contingencies).

Private network connections to access EDM-REQ sites may be at any point on the TSP's firewall boundary at the TSP's discretion on a nondiscriminatory basis. The specific type and speed of their connection should be mutually agreed. It is at the discretion of the TSP on how multiple private network connections should be managed. TSPs are not responsible for any additional security exposures when using private network connections.

TCP Communications

NAESB/GISB Principle 4.1.37 and NAESB/GISB Standard 4.3.70 restrict the TCP ports used as a standard for EDM-REQ communications. The use of NAESB/GISB standard ports may require modifications in the client-side firewall to allow for communications with the various service providers' EDM-REQ* implementations. Upon request, the TSP should indicate to their trading partners which specific TCP ports they will require to be opened to conduct electronic communication.~~Allowable TCP Ports (not UDP ports)~~

~~HTTP 80, 5713, 6112, 6304, 6874, 7403~~
~~SSL 443~~
~~ICA® 1494~~
~~RMI(Java®) 1099-1100~~
~~Java® Telnet 31415~~
~~TCP Optional 8001-8020**~~

~~Allowable UDP Ports (not TCP ports)~~

~~Secure ICA 1604~~

~~There are other technologies available that would require additional ports to be opened, such as FTP, Telnet, and SMTP. If and when GISB approves such technologies, FTTF will modify this list of allowable ports accordingly. The client-side firewall implementation and client browser settings should permit the downloading and installation of GISB approved plug-ins and modules. Please refer to the GISB defined Minimum Technical Characteristics for Accessing Customer Activities Web Sites for the listing of GISB approved plug-ins and modules.~~

These guidelines will be reviewed and updated by the Future Technology Task Force, at a minimum, by the spring of each year and presented to the NAESB/GISB Executive Committee for adoption by the June meeting of that group.

*All NAESB/GISB standard Internet communications.

Major functions of ~~Internet~~ EDM-REQ covered by ~~the~~ NAESB/GISB Standards~~Major functions of the Internet EDM Model covered by the Standards~~

Communication Protocols

HTTP is the standard protocol and Post is the standard method by which transactions will be transmitted over the public Internet. The content type used to package the X12 or NAESB/GISB standard format file and its related parameters for the HTTP request is multi part. This provides more flexibility in the coding of the messaging components in the application because of the way it handles the delimiting of data parts passed in the body of the form as the "package"~~ is typically called in technology circles~~.

ICA® is a registered trademark of Citrix Systems Inc.

JAVA® is a registered trademark of Sun Microsystems, Inc.

Sending Transactions (Client)

It is possible to send transactions using widely available interactive web browsers. This may be appropriate for ~~shippers~~ parties who do not have a significant number of transactions to send each day.

It was determined that in order to provide the level of automation required by some organizations such as a large ~~pipeline~~ energy company to handle the volume of transactions and the level of interface needed for possibly many back-end process applications, a fully automated batch browser is a required component of the application. In this form, the batch browser can be an event-driven mechanism used to push the transaction from the sender's previous processes (the back-end application, the translation, and the security process) across the Internet to the trading partner's server site where receipt of the transaction is acknowledged. The automated batch browser would also better serve the logging function of transactions being sent.

Receipt of Transactions (Server)

The receipt of transactions in the multi part HTTP Post request would require some form of Common Gateway Interface (CGI) program in order to send back a response that would notify the batch browser that it has received the transaction and whether the file in its unprocessed form and its parameters were accepted as sent or rejected. This component of the application would be able to parse out the parameters and related file and determine if the appropriate parameters had been transmitted with the file, log the appropriate statistics including a time stamp about the file and parameters, store the file and send the response back to the batch browser with the time stamp and other required response elements. If the transacting parties mutually agree to use signed receipts, then the application would additionally attach a digital signature to the response. After the appropriate processes have taken place in the CGI, the file would then be forwarded to the security process, any translation necessary, and finally the back-end processor.

Security

Though many decisions as to overall security measures are left to each trading partner and their environment, several security measures were established as standards to ensure a minimum level of confidence in conducting business over the Internet and to provide some uniformity in the implementation of security.

Four primary security aspects were considered as vital in providing the level of protection of transactions needed for energy industry commerce:

- data privacy
- data integrity
- authentication
- non-repudiation

The FTTF found that these concerns are addressed by the use of encryption and digital signature capability of the Pretty Good Privacy (PGP) security application. Any process used for encryption and decryption compatible with PGP 2.6 (using keys generated with the RSA algorithm) meets the minimum standard to be applied to files transmitted over

the Internet.

Additionally, the OpenPGP standard, defined by IETF RFC 2440, is a supported alternative to PGP 2.6. Implementers of the PGP product should consider upgrading to PGP version 6.5 for compatibility with the OpenPGP standard and all previous versions of PGP. To prevent unwanted intruders from connecting to the Web sites, basic authentication is the required standard. Additional issues such as firewall security are discussed in the standards, but are considered implementation issues to be addressed by each organization.

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 ~~natural gas~~ energy transactions.

0.1.2 For NAESB/GISB purposes, 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.

Standard:

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.

1. when 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.

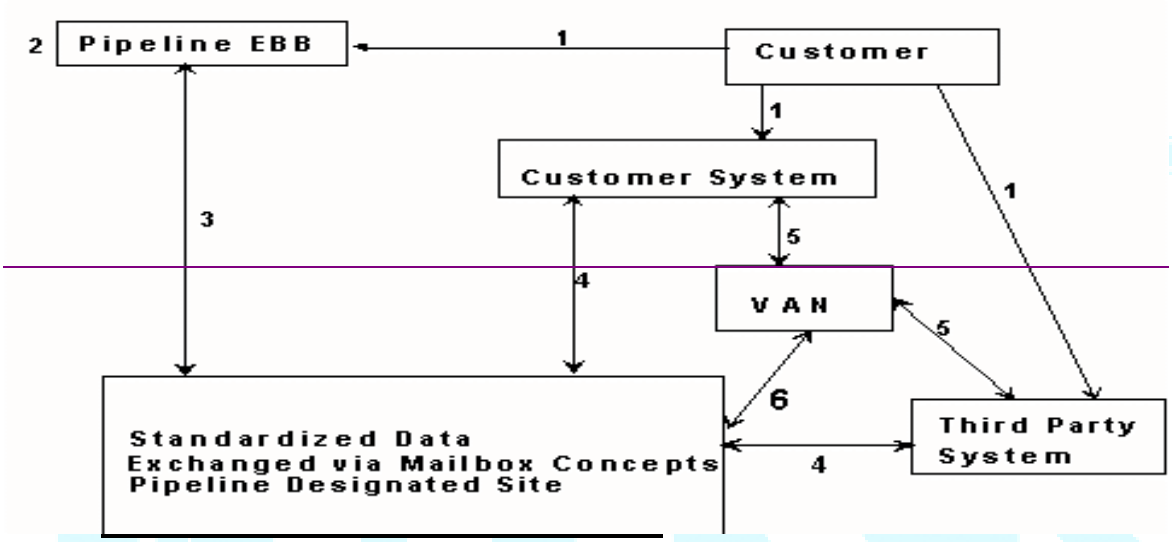
C. Electronic Delivery Mechanism Related Standards

Principles:

4.1.1 [Deleted] ~~The technology model and principles should be followed in implementing GISB's business standards electronically. The following schematic describes the EDM technology model that should exist post 4/1/97, that as agreed upon in the following standard is subject to validation:~~

~~**FUTURE TECHNOLOGY MODEL**~~

~~1. Technology and mechanisms that are at the sole discretion of the customer.~~
~~2. Technology and mechanisms that are at the sole discretion of the provider.~~



4.1.2 The EDM-REQ does not pick winners, rather it should create an environment where the marketplace can dictate a winner or winners.

4.1.3 The solutions should be cost effective, simple and economical.

4.1.4 The solutions should provide for a seamless marketplace for ~~natural gas~~energy.

4.1.5 [Deleted]

4.1.6 Data providers (transportation service providers) should interface with ~~third party~~third-party vendors according to NAESB/GISB standards.

4.1.7 Electronic communications between parties to the transaction should be done on a nondiscriminatory basis, whether through an agent or directly with any party to the transaction.

4.1.8 [Deleted]

4.1.9 Service providers should post clear and precise business processing rules at the designated site, or in writing, upon request.

4.1.10 There should be at least one standard (computer-to-computer exchange of transactional data) for data exchange format.

4.1.11 ~~The proposed future technology model reflects a minimum standard capability for 4/1/97. This model represents an ongoing process and is subject to later revisions depending on the findings of the Future Technology Task Force.~~[Deleted]

4.1.12 Protocols and tools that parties elect to support should be “Internet-compatible”.

4.1.13 ~~Regarding the request that EBBs need to provide the ability to create and print specialized reports, the data should be made available so as to permit the users of the information to download the data to be used in their applications.~~[Deleted]

4.1.14 The industry should use standard policies and guidelines for testing new data sets. These guidelines are currently being developed using the NAESB/GISB guideline adoption procedures (GAP).

4.1.15 ~~The~~ NAESB/GISB should not set standards for site-level security. Individual organization security standards should be relied upon.

4.1.16 ~~Informational Postings Web Sites should be easy to locate.~~[Deleted]

4.1.17 ~~Information within an Informational Postings Web Site should be easy to locate.~~[Deleted]

4.1.18 ~~Information across Informational Postings Web Sites should be consistently displayed.~~[Deleted]

4.1.19 ~~Information across Informational Postings Web Sites should be easy to download.~~[Deleted]

4.1.20 ~~Display space for content on Web sites should be maximized.~~[Deleted]

4.1.21 ~~On the Web sites, the use of scrolling, especially left to right, should be minimized.~~[Deleted]

4.1.22 ~~Web site standards should not preclude various levels of user response and inter-activity. Minimum levels of user response or inter-activity should be developed.~~[Deleted]

4.1.23 ~~Web site standards should not dictate or limit back-end development technology or systems. Industry Web sites should be accessible by a Standard Client Configuration.~~[Deleted]

4.1.24 ~~A standardized Web site navigational structure should be developed to provide access to business functions. The hierarchical relationship, structure and order for navigation on the Web site should be established in a standardized manner.~~[Deleted]

4.1.25 ~~Additional Informational Postings under Standard No. 4.3.6 which are not yet standardized for Web sites should be communicated over the Internet via a “common look and feel” standardized Web page.~~[Deleted]

4.1.26 ~~Customer Activities Web sites should be designed for ease of user interaction.~~[Deleted]

4.1.27 ~~There should generally be a one-to-one relationship between data elements used for EDI and/or flat files and the data displayed on Customer Activities Web pages.~~[Deleted]

4.1.28 ~~Standard field name descriptors or abbreviations, and navigation and functional screen layouts should be used on all Customer Activities Web pages. There should be no standards for font size, colors, etc. Functional screen layouts should be developed as standards which would divide each transactional screen into separate areas and define which data elements belong in each specific area.~~[Deleted]

4.1.29 ~~Information that is constant for the displayed Content Area may be placed in the page Header.~~[Deleted]

4.1.30 ~~Data elements that have default values may be placed last to minimize scrolling.~~[Deleted]

4.1.31 ~~As a general guideline, the initial phase of each business function category (of a multiple phase implementation) of common look and feel for Internet transactions that are not currently standardized should begin subsequent to the implementation of the currently standardized data sets to the Web. This does not preclude the implementation of new standardized data sets as they become available.~~[Deleted]

4.1.32 ~~There is displayed information on Customer Activities Web sites which does not have a comparable data element in EDI; however, the data (e.g. totals, reports, calculations) is derived from other EDI data elements. Provision of such information does not require the development of an EDI data set to accomplish a one-to-one match. However, any Customer Activities Web function should be derivable from information available in EDI data sets.~~[Deleted]

4.1.33 When standardized, all elements used in standard ~~EBB/EDM,~~ EDI/EDM ~~and FF/EDM~~ should be defined in the related NAESB/GISB x.4.z standard.

4.1.34 ~~For GISB FF/EDM, the content and usage of flat files should reasonably correspond to the GISB data sets used for GISB EDI/EDM.~~[Deleted]

4.1.35 ~~If GISB FF/EDM is implemented, flat files should be exchanged via the GISB EDI/EDM site or the Customer Activities Web site.~~[Deleted]

4.1.36 Trading partners should maintain redundant connections to the public Internet for EDM-REQ Web sites, which include all NAESB/GISB standardized Internet communication. These redundant connections should be topographically diverse (duality of) paths to minimize the probability of a single port of failure.

4.1.37 ~~Transportation Service Provider~~ EDM implementations should minimize the number of outbound ports required to be opened on the client-side firewall.

4.1.38 ~~Until such time as GISB standardizes field lengths for data elements, data element field lengths for FF/EDM should not exceed the corresponding field lengths defined for EDI/EDM as defined in the ANSI ASC X12 version in the GISB implementation guide in which the GISB data element was adopted.~~[Deleted

4.1.39 Trading Partners should mutually select and ~~utilize~~use a version of the EDM-REQ standards under which to operate, unless specified otherwise by government agencies. Trading Partners should also mutually agree to adopt later versions of the EDM-REQ standards, as needed, again unless specified otherwise by government agencies.

Definitions

4.2.1 [Deleted]~~"Informational Postings" is the term that identifies common information, which would include the five required postings under Standard 4.3.6.~~

4.2.2 ~~"Download" is the term used to describe the retrieval of information from a Web site in a format suitable for storage.~~[Deleted]

4.2.3 ~~"Display" is the term used to describe the typical visual presentation derived by a browser as a result of retrieval of information from a given URL.~~[Deleted]

4.2.4 ~~"Printing" is the term used to describe the typical printed layout derived when a document is printed from a display tool (browser, word processor, etc.).~~[Deleted]

4.2.5 ~~"Site Map" is the term used to describe a Web page of URL links, which resembles a table of contents or directory tree structure, of categories and subcategories of information.~~[Deleted]

4.2.6 ~~"Central Address Repository" (CAR) is the term used to describe: 1) the Web site providing links to all Transportation Service Providers' Informational Postings, and 2) the entity administering and maintaining the above Web site and repository.~~[Deleted]

4.2.7 ~~"Navigational Area" is the term used to describe the area on the left side of the browser display providing links to the Content Area and other navigational links. Navigational Area is not required to be displayed on Customer Activities Web pages where data entry, reporting or inquiry are displayed.~~[Deleted]

4.2.8 ~~"Content Area" is the term used to describe the area directly to the right of the Navigational Area of the browser display. When the Navigational Area is not displayed the entire browser display is content area.~~[Deleted]

4.2.9 ~~"Standard Client Configuration" is the term used to describe the configuration that allows simultaneous access to multiple industry Web sites.~~[Deleted]

4.2.10 ~~"Customer Activities" is the term used to refer to the business function categories relating to Nominations, Flowing Gas, Invoicing, Capacity Release, Contracts and other business functions on industry Web sites.~~[Deleted]

4.2.11 "NAESB/GISB 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 NAESB/GISB standards in the NAESB/GISB Implementation Guides and communicated between trading partners over the Internet using the EDM-REQ.

4.2.12 ~~"GISB 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 GISB standards. GISB FF/EDM is communicated between trading partners over the Internet using the GISB Electronic Delivery Mechanism.~~[Deleted]

4.2.13 ~~"GISB EBB/EDM" is the term used to describe the GISB standardized electronic interchange of information for Customer Activities Web site presentations. GISB EBB/EDM is communicated between trading partners over the Internet using the GISB Electronic Delivery Mechanism for GISB EBB/EDM.~~[Deleted]

4.2.14 ~~"Header" is the term used to describe the area at the top of the Content Area of the browser display.~~[Deleted]

4.2.15 ~~"Detail" is the term used to describe the area directly below the Header in the Content Area of the browser display.~~[Deleted]

4.2.16 ~~"Form" is the term used to describe the portion of the Content Area of the browser display on Customer Activities Web sites used for single transaction entry or display as well as, optionally, data selection. The Form should be either in the upper portion of the Content Area or, alternatively, a single page linked to the Matrix.~~[Deleted]

4.2.17 ~~"Matrix" is the term used to describe the portion of the Content Area of the browser display on the Customer Activities Web sites used to display selected data entered on the Form and, when appropriate, for data entry. The Matrix should be either the lower portion of the Content Area (that area below the Form) or, alternatively, a single page linked to the Form.~~[Deleted]

4.2.18 ~~"Batch Flat File" is the term used within GISB FF/EDM to describe the automated computer-to-computer transfer of flat files.~~[Deleted]

4.2.19 ~~"Interactive Flat File" is the term used within GISB FF/EDM to describe the transfer of flat files using an interactive browser.~~[Deleted]

4.2.20 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/GISB EDM Related Standards).

4.2.21 "Failover" defines a scenario a prescribed process is executed when a NAESB/GISB client fails to establish a connection to the target NAESB/GISB server.

4.2.22 "EDM-REQ" is the version of the NAESB/GISB EDM that has been tailored to the specific needs of the Retail Electric Quadrant, and based on the NAESB/GISB WGQ EDM. The REQ expects that this version will one day be merged back into a NAESB-

wide EDM.

4.2.23 "Trading Partner" is a party that enters into an agreement with another party to transact business electronically using the EDM-REQ standard.

4.2.24 "TDSP" – Transmission and Distribution Service Provider. Texas ERCOT term for a Utility; generally analogous to LDC, EDC.

4.2.25 "LDC" – Local Distribution Company

[Do we want to include some of the names of entities in the REQ, such as those above?]

4.2.26 "Originating party" is any party originating/creating the document reflecting the transaction to be submitted. This could also include a third-party.

4.2.27 "Third-Party" is any organization that a trading party uses to provide services to comply with the required elements of the EDM-REQ.

4.2.28 "Receiving Party" is any party that hosts (either in-house or outsourced) an EDM-REQ compliant server capable of receiving EDM-REQ transaction files.

4.2.29 "Trading Partner Agreement" is a legal agreement between trading parties. This agreement often dictates service level agreements and problem remediation processes. [Will there be an REQ TPA standard?]

Standards

4.3.1 By 4/1/97, all parties sending and receiving data should accept a TCP/IP connection. At a minimum, sending and receiving parties should designate an Internet address as a designated site for the receipt and delivery of NAESB/GISB standardized data sets subject to the successful completion of pilot testing by 1/1/97 to ensure that security, performance (within NAESB/GISB standard data transmission time), and reliability are acceptable. The NAESB/GISB data file format should be ~~utilize~~used. The Future Technology Task Force should determine the direction of outstanding issues such as security, archiving, receipt notification, etc., by 7/1/96.

4.3.2 On time stamping, data leaves control of the originator by the same time (deadline), regardless of mechanism (third-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 by 4/1/97.

4.3.3 ~~Originating party is any system originating/creating the document reflecting the transaction to be submitted (this could also include a third-party service provider or a transportation service provider's EBB).~~ {Within the 15-minute communication window identified in 4.3.2, the transaction file should be received by the receiving party. Errors in transmission shall be governed by the terms and conditions of the trading partner agreement between the parties. The receiving party may also waive the 15-minute window requirement at its own discretion.}

4.3.4 For audit purposes parties ~~Trading partners~~ should retain transactional data for at least 24 months ~~for audit purposes~~. This data retention requirement only applies to the ability to recover or regenerate electronic records for a period of two years and does not otherwise modify statutory, regulatory, or contractual record retention requirements.~~Transactional data should be retained for at least 24 months for audit purposes.~~

~~This data retention requirement only applies to the ability to recover or regenerate electronic records for a period of two years and does not otherwise modify statutory, regulatory, or contractual record retention requirements.~~

4.3.5 ~~Documents that are made available on the Transportation Service Provider's designated site should be downloadable on demand in a GISB specified electronic structure.~~[Deleted]

4.3.6 ~~Transportation Service Providers should establish a HTML page(s) accessible via the Internet. The following information should be posted:~~[Deleted]

~~1) Notices (critical notices, operation notices, system wide notices, etc.)~~

~~2) FERC Order No. 566 affiliated marketer information. (affiliate allocation log, 24 hr. discount posting, etc.)~~

~~3) Operationally available and unsubscribed capacity~~

~~4) Index of customers~~

~~5) Transportation Service Provider's tariff (Terms, conditions and rates), or general terms and conditions.~~~~By August 1, 1997 Transportation Service Providers should establish a HTML page(s) accessible via the Internet's World Wide Web. The information that is currently provided should be posted as follows:~~

~~1)Notices (critical notices, operation notices, system wide notices, etc.)~~
~~2)FERC Order No 566 affiliated marketer information. (affiliate allocation log, 24 hr. discount postings, etc.)~~
~~3)Operationally available and unsubscribed capacity~~
~~4)Index of customers~~
~~5)Transportation Service Provider's tariff (Terms, conditions and rates), or general terms and conditions.~~
~~and~~

~~Transportation Service Providers should make all pertinent EBB functions and information available via the Internet or via the technology recommended by GISB within a reasonable amount of time after each such function or information has become standardized as appropriate by GISB.~~
~~and~~

~~Within a reasonable amount of time, all EBB information, functions and transactions should be achieved via one mode of communications. Information and functions should remain available through existing systems until one mode of communication is available. Implementation time lines for this activity would be determined during the 1997 annual planning activities held in 1996.~~ 4.3.7 ~~At a minimum, the designated 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.~~[Deleted]

4.3.8 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/GISB.~~The minimum acceptable protocol should be HTTP. All sending and receiving parties should be capable of sending and receiving using HTTP.~~

4.3.9 ~~For NAESB/GISB EDI/EDM, there is~~ EDM REQ has a time stamp (HTTP Timestamp) that designates the time that a file is received at the designated site. The receiving party should generate a timestamp upon successful receipt of the complete file and send as an immediate response to the sending party. The timestamp should be generated by Common Gateway Interface (CGI) of the receiving party, prior to further processing by the CGI.

4.3.10 The time-stamp should be included in the HTTP response back to the sender of ~~the~~ original HTTP transaction. The server clock generating the time-stamp should be synchronized with the National Institute of Standards and Technology (NIST) time in order to mitigate the discrepancies between the clocks of the sender and receiver.~~The time-stamp should be included in the HTTP response back to the sender of the original HTTP transaction. It is recommended that the server clock generating the time-stamp 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.~~

4.3.11 The HTTP response should be sent to the sending Internet Protocol (IP) address. Other response documents should be returned to the official designated site defined in the Trading Partner Agreement.

4.3.12 As a minimum, within a trading partner agreement, 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.

4.3.13 The sender should make three attempts to complete a unit of work. After three failed attempts, it should be considered a failure.

4.3.14 The roles of sender and receiver are defined in following table. The entire table defines a unit of work:

Client (Sender)	Server (Receiver)	CGI (Receiver)
	Listen for Connect	
Connect	Accept Connection	
Write	Read	Start of Receipt
Write	Read	
EOF (send)	Read	End of Receipt

Read (HTTP response) Write (HTTP response)
Received
EOF (HTTP response)

4.3.15 Trading partners should implement all security features (secure authentication, integrity, privacy, and non-repudiation) using a file-based approach via a commercially available implementation of PGP 2.6 or greater (or compatible with PGP 2.6) or an OpenPGP compatible product, such as GNU Privacy Guard. Trading partners should also implement basic authentication. This should be regarded as an interim solution since this technology is not an open standard. This technology supports all of the above security features while providing independence of choice of Web servers and browsers. Encryption keys should be self-certified and the means of exchange should be specified in the trading partner agreement. 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 PGP public key. A lifetime of one year or less is recommended.~~Trading partners should implement all security features (secure authentication, integrity, privacy, and non-repudiation) using a file-based approach via a commercially available implementation of PGP 2.6 or greater (or compatible with PGP 2.6). Trading partners should also implement basic authentication. This should be regarded as an interim solution since this technology is not an open standard. This technology supports all of the above security features while providing independence of choice of Web servers and browsers. Encryption keys should be self-certified and the means of exchange should be specified in the trading partner agreement.~~

4.3.16 ~~The documents identified in~~ NAESB/~~GISB~~ ~~Standard 4.3.6 should be made available in HTML or RTF format, except with respect to the Index of Customers document which may be displayed in HTML or RTF and which should be downloadable in a defined, tab-delimited ASCII text file, with provisions for title information and footnote capability, as set forth in Code of Federal Regulations Part 284, Section 223. (Reference Order Number 637, Docket No.RM98-10-000, issued February 9, 2000, "Appendix A, Instruction Manual for Electronic Filing of the Index of Customers" issued pursuant to the above referenced order.'~~[Deleted]~~The documents identified in GISB Standard 4.3.6 should be made available in HTML or RTF format, except with respect to the Index of Customers document which may be displayed in HTML or RTF and which should be downloadable in a defined, tab-delimited ASCII text file, with provisions for title information and footnote capability, as set forth in Code of Federal Regulations Part 284, Section 223. (Reference Order Number 637, Docket No. RM 98-10-000, issued February 9, 2000, "Appendix A, Instruction Manual for Electronic Filing of the Index of Customers" issued with the above referenced order.)~~

4.3.17 ~~"Informational Postings" should be the label used for navigation to or within the Web site.~~[Deleted]

4.3.18 ~~Transportation Service Providers should provide and keep current to the Central Address Repository the addresses (URLs) for the following in a specified format and communication method(s):~~[Deleted]

~~Informational Postings~~
~~Affiliated Marketer Info.~~

~~Capacity~~
~~Index of Customers~~
~~Notices~~
~~Tariff~~
~~Downloads~~
~~Site Map~~

~~This specification and any changes to it should be subject to GISB approval.~~

4.3.19 ~~The Central Address Repository should make available a consolidated repository of the Transportation Service Providers' current URLs listed in Standard 4.3.18 in two ways: 1) a vehicle to link to sites and categories, and 2) a downloadable list.~~[Deleted]

4.3.20 ~~A user ID or password should not be required to access the Central Address Repository or the Transportation Service Provider's Informational Postings Web Site.~~[Deleted]

4.3.21 ~~The categories and the labels for Informational Postings required under Standard 4.3.6 should be as follows:~~[Deleted]

4.3.22 ~~The following navigational links should appear last in the Navigational Area and be labeled as follows:~~[Deleted]

~~Downloads~~
~~Search~~
~~Site Map~~

4.3.23 ~~The subcategories and labels for the categories of Informational Postings should be as follows:~~[Deleted]

~~CATEGORIES~~	~~SUBCATEGORIES~~
~~Affiliated Marketer Info.~~	~~Capacity Allocation Log (when applicable)~~ ~~Discount Offers~~
~~Capacity~~	~~Operationally Available~~ ~~Unsubscribed~~
~~Index of Customers~~	
~~Notices~~	~~Critical~~ ~~Non-Critical~~
~~Tariff~~	~~Title Page~~ ~~Table of Contents~~ ~~Preliminary Statement~~ ~~Map~~ ~~Currently Effective Rates~~ ~~Rate Schedules~~ ~~General Terms and Conditions~~ ~~Form of Service Agreement~~ ~~Entire Tariff~~

~~Sheet Index~~

~~Posted Imbalances~~

4.3.24 ~~The Transportation Service Provider's Informational Postings Web Site should include the name, nickname, or name abbreviation of the Transportation Service Provider so that it will appear first in the browser title bar. Content Area documents should have a similar name when printed.~~[Deleted]

4.3.25 ~~The Site Map should be provided in the Content Area and should include links to all levels of categories described in Standard 4.3.21 and Standard 4.3.23. Each level of category and subcategory should be indented to show its relationship and should be presented in text form to best utilize space.~~[Deleted]

4.3.26 ~~Transportation Service Providers should provide search capability for a word or phrase within the text, headers, and footers of the entire tariff and within any of the following tariff subcategories: 1) Rate Schedules, 2) General Terms and Conditions, and 3) Form of Service Agreement. The results of the search should provide a list of links to the pages containing the word or phrase. "Search" should appear as a link and be labeled as such, appearing immediately above the Site Map link.~~[Deleted]

4.3.27 ~~The "Notices" category (as shown in the Navigational Area) should expand to a list of subcategories (in the Navigational Area) when clicked; there are no display requirements for the Content Area. Each of these subcategories, when clicked, should display a list of notices for that subcategory in the Content Area.~~[Deleted]

4.3.28 ~~For the subcategories of Notices, the first column headings in the Content Area should be Notice Type, Posted Date/Time, Notice Effective Date/Time (and Notice End Date/Time, when applicable), Notice Identifier (optional*), Subject and Response Date/Time, when applicable, with the list sorted in reverse chronological order by Posted Date/Time.~~[Deleted]

~~* When used as a reference, the Notice Identifier should be displayed.~~

4.3.29 [Deleted]~~The words or labels that should appear in the "Notice Type" column in Standard 4.3.28 should be:~~

~~Words~~	~~Labels~~
~~Capacity Constraint~~	~~Cap. Constraint~~
~~Capacity Discount~~	~~Cap. Discount~~
~~Curtailment~~	~~Curtailment~~
~~Force Majeure~~	~~Force Majeure~~
~~Intraday Bump~~	~~Bump~~
~~Maintenance~~	~~Maintenance~~
~~Operational Flow Order~~	~~OFO~~
~~Phone List~~	~~Phone List~~
~~Press Release, Company News~~	~~News~~
~~Other~~	~~Other~~

4.3.30 ~~The links to categories of Informational Postings should be displayed vertically on the left (Navigational Area) of the screen at all times.~~[Deleted]

4.3.31 ~~With regard to Informational Postings, when using abbreviations to display column and field names, the following abbreviations should be used:~~[Deleted]

~~Available~~	~~Avail~~
~~Capacity~~	~~Cap~~
~~Date/Time~~	~~D/T~~
~~Description~~	~~Desc~~
~~Effective~~	~~Eff~~
~~Location~~	~~Loc~~
~~Quantity~~	~~Qty~~
~~Maximum Daily Quantity~~	~~MDQ~~
~~Maximum Storage Quantity~~	~~MSQ~~

4.3.32 ~~Each line of the Table of Contents of the Tariff should provide a link to a corresponding sheet by clicking on the sheet number shown. The subcategories Currently Effective Rates, Rate Schedules, General Terms and Conditions, and Form of Service Agreement should provide either a table of contents or a similar breakdown, when applicable, and a link function to a corresponding sheet. For example, if General Terms and Conditions has a separate table of contents, it should provide corresponding links.~~[Deleted]

4.3.33 ~~For Tariff documents, "previous" and "next" links should be displayed at the top of each HTML document. If the "previous" and "next" links may scroll off the display, they should also be provided at the bottom of the HTML document.~~[Deleted]

4.3.34 ~~Columns and data fields that would contain data not supported by the Transportation Service Provider should be eliminated on display and/or entry, and left empty on download.~~[Deleted]

4.3.35 ~~For the "Index of Customers", the column headings for the web site display for the "Index of Customers" should be displayed in the order provided for in reference Order No.637, Docket No. RM98-10-000, issued February 9, 2000, "Appendix A, Instruction Manual for Electronic Filing of the Index of Customers" issued June 29, 2000, pursuant to the above referenced order, for those fields identified as "detail fields". In addition, the other "Index of Customers" information not included in the columnar display should be accessible from the columnar display.~~[Deleted]

~~For the "Index of Customers", the column headings for the web site display for the "Index of Customers" should be displayed in the order provided for in reference Order No. 637, Docket No. RM98-10-000, issued February 9, 2000, "Appendix A, Instruction Manual for Electronic Filing of the Index of Customers" issued June 29, 2000, pursuant to the above referenced order, for those fields identified as "detail fields". In addition, the other "Index of Customers" information not included in the columnar display should be accessible from the columnar display.~~4.3.36 Internet protocols should be used for accessing all industry business functions.

4.3.37 ~~Web browser interface should use Internet compatible common browser software.~~[Deleted]

4.3.38 ~~Industry Web sites should be accessible via the public Internet using common browser software.~~[Deleted]

4.3.39 ~~Each implementation of a current proprietary business function category on EBBs should remain available until such time as that business function category is tested and implemented via a Customer Activities Web site.~~[Deleted]

4.3.40 ~~Standard navigation should be used to access all business functions on industry Web sites.~~ [Deleted]

4.3.41 ~~Navigation through the industry Web site menus should be consistent for location and technique.~~[Deleted]

4.3.42 ~~The categories and the labels for Customer Activities Web sites should appear, if applicable, in the Navigational Area as follows:~~[Deleted]

~~Nominations~~
~~Flowing Gas~~
~~Invoicing~~
~~Capacity Release~~
~~Contracts~~
~~Informational Postings~~
~~Site Map~~

~~Links supporting Mutually Agreeable categories should precede Informational Postings~~

4.3.43 ~~The sub-categories and the labels for the category of Nominations should appear, if applicable, in the Navigational Area as follows:~~[Deleted]

~~Nomination~~
~~Confirmation~~
~~Scheduled Quantity~~

~~Links supporting additional sub-categories will follow these links. This does not preclude a further breakdown within each sub-category from being listed in the Navigational Area.~~

4.3.44 ~~A Customer Activities Web page may display information (data elements and code values) from multiple functionally related EDI data sets (i.e. nominated quantities and scheduled quantities may appear on the same Web screen).~~[Deleted]

4.3.45 ~~GISB standard code value descriptions should be displayed for code values where appropriate.~~[Deleted]

4.3.46 ~~The Customer Activities Web Site should include the name, nickname, or name abbreviation of the Transportation Service Provider in the browser title bar. The name of the business function should be displayed in the Header.~~[Deleted]

4.3.47 ~~Where they exist for the same business function, flat files and EDI should use the same nomenclature for data set names, data element names, code values and/or code value descriptions, abbreviations and message text. Corresponding Web pages should use data set names, data element names, code value descriptions, abbreviations and message text that correspond to those used in flat files and EDI, where they exist.~~[Deleted]

4.3.48 ~~Totals, when appropriate, should be displayed within the Content Area of the Web page in a manner which distinguishes them from the data.~~[Deleted]

4.3.49 ~~Where navigation and/or processing functions exist for a Customer Activity, the Content Area should contain navigation in the Header on the left and processing functions in the Header on the right.~~[Deleted]

4.3.50 ~~Navigation for input data lookups, if provided, should be placed near the field being looked up. Navigation for informational lookups, if provided, should be included in the Header.~~[Deleted]

4.3.51 ~~GISB Common Codes for entity and location should be available for data validation or selection (viewing) on a Customer Activities Web site and in a standardized downloadable format for use by customers and third party service providers. Cross-references to proprietary codes may be provided on a mutually agreeable basis.~~[Deleted]

4.3.52 ~~A Transportation Service Provider (TSP) which determines to provide new features utilizing existing transaction sets via GISB EBB/EDM, for each transaction upon inception of support for such service, should:~~[Deleted]

4.3.53 Where a (Transportation Service Provider (TSP) ~~utilize~~uses a subset of available NAESB/GISB code values for specific data elements for inbound documents to the TSP, the TSP should make available a list of the supported code values in a download utilizing a NAESB/GISB electronic format.

4.3.54 ~~With regard to the navigational links on Customer Activities Web sites, when using abbreviations, the following should be used:~~ [Deleted]

~~Full Name~~	~~Abbreviation~~
~~**Customer Activities**~~	~~**Customer Activities**~~
~~Nominations~~	~~Nominations~~
~~Flowing Gas~~	~~Flowing Gas~~
~~Invoicing~~	~~Invoicing~~
~~Capacity Release~~	~~Capacity Release~~
~~Contracts~~	~~Contracts~~
~~Informational Postings~~	~~Info Postings~~
~~Site Maps~~	~~Site Maps~~
~~**Nomination Area**~~	~~**Nominations**~~
~~Nomination~~	~~Nom~~
~~Nomination Quick Response~~	~~Nom QR~~
~~Request for Confirmation~~	~~Req for Conf~~
~~Confirmation Response~~	~~Conf Resp~~
~~Confirmation Response Quick Response~~	~~Conf Resp QR~~
~~Scheduled Quantity~~	~~Sched Qty~~
~~Scheduled Quantity for Operator~~	~~Sched Qty Oper~~
~~**Flowing Gas Area**~~	~~**Flowing Gas**~~
~~Pre-determined Allocation~~	~~PDA~~
~~Pre-determined Allocation Quick Response~~	~~PDA QR~~
~~Allocation~~	~~Allocation~~

~~Shipper Imbalance~~	~~Shipper Imbal~~
~~Measurement Information~~	~~Meas Info~~
~~Measured Volume Audit Statement~~	~~Meas Vol Audit~~
~~Authorization to Post Imbalances~~	~~Auth to Post Imbal~~
~~Posted Imbalances Download Post~~	~~Imbal Dwnld~~
~~Request for Imbalance Trade~~	~~Req for Imbal Trd~~
~~Request for Imbalance Trade Quick Response~~	~~Req for Imbal Trd QR~~
~~Withdrawal of Request for Imbalance Trade~~	~~W/D of Req for Imbal Trd~~
~~Request for Confirmation of Imbalance Trade~~	~~Req for Conf of Imbal Trd~~
~~Imbalance Trade Confirmation~~	~~Imbal Trd Conf~~
~~Imbalance Trade Notification~~	~~Imbal Trd Notify~~
~~Invoicing Area~~	**~~Invoicing~~**
~~Invoice~~	~~Invoice~~
~~Service Requester Level Charge/Allowance Invoice~~	~~Svc Req Invc~~
~~Payment Remittance~~	~~Pmt Remit~~
~~Statement of Account~~	~~Stmt of Acct~~
~~Capacity Release Area~~	**~~Capacity Release~~**
~~Offers~~	~~Offers~~
~~Bids~~	~~Bids~~
~~Awards~~	~~Awards~~
~~Contracts Area~~	**~~Contracts~~**

4.3.55 ~~Where display information on a Customer Activities Web site is derivable from data provided in a previous upload or download, the information should not be included in the EDI/EDM standards [or FF/EDM standard, for later consideration] that directly correspond to the EBB/EDM Web page being displayed.~~[Deleted]

4.3.56 The industry should use common codes for location points and legal entities when communicating via EDI/EDM~~, EBB/EDM and/or FF/EDM. The corresponding common code name should also be used in EBB/EDM.~~

4.3.57 ~~Customer Activities Web pages should support entry of the maximum length for valid data, however, display can be done in a manner to minimize left to right scrolling.~~[Deleted]

4.3.58 ~~On Customer Activities Web pages, informational display fields can be displayed with related data.~~[Deleted]

4.3.59 ~~Providers of Customer Activities Web sites should ensure that the site operates within the guidelines of the "Technical Characteristics of the Client Workstation" described in the Appendix of the Electronic Delivery Mechanism Related Standards Manual. This appendix, listing examples of hardware and software configurations that providers should meet, should be reviewed and updated by the Future Technology Task Force, at a minimum, by the spring of each year and presented to the GISB Executive Committee for adoption by the June meeting of that committee.~~[Deleted]

4.3.60 ~~Access to the Customer Activities Web Site should be protected by HTTP Basic Authentication or similar logon/password mechanism(s). A Customer Activities Web site should typically require a single logon/password pair for each user session.~~[Deleted]

4.3.61 ~~Data communications for Customer Activities Web sites should utilize 128-bit Secure Sockets Layer (SSL) encryption.~~[Deleted]~~At a minimum, data communications for Customer Activities Web sites should utilize 40-bit encryption. Where possible, 128-bit encryption is strongly recommended.~~

4.3.62 ~~Custom downloadable modules presented by a Customer Activities Web site should be signed by the author. The signatures on these modules should be communicated in advance to Web site users.~~[Deleted]

4.3.63 ~~In the Navigational Area of the Informational Postings Web Site, the navigational link for "Customer Activities" should appear directly above the navigational link for "Site Map".~~[Deleted]

4.3.64 Private network connections to EDM~~-~~REQ Web sites which include all NAESB/GISB standardized Internet communication may be at any point on the Transportation Service Provider's (TSP's) firewall boundary at the TSP'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 the TSP on how multiple private network connections should be managed, so long as such management is done on a non-discriminatory access basis. TSPs are not responsible for any additional security exposures when using these private network connections.

4.3.65 ~~The Transportation Service Provider's Customer Activities Web Site should include the name, nickname, or name abbreviation of the parent company and/or Transportation Service Provider so that it will appear first in the browser title bar.~~[Deleted]

4.3.66 ~~When the Form and the Matrix for Customer Activities Web sites are separate Web pages, a subset of the Form may be included by the Transportation Service Provider in the upper Content Area of the Matrix page.~~[Deleted]

4.3.67 ~~A Transportation Service Provider which determines to provide new services which do not utilize existing transaction sets via GISB EBB/EDM, should, prior to implementation, submit a request for standardization to GISB including descriptions of the EBB/EDM, EDI/EDM and, as applicable, FF/EDM implementation.~~[Deleted]

4.3.68 ~~On Customer Activities Web sites, information which is not part of the data dictionary may be displayed.~~[Deleted]

4.3.69 ~~On Customer Activities Web sites, the following standard nomenclature should be used for processing functions, when the associated function is supported by the Transportation Service Provider (TSP). TSPs may also support additional processing functions.~~ [Deleted]

~~Processing Function~~	~~Nomenclature~~
~~Create a new line item for data entry in the Matrix.~~	~~New~~

~~Copy existing data on a screen or window.~~	~~Copy~~
~~Delete the current line item from the Matrix, the screen or the window prior to Submit.~~	~~Delete~~
~~Back out of a screen or window without executing the process, which will cause the loss of all updates since the last Submit.~~	~~Cancel~~
~~Print application data.~~	~~Print~~
~~Send record/records from the Matrix to the TSP for processing.~~	~~Submit~~
~~Sort displayed records based on specified criteria.~~	~~Sort~~
~~Retrieve information from the TSP based on specified criteria.~~	~~Retrieve~~
~~Post a line item from the Form to the Matrix as a change to the current line item in the Matrix prior to Submit.~~	~~Change~~
~~Clear fields on the Form.~~	~~Clear~~
~~Post a line item from the Form to the Matrix as a new record.~~	~~Add~~
~~Provide information regarding the current page or function.~~	~~Help~~
~~Filter displayed records based on specified criteria.~~	~~Filter~~

4.3.70 Transportation Service Providers should be limited to the NAESB/GISB approved list of available TCP ports and UDP ports for EDM-REQ implementations included in the Appendix of the EDM-REQ Related Standards Manual under Client Firewall Requirements for Service Provider EDM-REQ Implementations.

4.3.71 Transportation Service Provider EDM implementations should not require any inbound ports to be opened on the client-side firewall.

4.3.72 ~~Providers of Customer Activities Web sites, at their discretion, may provide alternate views to data and transactions in addition to the GISB basic views (industry common views). The alternate views should not replace GISB basic views and should be offered as separate views, if available. If an alternate view is offered, the GISB basic view should be the default view and clearly labeled as the GISB basic view. Any alternate views must offer the same business result as the basic view and be accessible to all applicable users. The basic views must offer the same business result as the alternate views and be accessible to all applicable users.~~[Deleted]

4.3.73 ~~Data fields used to populate or control population of other fields can be placed before the fields to be populated. If these data elements apply to the entire Content Area they can appear in the Header. If the Transportation Service Provider elects to place such data fields in an order outside of the standardized order, the labels for these data fields should be distinguishable through visual cues from the labels of data elements in the standardized order.~~[Deleted]

4.3.74 Each data element which has been submitted for standardization in the NAESB/GISB process should follow the NAESB/GISB ordered data elements on the Form within a data group selected by the Transportation Service Provider.

4.3.75 ~~The sub-categories and the labels for the category of Flowing Gas should appear, if applicable, in the Navigational Area as follows:~~[Deleted]

~~Pre-determined Allocation~~
~~Allocation~~
~~Imbalance~~
~~Measurement~~

~~Links supporting additional sub-categories will follow these links. This does not preclude a further breakdown within each sub-category from being listed in the Navigational Area.~~

4.3.76 ~~On a Customer Activities Web page, where the Form and the Matrix are combined, any data groupings and ordering for the corresponding Form should apply.~~[Deleted]

4.3.77 [Deleted]

4.3.78 ~~When a Form and a Matrix exist for a Customer Activities Web page, a mechanism should exist to populate the Form with data from a selected item in the Matrix.~~[Deleted]

4.3.79 ~~The sub-categories and the labels for the category of Invoicing should appear, if applicable, in the Navigational Area as follows:~~[Deleted]

~~Invoice~~
~~Payment Remittance~~
~~Statement of Account~~

~~Links supporting additional sub-categories will follow these links. This does not preclude a further breakdown within each sub-category from being listed in the Navigational Area.~~

4.3.80 ~~GISB FF/EDM flat files should be formatted as ASCII comma separated value (CSV) files. This means:~~[Deleted]

~~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.~~

~~Date/Time fields should be formatted as YYYYMMDD HH:MM or YYYYMMDD HH:MM:SS when date and time are expressed in one GISB 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.~~

4.3.81 ~~For a GISB FF/EDM flat file, the first row of the file should be comprised of the standard abbreviations for GISB data elements, including any additional data elements added per GISB Standard No. 4.3.52, in the order in which the corresponding data is to appear in all 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.~~[Deleted]

4.3.82 ~~For GISB FF/EDM flat files, each transaction (e.g. nomination) should be contained in a single row.~~[Deleted]

4.3.83 ~~For Interactive Flat File EDM, 128-bit Secure Sockets Layer (SSL) encryption should be used.~~[Deleted]~~For Interactive Flat File EDM, 40-bit Secure Sockets Layer (SSL) encryption should be used. Where possible, 128-bit SSL encryption is strongly recommended.~~

4.3.84 ~~Access to Interactive Flat File EDM should be protected by HTTP Basic Authentication.~~[Deleted]

4.3.85 ~~The sub-categories and the labels for the category of Capacity Release should appear, if applicable, in the Navigational Area as follows:~~[Deleted]

~~Offers~~
~~Bids~~
~~Awards~~

~~Links supporting Mutually Agreeable sub-categories will follow these links. This does not preclude a further breakdown of sub-sub-categories within each sub-category from being listed in the Navigational Area.~~

4.3.86 ~~To the extent that multiple electronic delivery mechanisms are used, the same business result should occur.~~[Deleted]

4.3.87 [Deleted]~~When the receiver of:~~

~~1) a Nomination,~~
~~2) a Pre-determined Allocation, or,~~
~~3) a Request for Confirmation,~~

~~has determined to change the business rule(s) it will apply to the processing of (and/or response to) one or more of these documents; or, when the sender of:~~

~~1) a Confirmation Response (solicited and unsolicited),~~
~~2) a Scheduled Quantity,~~
~~3) a Scheduled Quantity for Operator,~~
~~4) an Allocation,~~

~~5) a Shipper Imbalance, or,~~
~~6) an Invoice~~

~~has determined to change the business rule(s) it will apply to the generating of (and/or content within) one or more of these documents, then it should notify its trading partners of same at least two weeks in advance of the change(s). The notification should include identification of the data element(s) that are changing (or whose content is 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 which is received by the trading partner sending notice;~~
~~b) a new business response to an accepted data element which is received by the trading partner sending notice;~~
~~c) a new business response to the acceptable content of a data element which is received by the trading partner sending notice; or,~~
~~d) a new intended business result to be communicated to a receiver by the trading partner sending notice;~~

~~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 this standard 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).~~

~~Trading partners receiving notice of such change(s) from their 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.~~

4.3.88 For EDI/EDM, 128-bit Secure Socket Layer (SSL) encryption should be used.

D. Interpretations

NAESB/GISB has adopted the following interpretations of standards that relate to EDM-REQ Related Standards implementation:

7.3.24 ~~Does the language of Standard 2.3.14, 2.3.26, 3.3.15 and 4.3.4 mean that contractual audit rights are excluded from the six-month time limitation and that no statement adjustments can be made after the six-month period? In addition, is GISB recommending that audit rights be excluded from contracts or otherwise limited in contracts to a six-month period?~~[Deleted]

7.3.35 ~~According to Standard 4.3.6, notices are now supposed to be posted on the Transportation Service Providers' (TSP) Web pages. Does this mean that a TSP is not required to provide any alternative form of communication for notices such as telephone or fax, particularly for those notices issued outside of business hours and on weekends?~~[Deleted]

~~According to GISB Standard 4.3.6, notices (critical notices, operation notices, system wide notices, etc.) are supposed to be posted on the Transportation Service Providers' (TSP) Web pages. Does this mean that a TSP is not required to provide any alternative form of communication for these specified notices?~~

~~Interpretation:~~

~~GISB Standard 4.3.6 does not specify any alternative means of notification aside from the Web page nor does it specify that the only means of notification is by means of the Web page. Alternative means of notification for particular information may be required by regulation, tariff or other GISB standards. For example notices pertaining to system wide events of both a critical and non-critical nature (GISB Standard 5.3.18) are implemented via both downloads (GISB Standard 5.4.16) and the Web pages (GISB Standard 4.3.6).~~

Location	Details of Change	Comments
Pargraph 1 & 2	Deleted – dealt with history of DRN common codes and Gas Transaction Points	
Paragraph 3	Modified - EBB working group 5 to REQ-TEIS, deleted reference to FERC order 563, and changed GISB to NAESB while removing references to Capacity Release and	

	Nominations	
Paragraph 4	Changed WGQ to REQ, two places	
Paragraph 5	Deleted – deals with flagging CommonCode fields with *.	
NAESB WGO Electronic Data Interchange Trading Partner Agreement	Deleted entire section – see comments.	I doubt we want to use the WGQ EDI TPA as it stands but we do need a standard document for exchange of technical information. Possibly the Texas model would work, just a thought. Here is the URL for the document discussed in the original paragraph. http://www.naesb.org/protected/tpa980820.doc
Party section	Deleted most of this because it deals with W. G. entities only.	Made a feable attempt at describing Retail Electric Party or Entitiy roles. I am not a word smith so feel free to add/delete/re-write. I think it would be helpful to have a section defining all the entities involved.
ANSI ASC X12 Standards	changed WGQ to REQ	
ISA contents paragraph 2	changed WGQ to REQ & deleted last sentence.	Last sentence can be added back once we decide what to do about a standard document to trade technical information.
ISA contents paragraph 4	changed WGQ to REQ	
GS Contents	change WGQ to REQ	
997 Usage	change WGQ to REQ	
Hypertext Transfer Protocol (HTTP)	change WGQ to REQ	
HTTP Trnasaction-set Codes	Deleted entire table since it is Gas transaction names only.	I feel the tranasction set table needs to be a State by State list, should we just put a reference to each state's documentation or a note of future reference once the standard documents are Identified.

RELATED STANDARDS

Common Codes

~~A decision made in 1993 by a FERC established standards development group (EBB Working Group 5) resulted in a location coding system which cross-references proprietary point codes to a common industry supported location code. This common location code, called the GRID Code, was developed based on the American Petroleum Institute (API) well code model. The FERC, in Order 563-A, directed the industry to establish any necessary relationships and to proceed with the implementation of the GRID Code. To achieve this implementation, in August 1994 trade associations representing three segments of the natural gas industry entered into an agreement with Petroleum Information Corporation (PI) to develop and maintain the PI *GRID*™ Common Code database. As GISB prepared standards for capacity release (July 1995) and nominations (September 1995), GISB fully endorsed the use of the PI *GRID*™ common codes.~~

~~However, after extensive consideration by GISB's Common Code Subcommittee, GISB adopted, on September 30, 1996, a new Common Code for Gas Transaction Points, the NAESB WGQ/PI Data Reference Number (generally referred to as "DRN"). The DRN is a one-to-nine digit, non-intelligent number also assigned by IHS (successor to PI), which has a one-to-one relationship with the PI *GRID*™ Code. For more information, access the NAESB Web Page at www.naesb.org.~~

In keeping with the trends in other industries involved with EDI, ~~EBB Working Group 5~~REQ TEIS ~~recommended~~ recommends the acceptance of the D-U-N-S®[1] Number as a common company identifier. ~~This recommendation was also adopted in FERC Order 563-A.~~ The D-U-N-S® Number is assigned to companies by the Dun & Bradstreet Corporation (D&B). Similarly, ~~as GISB~~ NAESB ~~prepared standards for capacity release (July 1995) and nominations (September 1995), GISB~~ fully endorsed the use of the D-U-N-S® Number common code.

For NAESB ~~WGQ~~ REQ 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~~ REQ 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.~~

~~NAESB WGQ Electronic Data Interchange Trading Partner Agreement~~

~~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~~

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

~~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 utilites, marketers, government entities, and various service providers. The Utilities and Marketers are self explanitory. The government entities may be a state commission such as ERCOT in Texas. The service providers can be a CIS provider and/or EDI/EDM providers.~~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 providers normally will not be identified in the envelope or body of the transaction. The utility, marketer, and government entity will be Identified both in the envelope, or ISA/GS segments and the body of the transaction in the N1 name segments.

~~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).~~

ANSI ASC X12 Standards

The NAESB ~~WGQ~~ REQ standards reflect an industry utilization 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~~ REQ 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~~ REQ 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~~ REQrecognizes this and will add interim usages and code values when required. When NAESB ~~WGQ~~ REQ utilizes an interim solution, NAESB ~~WGQ~~REQ 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~~ REQ 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~~ REQ X12 standards. The segment identifies the sender and receiver of the document. The Interchange Sender 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~~ REQ ~~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~~ REQ 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~~ REQ 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~~ REQ 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 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~~ REQ compliant information into the receiver's application processing. Compliance checking, in a translator, may be set to any of several levels. NAESB ~~WGQ~~ REQ 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.

Hypertext Transfer Protocol (HTTP)

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~~REQ.

~~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 WGQ Standard Number~~	~~Transaction Set Description~~
~~G873NMST~~	~~1.4.1~~	~~Nomination~~
~~G874NMQR~~	~~1.4.2~~	~~Nomination Quick Response~~
~~G873RQCF~~	~~1.4.3~~	~~Request for Confirmation~~
~~G873RRFC~~	~~1.4.4~~	~~Confirmation Response~~
~~G873SQTS~~	~~1.4.5~~	~~Scheduled Quantity~~
~~G873SQOP~~	~~1.4.6~~	~~Scheduled Quantity for Operator~~
~~G874CRQR~~	~~1.4.7~~	~~Confirmation Response Quick Response~~
~~G860PDAL~~	~~2.4.1~~	~~Pre-determined Allocation~~
~~G865PDQR~~	~~2.4.2~~	~~Pre-determined Allocation - Quick Response~~
~~G865ALLC~~	~~2.4.3~~	~~Allocation~~
~~G811IMBL~~	~~2.4.4~~	~~Shipper Imbalance~~
~~G867MSIN~~	~~2.4.5~~	~~Measurement Information~~
~~G867MAUS~~	~~2.4.6~~	~~Measured Volume Audit Statement~~
~~G814RQIN~~	~~2.4.7~~	~~Request for Information~~
~~G814RRIN~~	~~2.4.8~~	~~Response to Request for Information~~
~~G811TSIN~~	~~3.4.1~~	~~Transportation/Sales Invoice~~
~~G820PYRM~~	~~3.4.2~~	~~Payment Remittance~~
~~G822STAC~~	~~3.4.3~~	~~Statement of Account~~
~~G811SRCA~~	~~3.4.4~~	~~Service Requester Level Charge/Allowance Invoice~~
~~G840CROF~~	~~5.4.1~~	~~Offer Download~~
~~G843CRBR~~	~~5.4.2~~	~~Bid Download~~
~~G843CRAN~~	~~5.4.3~~	~~Award Download~~
~~G832CRRC~~	~~5.4.4~~	~~Replacement Capacity~~
~~G843CRWD~~	~~5.4.5~~	~~Withdrawal Download~~
~~G840UPWD~~	~~5.4.6~~	~~Withdrawal Upload~~
~~G840UDOF~~	~~5.4.7~~	~~Offer Upload~~
~~G843UDVL~~	~~5.4.8~~	~~Offer Upload Quick Response~~
~~G840UDRC~~	~~5.4.9~~	~~Offer Upload Notification~~

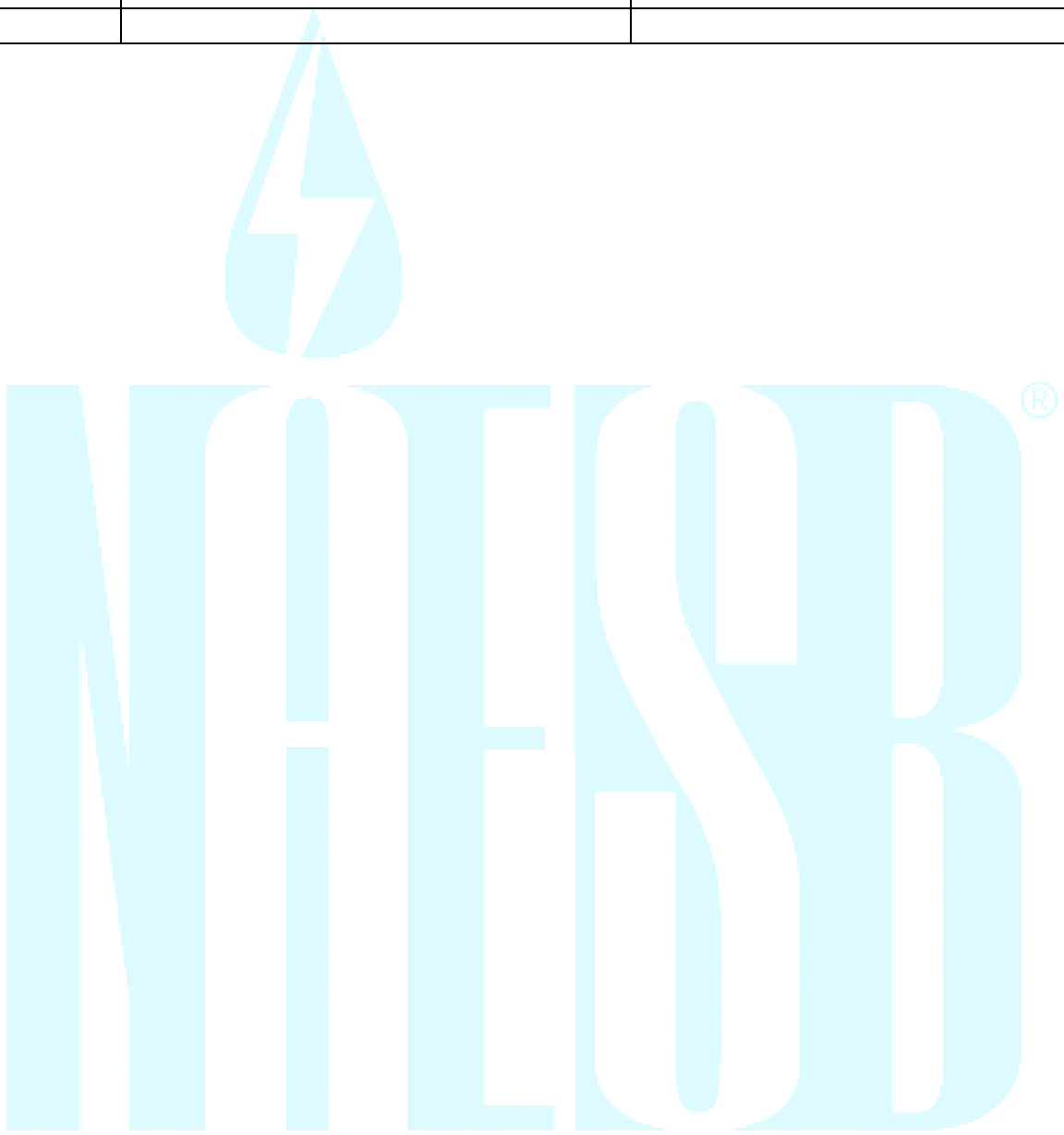
HTTP transaction-set Code Values	NAESB WGQ Standard Number	Transaction Set Description
G843UDBC	5.4.10	Offer Upload Bidder Confirmation
G824UDCV	5.4.11	Offer Upload Bidder Confirmation Quick Response
G567UDFD	5.4.12	Offer Upload Final Disposition
G840OAUC	5.4.13	Operationally Available and Unsubscribed Capacity
G846UPRD	5.4.14	Upload of Request for Download of Posted Datasets
G846RURD	5.4.15	Response to Upload of Request for Download of Posted Datasets
G864SWNT	5.4.16	System-Wide Notices
G864CRNS	5.4.17	Note/Special Instruction
G843BDUP	5.4.18	Bid Upload
G843BDQR	5.4.19	Bid Upload Quick Response
G997FNAK	N/A	Functional Acknowledgement

CHANGE LOG

Tab 6

Section/ Paragraph	Area to Change/Comment	Suggested Change
[all]	Numerous references to WGQ.	Replaced WGQ with REQ
[all]	Numerous references to Batch FF/EDM	Removed references to Batch FF/EDM
Page 51	Extraneous “to”	Removed
Page 52	Common Code Identifier fromat	Tagged as OPEN ISSUE
[all]	Numerous references to gisb-acknowledgment-receipt	Tagged as OPEN ISSUE
Page 52	Description of input-format data element incorrect for REQ use	Removed reference to FF, added XML
[all]	Numerous references to CDI/script	Removed references to CGI/script
Page 52	request-status	Removed reference to decryption process
Page 53	time-c data element lacks time-zone indicator	Added time-zone indicator
Page 53	Transaction-set data element requires enhancement to remove gas industry specific references	Changed transaction-set to 16 character free form text field
Page 54	Diagram	Added EDM Server and simplified
Page 58	Reference to pipeline under Throughput Considerations	Removed pipeline reference
Page 58	HTTP Request Data Elements	Brief description added
Page 59	Incorrect description of transaction-set for REQ purposes	Provided new description for transaction-set, and tagged 8-character names as an OPEN ISSUE
Page 59	Writing a Batch Browser	Removed reference to NAESB home page
Page 59	Description of content type line	Rephrased to indicate that this referred to the specific example on page 59
Page 60	Description of content length	Rephrased to indicate that this referred to the specific example earlier on page 59
[all]	Several references to version 1.4	Changed to 1.6
Page 65	Reference to multipart POST	Tagged implementation as an OPEN ISSUE
Page 67	References to Central time zone	Removed restriction to use Central time
Page 67	Synchronization of client	Added reference to clock accessible via the Internet
Page 67	References to gas nominations	Removed references to gas nominations

Page 67	Brief description of HTTP Request	Moved the description to page 58
Page 68	Using a Web Server	Added reference to the POST method as the only supported HTTP method
Page 68	Timestamp time-c references lack timezone indicator	Added identifier for time zone
Page 68	Text incorrectly indicates that SSL or S-HHTP are optional	Removed references to SSL being optional and all references to S-HTTP
Page 68	The CGI Process	Changed to The Receive Process
Page 68	Text specific to pipelines and gas industry	Replaced with more generic text
Page 69	Reference to C program	Removed
Page 69	Reference to BGI programming	Removed
Page 69	Writing the CGI Process	Changed to Developing the Receive Process
Page 69	Reference to GET operation	Removed
[all]	References to CGI process	Changed to receiving program
Page 69	Reference to standard input	Changed to input stream
Page 71	Reference to standard output	Changed to sending program
Page 71	URL/CGI Implementation Guidelines	Changed to Receive Process URL Implementation Guidelines
Page 71	References to WGQ standard 4.3.12	Tagged as OPEN ISSUE
Page 71	A separate URL for nominations	Replaced by a separate URL may be used for customized processing
Page 72	Text specific to gas industry regarding capacity release	Replaced with more generic text
Page 72	References to Central Time zone	Removed
Page 72	References to nomination deadline	Removed
Page 74	time-c data element has no time zone indicator	Added time zone indicator and provided description of its use
Numerous Examples	examples of gisb-acknowledgement-receipt containing time-c missing time zone indicator	Updated all examples of time-c to include time zone indicator



TECHNICAL IMPLEMENTATION - INTERNET EDM

Technologies Selected by NAESB REQ

The transport protocol for communication of future NAESB REQ transactions should be TCP/IP. In addition, standard Internet protocols should be chosen for specific tasks. Various Internet protocols were considered to accomplish delivery of a transaction at the application protocol level. The Hyper-Text Transfer Protocol (HTTP) was chosen.

Practical information systems require more functionality than simple retrieval, including search, front-end update, and annotation. HTTP allows an open-ended set of methods to be used to indicate the purpose of a request. HTTP is also used as a generic protocol for communication between user agents and proxies/gateways to other Internet protocols, allowing basic hypermedia access to resources available from diverse applications and simplifying the implementation of user agents.

There are two primary Internet software components involved in Web communications. The first is called a browser and runs as client software. The second is called a Web server, or HTTP server and usually runs on a dedicated server computer.

The standard data elements, each with element name and description, have been defined in the Section "Data Dictionary For Internet EDM". The following two sections identify what is involved in sending and receiving transactions. After that comes a discussion regarding the securing of the transactions to be sent. The remaining sections cover considerations for other aspects of the overall process. While these were not the focus of the Internet EDM process as mentioned above, selected topics that may affect your overall implementation are discussed.

Data Dictionary For Internet EDM

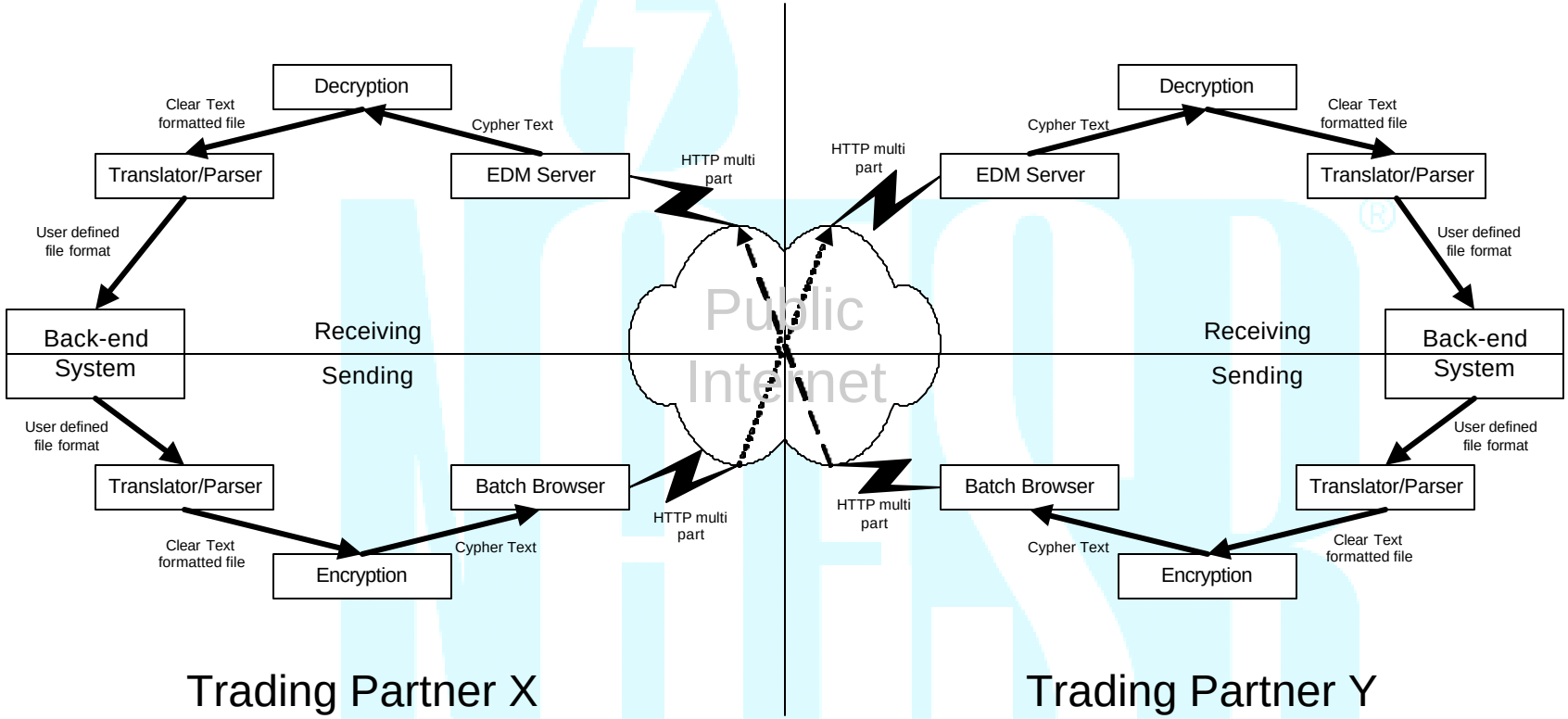
Business Name	Definition	Format	Usage*	Condition
from**	the party sending the transaction	Common Code Identifier format (OPEN ISSUE)	in Request; M	used in file transmittal; displayed in HTTP response; and, used in posting back decryption-related errors
input-data	the filename for the transaction data set transmitted	including drive letter and directory name with filename if needed	in Request; M	used in file transmittal of any transaction data sets; and, used for posting back all transaction value pairs for a transmittal that had decryption-related errors.
input-format	descriptor of the data format used for the file transmit ted	X12 ;XML;error	in Request; M	"X12","XML", or other NAESB REQstandard format indicator used in file transmittal; "error" used in posting back any decryption-related errors
receipt-disposition-to	the party to receive receipts, the value should be the same as the "from"	Common Code Identifier format	in Request; M	used in file transmittal and in posting error notifications
receipt-report-type	type of receipt type being requested by sender	gisb-acknowledgement-receipt (OPEN ISSUE)	in Request; M	used in file transmittal and in posting error notifications
receipt-security-selection	used to request signed receipts	signed-receipt-protocol=required,pgp-signature;signed-receipt-micalg=required,md5	in Request; MA	used in file transmittal and in posting error notifications
refnum	used by the party to assign a unique message identifier for tracing purposes	maximum 40 character integer value	in Request; MA	May be used by sender to send tracking information to a recipient. Use of this data element is by mutually agreed. This data element is conceptually similar to a Message-ID filed within RFC 822.
request-status	status describing success or failure of transmission at recipient server	ok; EEDM###:error description; WEDM###:warning description. see Table A, "Internet EDM Standard Error Codes and Messages"	in Response; M	"ok" is returned if all is fine with processing; error messages/warnings and their related descriptions are returned if problems were encountered in processing.
server-id	uniquely id entifies the server processing the transaction	*domainname* or *hostname.domainname*; no embedded spaces allowed	in Response; M	displayed in the HTTP response and posted back for any decryption-related errors
time-c	the time file transfer is complete at the server, where + or -ZZ indicates delta from UTC (ref ISO 8601)	*yyyymmddhhmmss-ZZ; yyyymmddhhmmss+ZZ*	in Response; M	displayed in the HTTP response and posted back for any decryption-related errors
to **	the party the transaction was sent to	Common Code Identifier format (OPEN ISSUE)	in Request; M	used in file transmittal and displayed in HTTP response and posted back for any decryption-related errors

Business Name	Definition	Format	Usage*	Condition
transaction-set	name of the document type being sent	8 character code (OPEN ISSUE); refer to NAESB REQ Implementation Guide, Related Standards Tab, Hypertext Transfer Protocol (HTTP) section, HTTP transaction-set Code Values table.	in Request; MA	used in file transmittal
trans-id	sequential number assigned to the transaction by the server upon processing before being passed to the decryption process	integer up to 15 characters in length	in Response; M	displayed in the HTTP response and posted back for any decryption-related errors
version	the NAESB REQ EDM version being used by the sender	numeric, decimal notation (e.g. 1.4)	in Request; M	used in file transmittal and in posting error notifications

*The **Usage** column defines whether the element appears in the HTTP Request (Client-generated) or the HTTP Response (Server-generated), the order in which the element appears in the data stream, and whether the field is Mandatory (M) or Mutually-Agreed-To (MA).

** Common Code Identifier (OPEN ISSUE)

Batch Flow Diagram



Batch Flow Diagram

SENDING TRANSACTIONS

General Flow

The following is an example of the steps necessary to send an Internet EDM file:

1. Open HTTP connection
2. Check connection status. If in error, re-queue file according to NAESB REQ standards (this check should be performed here and throughout the following processes)
3. Post
   A. Authentication (password must be base64-encoded)
   B. Send multipart form
   C. Receive HTTP response data
4. Check connection status. If in error re-queue file according to NAESB REQ standards
5. Check HTTP status code (200 is good, less than 300 may be acceptable). If status is not successful re-queue file according to NAESB REQ 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 file according to NAESB REQ standards
11. Remove file from sending queue when successful or when failed completely

If trading partners agree to implement signed receipts then the sending party must include the "receipt-security-selection" data element in the posted data. The receiving party must digitally sign the gisb-acknowledgement-receipt (OPEN ISSUE) and encapsulate the gisb-acknowledgement-receipt (OPEN ISSUE) and digital signature body parts within a MIME envelope with a Content-type of application/pgp-signature.

HTTP Post

Most people think of the Web as the process of using a browser to fetch, or download, documents, not upload them. Indeed, this capability is most prevalent. HTML pages, text files, and other documents can be retrieved by a browser using HTTP, FTP, or other protocols. However Web browsers allow the user to input data to a server using HTML forms. Data is entered into the fields of the form and is transmitted to the server by pressing a pushbutton or hitting the enter key.

The HTTP protocol has two methods for transmitting a request to a server. Both methods return a response to the client, which may be a document retrieved from the server. Both methods can be used to transmit form data. The GET method is the simplest and is used for requests that pass a small amount of information. Data passed with the GET method must be translated into a special format known as "URL encoding." Furthermore, the data stream transmitted by the GET method has a limit of 1024 characters. The POST method, on the other hand, allows the upload of complete datasets without special encoding. It is this method which will be used to send NAESB REQ standard format transactions and receive the response from the server.

Using an Interactive Browser

When most of us think of Web surfing, we think of using an interactive browser. When you enter an HTTP Uniform Resource Locator (URL), the browser opens the HTML document identified by the URL. Basically, a URL is an "address" of an HTML document on a Web server. For purposes of NAESB REQ standards Uniform Resource Locator (URL) is as defined by the Internet Engineering Task Force (IETF).

In order to use an interactive browser to upload data, an HTML document must be created for that function. The HTML document can reside on either the server to which you are uploading or the client's system. The "form" feature of HTML allows that within an HTML document, a form can be created which allows the client to type in any necessary data elements, such as to, from, and input format and then specify a file to be uploaded from the PC. Some type of "Send" button would be on the form and when selected, the form would cause an HTTP POST to be issued, thereby uploading the file. Below is an example of an HTML document with a form which specifies the POST method and contains the required data elements.

An HTML form like that described here could be used with any retail browser that supports multipart POST with a file upload. When choosing a packaged browser, it is mandatory that it supports multipart encoding.

Sample of HTML document with a form to perform a multipart post using an interactive browser:

```
<HTML>
<HEAD>
<TITLE>NAESB REQ File Upload</TITLE>
<H1><CENTER>NAESB REQ File Upload</CENTER></H1>
</HEAD>
<HR>
<BODY>
<form ENCTYPE="multipart/form-data" ACTION="http://www.target.server/cgi-bin/upload.exe"
METHOD=POST>
Enter Common Code Identifier for From and To
From: <input TYPE="text" NAME="from" SIZE=20 VALUE=""><br>
To: <input TYPE="text" NAME="to" SIZE=20 VALUE=""><br>
NAESB REQ EDM Version: <input TYPE=”text” NAME=”version” SIZE=5 VALUE=”1.6”><br>
Deliver Receipt To: <input TYPE=”text” NAME=”report-disposition-to” SIZE=20 VALUE=””><br>
Receipt Type: <input TYPE=”text” NAME=”receipt-report-type” SIZE=30
VALUE=”gisb-acknowledgement-receipt”><br> (OPEN ISSUE)

IF requesting signed receipts also include:

Receipt Type: <input TYPE=”text” NAME=”receipt-security-selection” SIZE=30 VALUE=”signed-receipt-
protocol=required, pgp-signature;signed-receipt-micalg=required, md5”><br>

Format of this file: <input TYPE="text" NAME="input-format" SIZE=6 VALUE="X12"><br>
Send this file: <INPUT NAME="input-data" TYPE="FILE"><br>
<input TYPE="submit" VALUE="Send File"><br>
</form>
</BODY>
</HTML>
```

The non-bolded text in this example is the basic HTML required for a document and allows your page to show a title in the title bar. The bolded text is the form within the document and is described in more detail.

The important characteristics of the form within the HTML document are:

ENCTYPE= specifies the encoding type. The “multipart/form-data” encoding type is identified as the standard encoding methodology.

- ACTION= specifies the URL that will receive the uploaded data. The Trading Partner Agreement identifies the URLs for both parties.
- METHOD= specifies the HTTP protocol method. “POST” has been defined as the NAESB REQ standard method.
- <input ...> Five input areas are specified on this form: from, to, file format, file name, “Send File” button.

NOTE: This document often refers to “multipart POST” which implies the encoding type and method as described in this example.

When a user selects the “Send File” button, the browser will take the values entered in the input fields and reformat them according to the encoding type into a data stream. For the file identified for upload, the file is opened and its contents are included in the data stream, rather than the file’s name. The data stream is then sent to the URL specified by **ACTION=**. The URL will indicate an HTTP server script or program written to receive the data.

For a smaller site only performing a few transactions or file transfers this manual process would be viable as a primary transmission tool. This method could also be considered a back-up method to any batch or automated process that may be implemented. If the client provides its own form, the form can be copied for each trading partner. The only change to the HTML would be to modify the URL shown for the **ACTION=** attribute.

Using a Batch Browser

For companies that have automated much of their back-end process and prefer to avoid unnecessary human involvement, a so-called "batch browser" is needed. This browser needs to be capable of program-based or script-based initiation. At this time, there are few off-the-shelf batch browsers which use the POST method. Most packaged batch browsers use the GET method.

However, a batch browser can be created using custom programming. The batch browser will be coded to perform all of the same formatting that the interactive browser performed to send a data stream which conforms to the HTTP protocol. A batch browser must be coded as a sockets program. See Section “Writing a Batch Browser”.

A sockets program can be written with various programming languages which offer the required library to achieve this function.

Authentication

HTTP basic authentication includes a user-id and password. Interactive browsers include a basic authentication feature which automatically prompts for user-id and password. In a batch browser, the authentication must be specifically coded. The user-id and password are to be base64-encoded within the document header. Base64-

encoding utilities are readily available on the Internet as either public domain software or commercial libraries.

Server Response

The receiving server will send a gisb-acknowledgement-receipt (OPEN ISSUE) as an HTTP response to the client before dropping the client's connection. If the transacting parties agree to use signed receipts, then the receiving server applies a digital signature to the gisb-acknowledgement-receipt (OPEN ISSUE) and encapsulates the entire package in a MIME envelope of Content-type: application/pgp-signature. The response returned from the Web server will contain timestamps that include a timestamp recorded when the final byte from the file upload is received and stored. This timestamp is the official timestamp regarding transaction turnaround deadlines defined in NAESB REQ standards. This timestamp and all other pertinent file transmittal information should be logged when the posted file is stored on the receiving server as well as logged by the client. Likewise, any errors or warnings should be logged at both the server and client.

Throughput Considerations

The performance of the batch browser is one component critical in meeting deadlines. It is conceivable that it may be called many times for a busy site. It should therefore utilize whatever performance techniques are possible. For example, it may be desirable to write a multithreaded version which can handle a certain number of requests simultaneously with a single copy of the program.

HTTP Request Data Elements

The HTTP Request will provide all required data elements in the order defined. Any mutually agreed to data elements will follow the required data elements in the data stream.

Required Data Elements (listed in the required order)

Data Element Name	Description
from	Common Code Identifier of sending/client company.
to	Common Code Identifier of receiving/server company.
version	The NAESB REQ EDM version being used by the sender, in decimal notation (e.g. 1.6) The sending of the "version" data element is intended to assist in the early identification of EDM configuration errors and will not in itself dictate the version which a receiving party will support.
receipt-disposition-to	Common Code Identifier of the party to receive the acknowledgement receipt.
receipt-report-type	Type of receipt requested "gisb-acknowledgement-receipt". (OPEN ISSUE)
input-format	Descriptor of the data format within the input data set.
input-data	The properly formatted file of electronic commerce data.

Mutually Agreed Upon Data Elements

Data Element Name	Description
transaction-set	Descriptor of the transaction types included in the input-data. The values used must be from the unique 8-character names (OPEN ISSUE) defined in the Implementation Standards. See the HTTP transaction-set Code Values table in the Hypertext Transport Protocol (HTTP) section Related Standards Tab for the various transaction types and their corresponding 8-character names. (OPEN ISSUE)
receipt-security-selection	Used to request signed receipts from the party receiving a file upload.

Writing a Batch Browser

A batch browser needs to simulate the actions of an interactive browser. As stated earlier, the interactive browser will take the HTML form and reformat the information according to the HTTP protocol before it sends the data stream to the HTTP server. The reformatting involves adding a header and placing field delimiters around the data items. A batch browser needs to produce the same kind of data stream and therefore, writing a batch browser requires some specific knowledge of the HTTP protocol. First, consider the header:

Example of a typical header sent to the HTTP server

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
Referer: http://www.get.a.life/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
Host: localhost
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Content-type: multipart/form-data; boundary=---------------------------87453838942833
Content-Length: 5379
```

This information is documentary in purpose. The parts that are important are:

The first line: *POST /cgi-bin/AS2dispatcher HTTP/1.1* indicating that the POST method is used and which program to call.

In the example above the content type line is:

Content-type: multipart/form-data; boundary=---------------------------87453838942833

The content-type element indicates that the encoding method is multipart. It also identifies the character string used as the boundary. The boundary will appear between each field as a delimiter. **In this example**, the boundary is comprised of 27 hyphen characters followed by a number.

The boundary can be any character string that you choose except that it is required that it will not to occur anywhere else in the form or in the transaction being sent. This is usually accomplished by using either the system clock or a random number so that even if by some remote chance the string appears in the document it would not appear in any re-transmission of the file. It is strongly recommended that a relatively long string be used as a boundary. The boundary when used as a separator requires two hyphen characters appended to the front of the string as you can note by the lines between the

data fields in the example. The last boundary required in the form is two hyphen characters appended to the back of the separator boundary, this is used to indicate to the server program that this is the end of the data.

In the example above,the content length is:

Content-Length: 5379

The content-length value should match the number of bytes contained in the entity body including the characters in the boundary lines, variable content, blank lines, etc. In essence, it tells the server how much is going to come after this point.

In this example, the data portion, or body, sent to the server program is as follows and assumes only required data elements are sent (not mutually agreed data elements):

```
----------------------------87453838942833
Content-Disposition: form-data; name="from"

123456789
----------------------------87453838942833
Content-Disposition: form-data; name="to"

234567890
----------------------------87453838942833
Content-Disposition: form-data; name="version"

1.6
----------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
----------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt (OPEN ISSUE)
----------------------------87453838942833
Content-Disposition: form-data; name="input-format"

x12
----------------------------87453838942833
Content-Disposition: form-data; name="input-data"; filename="c:\temp\smallnom.bin"
Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"

--8760
Content-Type: application/pgp-encrypted

Version: 1

--8760
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8
sb7ErC340MrNA/dw3taGMjmI+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODGIQxhSuc
z8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/43fkB+alATtgydxX4g8QK6
64ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1Eh785zC03UAw0qg0ug
Mt86dPeyd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8Ocp2IWClxKOGUbxpVNOnNT
qWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ1RqbeNaqx2Dq/ra9g65HNchOCzjul5Vi8
HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0Cvzpb4JE+gMDf3q4ISUb1Fv7/+SSFHDdnh
dC5YTpqf1Bc3B07hiLmtTXqNit31EbX9UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6
FeC9W4cqXLj7IZySaRO8Vtff+4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
--8760--
----------------------------87453838942833--
```

The important characteristics of the above stream are:

- The boundary string appears at the beginning of each data field in the body.
- For each body data field, two identifiers define the contents of the data field. The Content-disposition identifier defines that “form-data” is contained in the element. The name identifier defines the name of the data element. These data element

names must match the name specified by NAESB REQ. The name identifier is not completely relevant since the fields should be present in the correct order but this field should be checked to verify the validity of the form content.

- The actual data value of the field is always preceded by a line termination. This is typically used as a marker for the server program to indicate that a data value will follow. For example, note the blank line preceding "X12" in the above sample. In most programming libraries and commercial products the starting delimiter is "\r\n\r\n" (c notation).

- The data field containing the NAESB REQ standard file has two extra identifiers: first the name of the file sent from the source computer, filename="c:\temp\smallnom.bin", and second a content type identifier on a separate line. This line should always be constructed to reflect the content-type of the data being transmitted, in accordance with accepted Internet standards. If the data file contains clear text, X12 data, as shown in the above example, the content-type identifier follows the recommendations of RFC 1767, "MIME Encapsulation of EDI Data", and the "Content-Type:application/EDI-X12" is used. However, for security purposes it is recommended that all data be encrypted and digitally signed prior to transmission over the Internet. There are IETF standards for describing and packaging encrypted data files, most notably, "MIME Security with Pretty Good Privacy (PGP)", RFC 2015 and "MIME-based Secure EDI", RFC TBD.

- After the contents of the last data field, the boundary appears again as the last item of the form with the required two hyphen characters following the boundary at the end of the form to indicate the end of the data.

When the sender of a file intends to use encryption and digital signature functions to secure the contents of a data file the file must be prepared in accordance with the above mentioned IETF standards. ASC X12 data must first be prepared in canonical form as specified in RFC 1767. The ASC X12 data file would be concatenated with the MIME Content-type of application/EDI-X12 as the first line of the file.

For example below is a file before encryption:

Content-type: application/EDI-X12
ISA~00~ ~01~AAA6300300~14~1234567890000 ~14~2345678900000
... more data from the X12 file…
IEA~1~000003616

This file is encrypted, signed and packaged, which follows EDIINT AS1 and RFC 2015, which produces a file containing MIME headers and encrypted content as follows.

Below is the file after encryption:

Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"

--8760
Content-Type: application/pgp-encrypted

Version: 1

--8760
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xm
wiMkiwYsHsz0e8sb7Er340MrNA/dw3taGMjmI+CXYRF/PLEdg1NZE1ZCt
NeL4YdIHAMLWwODGlQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9Ul
juJjYc1uZ6C03eFQv/43fkB+alATtgydxX4g8QK664ad+Jo/XUICSmWBL6
6fqJR1KLeLf4wTaqGy174Aq48Wpwvg1Eh785zC03UAw0qg0ugMt86dPe
yd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8Ocp2IWClxKOGUbxpV
NOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ1RQbeNaqx2Dq/
ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cVz
pb4JE+gMDf3q4ISUb1Fv7/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit3
1EbX9.UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7I
ZySaRO8Vtff+4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
--8760—

This file is associated with the “input-data” data element of the multipart-form-data and is sent to the recipient using the HTTP POST method.

The HTTP POST data stream used to send this file would appear as follows:

-----------------------------87453838942833
Content-Disposition: form-data; name="from"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="to"

234567890
-----------------------------87453838942833
Content-Disposition: form-data; name="version"

1.6
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt (OPEN ISSUE)
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-security-selection"

signed-receipt-protocol=required, pgp-signature; signed-receipt-micalg=required, md5

----------87453838942833
Content-Disposition: form-data; name="input-format"

X12
----------87453838942833
Content-Disposition: form-data; name="input-data"; filename=”c:\temp\smallnom.bin”
Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"

--8760
Content-Type: application/pgp-encrypted

Version: 1

--8760
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xm
wiMkiwYsHsz0e8sb7ErC340MrNA/dw3taGMjmI+CXYRF/PLEdg1NZE1Z
CtNeL4YdIHAMLWwODGlQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9
UljuJjYc1uZ6C03eFQv/43fkB+alATtgydxX4g8QK664ad+Jo/XUICSmWBL
66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1Eh785zC03UAw0qg0ugMt86dP
eyd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8Ocp2IWClxKOGUbxp
VNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ1RQbeNaqx2D
q/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0c
Vzpb4JE+gMDf3q4ISUb1Fv7/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqN
it31EbX9UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj
7IZySaRO8Vtff+4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----

--8760--

----------87453838942833--

Although the specifications for multipart POST include several variations on this method, the NAESB REQ standards do not include implementing them at this time (OPEN ISSUE). The most significant of these variations is to send several files in a single post. Additionally, sending a single file split into more than one post is not expected by the HTTP server.

The output from the browser is important to the understanding of the processing needed by the server script or program which must interpret the result. The complete data stream from the browser will look like:

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
Referer: http://www.get.a.life/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
Host: localhost
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Content-type: multipart/form-data; boundary=---------------------------87453838942833
Content-Length: 5379

-----------------------------87453838942833
Content-Disposition: form-data; name="from"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="to"

234567890
-----------------------------87453838942833
Content-Disposition: form-data; name="version"

1.6
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt (OPEN ISSUE)
-----------------------------87453838942833
Content-Disposition: form-data; name="input-format"

X12
-----------------------------87453838942833
Content-Disposition: form-data; name="input-data"; filename="c:\temp\smallnom.bin"
Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"

--8760
Content-Type: application/pgp-encrypted

Version: 1

--8760
Content-Type: application/octet-stream
```

```
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8sb7ErC3
40MrNA/dw3taGMjmI+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODGlQxhSucz8rMSgQ5mZzcO
JwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/43fkB+alATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJ
R1KLeLf4wTaqGy174Aq48Wpwvg1Eh785zC03UAw0qg0ugMt86dPeyd91e2JigqwDYEf/DYEKD0J9
BGiGpS/uAupNKj8Ocp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ
1RqbeNaqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cVzpb4JE+g
MDf3q4ISUb1Fv7/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9UVElObzSa9ZhxbC6/eSl7N
uf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZySaRO8Vtff+4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CA
e4=
=Oiuo
-----END PGP MESSAGE-----
--8760--
----------------------------87453838942833—
```

Client Specifications

Each client should be synchronized to a clock in the network of atomic clocks that is accessible via the Internet. Each trading party should observe the client clock over a period of time to determine the amount of "drift" occurring throughout the day with respect to the atomic clock. The client should be synchronized as many times per day as necessary to ensure synchronization. Please refer to Appendix A, "Time Synchronization" for references on public sites for synchronization.

RECEIVING TRANSACTIONS

General Flow

The following is an example of the steps necessary to receive an EDM file:

1. Parse multi-part form
2. Validate HTTP request data elements
3. If HTTP request data elements in error, return appropriate standard error code in the HTTP response data elements
4. Save data
5. Create gisb acknowledgement receipt (OPEN ISSUE)

5.1 If using signed receipts:

5.1.1 Produce a digital signature over the gisb acknowledgement receipt (OPEN ISSUE) created in step 5.

5.1.2 Encapsulate the gisb acknowledgement receipt (OPEN ISSUE) and Digital Signature body parts in a content-type of application/multipart/signed envelope

6. Return HTTP response, the gisb acknowledgement receipt (OPEN ISSUE) object, back to server
7. Close connection
8. Log final results
9. Route data file to the next process based upon input format

Using a Web Server

As was stated above, the protocol HTTP using the POST method is the only HTTP method supported by the NAESB REQ. On the receiving side of this HTTP request is the Web server, the second primary component in Web technology. However, the Web server does not actually save the uploaded file. Instead, it hands this responsibility over to a special program which, in effect, extends the Web server's functionality with custom programming. Besides storing the file, this program has the task of parsing the incoming HTTP message, noting the date, time and time zone indicator so to create the timestamp, and creating an HTML response to the sender.

The NAESB REQ standard places no particular requirements on the vendor for the Web server. Most commercially available Web servers will provide the needed functionality. However, please refer to comments regarding performance under "Throughput Considerations" later in this section. Determine whether the product you are considering provides a secure version capable of either SSL .

The Receive Process

A receiving program must be able to parse the multipart form. It accomplishes this by finding the boundary string in the Content-Type header and scanning for its occurrences further within the uploaded stream. Upon finding these boundary strings, the program must next determine the content-disposition for each data element. This allows detection of the required text elements as well as the NAESB REQ standard format file.

The receiving program is not concerned with the content of the NAESB REQ standard format data. In fact, the standard format file will be encrypted (see the Security section). The program will merely accept the standard format data and store it as a file. It will use the Content-Length to determine how much data to expect in the body.

Throughput Considerations

It is critical that the Web server and the associated receiving programs perform efficiently. This is particularly true for high volume sites processing time sensitive materials. For the greatest possible throughput, the Web server should be multithreaded. The receiving program should be multithreaded or as small and efficient as possible. It is also suggested that a Web server and operating system be chosen that allow for scaling to a more powerful computer (possibly multi-CPU). Transaction volumes are likely to be light at first but may become heavy rather quickly.

Developing the Receive Process

A receive process requires an executable program or module that is called by the HTTP server when it is identified by a POST operation.

When the HTTP server receives a POST it will first read the header and populate environment variables before calling the receiving program. A sample header is shown below.

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
Referer: http://www.get.a.life/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
```

```
Host: localhost
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Content-type: multipart/form-data; boundary=---------------------------87453838942833
Content-Length: 5379
```

The important point to note is that you will not specifically code the step of reading the header and populating the environment variables, the HTTP server performs it for you. The variables populated are usually listed with the HTTP server documentation.

After reading this header the server will buffer the remaining data transmitted and then call the receiving program specified in the POST statement. Do not assume that the receiving program is called as soon as the header is read. The more common implementations will buffer the entire transmission before calling the program. You may want to check your server implementation if this characteristic is important to you.

The receiving program will have the following input stream available, and will have most of the header data available in environment variables.

```
-----------------------------87453838942833
Content-Disposition: form-data; name="from"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="to"

234567890
-----------------------------87453838942833
Content-Disposition: form-data; name="version"

1.6
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt (OPEN ISSUE)
-----------------------------87453838942833
Content-Disposition: form-data; name="input-format"

X12
-----------------------------87453838942833
Content-Disposition: form-data; name="input-data"; filename="c:\temp\smallnom.bin"
Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"

--8760
Content-Type: application/pgp-encrypted

Version: 1

--8760
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8sb7ErC340MrNA/d
w3taGMjmI+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODGlQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/
9UljuJjYc1uZ6C03eFQv/43fkB+alATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48
Wpwvg1Eh785zC03UAw0qg0ugMt86dPeyd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8Ocp2IWClxKOG
UbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ1RQbeN.aqx2Dq/ra9g65HNchOCzjul5Vi8HHf
6Yhg2WnROe+npByyCue6rihqgNVOJwj0cVzpb4JE+gMDf3q4ISUb1Fv7/+SSFHDdnhdC5YTpqf1Bc3B07hiL
```

```
mtTXqNit31EbX9UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZySaRO8Vtff+4ktqeuhYu
sT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
--8760--
----------87453838942833—
```

This process should check for basic validity in the environment variables and the data stream. It will parse the variables/data from the format. The data validations should include:

- The “REQUEST_METHOD” environment variable is “POST”.
- The “CONTENT_TYPE” environment variable should be “multipart/form-data” and a boundary, which is unique in that it cannot appear anywhere in the transaction being sent (see above stream for an example).

The input stream should support binary mode to accommodate encrypted files.

- Each data element should be preceded by the boundary with the required two hyphen characters appearing before it.
- Each data element should contain the correct name on the *Content-Disposition* line.
- Each data element should have \r\n\r\n (c notation) before the start of the data.
- In the receiving program, all tag values in the HTTP header should be evaluated in a case insensitive manner.

Finding the end of the stream using both content length and the boundary end mark (the boundary with two required hyphen characters in front and behind) is usually the best method to detect improperly formatted input.

Immediately after the receiving program validates (as above), parses, and saves the data, it should record the time and construct an acknowledgement receipt described in the following section. This receipt is sent from the receiving program to the sending program. If using signed receipts, the receiving party must produce a digital signature of the acknowledgement receipt and send both the acknowledgement receipt and digital signature body parts within a multipart/signed MIME envelope.

Receive Process URL Implementation Guidelines

NAESB REQ standard 4.3.12 (OPEN ISSUE) states

> *"As a minimum, with a trading partner agreement, 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."*

Each company must offer at least one URL to accept files using EDM. However, a maximum number of URLs per company is *not* included so that companies that wish to offer additional URLs will not be held back from doing so. Though companies are free to

construct a Web site with multiple "single-purpose" URLs, NAESB REQ recommends the use of one "general-purpose" URL.

Error notifications include errors that occur some time after the acknowledgement receipt is sent (such as a file decryption error) as well as errors on the transactions. A general-purpose URL would handle all error notifications.

Companies that wish to offer multiple URLs must negotiate additional URLs with their trading partners. All URLs that will be required for use in the EDM process must be agreed to and defined in the Trading Partner Agreement (TPA) signed by both companies. For example, a separate URL may be used for customized processing, such as high or low priority transactions.

To those companies who wish to offer multiple URLs, NAESB REQ strongly recommends that you divide URL usage along transactional grouping lines. Create groupings that are likely to correlate to business functions in a company.. Do not divide URL usage along an arbitrary internally-understood group such as region of the country. Remember that the intent of not specifying a maximum number of URLs is to allow companies the freedom to offer services, not to further complicate the EDM process.

Server Specifications

The HTTP server should be synchronized to a clock in the network of atomic clocks that is accessible via the Internet. Each trading party should observe the server clock over a period of time to determine the amount of “drift” occurring throughout the day with respect to the atomic clock. The server should be synchronized as many times per day as necessary to ensure synchronization. Please refer to Appendix A, “Time Synchronization” for references on public sites for synchronization.

The HTTP server will provide an HTTP response to the client according to NAESB WGQ standards.

All data element names of the HTTP request and response fields will be in lower case. Note that the NAESB REQ standard format file contained in the request and response may follow a different standard.

Carriage returns and line feeds will be ignored in all files.

A field delimiter of “*” will be used in the HTTP response. Please refrain from displaying a “*” anywhere else in the response so as not to confuse programs that need to parse on this basis.

No spaces should surround the equal sign or the field delimiter.

The required data elements must appear first in the response.

Additional information can be included after the required elements at the server’s discretion.

The gisb acknowledgement receipt must be enveloped in a multipart/report, as specified in EDIINT AS2 following the rules for Generalized Receipts. If signed receipts are used, the gisb acknowledgement receipt (including the multipart/report envelope) is digitally

signed, producing a application/pgp-encrypted body part. Both the multipart/report (gisb acknowledgement receipt) and the application/pgp-signature body parts are placed in a multipart/signed envelope and the entire package is returned to the sender.

The first occurrence of the field name within the response will contain the value.

If an HTML response is given, all data must be presented in a user-readable fashion. For example, if the required machine-readable fields are embedded in comments, another representation of these fields must be presented to the user.

Servers should be configured to use one of the allowable TCP ports listed in Appendix E.

HTTP Response Data Elements

Required Data Elements (listed in the required order)

Data Element Name	Description
time-c	the time of transfer completion at the server. The format will be *yyyymmddhhmmss-ZZ*. The –ZZ indicates the difference, in hours, between local time and Coordinated Universal Time (UTC). For example, 20030107142004-06, reflects a timestamp that was issued by a machine within the Central time zone. In cases where a machine is within a time zone that is ahead of UTC the (-) would change to a (+). For example, a machine located in Germany would issue timestamps with a +01, indicating a 1 hour difference ahead of UTC.
request-status	a text status indicator by the server. The only defined value at this time is “ok” for a successful transfer. The server should supply a descriptive indication of the error detected following the standards for error codes and messages presented in Table A, “Internet EDM Standard Error Codes and Messages”.
server-id	a *domainname* or *hostname.domainname* uniquely identifying the server associated with the CGI that received and processed the file.
trans-id	a number (integer) up to 15 characters in length uniquely identifying the received transaction file at the server. The trans-id will uniquely identify the file only at the receiving server. A client may receive non-unique trans-ids across multiple servers.

Samples of HTTP Response Required Data Elements:

successful, plain text format:

```
Content-Type: multipart/report; report-type="gisb-acknowledgement-receipt"; boundary="GISB7867"

--GISB7867
Content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Success</TITLE></HEAD> <BODY><P>
time-c=19960619082855-06*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
</P> </BODY></HTML>
--GISB7867
Content-type: text/plain

time-c=19960619082855-06*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
--GISB7867--
```

or

error, plain text format:

```
Content-Type: multipart/report; report-type="gisb-acknowledgement-receipt"; boundary="GISB7866"

--GISB7866
Content-type: text/html
```

```
<HTML><HEAD><TITLE>Acknowledgement Receipt Error</TITLE></HEAD> <BODY><P>
time-c=19960619082855-06*
request-status=EEDM106: Invalid To Common Code Identifier*
server-id=coolhost*
trans-id=234423897*
</P> </BODY></HTML>
--GISB7866
Content-type: text/plain

time-c=19960619082855-06*
request-status=EEDM106: Invalid To Common Code Identifier*
server-id=coolhost*
trans-id=234423897*
--GISB7866--
```

or

warning, plain text format:

```
Content-Type: multipart/report; report-type="gisb-acknowledgement-receipt"; boundary="GISB7866"

--GISB7866
Content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Warning</TITLE></HEAD> <BODY><P>
time-c=19960619082855-06*
request-status=WEDM100: Transaction Set Sent, Not Mutually Agreed*
server-id=coolhost*
trans-id=234423897*
</P> </BODY></HTML>
--GISB7866
Content-type: text/plain

time-c=19960619082855-06*
request-status= WEDM100: Transaction Set Sent, Not Mutually Agreed *
server-id=coolhost*
trans-id=234423897*
--GISB7866--
```

or, as a more elaborate response to a successful transmittal,

```
Signed Receipt
Content-Type:multipart/signed; micalg=pgp-md5; protocol="application/pgp-signature";
boundary=8760

--8760

Content-Type: multipart/report; report-type="gisb-acknowledgement-receipt"; boundary="GISBB7867"

--GISB7867
Content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Success</TITLE></HEAD> <BODY><P>

time-c=19960619082855-06*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
```

```
</P> </BODY></HTML>

--GISB7867
Content-type: text/plain.
time-c=19960619082855-06*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
--GISB7867--
--8760
Content-Type: application/pgp-signature

-----BEGIN PGP MESSAGE-----

Version: 2.6.2

iQCVAwUBMJrRF2N9oWBghPDJAQE9UQQAtl7LuRVndBjrk4EqYBIb3h5QXIX/LC//JV5bNvkZIGPIcEmI5iF
d9boEgvpirHtIREEqLQRkYNoBActFBZmh9GC3C041WGquMbrbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/
W72vgSxLhe/zhdfolT9BrnHOxEa44b+EI=
=ndaj

-----END PGP MESSAGE-----

--8760—
```

HTML format (this example is for a successful transmittal):

```
HTML format (this example is for a successful transmittal): <html> <head> <title>
Upload OK</ title></ head> <!-- time- c= 19960123203618-06*-->_ <!-- request-
status= ok* --> <!-- server- id= coolhost*--> <!-- trans- id= 232323897*--> <h1>
Upload OK </ h1>< br> <body> <B> File Saved at (time- c): </B>
19960123203618-06< br> <B> Status (request- status): </ B> ok< br> <B>
Server (server- id): </ B>coolhost< br> <B> Transaction ID (trans- id): </ B>
232323897< br> </ body> </ html>
```

Using a Service Provider for Web Hosting

If you do not wish to install and maintain a Web server, you may wish to contact an Internet Service Provider (ISP) to provide the hosting service for you. Consider the following when selecting an ISP for Web hosting:

- limit on storage space for receiving files
- ability to meet NAESB REQ standards for HTTP response
- accommodation for CGI to meet NAESB REQ standards for validation and processing.

SECURITY

Security Concepts

The security requirements include the current four primary security aspects: data privacy, data integrity, authentication, and non-repudiation.

- Data privacy: unauthorized parties cannot decipher the content of the data.
- Data integrity: unauthorized parties cannot modify or corrupt the data.
- Authentication: the receiver is certain of the identity of the sender.
- Non-repudiation: the sender cannot deny ownership of the transaction if it was sent with his/her digital signature.

In general, these needs are met by using the Basic Authentication capability of the Web server and the encryption and digital signature capability of the PGP and OpenPGP security application for securing transactions.

Understanding PGP or OpenPGP

Pretty Good Privacy (PGP) is the name of the chosen security application. OpenPGP is the Internet Engineering Task Force standard version of PGP which excludes all patented algorithms, allowing free commercial use of the standard. See the NAESB WGQ home page for information on software packages to implement the PGP or OpenPGP security application. Both OpenPGP and PGP utilizes a public key/private key pair to accomplish secure file transfers. The private key must be known only to the company which generated it. The public key counterpart is shared with trading partners.

Each company must generate its public key and private key pair. The RSA key generation algorithm should be chosen for versions of PGP which offer alternatives. Implementers of OpenPGP should choose DSA and El Gamal when creating their key pair. The public keys will be distributed using a secure method (eg., courier mail) to the company's trading partners. You must use the utmost care in protecting your private key. If it is compromised, the security is broken. It is recommended that a key size of 1024 be chosen when generating the key pair. This provides a significantly secure transaction.

When a company wishes to send transactions to its trading partner, it will use the partner's public key to encrypt the file. Encryption provides data privacy. Only the private key counterpart can decrypt this file. Hence, the need to guard your private key.

When the sending party encrypts the file, it also uses its own private key to "sign" the transaction. The receiving party can use the sender's public key to verify the signature. The digital signature provides non-repudiation.

Encryption / Digital Signature

Encryption and signatures are applied to files already translated to a NAESB REQ standard data format, and before the data is sent to the batch browser. (Use of internal

encryption such as X12.58 encryption is outside the scope of NAESB WGQ encryption standards but does not conflict with PGP.).

Encryption and signatures can be accomplished manually for each file using the on-line PGP or, on a mutually agreed basis, OpenPGP software, or in an automated (or "batch") fashion using programs to encrypt and sign. Whether encrypting in a manual or automated fashion, it is essential that the correct public key of the trading partner be used to encrypt and just as essential that the correct sender's own private key be used to digitally sign the file.

Digital signatures may also be applied, on a mutually agreeable basis, to the HTTP response by the receiver of the transaction.

Decryption / Signature Verification

After a transaction is received and processed by the CGI program, it is ready to be decrypted and have its signature verified. PGP and OpenPGP software will utilize the appropriate key pair when encrypting, signing, and decrypting if given the correct userID in the key ring identifying the trading partner. Upon request for signature verification, the PGP and OpenPGP software will return a human-readable company name.

It is recommended that all implementers create a process where the name is used to look up the ID of the company in a database table. If the ID is passed along with the decrypted file, a process could be created to verify that the company which sent the transaction corresponds to the company identified within the file, once the data has been translated.

When digital signatures are applied, on a mutually agreeable basis, the HTTP response received by the sender of the transaction may be verified to ensure non-repudiation of receipt of the transaction.

Throughput Considerations

Encryption, digital signing, decryption and signature verification are all very CPU intensive. It is not recommended that decryption or signature verification be performed within the CGI that receives and processes the file. In fact, it would not be a good idea to have these steps performed on the same computer that is attempting to receive transactions at a time close to a deadline. Therefore, it is recommended that the secured or to-be-secured transaction be passed to a separate computer for security processing. This "passing" would likely be accomplished by using the File Transfer Protocol (FTP). The security processing computer should be optimized for CPU and memory.

Implementers of Internet EDM sites should review and evaluate Domain Name Server (DNS) cache refresh intervals so as to ensure trading partner address changes are recognized on a timely basis. A refresh interval of 24 hours or less is common.

Because decryption and signature verification are not handled at the time the file is received, the sender will get an HTTP response of successful transfer but doesn't know if the file can be decrypted by the receiver. Guidelines for communicating the status of the decryption step have been developed. See Section "Sending Error Notification Transactions" and Table A, "Internet EDM Standard Error Codes and Messages".

Security Requirements

Basic Authentication

Basic authentication, also known as realm one security, has been defined as one of the security standards for transmission on the Internet. The userid and password will be assigned by the server party according to site standards. The trading party agreement must identify the userid and password for this security as well as procedures for changing the password, if applicable.

PGP or OpenPGP File Encryption

File encryption of the EDI file is also selected as a security standard for transmission on the Internet. The encryption software employed is required to be compatible with PGP 2.6 or greater (using keys generated with the RSA algorithm) or the OpenPGP standard, specified in IETF RFC 2440, on a mutually agreed basis. There are freely available software implementations of the OpenPGP standard available at http://www.gnupg.org/.

General Security Recommendations

Firewall

A firewall is one or more computers running special software which is designed to provide control of communications between two networks. Its purpose is to limit the types of services between these two networks. Often, a company's connection to the Internet is intended to provide several other services to its employees who are connected by an internal network such as a Local Area Network or Wide Area Network (LAN or WAN). Examples of these services include access to the World Wide Web, use of e-mail, use of file transfer capabilities and publishing content intended for viewing by the external world on a Web server. In addition, the internal network will likely have connections to host computers which provide internal services such as file and print sharing, fax and database capabilities. So that availability of these services and confidential internal data are not compromised by unwelcome intruders from the Internet, there should exist a protective mechanism between the internal network and the public Internet, the firewall.

There are two general mechanisms employed by firewalls to provide this control: packet filtering and proxy services. Packet filtering examines important components of the messages such as the address of the sending and target computers and the designator (port number) for a specific application running on the target computer. By doing this, it can prevent access to specific computers or programs on those computers. It can also reject messages from certain computers. Proxy servers have various capabilities. They can act as relay agents that can examine attempted use of certain features within an application thus limiting access to these features. They can also hide (by substituting its own address) the internal addresses of clients communicating with external hosts. This hiding makes it difficult for potential attackers to focus on specific internal hosts.

Because firewalls are designed to deal with a broad set of security issues, which may vary at each organization, and are not specific to the use of HTTP, this guide does not attempt to provide specific implementation information. Deciding on a specific firewall

architecture, organizational security policies, and choosing between numerous products may require outside resources to address these issues.

SENDING ERROR NOTIFICATION TRANSACTIONS

Error Notification

When a client sends a file to a server, the server responds to the receipt of the file. Though the file may be received correctly, some further processing must be done, such as decryption and X12 translation. The decryption step which will have a pass/fail status and then the X12 general translation step which will have a pass/fail status. The X12 general translation is merely the check that the file meets the X12 standards and has not been corrupted. Further translation and processing of specific transactions and elements is outside the Internet EDM scope.

When a file passes the decryption step and passes the general translation step, no notifying communication is sent back to the client. However, if either the decryption step or the general translation step fails, an error notification must be sent to the client.

In general, this standard format for error notification applies to the posting of an error message after sender's session has been disconnected. This error notification has the potential of occurring only after the original HTTP Response is returned with an "ok" or a warning (WEDM999 format) for the request-status value, not an error (EEDM999).

Additionally, trading partners are permitted to utilize digitally signed error notifications, if both parties mutually agree to do so.

Error Notification Data Elements

The data elements for the error notification are the same as those described in Section "Sending Transactions", with the exception of the "input-format" and "input-data" elements. The file containing the data elements for error notification should not be encrypted.

Required Data Elements for Error Notification (listed in the required order)

Data Element Name	Description
from	Common Code Identifier of sending/client company, the server company which detected the error
to	Common Code Identifier of receiving/server company, the client company which sent the data set in error
input-format	"error"

input-data	A text block containing the following items:	
	orig-from	The "from" value from the original transmission
	orig-to	The "to" value from the original transmission.
	orig-input-format	The "input-format" value from the original transmission.
	resp-time-c	The "time-c" value from the original response.
	resp-server-id	The "server-id" value from the original response.
	resp-trans-id	The "trans-id" value from the original response.
	request-status	The new status of the transaction based on some process beyond CGI such as decryption; see Table A, "Internet EDM Standard Error Codes and Messages".
	comments	Any comments the original receiving server wishes to include.

Mutually Agreed Upon Data Elements for Error Notification

none defined at this time

Error Notification "input-data" Element Specifications:

The file containing the data elements for error notification should not be encrypted.

All data element names will be in lower case in the Error Notification.

Carriage returns and line feeds will be ignored in all files.

A field delimiter of "*" will be used in the Error Notification. Please refrain from displaying a "*" anywhere else in the error notification so as not to confuse programs that need to parse on this basis.

No spaces should surround the equal sign or the field delimiter.

The required data elements must appear first in the response.

Additional information can be included after the required elements at the server's discretion.

The first occurrence of the field name within the response will contain the value.

If an error notification is given, a NAESB REQ Error Notification contains two body parts nested within a multipart/report outer envelope. The first body part contains human readable content in HTML. The second body part contains machine readable content in HTML. Additionally, consenting trading partners can mutually agree to digitally sign error notifications. If digital signatures are used, the multipart/report containing the NAESB REQ Error Notification is used to create a digital signature body part, identified by a content-type of application/pgp-signature. Both the multipart/report NAESB REQ Error Notification and application/pgp-encrypted digital signature body parts are combined in a multipart/signed envelope.

Error Notification Example:

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
Referer: http://www.get.a.life/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
Host: localhost
```

```
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Content-type: multipart/form-data; boundary=---------------------------87453838942833
Content-Length: 1958
---------------------------87453838942833
Content-Disposition: form-data; name="from"

234567890
---------------------------87453838942833
Content-Disposition: form-data; name="to"

123456789
---------------------------87453838942833
Content-Disposition: form-data; name="version"

1.4
---------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
---------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt
---------------------------87453838942833
Content-Disposition: form-data; name="input-format"

error
---------------------------87453838942833
Content-Disposition: form-data; name="input-data"; filename="c:\temp\error.not"
Content-Type: multipart/report; report-type="gisb-error-notification"; boundary="GISB7868"

--GISB7868
Content-type: text/html

<HTML><HEAD><TITLE>Error Notification</TITLE></HEAD> <BODY><P>
orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855-06*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*
</P> </BODY></HTML>

--GISB7868
Content-Type: text/plain

orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855-06*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*
--GISB7868--
---------------------------87453838942833—

Signed Error Notification

Content-Type:multipart/signed; micalg=pgp-md5; protocol="application/pgp-signature";
```

```
boundary=8760

--8760

Content-Type: multipart/report; report-type="gisb-error-notification"; boundary="GISB7868"

--GISB7868
Content-type: text/html

<HTML><HEAD><TITLE>Error Notification</TITLE></HEAD> <BODY><P>
orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855-06*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*

</P> </BODY></HTML>

--GISB7868
Content-Type: text/plain

orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855-06*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*

--GISB7868--
--8760

Content-Type: application/pgp-signature
-----BEGIN PGP MESSAGE-----

Version: 2.6.2

iQCVAwUBMJrRF2N9oWBghPDJAQE9UQQAtl7LuRVndBjrk4EqYBIb3h5QXIX/
LC//JV5bNvkZIGPIcEmI5iFd9boEgvpirHtIREEqLQRkYNoBActFBZmh9GC3C041
WGquMbrbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/W72vgSxLhe/zhdfolT9BrnH
OxEa44b+EI=
=ndaj

-----END PGP MESSAGE-----

--8760--.
```

Pre-validation before Decryption

Proper trapping of the range of decryption process errors listed in Table A (Internet EDM Standard Error Messages and Codes) may require program code which is external to the decryption algorithm. Some versions of the PGP software do not explicitly discriminate between EEDM601, EEDM602, EEDM603, and EEDM699 type errors. Under such a circumstance, files inbound to the decryption process should be

preprocessed to trap the errors not identified by the PGP version being used. For example, searching the file for the text strings “BEGIN PGP MESSAGE” and “END PGP MESSAGE” can quickly identify “EEDM602 File not encrypted” and “EEDM603 Encrypted file truncated” type errors when the implemented PGP version only identifies decryption success, invalid public key (EEDM601), and decryption failure (EEDM699).

CHECKLIST OF TESTING STEPS

Purpose

Preliminary steps in testing are helpful before the full batch browser and server applications are completed. This checklist is intended to provide a series of small achievements leading up to the complete solution.

Client/Browser

NOTE: Throughout all transfer tests, compare files stored on the server against the source file to ensure that the file transferred intact. While transferring to another company’s server, you may have to contact that company to send the file back to you so that you can perform the compare.

1. Install an interactive browser. Identify an existing Web server from among NAESB REQ compliant servers offering interactive upload for test. See the NAESB REQ home page for a list of organizations willing to act as testing partners. These organizations should have a URL complete with the CGI program name to which a tester may send test files. File content does not need to be X12 or other NAESB REQ standard format to accomplish this step in testing.
2. Develop or acquire a batch browser that uses multipart for the encoding methodology. Transfer the same test file as in step 1 to the URL not requiring Realm One security.
3. Add Realm One security to your file transfer, and change the URL to the secure URL. Continue transfer tests with your batch browser.
4. Acquire and install PGP or OpenPGP compliant software. Generate your public and private key pair. Make sure to choose the RSA key generation algorithm for PGP or DSA and El Gamal for OpenPGP. Download the test server’s test public key. Encrypt your data file using this key. Modify your file transfer to send the encrypted file. Continue transfer tests. Request that the test server contact decrypt your file.

HTTP Server and CGI

1. Install Web server. Establish an Internet connection to your server. Ensure that you have ample storage space for transferred files. Ensure that permissions are granted to the directories.
2. As an optional preliminary step, acquire or develop an HTML page for interactive file upload (sample code is earlier in this document). Test interactive file upload to your own server using an interactive browser.
3. Acquire or develop a CGI program to receive file transfers and process according to NAESB REQ standards. Test transfers to your CGI using your batch browser.
4. Transfer a X12 or other NAESB REQ standard format dataset to your server and

process it through your translator or other appropriate processes.

5. Copy the CGI to a “secure” directory where Realm One security, or basic authentication, is enabled. Using your batch browser, transfer to both URLs, with and without authentication. Thoroughly test using the incorrect userid and password against the secure directory.
6. Generate a second public/private key pair. Use the second key to encrypt a file and transfer the file to your server. Decrypt the file.
7. Once your site security is established, contact a trading partner to test transfers against your server.
8. Test with various file sizes to ensure that your CGI can process small and large files.
9. Request that several other trading partners and/or several clients within your own company transfer concurrently to ensure that your server can withstand the load.
10. Test application with various simulated errors in both file transfers and in PGP or OpenPGP decryption.

FREQUENTLY ASKED QUESTIONS

As an end user, do I need a continuously connected internet Web server to participate in the Internet EDM in the gas industry, or can I just use a dial-up connection to my ISP and my favorite shrink-wrapped browser software?

An interactive browser connection is not enough to actively participate in the system. It is not necessary to have a private Web server, you can use a service, however the system requires that you have access to a permanent internet connection which is capable of both sending and receiving files (with CGI or BGI) without operator intervention.

If we use ANSI X12.58 encryption do we still need to use PGP or OpenPGP encryption?

The use of internal encryption such as X12.58 is outside the scope of the NAESB WGQ encryption standards.

TABLE A - Internet EDM Standard Error Codes And Messages

These errors and warnings are strictly related to problems found in the recipient CGI or decryption levels of processing before translation. Errors and warnings generated by the client batch browser are assumed to be documented at the client site to distinguish them from problems occurring in the recipient CGI or decryption. Numbering schemes and descriptions should aid in this distinction.

Note: For HTTP error codes see the NAESB REQ home page for information sources.

EEDM### standard error format with ### representing a numeric value further processing will not take place

WEDM### standard warning format with ### representing a numeric value further processing will take place

The string for the error or warning should appear in the following format:

Validation Code:Description;supplemental message to be defined by the issuing site up to 80 characters

Internet EDM Standard Error Codes and Messages

Validation Code	Description	Data Element	Required vs. Mutually Agreed
EEDM100	Missing "from" Common Code Identifier code	From	required
EEDM101	Missing "to" Common Code Identifier	To	required
EEDM102	Missing input format	input-format	required
EEDM103	Missing data file	input-data	required
EEDM104	Missing transaction set	transaction-set	mutually agreed
EEDM105	Invalid "from" Common Code Identifier	From	required
EEDM106	Invalid "to" Common Code Identifier	To	required
EEDM107	Invalid input format	input-format	required
EEDM108	Invalid transaction set	transaction-set	mutually agreed
EEDM109	No parameters supplied	parameter string	required
EEDM110	Invalid "version"	Version	required
EEDM111	Missing "version"	Version	required
EEDM112	"receipt-security-selection" not mutually agreed	receipt-security-selection	mutually agreed
EEDM113	Invalid "receipt-security-selection"	receipt-security-selection	mutually agreed

Validation Code	Description	Data Element	Required vs. Mutually Agreed
EEDM114	Missing "receipt-disposition-to"	receipt-disposition-to	required
EEDM115	Invalid "receipt-disposition-to"	receipt-disposition-to	required
EEDM116	Missing "receipt-report-type"	receipt-report-type	required
EEDM117	Invalid "receipt-report-type"	receipt-report-type	required
EEDM118	Missing "receipt-security-selection"	receipt-security-selection	mutually agreed
EEDM119	Mutually agreed element, refnum, not present	Refnum	mutually agreed
EEDM601	Public key invalid	file itself	required - security
EEDM602	File not encrypted	file itself	required - security
EEDM603	Encrypted file truncated	file itself	required - security
EEDM604	Encrypted file not signed or signature not matched		
EEDM699	Decryption Error		required for general decryption errors not specifically identified by PGP or OpenPGP messages or exit codes
EEDM701	EDM party not associated with EDI party		required
EEDM702	Data Structure Error		required if the translator does not handle this exception
EEDM703	Data set exchange not established for Trading Partner		required if the translator does not handle this exception
EEDM999	System error		required for general system errors to indicate severe errors in processing at the receiving site
WEDM100	Transaction set sent not mutually agreed	transaction-set	mutually agreed
WEDM102	"receipt-security-selection" not mutually agreed	receipt-security-selection	mutually agreed
WEDM103	Missing "receipt-security-selection"	receipt-security-selection	mutually agreed
WEDM104	Element refnum received, not mutually agreed; ignored	Refnum	mutually agreed

CHANGE LOG

Appendix

Section/ Paragraph	Area to Change/Comment	Suggested Change
[all]	References to WGQ	Replaced with REQ
Page 104	"natural gas industry" reference under definition of NAESB	Replaced "natural gas industry" with "energy industry"
Page 104	Missing reference to PGP Corporation	Added reference to PGP Corporation
Page 108-112	Appendix C and D not applicable to REQ at this time	Removed pages 108-112
Page 113	Reference to WGQ Customer Activities Web Site	Removed reference.

APPENDIX A - Reference Guide

CGI

An excellent source on CGI is a book entitled “Special Edition Using CGI” by Jeffrey Dwight and Michael Erwin.

Firewall Security

An excellent source which covers this topic in detail is a book entitled "Firewalls and Internet Security: Repelling the Wily Hacker" by William Cheswick and Steven Bellovin.

NAESB

NAESB Web Site: (http://www.naesb.org) Primary reference for ~~natural gas~~ energy industry standards

General NAESB WGQ FTTF Reference Page: (http://www.naesb.org/fttf.htm). This location provides pointers to samples and further documentation.

HTTP

The NAESB REQ~~WGQ~~ EDM architecture is based on HTTP 1.1, and all implementations should be compatible with this version.

W3C WorldWide Web Consortium. All aspects of HTTP, HTML, and other Web-related topics are documented at:
http://www.w3.org/pub/WWW/

General information regarding HTTP with basic terminology included are documented at:
http://www.w3.org/pub/WWW/Protocols/HTTP/1.1/spec.html

Syntax information for multipart can be found in IETF RFC1341 section 7.2. (www.ietf.org)

HTML

Before April 24, 1998, the recommended standard from the WorldWide Web Consortium was HTML 3.2. The specification for this standard can be found at:
http://www.w3.org/pub/WWW/TR/REC-html32.html

Effective April 24, 1998, the WorldWide Web Consortium has made a recommendation for HTML 4.0. Information on HTML 4.0 may be found at http://www.w3.org/TR/REC-html40/.

http://www.ncsa.uiuc.edu/General/Internet/WWW/HTMLPrimer.html

http://www.interlink-2000.com/guide-to-publishing-html.html

Special Edition Using HTML, Second Edition, Mark Brown, John Jung, and Tom Savola, Que Corporation, 1996.

PGP Software

PGP is available for a variety of operating systems and platforms. For more information contact Network Associates (http://www.nai.com) or PGP Corporation, (http://www.pgp.com)

OpenPGP Software

The IETF OpenPGP standard is available at http://www.ietf.org/rfc/rfc2440.txt

Software implementations of the OpenPGP standard are freely available for commercial use from the Free Software Foundation at http://www.gnupg.org.

Time Synchronization

Testing has shown that the clocks on all computer systems drift. It has also been surprising to see just how much they do. Time synchronization is required to assure that all trading partners transaction times are accurate. 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.

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

A easy way to obtain the current time is from the U. S. Naval Observatory's Web site at http://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. Among them are NTP (which is an internet standard), internet daytime, nisttime / usnotime.

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

http://www.eecis.udel.edu/~mills/ntp/test.html

http://tycho.usno.navy.mil/ntp.html

http://www.ccd.bnl.gov/xntp

http://www.txdirect.net/users/sfisher/clock.html

http://www.is.co.za/resources/ftpsite/tucows/softsync.html

APPENDIX B - Repudiation and Validation Examples

Repudiation and Validation examples:

When a transaction file is received using the EDM mechanism there are several questions that typically must be answered:

1.) Is the HTTP sender (from) valid to send to the HTTP 'to' party?
2.) Does the HTTP sender match the party who encrypted and signed the file?
3.) Does the HTTP sender match the sender within the file?
4.) Is that sender with the data valid to 'speak' for the parties transacting business?

Is the HTTP sender (from) valid to send to the HTTP 'to' party?

The first validation, determining that a party is a valid sender must be done during CGI execution. This is simply a 'look up' verification that the Common Code Identifier 'from' is recognized as a valid sender.

Does the HTTP sender match the party who encrypted and signed the file?

The next validation, determining that the HTTP sender is the same as the signer, requires that the following information be available:

The 'from' common code identifier (9 digit D-U-N-S® Number). This is the second field in the HTTP post message sent to the CGI. This information must be preserved from that earlier process and passed to the 'post-CGI' process.

The Pretty Good Privacy (PGP) or OpenPGP User ID associated with that same party

To compare these items a 'table' would most likely be established that would allow the post-CGI process to identify that there is a correlation between these identifiers. The origin of the 'from' identifier is the HTTP POST 'from' field. The origin of the PGP or OpenPGP user ID is the decryption process. The PGP or OpenPGP User ID of the signer is a byproduct of file decryption on a signed file. If PGP or OpenPGP software is executed from the command line the output would be presented in a format like:

Good signature from user "ABC CORP".
Signature made 1997/05/13 19:30 GMT
Plaintext filename: test3

If PGP or OpenPGP is executed using a program interface the User ID that signed the file will be provided in a buffer. Comparing this buffer to the expected User ID would serve to verify this value.

Does the HTTP sender match the sender within the file?

The data file itself indicates (in the case of X12 data) the sender and the intended recipient within the ISA segment. Although this may be the same (D-U-N-S® Number) as the 'from' data these fields are not standardized. This may require the use of a 'table' to relate these identifiers.

Consider also that, although it is strongly recommended that only a single ISA be contained within a file, that the process should account for the possibility of several ISA segments. This comparison will ensure that the parties used during translation are in fact the parties that sent, encrypted and signed the data.

Is that sender with the data valid to 'speak' for the parties transacting business?

This last validation is listed here only to complete the chain of identity. The process that would evaluate this relationship would typically be the business application. Since we have checked the identity through each step of this process this is the point at which the identity of the sender would finally be verified as having a business relationship to conduct the business specified.

APPENDIX C - Minimum Technical Characteristics and Guidelines for the Developer and User of the Customer Activities Web Site[2]

Browser Characteristics (includes defined NAESB WGQ current versions):

Features as supported by the latest generally available (GA) versions of both Netscape®[3] and Internet Explorer®[3] within 9 months of such GA version becoming available, including -

- Frames & Nested Frames
- Tables & Nested Tables
- HTML
- Cookies
- JavaScript
- SSL 128-bit RSA Encryption
- Style Sheets

Plug-ins (Generally Available (GA) versions within 9 months of such GA versions becoming available)

- JAVA®
- ActiveX®[4] (Plug-in for Netscape®)
- Adobe Acrobat PDF Reader®[5]
- Systems Incorporated
- Independent Computer Architecture (ICA®) - Protocol used for remote control access to an application

Operating Systems:

Operating systems on a client workstation should be multithreaded and pre-emptive.

Hardware:

CPU	>=500 MHz
Memory	>=256 MB Physical

---

[2] Configuration shown indicates a minimum except where a specific level is established. 'Minimum' implies a level where a reasonable experience for the user may be achieved. These levels also indicate the level that a user may expect that a client has been tested. Results may be less than satisfactory, or may preclude use of a site, if the user chooses to use anything less than those levels shown.

[3] Netscape® is a registered trademark of Netscape Communications Corp.

[3] Internet® Explorer is a registered trademark of Microsoft Corporation.

[4] ActiveX® is a registered trademark of Microsoft Corporation.

[5] Adobe Acrobat® is a registered trademark of Adobe.

Display Resolution	>=1024 x 768, 16K colors
Connection	>=56 KB (v.90)

Example Configuration[1]

Hardware:	CPU: P500 MHz or higher Memory: 256MB Physical Display Resolution: 1024 x 768, 16K colors Pointing Device with left and right click capability
Operating Systems:	Windows®[2] 98 Windows® NT 4.0 Windows® 2000
Connection:	56KB (v.90) modem ISDN Direct Connect (T1, Fractional T1, etc.) DSL Cable-Modem
Browser:	Netscape® Communicator/Navigator Microsoft® Internet Explorer
Plug-ins:	JAVA® ActiveX® (Plug-in for Netscape®) Adobe Acrobat Reader® ICA®

Memory - Users who want to have multiple applications or EBBs open simultaneously should consider more memory.

CPU Speed - Users should be aware that higher CPU speeds my result in better performance.

[1] Specific products should be reviewed prior to implementation for Year 2000 compliance. Examples provided represent a non-comprehensive set of configurations that a client may use. This example list in no way should be construed as an endorsement by NAESB WGQ of any specific products. Other products meeting the minimum technical characteristics of the client workstation may be used.

[2] Windows® is a registered trademark of Microsoft Corporation.

~~APPENDIX D - Minimum and Suggested Technical Characteristics and Guidelines for the Developer and User of the Informational Postings Web Site~~

~~User technical characteristics provide specifications to the developer on the user environment for which the application will be designed and tested. Likewise, they will serve as guidelines to the user when purchasing the appropriate hardware and software to enable him/her to use the application.~~

~~Informational Postings Web Site User Technical Characteristics~~

	~~Minimum~~	~~Suggested~~
~~Connection Device:~~	~~28.8 KB~~	~~Direct Connect~~
~~Operating System:~~	~~Multi-threaded & Preemptive~~	
~~RAM:~~	~~128 MB~~	~~>128 MB~~
~~Browser Capabilities:~~	~~Cookies & JavaScript~~ ~~Frames & Nested Frames~~ ~~Tables & Nested Tables~~ ~~HTML 3.2~~	
~~Display Resolution:~~	~~1024x768, 16k colors~~	~~>1024x768, 16k colors~~

~~Definitions:~~

~~*Minimum user technical characteristics -*~~

~~The environment and components for which the Web site application is designed and tested. This should include:~~
~~- a client environment comprised only of characteristics listed above, and,~~
~~- support for all mandated functions in accessing Informational Postings.~~

~~*Suggested user technical characteristics -*~~

~~Environment or components not required to perform all mandated functions in accessing Informational Postings, but could provide an enhanced user experience.~~

~~Examples of User Workstations Meeting Criteria of Informational Postings Web Site User Characteristics~~[1]

	~~Minimum~~	~~Suggested~~
~~Hardware:~~	~~Pentium®[2] 200MHz or equivalent~~	~~Pentium® 500MHz or greater~~
~~RAM:~~	~~128 MB~~	~~> 128 MB~~
~~Communication Device:~~	~~28.8~~	~~Direct Connect~~ ~~ISDN~~ ~~Satellite~~ ~~56 KB modem~~ ~~DSL~~ ~~Cable Modem~~
~~Monitor:~~	~~12" Laptop~~ ~~15" Desktop~~	~~> 12" Laptop~~ ~~> 15" Desktop~~
~~Display Capabilities:~~	~~1024x768~~ ~~16k colors~~	~~> 1024x768~~ ~~> 16k colors~~
~~Operating System:~~	~~Windows® 95~~ ~~System 7®[3]~~ ~~Solaris®[4] 2.5~~	~~Windows® XP~~ ~~Windows® 98~~ ~~Windows® NT 4.0~~ ~~Solaris® 2.6~~ ~~System 8®~~ ~~Windows® 2000~~ ~~Windows® ME~~ ~~Linux~~
~~Browser:~~	~~Microsoft Internet Explorer®~~	~~Microsoft Internet Explorer®~~

[1] ~~Technical implementations above represent a non-comprehensive set of choices which an implementer may use. This list in no way should be construed as an endorsement by NAESB WGQ of any specific products. Other products supporting technical implementation may be used.~~

[2] ~~Pentium® is a registered trademark of Intel Corporation.~~

[3] ~~System 7® and System 8® are registered trademarks of Apple Computers, Inc.~~

[4] ~~Solaris® is a registered trademark of Sun Microsystems, Inc.~~

~~Netscape® Communicator~~	~~Netscape® Communicator~~

~~Informational Postings Web Site Developer Technical Characteristics~~

~~User's environment supporting the above minimum characteristics should be able to access all NAESB WGQ standardized features of Informational Postings Web Sites.~~

~~Any other Web technologies may be considered for use by the developer as long as they can be used by the client without requiring special actions including firewall rule changes, use of a specific browser, logons and downloads of special helper applications such as plug-ins, viewers or readers.~~

APPENDIX E - MINIMUM TECHNICAL CHARACTERISTICS FOR AN EDM SERVER

Allowable TCP Ports (not UDP ports)

HTTP HTTPS 80, 443, 5713, 6112, 6304, 6874, 7403
ICA® 1494
RMI(Java®) 1099-1100
Java® Telnet 31415
TCP Optional 8001-8020**
SMTP 25

Allowable UDP Ports (not TCP ports)

Secure ICA 1604

There are other technologies available that would require additional ports to be opened, such as FTP and Telnet. If and when NAESB REQ~~WGQ~~ approves such technologies, FTTF will modify this list of allowable ports accordingly. The client-side firewall implementation and client browser settings should permit the downloading and installation of NAESB ~~WGQ~~ REQ approved plug-ins and modules. ~~Please refer to the NAESB WGQ defined Minimum Technical Characteristics for Accessing Customer Activities Web Sites for the listing of NAESB WGQ approved plug-ins and modules.~~

**The reservation of 20 optional ports was to provide room for implementations such as DCE, IIOP, and load balancing implementations. TSPs should endeavor to minimize the usage of these ports.

ICA® is a registered trademark of Citrix Systems Inc.

JAVA® is a registered trademark of Sun Microsystems, Inc.