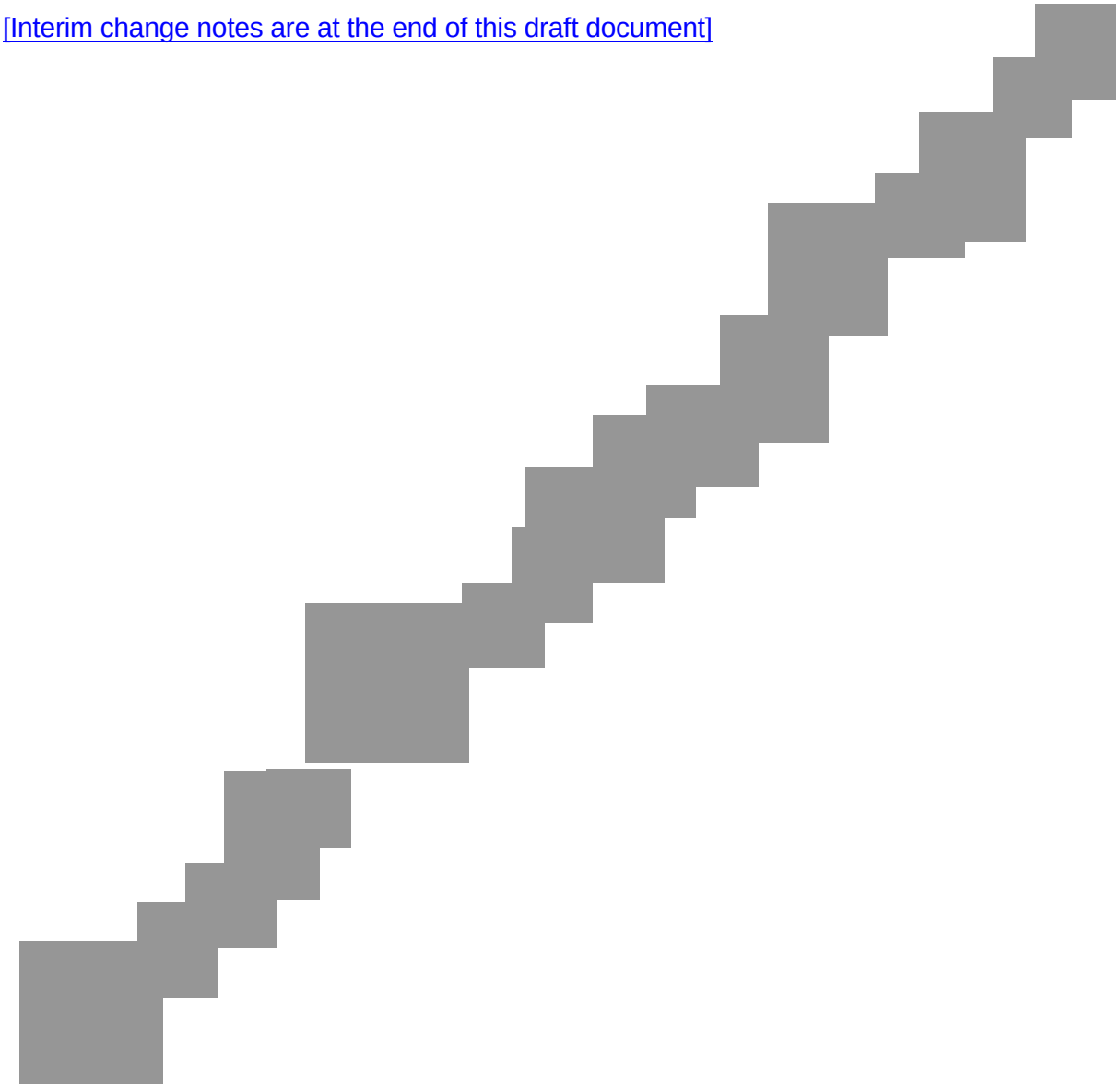
1 – VERSION HISTORY

1.0 12/31/2003

[DRAFT This is the first draft version of the Internet Electronic Transport (ET) standard]

[Interim change notes are at the end of this draft document]



2 – INTRODUCTION

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

NAESB Internet Electronic Transport (ET) Standards are used by the Wholesale Gas Quadrant (WGQ), Retail Electric Quadrant (REQ), and the Retail Gas ~~and Wholesale Gas Q~~quadrant~~s~~ (~~REQ, (~~RGQ~~), WGQ~~). ~~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 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 detailing the change to the NAESB office so that the appropriate process may take place to amend the standards.

TAB 1 Version Notes

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

TAB 2 Introduction

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

TAB 3 Executive Summary

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

TAB 4 Business Process & Practices

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

TAB 5 Related Standards

Provides a reference to any related standards.

TAB 6 Technical Implementation - Electronic Transport (ET)

Provides an overview of the business process for ET.

Data Dictionary

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

Batch Flow Diagram

Sending Electronic Packages

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

Receiving Electronic Packages

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

Security

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

Other Considerations

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

TAB 7 Testing Guidelines

??need something

TAB 8 Appendices

Appendix ??A - Reference Guide
Appendix ??B - Repudiation and Validation Examples
Appendix ??C - Minimum Technical Characteristics for an EDM Server
Appendix E – TCP standards

3 – EXECUTIVE SUMMARY

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

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

Overview of Electronic Transport Life Cycle

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

The receiving party, the "Receiver", receives and decrypts the package, then forwards the payload data to back-office processes. A receipt is sent from the Receiver to the Sender with timestamps and any error notices. The Receiver back-office systems process the data according to NAESB Quadrant-specific Electronic Delivery Mechanisms (QEDM). If the Receiver decrypts in a separate process, the Receiver may send an Error Notification package to the Sender to identify errors found during decryption.

Trading partners take turns being the Sender and Receiver depending on what information and data needs to be exchanged.

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

Open Standards

There are several major topic areas covering ~~related to~~ ET ~~covered~~ in this manual. When looking to implement ET, one should become familiar with the following components of the implementation:

- Communications Protocols
- Sending of Secure Electronic Packages
- Receipt of Secure Electronic Packages
- Security

- ??update when we know more about disposition of AS2 and GISB EDM; IETF EDIINT AS2 – "HTTP Transport for Secure ~~EDI~~ EDI"~~(a.k.a. IETF EDIINT AS2)~~

The open standard technologies selected by NAESB ~~WGQ/REQ/RGQ~~ 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., utilities, financial institutions, suppliers, retail customers)
- Makes it more likely that Commercial Off-The-Shelf (COTS) software packages can be purchased to replace custom written applications currently in place to support legacy GISB/NAESB EDM
- Strengthens the surety of receipt and error notification

??AS2 GISB/UCC profiles; AS2 has lost GISB references; divergence regarding PKI/PGP??; HTTP Transport for Secure EDI (AS2)??AS2 profiles?? 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 Internet ET Application Implementation For All Trading Partners

The Internet ET application is not platform-specific. An organization's Internet ET application serves the role of communicating with all trading partners in the energy industry no matter what hardware, operating system and programming languages their trading partners use. For this reason, testing with other trading partners on a variety of platforms is very important in ensuring that each Internet ET application is compatible with a range of platforms used by various trading partners.

Concerns About Future Reliability of the Public Internet

The nature of Internet design requires that c~~C~~ontinued monitoring of the Internet's viability as an infrastructure ~~will~~ take place. Business processes that have firm or tight timing requirements should properly mitigate the risk associated with the lack of guaranteed Internet Quality of Service. ~~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.~~

Key Assumptions

This document makes the following assumptions:

- Contents of the Electronic Package Do Not Matter - ET standards focus on the transport of the electronic package and not the contents of the package. Each business process may define different contents, and the ET is designed to work with any type of contents (e.g. EDI, flat files, etc). The Internet ET's main function is to get the package from point X to point Y reliably with privacy, authentication, integrity, and non-repudiation.
- Importance of the Trading Partner Agreement (TPA) - The expectations of who will perform what function and how it will be accomplished in Internet ET should be laid out in the trading partner agreement. ??review TPA; should we add a section that details elements of the TPA that are relevant to the ET??.
- Testing With Energy Industry Internet ET Participants - The Internet ET requires basic connectivity testing between trading partners. Testing should ensure receipt of the package, proper decryption, and appropriate receipts were sent.

Further Information

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

~~TAB~~ 4 – BUSINESS PROCESS AND PRACTICES

[refer to iet_Tab04-20031015.doc for change history]

A. OVERVIEW

Role of Internet Electronic Transport (ET) in NAESB WGQ, REQ, and RGQ Quadrants

Business processes defined by NAESB quadrants require the exchange of transactions and transaction data. The Internet ET, in concert with Quadrant-specific Electronic Delivery Mechanisms (QEDMs), enables NAESB parties to securely and reliably exchange transactions over the Internet. Internet ET electronic 'packages' are created using the standards defined in this document.

Version ??XX (OPEN ISSUE 028) of the Internet ET standard incorporates all technical specifications of the NAESB WGQ EDM Version 1.6, including mutually-agreeable business practices to protect the sender of a document with non-repudiation and with digitally-signed Error Notifications.

Business Reasons for Using Internet ET

Using the Internet ET for communications standardizes how transactions and other electronic packages are exchanged among trading partners. This eliminates or reduces the complexity of different connection methods for different trading partners.

??security, error notifications/messages, minimum technology requirements, browser and batch capabilities; payload-agnostic; efficiency; open technologies; low-cost; PAIN;

Roles in Electronic Commerce

In most NAESB business processes, one party initiates, or sends, a transaction and the other party receives the transfer. The sender is referred to as the Client and the receiver is referred to as the Server. Parties act in both the Client and Server roles during the electronic commerce process. Once a payload file is successfully received for processing, the original receiving party switches to the Client role to send an acknowledgement back to the original sender. Internet ET implementations need to implement both Client and Server features.

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

The Trading Partner Agreement is a key reference in electronic commerce. It includes "designated site" for each partner, values used for variable parameters, and optional features that will be used by the partners (OPEN ISSUE 008).

In-house Development, COTS Software, and Outsourced Solutions

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

All parties should fully investigate the ramifications of implementing electronic commerce using the Internet. This includes ensuring that all customer data, internal data, and applications are secured from intruders or other parties not authorized for access.

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

Third-party providers offer a variety of services from a full "turn key" solution to assistance where you require it, including programming, system configuration, system administration and private communication links.

Internet ET Network Connections

Trading partners should maintain redundant connections to the public Internet for Internet ET 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.

Servers 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 Internet ET access, the following conditions should be met:

- The information provided by each URL should be exactly the same, although the "trans-id" sequences may differ.
- The trading partners should be informed of both URLs and their availability by system wide notice or by TPA.
- 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

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 includes firewalls, DNS servers, routers, hubs, LANs, etc. between your HTTP server and your Internet Service Provider's point of presence.

In this context redundancy refers to normal operations redundancy, as opposed to disaster recovery contingencies.

Private network connections to access NAESB Internet ET sites may be at any point on a party's firewall boundary at the party's discretion on a non-discriminatory basis. The specific type and speed of their connection should be mutually agreed. It is at the discretion of the party how multiple private network connections should be managed.

Disaster recovery contingencies are not addressed in NAESB Internet ET.

TCP Communications

NAESB WGQ Principle 4.1.37 and NAESB WGQ Standard 4.3.70 restrict the TCP ports used as a standard for Internet ET communications. The use of NAESB standard TCP ports may require modifications in the client-side firewall to allow for communications with the various service providers' Internet ET implementations. Upon request, parties should indicate to their trading partners which specific TCP ports they require opened to conduct electronic communication. See Appendix E for a list of allowable TCP ports. (OPEN ISSUE 007)

??TCP guidelines will be reviewed, updated, and changes presented to the NAESB Executive Committees for adoption for inclusion in the next Internet ET release.

Major Functions of NAESB Internet ET

Communication Protocols

HTTP POST - HTTP POST is the standard method for transporting Internet ET packages to trading partners. The POST method allows the upload of complete datasets without special encoding.

Mime type "multipart" - Internet ET packages are created using the "multi-part" content type.

Sending Transactions (Client)

A batch browser allows organizations to maximize their level of automation. The batch browser can be an event-driven mechanism used to push Internet ET packages to your trading partners in real-time or near real-time, while providing better audit trails.

Receipt of Transactions (Server)

Receipt of Internet ET packages and transaction payloads require a Receiving program. The Receiving program:

- Parses the Internet ET package parameters and files to determine if the appropriate parameters were transmitted
- Saves a log including a time stamp for the package
- Stores the payload file
- Sends the Receipt as an HTTP Response to the Client with the timestamp and other required Receipt elements

??In some cases the Receiving program decrypts the file prior to sending the Receipt. In this scenario decryption errors would be communicated in the Receipt. Some trading partners decrypt after sending the Receipt. Decryption errors, detected after the Receipt is sent, are communicated to trading partners using Internet ET Error Notification standards. Parties should notify trading partners of how decryption errors will be communicated.

If trading partners mutually agree to use signed Receipts, then the application would additionally attach a digital signature to the Receipt.

After the Receiving program performs its functions without errors, the payload file is forwarded to other processes including security, translation, and back-office systems.

Security

NAESB Internet ET establishes several security measures as standards to ensure a minimum level of confidence in conducting business over the Internet, and to provide uniformity in the implementation of security. Four security concepts, often referred to by the acronym ~~known as~~ PAIN, are vital to protecting Internet ET packages:

- Data **P**rivacy
- **A**uthentication
- Data **I**ntegrity
- **N**on-repudiation

Data Privacy and Encryption

Privacy is the assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended. Data privacy is accomplished by encrypting payload files. Internet ET allows encryption using:

- PGP 6.5 or higher, with RSA keys. Previous versions of PGP are not compatible with OpenPGP.

  OR

- OpenPGP, defined by IETF RFC 2440. OpenPGP can be used on a mutually-agreed basis.

Starting in WGQ EDM v1.6 and Internet ET v1.0??, SSL is used to protect username and passwords.

Authentication

Authentication is the assurance to one entity that another entity is he/she/it claims to be. Basic authentication is the required standard to prevent intruders from connecting to Internet ET Web sites. Starting in NAESB WGQ EDM v1.6 and Internet ET v1.0??, SSL is used to protect

username and passwords. Additional techniques such as firewall security enable further authentication.

Integrity

Integrity is the assurance to an entity that data has not been altered, intentionally or unintentionally, between there and here, or between then and now. ??Data Integrity is established via PGP/OpenPGP encryption, and via the "content-length" HTTP header field.

Non-Repudiation

Non-repudiation is the assurance to an entity that a party cannot deny having engaged in the transaction, or having sent the electronic message. It is like a Notary seal. The Sender of a file includes in the Internet ET package a digital signature that is created using their Private key. The Receiver knows the Sender is legitimate by decoding the digital signature using the Sender's Public key.

B. GENERAL STANDARDS

Principles:

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

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

Standards:

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

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

OR

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

~~(OPEN ISSUE 001)~~

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

C. INTERNET ELECTRONIC TRANSPORT RELATED STANDARDS

Principles:

4.1.1 [Deleted]

4.1.2 The Internet Electronic Transport (ET) 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 energy.

4.1.5 [Deleted]

4.1.6 Parties should interface with third-party vendors according to NAESB Internet ET standards.

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

4.1.8 [Deleted]

4.1.9 [Not applicable to ET]

4.1.10 [Not applicable to ET]

4.1.11 [Deleted]

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

4.1.13 [Not applicable to ET]

4.1.14 The industry should use standard policies and guidelines for testing.

4.1.15 The NAESB Internet ET should not set standards for site-level security. Individual organization security standards should be relied upon.

4.1.16 [Not applicable to ET]

4.1.17 [Not applicable to ET]

4.1.18 [Not applicable to ET]

4.1.19 [Not applicable to ET]

4.1.20 [Not applicable to ET]

4.1.21 [Not applicable to ET]

4.1.22 [Not applicable to ET]

4.1.23 [Not applicable to ET]

4.1.24 [Not applicable to ET]

4.1.25 [Not applicable to ET]

4.1.26 [Not applicable to ET]

4.1.27 [Not applicable to ET]

4.1.28 [Not applicable to ET]

4.1.29 [Not applicable to ET]

4.1.30 [Not applicable to ET]

4.1.31 [Not applicable to ET]

4.1.32 [Not applicable to ET]

4.1.33 [Not applicable to ET]

4.1.34 [Not applicable to ET]

4.1.35 [Not applicable to ET]

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

4.1.37 Internet ET implementations should minimize the number of outbound ports required to be opened on the client-side firewall.

4.1.38 [Not applicable to ET]

4.1.39 Trading Partners should mutually select and use a version of the NAESB Internet ET standards under which to operate, unless specified otherwise by government agencies. Trading Partners should also mutually agree to adopt later versions of the NAESB Internet ET standards, as needed, unless specified otherwise by government agencies.

Definitions:

4.2.1 [Not applicable to ET]

4.2.2 [Not applicable to ET]

4.2.3 [Not applicable to ET]

4.2.4 [Not applicable to ET]

4.2.5 [Not applicable to ET]

4.2.6 [Not applicable to ET]

4.2.7 [Not applicable to ET]

4.2.8 [Not applicable to ET]

4.2.9 [Not applicable to ET]

4.2.10 [Not applicable to ET]

4.2.11 [Not applicable to ET]

4.2.12 [Not applicable to ET]

4.2.XX [Not applicable to ET]

4.2.13 [Not applicable to ET]

4.2.14 [Not applicable to ET]

4.2.15 [Not applicable to ET]

4.2.16 [Not applicable to ET]

4.2.17 [Not applicable to ET]

4.2.18 [Not applicable to ET]

4.2.19 [Not applicable to ET]

4.2.20 ??Testing electronic packages between trading partners includes testing of:
1. Connectivity;
2. Encryption/Decryption;
3. Digital signatures where appropriate

4.2.x21 "Failover" defines a scenario a prescribed process is executed when a NAESB Internet ET Client fails to establish a connection to the target NAESB Internet ET Server.

4.2.x22 "Trading Partner" is a party that enters into an agreement with another party to transact business electronically using the Internet ET standard.

4.2.x23 "Originating party" is any party originating/creating the package . This could also include a third-party.

4.2.x24 "Third-Party" is any organization that a trading party uses to provide services to comply with the required elements of the Internet ET.

4.2.x25 "Receiving Party" is any party that hosts (either in-house or outsourced) an Internet ET compliant server capable of receiving Internet ET packages.

4.2.x26 "Trading Partner Agreement" is a legal agreement between trading parties. This agreement often dictates service level agreements and problem remediation processes. (OPEN ISSUES 008)

4.2.xx "Batch Browser". A Browser that can be run with little or no manual operation or intervention. See "Browser"

4.2.xx "Browser". A software program capable of generating HTTP Requests, including HTTP POST requests.

4.2.xx "Client". The computer hardware and software used by the Sender to transmit an Electronic Package to the Receiver's Server. A Client can be fully-automated or manual.

4.2.xx "COTS". Commercial Off-The-Shelf; software that can be purchased that requires little or no customization.

4.2.xx "Electronic Package". A data stream sent via HTTP POST that contains envelope header information and Payload File(s). The Payload Files are encrypted using defined Internet ET encryption techniques.

4.2.xx "Error Notification". Errors that are trapped after the IET receipt is sent are communicated via an Error Notification package from the Receiver of the original data to the Sender.

4.2.xx "HTTP Request". The stream of data sent from the Client to the Server that includes header information and payload data.

4.2.xx "HTTP Response". The stream of data sent from the Server to the Client in response to an HTTP Request.

4.2.xx "HTTP Server". A computer capable of receiving HTTP Requests and responding with HTTP Responses.

4.2.xx "IETF". Internet Engineering Task Force; a body of technical experts that set

standards, known as Requests for Comments (RFC) for the Internet.

4.2.xx "Interactive Browser". A Browser that requires manual operation or intervention. See "Browser".

4.2.xx "Internet EDM". The GISB and NAESB WGQ standards up to and including Version 1.7. The "Internet ET" and "QEDM" standards were derived from these EDM standards.

4.2.xx "Internet Electronic Transport, ET". The NAESB standards for the secure transport of electronic information between trading partners.

4.2.xx "Package". See "Electronic Package."

4.2.xx "Payload Files". The data contents inside of an electronic package. NAESB Internet ET does not care what the contents of ET Electronic Packages contain.

4.2.xx "QEDM". Quadrant-specific Electronic Delivery Mechanism; the set of standards for each NAESB quadrant that define the business policies, practices and processes for that quadrant. The QEDM excludes electronic transport practices and standards. The QEDMs were derived from the Internet EDM from GISB and NAESB WGQ.

4.2.xx "Quadrant-Specific Electronic Delivery Mechanism". See "QEDM".

4.2.xx "Receipt". The HTTP Response sent from the Receiver to the Sender that includes a timestamp and OK/error status.

4.2.xx "Receiver". The party that receives an electronic package.

4.2.xx "Secure Electronic Package". See "Electronic Package"

4.2.xx "Sender". The party that sends an Electronic Package.

4.2.xx "Server". The computer hardware and software used by the Receiver to receive an Electronic Package from the Sender's Client. The Server is an HTTP/Web Server.

4.2.xx "Web Browser". See "Browser"

4.2.xx "Web Server". See "HTTP Server".

Standards:

4.3.x1 All parties sending and receiving data should accept a TCP/IP connection.

4.3.x2 ??On time stamping, data leaves control of the originator by the same time (deadline), regardless of mechanism (3rd party service provider time stamp is acceptable) and 15 minutes of communication time should be available to allow accumulation of all transactions to the pipeline. A standard network protocol (TCP/IP) should be in service for direct connect to the pipeline designated site by 4/1/97.

4.3.x3 ??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 window the transaction 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[Not applicable to ET]

4.3.4 Trading partners should retain audit trail data for at least 24 months. This data

retention requirement does not otherwise modify statutory, regulatory, or contractual record retention requirements. (OPEN ISSUE 033)

4.3.5 [Not applicable to ET]

4.3.6 [Not applicable to ET]

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.

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 Internet ET.

4.3.9 There is a time stamp ("time-c") that designates the time that a file is received at the designated site. The receiving party should generate a timestamp upon the successful receipt of a complete file and send an immediate response to the sending party. The timestamp should be generated by the Receiving program of the receiving party, prior to further processing by the Receiving program.

4.3.10 The timestamp should be included in the HTTP Response back to the sender of the original HTTP package. The server clock generating the timestamp should be synchronized with the National Institute of Standards and Technology (NIST) time in order to mitigate discrepancies between the clocks of the sender and receiver. (OPEN ISSUE 010)

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 (OPEN ISSUE 008).

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. (OPEN ISSUE 008)

4.3.13 The sender should make three attempts to complete a unit of work. A unit of work consists of one complete HTTP POST transaction as defined in the technical specification of the HTTP protocol (Internet Engineering Task Force RFC 1945). The roles of sender and receiver are also defined in that document. After three failed attempts, it should be considered a failure. ??timeframe between failures

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

Client (Sender)	Server (Receiver)	Receiving Program (Receiver)
	Listen for Connect	
Connect	Accept Connection	
Write HTTP Request	Read HTTP Request	Start of Receipt
Write HTTP Request	Read HTTP Request	
EOF (send)	Read HTTP Request	End of Receipt
Read ~~(~~HTTP Rr~~r~~esponse~~)~~	Write ~~(~~HTTP Rr~~r~~esponse~~)~~	

Received		
EOF ~~(~~HTTP R~~r~~esponse~~)~~		

4.3.15 Trading partners should implement all security features (privacy, secure authentication, integrity, and non-repudiation) using a file-based approach via a commercially available implementation of PGP 6.5 or greater (or compatible with PGP 6.5) or, on a mutually agreed basis, an OpenPGP compatible product. Trading partners should also implement basic authentication. These technologies support 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 public key. A lifetime of one year or less is recommended.

4.3.16 [Not applicable to ET]

4.3.17 [Not applicable to ET]

4.3.18 [Not applicable to ET]

4.3.19 [Not applicable to ET]

4.3.20 [Not applicable to ET]

4.3.21 [Not applicable to ET]

4.3.22 [Not applicable to ET]

4.3.23 [Not applicable to ET]

4.3.24 [Not applicable to ET]

4.3.25 [Not applicable to ET]

4.3.26 [Not applicable to ET]

4.3.27 [Not applicable to ET]

4.3.28 [Not applicable to ET]

4.3.30 [Not applicable to ET]

4.3.31 [Not applicable to ET]

4.3.32 [Not applicable to ET]

4.3.33 [Not applicable to ET]

4.3.34 [Not applicable to ET]

4.3.35 [Not applicable to ET]

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.

4.3.38 [Not applicable to ET]

4.3.39 [Not applicable to ET]

4.3.40 [Not applicable to ET]

4.3.41 [Not applicable to ET]

4.3.42 [Not applicable to ET]

4.3.43 [Not applicable to ET]

4.3.44 [Not applicable to ET]

4.3.45 [Not applicable to ET]

4.3.46 [Not applicable to ET]

4.3.47 [Not applicable to ET]

4.3.48 [Not applicable to ET]

4.3.49 [Not applicable to ET]

4.3.50 [Not applicable to ET]

4.3.51 [Not applicable to ET]

4.3.52 [Not applicable to ET]

4.3.53 [Not applicable to ET]

4.3.54 [Not applicable to ET]

4.3.55 [Not applicable to ET]

4.3.x56 The industry should use common codes for legal entities when using Internet ET.

4.3.57 [Not applicable to ET]

4.3.58 [Not applicable to ET]

4.3.59 [Not applicable to ET]

4.3.60 [Not applicable to ET]

4.3.61 [Not applicable to ET]

4.3.62 [Not applicable to ET]

4.3.63 [Not applicable to ET]

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

4.3.65 [Not applicable to ET]

4.3.66 [Not applicable to ET]

4.3.67 [Not applicable to ET]

4.3.68 [Not applicable to ET]

4.3.69 [Not applicable to ET]

4.3.70 Parties should be limited to the NAESB Internet ET approved list of available TCP ports and UDP ports for Internet ET implementations included in Appendix E?? of the Internet ET Standards Manual. (OPEN ISSUE 009)

4.3.71 Internet ET implementations should not require any inbound ports to be opened on the

client-side firewall.

4.3.72 [Not applicable to ET]

4.3.73 [Not applicable to ET]

4.3.74 [Not applicable to ET]

4.3.75 [Not applicable to ET]

4.3.76 [Not applicable to ET]

4.3.77 [Deleted]

4.3.78 [Not Applicable to ET]

4.3.79 [Not Applicable to ET]

4.3.80 [Not Applicable to ET]

4.3.81 [Not Applicable to ET]

4.3.82 [Not Applicable to ET]

4.3.83 [Not Applicable to ET]

4.3.84 [Not Applicable to ET]

4.3.85 [Not Applicable to ET]

4.3.86 [Not Applicable to ET]

4.3.87 [Not Applicable to ET]

4.3.88 For Internet ET, 128-bit Secure Socket Layer (SSL) encryption should be used.

D. Interpretations

NAESB REQ has adopted the following interpretations of standards that relate to Electronic Delivery Mechanism Related Standards implementation:

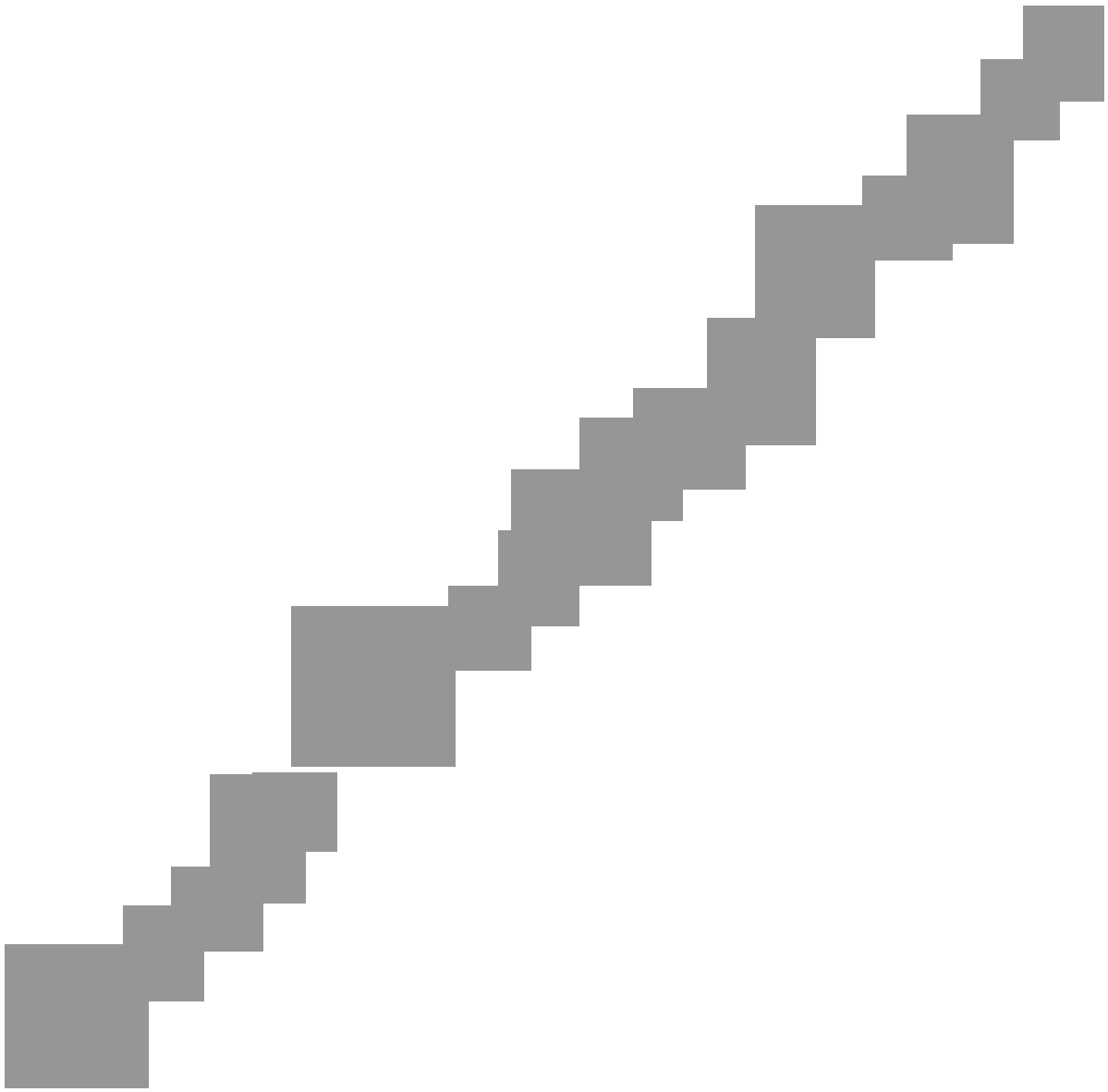
[NONE TO DATE]

7.3.24 [Not applicable to ET]

7.3.35 [Not applicable to ET]

5 – RELATED STANDARDS

[remains in separate document]



~~TAB~~ 6 ~~– ,~~ TECHNICAL IMPLEMENTATION - INTERNET ET

Technologies Selected by NAESB WGQ/REQ/RGQ Internet ET

The NAESB Internet ET uses TCP/IP and HTTP to securely and reliably transport electronic packages to trading partners.

The Internet ET uses two primary Internet software components. The first component is called a browser and runs at the Sender's site as client software, and is referred to in this document as "Client". The second component runs at the Receiver's site and is called a Web or HTTP server, and is referred to in this document as "Server". The Server usually runs on a dedicated computer.

The standard data elements, each with element name and description, have been defined in the Section "Data Dictionary For Internet ET". The next two sections identify what is involved in sending and receiving electronic packages. The "Security" section outlines how to encrypt and decrypt the electronic packages. ??The remaining sections cover considerations for other aspects of the overall process ?? may go away.

DATA DICTIONARY FOR INTERNET ET

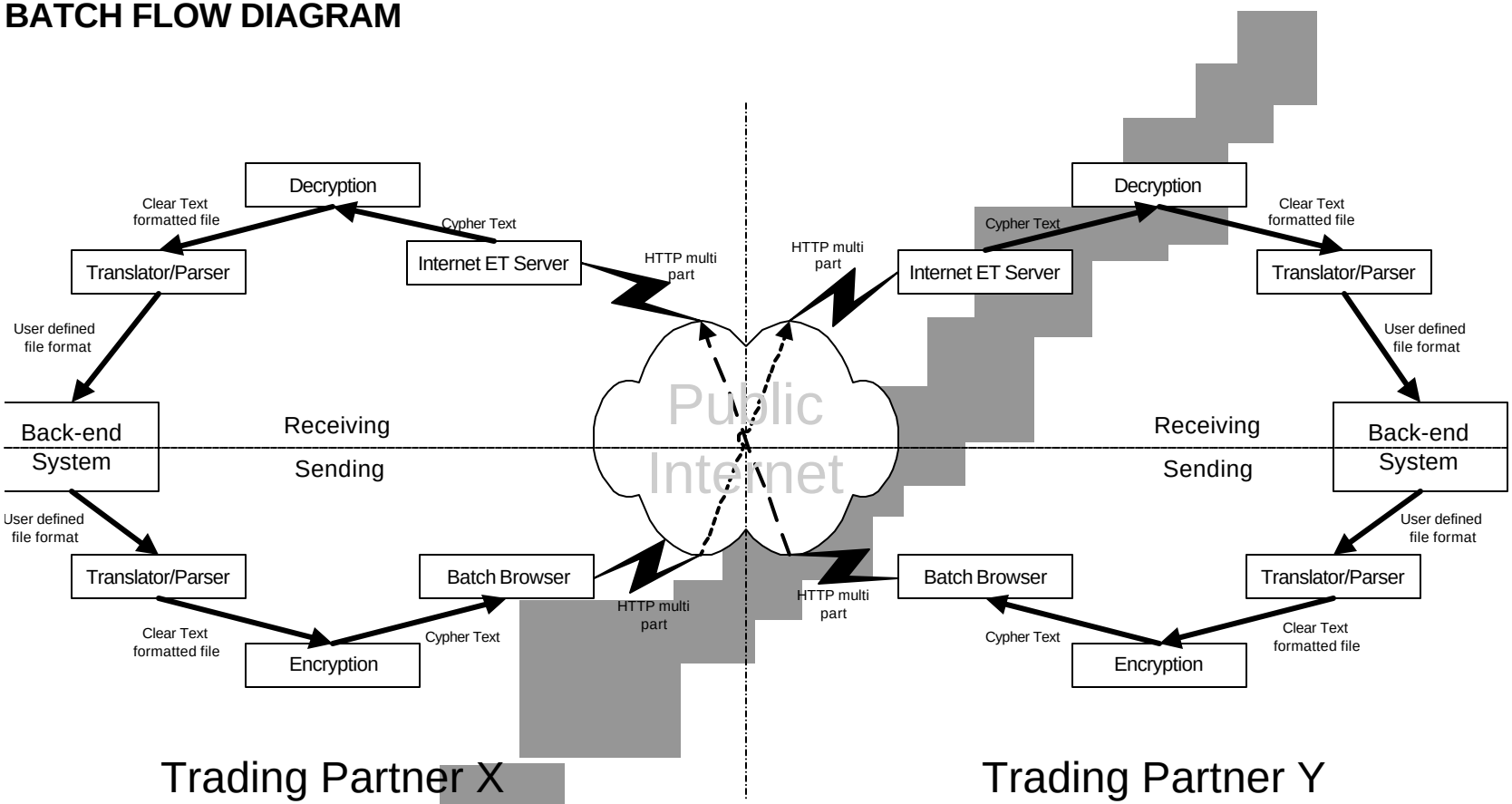
Business Name	Definition	Format	Usage*	Condition
from**	the party sending the transaction	Common Code Identifier format (OPEN ISSUE 001)	in Request; M	used in file transmittal; displayed in HTTP Response; and, used in posting back decryption-related errors
input-data	the filename for the transaction 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 transmitted	X12 ;XML;error	in Request; M	"X12","XML", or other NAESB ~~REQ~~ standard 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 ~~(OPEN ISSUE 001)~~	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 002)	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 identifies 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

Business Name	Definition	Format	Usage*	Condition
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 (OPEN ISSUE 010)	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 001)	in Request; M	used in file transmittal and displayed in HTTP Response and posted back for any decryption-related errors
transaction-set	name of the document type being sent	8 character code; (OPEN ISSUE 003) 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~~ Internet ET version being used by the sender	numeric, decimal notation (e.g. 1.6)	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 001)~~

BATCH FLOW DIAGRAM



Batch Flow Diagram

Electronic Transport Life Cycle

The life cycle of an Electronic Package using Internet ET is described below:

Sender	Receiver
• Collects payload data to be sent • Encrypts payload • Prepares digital signature if necessary	
• Uses browser to create Electronic Package multipart HTTP Request with header data elements and payload. • Uses HTTP POST to send the electronic package to the Receiver ↘	
	• Receives the HTTP Request on their Web/HTTP Server • Validates Sender information from HTTP Request Header data elements and payload • **Decrypts payload file • Prepares Receipt • Checks digital signatures if necessary
	↙ • Sends Receipt with either “OK” or error message
• Updates logs • If errors, correct errors then repeat process	• **Decrypts payload file
	↙ • If errors in decryption, sends Error Notification to Sender
• Receives Error Notification • Updates logs • correct errors then repeat process	• Updates logs • If no errors, Receiver processes contents of payload

**Parties may choose to decrypt file before or after Receipt is sent to Sender.

SENDING TRANSACTIONS

General Flow

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

1. Open HTTP connection
2. Check connection status. If in error, re-queue package according to Internet ET standards. This check should be performed here and throughout the following processes.
3. Post, including a) Authentication, b) Send multipart form, c) Receive HTTP Response data
4. Check connection status. If in error re-queue package according to Internet ET standards
5. Check HTTP status code (200 is good, less than 300 may be acceptable). If status is not successful re-queue package according to Internet ET standards
6. Close connection - wait for other end to close in a reasonable time
7. Parse HTTP Response data elements
8. If request-status ok, then log success
9. If request-status error, then log error
10. If no valid request-status re-queue package according to Internet ET standards
11. Remove package 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 002) and encapsulate the "gisb-acknowledgement-receipt" (OPEN ISSUE 002) and digital signature body parts within a MIME envelope with a "content-type" of application/pgp-signature.

~~**HTTP POST**~~

~~Internet ET uses HTTP POST to send electronic packages and responses. The POST method allows the upload of complete datasets without special encoding.~~ [??moved to 'communication protocols']

Using an Interactive Browser for Internet ET

Electronic packages can be uploaded to a trading partner using an interactive browser secured using SSL 128-bit encryption. Sending electronic packages via an interactive browser is ideal for a small volume of package transfers, or as a back-up method to any batch or automated process.

To use an interactive browser to upload data, an HTML document must be created with an HTML <FORM> element that allows the Sender to type in any necessary data elements, such as "to", "from", "input-format", and the name of the file to be uploaded. When the user submits the form, an HTTP POST is sent to the Server with the package, which includes the uploaded file and the required data elements.

The following example is an HTML document with a form that specifies the POST method and contains the required data elements. This type of HTML form could be used with any browser that supports multipart POST with a file upload.

EXAMPLE: HTML DOCUMENT WITH A FORM FOR MULTIPART POST USING AN INTERACTIVE BROWSER:

```
<HTML><HEAD><TITLE>NAESB Internet ET Package Upload</TITLE>
<H1><CENTER>NAESB Internet ET Package Upload</CENTER></H1>
</HEAD>
<BODY><HR>
<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 Internet ET 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 002)

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 (TPA) (OPEN ISSUE 008) identifies the URLs for both parties.
- METHOD= specifies the HTTP protocol method. "POST" has been defined as the Internet ET standard method.
- <INPUT ...>. HTML INPUT elements include the required data elements such as "from", "to", and "input-format". Refer to the data dictionary for the complete list of required data elements.

~~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 interactive browser will take the values entered in the input fields and reformat them into a data stream, formatted according to the encoding type. The file identified for upload is opened and its contents are included in the data stream. The data stream is then sent to the URL specified by "**ACTION=**", which indicates a Server Receiving script or program written to receive the package.

Using a Batch Browser for Internet ET

A batch browser is used by companies that want to automate their transport processes and/or prefer to minimize human involvement. A batch browser is initiated by a program or a script.

A batch browser can be created via custom programming. A batch browser is coded to perform the same formatting as an interactive browser, formatting a data stream that conforms to the HTTP and Internet ET protocols. A batch browser must be coded as a "TCP sockets" program. See the section "Writing a Batch Browser".

Authentication

??[GPD to research] Prior to NAESB WGQ EDM v1.6, userids and passwords had to be encoded using base64-encoded tools. NAESB WGQ EDM v1.6 requires use of SSL to encrypt this information. As a result, base64 encoding is no longer necessary.

HTTP basic authentication includes a "userid" and "password". Interactive browsers include a basic authentication feature which automatically prompts for "userid" and "password". In a batch browser, the authentication must be specifically coded. The "userid" 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 Server will send a "gisb-acknowledgement-receipt" (OPEN ISSUE 002) as an HTTP Response to the Client before dropping the Client's connection. If the transacting parties agree to use signed receipts, then the Server applies a digital signature to the "gisb-acknowledgement-receipt" (OPEN ISSUE 002) and encapsulates the entire package in a MIME envelope of "content-type: application/pgp-signature".

??The "gisb-acknowledgement-receipt" ~~response~~ returned from the ~~Web server~~ Server ~~will~~ contains the "time-c" and the "time-qualifier-??" receipt timestamp~~ss~~ that are ~~include a timestamp~~ recorded when the final byte from the package ~~file~~ upload is received and stored. This receipt timestamp is the official timestamp regarding transaction turnaround deadlines as defined in ~~NAESB WGQ REQ~~ Internet ET and QEDM standards. This timestamp and all other pertinent package ~~file~~ transmittal information should be logged by the receiver when the posted package ~~file~~ is stored on the ~~receiving server~~Server, and logged by the Client ~~as well as logged by the client~~. Likewise, any errors or warnings should be logged at both the Client and Server~~server and client~~. ~~(OPEN ISSUE 010)~~

HTTP Request Data Elements

The HTTP Request will provide all required data elements in the ORDER DEFINED BELOW. Any "mutually-agreed-upon" data elements will follow the required data elements in the data stream. Refer to the section "Data Dictionary for Internet ET" for descriptions of these data elements.

Required Data Elements, Listed in the Required Order:

~~1.~~12. from
~~2.~~13. to
~~3.~~14. version
~~4.~~15. receipt-disposition-to
~~5.~~16. receipt-report-type
~~6.~~17. input-format
~~7.~~18. input-data

Mutually Agreed Upon Data Elements

- transaction-set
- receipt-security-selection

??check deleted descriptions against data dictionary

Writing a Batch Browser

A batch browser Client needs to simulate the actions of an interactive browser Client. As stated earlier, the interactive browser Client will take the HTML form, reformat the information according to the HTTP protocol, then send the data stream to the Server. The reformatting ~~involves adding~~ adds a header and ~~places 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.

EXAMPLE: A TYPICAL HEADER SENT TO THE 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
```

POST Line - In the example above, the first line indicates the POST method was used and identifies which Receiving program to call:

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
```

Content Type - The "content-type" line indicates that the encoding method is multipart, and identifies the character string used as the boundary.

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

Boundary String - The "boundary=" identifies the string that will appear between each field as a delimiter. In this example, the boundary is comprised of 27 hyphen characters followed by a

number.

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

The boundary can be ANY character string that you choose. The string used CANNOT OCCUR ANYWHERE ELSE IN THE PACKAGE 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 string, ~~–~~when used as a separator, REQUIRES TWO HYPHEN CHARACTERS APPENDED TO THE FRONT of the string. The LAST boundary required in the form is TWO HYPHEN CHARACTERS APPENDED TO THE BACK of the separator boundary, used to indicate to the Server program that this is the end of the data.

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

Content Length - 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. "content-length" ~~It~~ indicates to the ~~tells the~~ Server how much data are~~is~~ going to come after this point. In the example above, the content length is:

Content-Length: 5379

Envelope / Required Data Elements – The envelope information for the package ("to", "from", etc) is included in a series of boundaries that include the "content-disposition" and "name=" qualifiers, followed by the data element value. The example below includes the "from" field as "123456789" and the "to" field as "234567890".

```
----------87453838942833
content-disposition: form-data; name="from"

123456789
----------87453838942833
content-disposition: form-data; name="to"

234567890
```

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 Internet ET Data Dictionary. 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 blank line. 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 example. In most programming libraries and commercial products the starting delimiter is "\r\n\r\n" (C notation).

```
----------87453838942833
content-disposition: form-data; name="version"

1.64
----------87453838942833
content-disposition: form-data; name="receipt-disposition-to"

123456789)
----------87453838942833
content-disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt (OPEN ISSUE 002)
```

```
------------------------------87453838942833
content-disposition: form-data; name="input-format"

x12
```

Payload – The important electronic data (EDI, etc) that is being packaged and sent is encrypted and included in its own boundary section.

The data field containing the Internet ET payload file has two extra identifiers. The "filename=" element indicates the name of the file sent from the sender/client computer. In the example the name of the file is **"c:\temp\smallnom.bin"**.

```
content-disposition: form-data; name="input-data"; filename="c:\temp\smallnom.bin"
```

The "content-type" element indicates the type of the data being transmitted according to accepted Internet standards.

```
content-type: multipart/encrypted; boundary=--boundary2--200309090001; protocol="application/pgp-encrypted"
```

Note that encrypted files can be multipart also, which means they will have their own boundary string.

```
------------------------------87453838942833
content-disposition: form-data; name="input-data"; filename="c:\temp\smallnom.bin"
content-type: multipart/encrypted; boundary=--boundary2--200309090001; protocol="application/pgp-encrypted"

----boundary2--200309090001
content-type: application/pgp-encrypted

Version: 1

----boundary2--200309090001
content-type: application/octet-stream

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

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8sb7ErC340MrNA/dw3taGMjmI
+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODGlQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/4
3fkB+alATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1Eh785zC03UAw0qg0ugMt86dPe
yd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8Ocp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl1
41QZ1RqbeNaqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0Cvzpb4JE+gMDf3q4ISUb1Fv7
/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZyS
aRO8Vtff+4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
----boundary2--200309090001--
```

Boundary String Terminators - Each multipart stream must be terminated with the boundary string terminator. After the contents of the last data field, the boundary string and the required two-hyphen terminator indicate the end of the multipart encrypted payload:

```
----boundary2--200309090001--
```

A second boundary terminator string indicates the end of the package:

```
------------------------------87453838942833--
```

??See section "??" for an outline of "content-type" values.

HTTP Features Not Supported by Internet ET

Internet ET DOES NOT SUPPORT:

- multiple files in a single POST
- a single file split into multiple POSTs

EXAMPLE: AN X12 EDI DATA STREAM BEFORE ENCRYPTION:

Content-type: application/EDI-X12

ISA~00~ ~01~AAA6300300~14~1234567890000 ~14~2345678900000
... more data from the X12 file…
IEA~1~000003616

EXAMPLE: THE SAME X12 EDI ENCRYPTED WITH PGP

content-type: multipart/encrypted; boundary=--boundary2--200309090001; protocol="application/pgp-encrypted"
----boundary2--200309090001
content-type: application/pgp-encrypted
Version: 1
----boundary2--200309090001
content-type: application/octet-stream
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5
hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8sb7Er340MrNA/dw3taGMjmI+
CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODGlQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/43f
kB+alATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1Eh785zC03UAw0qg0ugMt86dPeyd
91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8Ocp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141
QZ1RQbeNaqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cVzpb4JE+gMDf3q4ISUb1Fv7/
+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9.UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZyS
aRO8Vtff+4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
----boundary2--200309090001--

EXAMPLE: A COMPLETE ELECTRONIC PACKAGE DATA STREAM

```
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 (OPEN ISSUE 001)
------------------------------87453838942833
content-disposition: form-data; name="to"

234567890 (OPEN ISSUE 001)
------------------------------87453838942833
content-disposition: form-data; name="version"

1.46
------------------------------87453838942833
content-disposition: form-data; name="receipt-disposition-to"

123456789 (OPEN ISSUE 001)
------------------------------87453838942833
content-disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt (OPEN ISSUE 002)
------------------------------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=--boundary2--200309090001; protocol="application/pgp-encrypted"

----boundary2--200309090001
content-type: application/pgp-encrypted

Version: 1

----boundary2--200309090001
content-type: application/octet-stream

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

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8sb7ErC340MrNA/dw3taGMjmI
+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODGlQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/4
3fkB+alATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1Eh785zC03UAw0qg0ugMt86dPe
yd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8Ocp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl1
41QZ1RqbeNaqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cVzpb4JE+gMDf3q4ISUb1Fv7
/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZyS
aRO8Vtff+4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
----boundary2--200309090001--
------------------------------87453838942833--
```

RECEIVING TRANSACTIONS

General Flow

The following is an example of the steps necessary to receive an Internet ET package:

1. Parse multi-part form
2. Validate HTTP Request data elements
3. If HTTP Request data elements in error, return appropriate Internet ET standard error code in the HTTP Response data elements
4. Save data
5. Create "gisb-acknowledgement-receipt" (OPEN ISSUE 002)
6. If using signed receipts, Produce a digital signature over ??over what?? the "gisb-acknowledgement-receipt" (OPEN ISSUE 002) created in step 5.
7. Encapsulate the "gisb-acknowledgement-receipt" (OPEN ISSUE 002) and digital signature body parts in a "Content-Type" of "multipart/signed envelope"
8. Return HTTP Response with the "gisb-acknowledgement-receipt" (OPEN ISSUE 002) object back to Client
9. Close connection
10. Log final results
11. Route data file to the next process based upon "input-format"

Overview of Web Server Receiving Programs

The Web Server receives the POST and calls the appropriate Receiving script or program to:

- parse the incoming HTTP Request
- create the receipt timestamp using the current date and time
- create an HTML Response to the Client

An Internet ET Receiving program may be implemented using a variety of technologies and techniques, including Active Server Pages (ASP), Common Gateway Interface (CGI), Java Server Pages (JSP), Java Servlets, and Personal Home Pages (PHP). The Internet ET is supported by most commercially available Web/HTTP servers.

The Receiving Program and Process

The 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 Internet ET payload file.

The Receiving program only stores the payload file and is not concerned with the content of the payload file, which is encrypted. It will use the "content-length" to determine how much data to expect in the body of the package.

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

When the Server receives a POST it will first read the header and populate environment variables before calling the Receiving program. Most HTTP servers read header variables and populate environment variables. Check your HTTP server documentation for more information.

EXAMPLE: A SAMPLE HTTP POST HEADER

```
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
```

After reading the HTTP header information, the Server will buffer the remaining data transmitted and 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, which can impact your receipt timestamp. The more common implementations buffer the entire transmission before calling the program. Check your server implementation if this characteristic is important to you.

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

EXAMPLE: DATA STREAM AVAILABLE TO RECEIVING PROGRAM

```
----------87453838942833
content-disposition: form-data; name="from"
123456789
----------87453838942833
content-disposition: form-data; name="to"
234567890
----------87453838942833
content-disposition: form-data; name="version"
1.64
----------87453838942833
content-disposition: form-data; name="receipt-disposition-to"
123456789
----------87453838942833
content-disposition: form-data; name="receipt-report-type"
gisb-acknowledgement-receipt (OPEN ISSUE 002)
----------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=--boundary2--200309090001; protocol="application/pgp-encrypted"
----boundary2--200309090001
content-type: application/pgp-encrypted
Version: 1
----boundary2--200309090001
content-type: application/octet-stream
-----BEGIN PGP MESSAGE-----
Version: PGP 6.5
hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHsz0e8sb7ErC340MrNA/dw3taGMjmI
+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODGlQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/4
3fkB+alATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1Eh785zC03UAw0qg0ugMt86dPe
yd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8Ocp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl1
41QZ1RQbeN.aqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cVzpb4JE+gMDf3q4ISUb1Fv
7/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZy
SaRO8Vtff+4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
----boundary2--200309090001--
----------87453838942833--
```

This Receiving program should check for basic validity in the environment variables and the data stream, then . parse the variables/data from the format. Data validations should include:

- The "REQUEST_METHOD" environment variable is "POST"
- The "CONTENT_TYPE" environment variable should be "multipart/form-data" and the boundary, which cannot appear anywhere in the transaction being sent
- 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 a blank line ("\r\n\r\n" in C+ notation) before the start of the data
- All tag values in the HTTP header should be evaluated in a case insensitive manner
- Improperly formatted input. Finding the end of the stream using both "content-length" and the boundary string terminator end mark is a good method to detect improperly formatted input.

Acknowledgement Receipt: "gisb-acknowledgement-receipt"

The Acknowledgement Receipt is critical to non-repudiation and business process timing. Immediately after the Receiving program decrypts and saves the data, the Receiving program should record the time and construct a "gisb-acknowledgement-receipt" (OPEN ISSUE 002) described ??below or in section ??.

If using signed receipts, the Receiving program must also produce a digital signature of the "gisb-acknowledgement-receipt" (OPEN ISSUE 002) and send both the "gisb-acknowledgement-receipt" (OPEN ISSUE 002) and the digital signature body parts within a multipart/signed MIME envelope.

This receipt is sent from the Receiving program to the Client prior to closing the HTTP connection.

Additional Receiving Program Functions

- All data element names of the HTTP Request and Response fields will be in lower case. Note that the Internet ET standard format file contained in the Request and Response may follow a different standard. ??clean up examples; references to these??
- 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 HTTP Response and in the order specified. Additional information can be included after the required elements at the server's discretion.
- The "gisb-acknowledgement-receipt" (OPEN ISSUE 002) must be enveloped in a "multipart/report", as specified in ??EDIINT AS2 (OPEN ISSUE 005) following the rules for Generalized Receipts.
- If signed receipts are used, the "gisb-acknowledgement-receipt" (OPEN ISSUE 002) including the multipart/report envelope is digitally signed, producing an application/pgp-encrypted body part. Both the multipart/report ("gisb-acknowledgement-receipt" (OPEN ISSUE 002)) 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.

Receiving Process URL Implementation Guidelines

??got some work here?? Internet ET standard 4.3.12 (OPEN ISSUE 007) 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." (OPEN ISSUE 008)*

Each company must offer at least one URL to accept files using Internet ET. Companies can offer multiple URLs. Though companies are free to construct a Web site with multiple "single-purpose" URLs (e.g. nominations.xyzcorp.com; enrollments.xyzcorp.com) NAESB recommends the use of one "general-purpose" URL.

The Receiving program may initiate error notifications after the “gisb-acknowledgement-receipt” (OPEN ISSUE 002) is sent (e.g. file decryption errors). Error notifications posted to the Sender would be directed to the Sender’s general-purpose URL.

All URLs that will be required for use in the Internet ET process must be agreed to and defined in the Trading Partner Agreement (TPA) (OPEN ISSUE 008).

HTTP Response “gisb-acknowledgement-receipt” Data Elements

Required HTTP Response Data Elements (listed in the required order)	
WGQ	REQ/RGQ
time-c request-status server-id trans-id	time-c time-c-qualifier request-status server-id trans-id

Examples of HTTP Response Required Data Elements:

EXAMPLE: RESPONSE, SUCCESSFUL, MULTIPART FORMAT:

content-type: multipart/report; report-type="gisb-acknowledgement-receipt"; boundary="GISB7867" (OPEN ISSUE 002)

--GISB7867
Content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Success</TITLE></HEAD> <BODY><P>
time-c=19960619082855 (OPEN ISSUE 010)*
*request-status=ok**
*server-id=coolhost**
*trans-id=234423897**
</P> </BODY></HTML>
--GISB7867
Content-type: text/plain

time-c=19960619082855 (OPEN ISSUE 010)*
*request-status=ok**
*server-id=coolhost**
*trans-id=234423897**
--GISB7867--

EXAMPLE: RESPONSE, SUCCESSFUL, MULTIPART FORMAT, TIME-C-QUALIFER FOR TIME ZONE:

content-type: multipart/report; report-type="gisb-acknowledgement-receipt"; boundary="GISB7867" (OPEN ISSUE 002)

--GISB7867
Content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Success</TITLE></HEAD> <BODY><P>
time-c=19960619082855 (OPEN ISSUE 010)*
*time-c-qualifier=-05**
*request-status=ok**
*server-id=coolhost**
*trans-id=234423897**
time-c-qualifer=-0400
</P> </BODY></HTML>
--GISB7867
Content-type: text/plain

time-c=19960619082855 (OPEN ISSUE 010)*
*time-c-qualifier=-05**
*request-status=ok**
*server-id=coolhost**
*trans-id=234423897**
time-c-qualifer=-0400
--GISB7867--

EXAMPLE: RESPONSE, ERROR, MULTIPART FORMAT:

content-type: multipart/report; report-type="gisb-acknowledgement-receipt"; boundary="GISB7866" (OPEN ISSUE 002)

--GISB7866
Content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Error</TITLE></HEAD> <BODY><P>
time-c=19960619082855 (OPEN ISSUE 010)*
*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 (OPEN ISSUE 010)*
*request-status=EEDM106: Invalid To Common Code Identifier**
*server-id=coolhost**
*trans-id=234423897**
--GISB7866--

EXAMPLE: RESPONSE, WARNING, MULTIPART FORMAT:

content-type: multipart/report; report-type="gisb-acknowledgement-receipt"; boundary="GISB7866" (OPEN ISSUE 002)

--GISB7866
Content-type: text/html

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

time-c=19960619082855 (OPEN ISSUE 010)*
*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 (OPEN ISSUE 010)*
*request-status= WEDM100: Transaction Set Sent, Not Mutually Agreed **
*server-id=coolhost**
*trans-id=234423897**
--GISB7866--

EXAMPLE: RESPONSE, SUCCESSFUL , SIGNED RECEIPT:

content-type:multipart/signed; micalg=pgp-md5; protocol="application/pgp-signature";
boundary=--boundary2--200309090001

----boundary2--200309090001

content-type: multipart/report; report-type="gisb-acknowledgement-receipt"; boundary="GISBB7867" (OPEN ISSUE 002)

--GISB7867
Content-type: text/html

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

time-c=19960619082855 (OPEN ISSUE 010)*
*request-status=ok**
*server-id=coolhost**
*trans-id=234423897**

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

--GISB7867
Content-type: text/plain.
time-c=19960619082855 (OPEN ISSUE 010)*
*request-status=ok**
*server-id=coolhost**
*trans-id=234423897**
--GISB7867--
----boundary2--200309090001
content-type: application/pgp-signature

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

Version: 2.6.26.5

iQCVAwUBMJrRF2N9oWBghPDJAQE9UQQAtl7LuRVndBjrk4EqYBIb3h5QXIX/LC//JV5bNvkZIGPIcEmI5iFd9boEgvpirHt
IREEqLQRkYNoBActFBZmh9GC3C041WGquMbrbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/W72vgSxLhe/zhdfolT9BrnH
OxEa44b+EI=
=ndaj

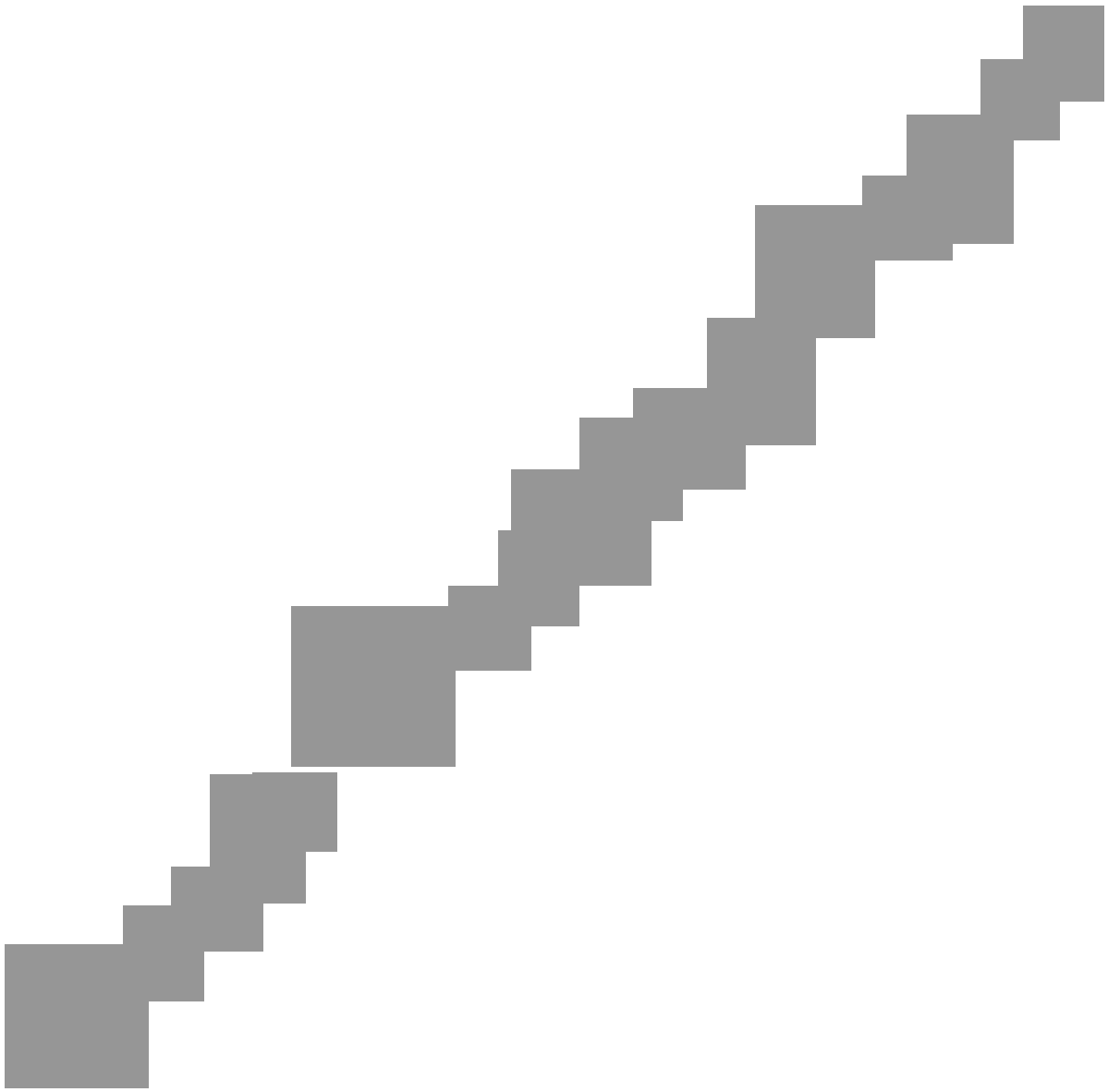
-----END PGP MESSAGE-----

----boundary2--200309090001—

EXAMPLE: RESPONSE, SUCCESSFUL:

HTML format (this example is for a successful transmittal): <html> <head> <title> Upload OK</ title></ head> <!-- time-

c= 19960123203618-->_ <!-- request- status= ok* --> <!-- server- id= coolhost*--> <!-- trans- id= 232323897*--> <h1> Upload OK </ h1>< br> <body> <B> File Saved at (time- c): </B> 19960123203618< 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> (OPEN ISSUE 010)*



SECURITY

Security Concepts

The security requirements include four primary security aspects: data Privacy, data Integrity, Authentication, and Non-repudiation (PAIN).

- Data privacy: unauthorized parties cannot decipher the content of the data.
- Authentication: the receiver is certain of the identity of the sender.
- Data integrity: unauthorized parties cannot modify or corrupt the data.
- 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 and 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 Web site for information on software packages to implement the PGP or OpenPGP security application. Both OpenPGP and PGP use 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 (e.g., courier mail) to the company's trading partners.

You must use the utmost care in protecting your private key. If 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.

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 ~~WGQ~~ ~~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 ~~REQ~~ encryption standards but does not conflict with PGP.)

Encryption and signatures can be accomplished manually for each file using the online PGP or, on a mutually-agreed-upon 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-agreed-upon basis, to the HTTP Response by the Receiver of the package.

Decryption / Signature Verification

After a package is received and processed by the Receiving program, it is ready to be decrypted and have its signature verified. Given the correct userID for a trading partner, PGP and OpenPGP software use the appropriate key pair to encrypt, sign and decrypt. Upon request for signature verification, the PGP and OpenPGP software will return a human-readable descriptive text.

NAESB ~~It is~~ recommends ~~recommended that all implementers that each party~~ create~~e~~ a process where the descriptive text is used to look up the ID of the trading partner in a database table. If the ID is passed along with the decrypted file, a process could be created to verify that the trading partner which sent the transaction corresponds to the trading partner identified within the file, once the data has been translated.

When digital signatures are applied, on a mutually-agreed-upon 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. Companies anticipating large volumes of Internet ET traffic should research state-of-the-art techniques for scalability, including but not limited to:

- separating decryption and signature verification processing from web server receiving and processing~~;~~
- passing secured or to-be-secured packages to a separate computer for security processing
- optimizing CPU and memory on security processing computers
- real-time or near real-time monitoring of website performance

Implementers of Internet ET 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 TPA must identify the userid and password for this security as well as procedures for changing the password, if applicable. (OPEN ISSUE 008 ~~and OPEN ISSUE 012~~)

PGP or OpenPGP File Encryption

Payload files are encrypted using PGP 6.5 or greater (using keys generated with the RSA algorithm); or on a mutually-agreed-upon basis the OpenPGP standard, specified in IETF RFC 2440. There are freely available software implementations of the OpenPGP standard available at http://www.gnupg.org/.

??~~General Security Recommendations~~Other Security Recommendations

~~Firewall~~

A firewall should be deployed to protect your HTTP servers.

~~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.~~

CLIENT AND SERVER SPECIFICATIONS

- Synchronization – ??waiting on recommendations. Each Client and Server should be synchronized to a clock in the network of atomic clocks that is accessible via the Internet. The Client and Server should be synchronized as many times per day as necessary to ensure synchronization with an atomic clock +/- ?? seconds. Please refer to Appendix A, "Time Synchronization" ??check this appendix?? for references on public sites for synchronization.
- HTTP Servers should be configured to use one of the allowable TCP ports listed in Appendix E (OPEN ISSUE 009).
- 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. Criteria for selecting an outsourced Internet ET service provider should consider their ability and experience with Internet ET standards for HTTP Request and Response validation and processing.

SENDING ERROR NOTIFICATIONS

Error Notification

When a Client sends an Internet ET package to a Server, the Server responds with a receipt. Further back-office processing (e.g. decryption) may be required, and additional errors may be found.

Error Notification transactions are used to communicate transport errors found by the Receiver after the initial receipt is sent to the Sender.

Errors from translation and other back-office processing are outside the scope of the Internet ET.

When a file passes the decryption step, no error notification is sent back to the Client. If the decryption step fails, an error notification must be sent to the Client.

The Error Notification format applies to the posting of an error message after the Sender's session has been disconnected. This error notification is used only if the original HTTP Response is returned with an "ok" or a warning (??WEDM999 format) for the request-status value.

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

Required Error Notification Data Elements

The data elements for the error notification are the same as those described in the 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 ~~(OPEN ISSUE 001)~~
to	Common Code Identifier of receiving/server company, the client company which sent the data set in error ~~(OPEN ISSUE 001)~~
input-format	"error"
input-data	A text block containing the following applicable 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 the receiving process such as decryption; see Table A, "Internet EDM Standard Error Codes and Messages". comments — Any comments the original receiving server wishes to include. FOR RGQ AND REQ ONLY: resp-time-c-qualifier — The "time-c-qualifier" value from the original response.

~~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.
- An error notification contains two body parts nested within a multipart/report outer envelope with the content-type of "gisb-error-notification". (OPEN ISSUE 014)
- The first body part contains human readable content in HTML. The second body part contains machine readable content in plain text. Additionally, consenting trading partners can mutually agree to digitally sign error notifications.
- If digital signatures are used, the multipart/report containing the Error Notification is used to create a digital signature body part, identified by a "content-type" of application/pgp-signature. Both the multipart/report Error Notification and application/pgp-encrypted digital signature body parts are combined in a multipart/signed envelope.

EXAMPLE: ERROR NOTIFICATION INTERNET ET PACKAGE:

```
POST /cgi-bin/AS2dispatcher HTTP/1.1
Referer: http://www.acmeenergy/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"

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

123456789
------------------------------87453838942833
content-disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt   (OPEN ISSUE 002)
------------------------------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"  (OPEN ISSUE 014)

--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*  (OPEN ISSUE 010)
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*  (OPEN ISSUE 010)
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*
```

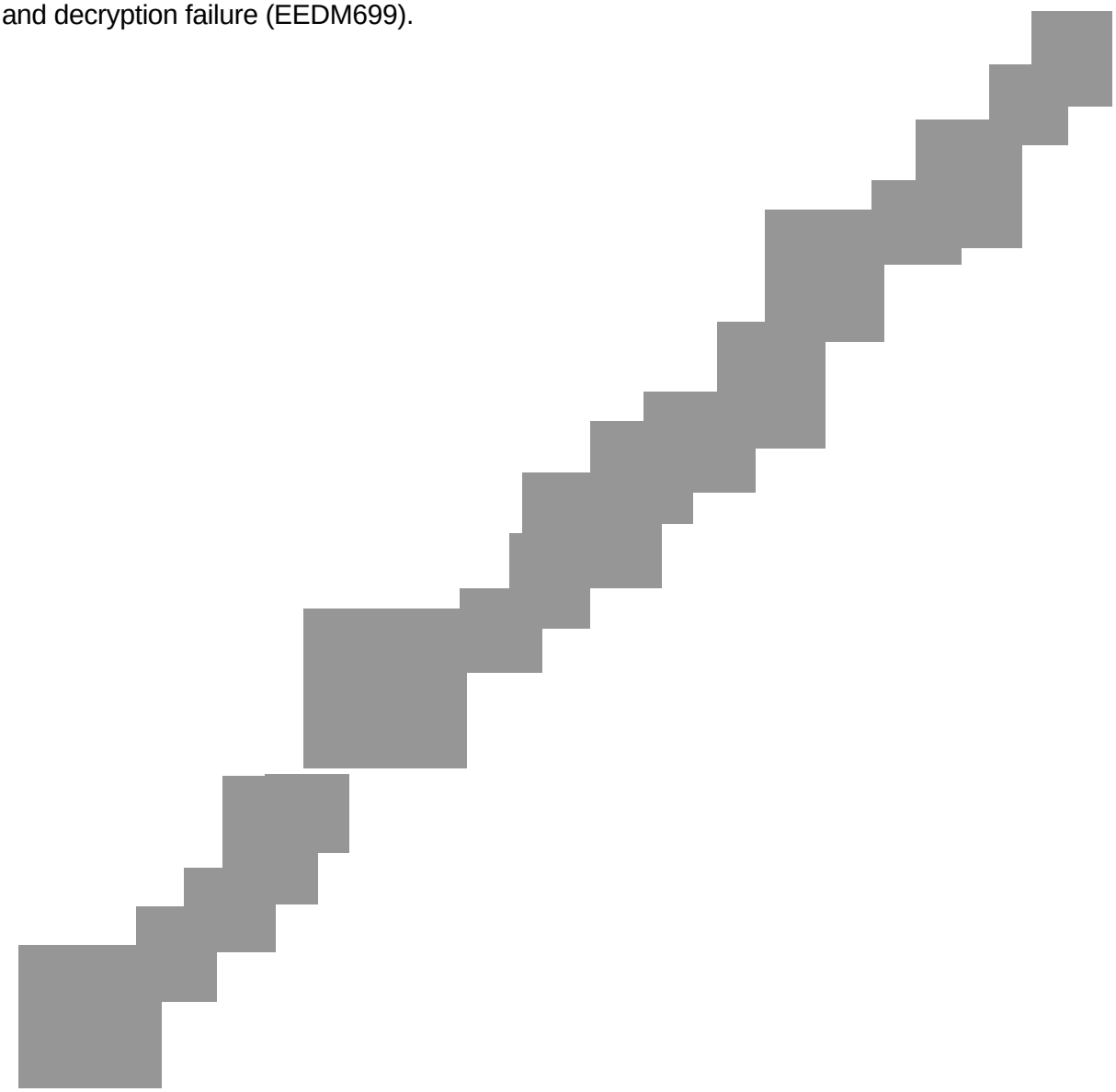
```
--GISB7868--
------------------------------87453838942833—

Signed Error Notification

content-type:multipart/signed; micalg=pgp-md5; protocol="application/pgp-signature";
boundary=--boundary2--200309090001

----boundary2--200309090001

content-type: multipart/report; report-type="gisb-error-notification"; boundary="GISB7868"  (OPEN ISSUE 014)

--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*  (OPEN ISSUE 010)
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*  (OPEN ISSUE 010)
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--
----boundary2--200309090001

content-type: application/pgp-signature
-----BEGIN PGP MESSAGE-----

Version: 6.5

iQCVAwUBMJrRF2N9oWBghPDJAQE9UQQAtl7LuRVndBjrk4EqYBIb3h5QXIX/LC//JV5bNvkZIGPIcEmI5iFd9boEgvpirHt
IREEqLQRkYNoBActFBZmh9GC3C041WGquMbrbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/W72vgSxLhe/zhdfolT9BrnH
OxEa44b+EI=
=ndaj

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

----boundary2--200309090001--
```

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).



7 - TESTING

NAESB ELECTRONIC TRANSPORT (ET) TEST PLAN

Implementation of Internet ET requires testing to assure all parties are prepared to operate according to the Internet ET. This document focuses on testing standards for establishing Electronic Transport (ET) connectivity with a trading partner. Testing for transaction and other quadrant-specific testing standards can be found in each quadrant's QEDM.

ET Connectivity testing standards include:

- Connectivity test scripts – These scripts define the steps needed to adequately test connectivity.
- Testing Connectivity Worksheet – This worksheet defines key operations parameters for a trading partner. The parameters include ET URL's, contacts and other information.
- Testing Signoff Worksheet – This worksheet defines critical operations environment characteristics of the trading partner. The characteristics include testing environments.

GENERAL TESTING ASSUMPTIONS

The following assumptions apply to ET testing:

- This Test Plan covers ET testing. Transactions and business process test plans can be found in the QEDM.
- Testing may uncover problems. Problems found during testing should be expected.
- This Test Plan is a basic demonstration of competency, and may not uncover all problems that may eventually require correction.
- The primary goals of this test are to establish connectivity including encryption, to test transfer of a large file, and to exercise the exchange failure process.
- This Test Plan assumes that automated processes will be used when testing. Any solutions that involve manual interaction or data manipulation are documented in advance in the Testing Signoff Worksheet, and are communicated to testing partners at the beginning of the testing cycle.
- Testing is done on dedicated test systems. Production systems should not be used for testing.
- ET connectivity testing should last no longer than two weeks once begun.

TESTING GOALS

The specific testing goals of this ET Test Plan are:

- Establish ET connectivity between CRs and TDSPs, including Internet connections and encryption compatibility.
- Validate that normal production transaction files can be sent.
- Validate that ET timestamps are being delivered.
- Validate that protocol failures are handled properly.
- Validate that exchange failures are handled properly.
- Validate that encryption/decryption and digital signature failures are handled properly.

TEST EXECUTION

Scripts and Frames

The Test Scripts defined in this document detail each step of the testing process for Connectivity. There may be several test scripts for a defined business process scenario. For example, a number of scenarios are tested for both positive (accept) and negative (reject) results.

Each Test Script involves an exchange (Request and Response) of data between trading partners. Each step in the process is referred to as a 'Frame'.

Testing Scripts

Each TP will confirm receipt of test file exchange via normal ET standards and via e-mail.

- Each TP should confirm that received files were not corrupted.
- Each TP shall exercise fail-over mechanisms by simulating a protocol failure and an exchange failure, triggering the appropriate notices to the identified Market Participant contacts.
- Each TP shall exercise encryption failure processes by simulate an encryption/decryption failure, triggering the appropriate notices to the identified Market Participant contacts.
- Each TP shall send a formal notice of successful certification completion to their TP

[??more detailed scripts?]

Recommended Internal Tests

In addition to tests executed with trading partners, the following tests are recommended as internal tests of ET systems.

- Stress Test – Ability to send and receive large production files (e.g. 10MB minimum uncompressed).
- Fail-over test – Test any processes triggered by a protocol or exchange failure by your

trading partner.

Testing Responsibilities

The 'Testing Responsibilities' section details the responsibilities each party has in the testing process. This Test Plan is focused on testing connectivity. Each party has certain obligations prior to, during and after testing.

Prior to Testing

- Parties should provide daily and emergency contact information for the test lead, and the test lead alternate.
- Complete applications for certification, licensing, etc. required for the target marketplace.
- Implement a dedicated test system.
- Provide TSW and TCW to target trading partner.

During Testing

- Participate in scheduled testing conference calls with your trading partners.
- Adhere to the established test schedule.
- Execute test frames as defined.

After Testing

- Communicate formally success or failure of testing with trading partner.

CHECKLIST OF TESTING STEPS (OPEN ISSUE 015)

[??from original EDM??]

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.

- Install an interactive browser. Identify an existing Web server from among NAESB WGQ compliant servers offering interactive upload for test. See the NAESB WGQ 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 WGQ standard format to

accomplish this step in testing.

- 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.
- Add Realm One security to your file transfer, and change the URL to the secure URL. Continue transfer tests with your batch browser.
- 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.

Server and CGI

- 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.
- 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.
- Acquire or develop a CGI program to receive file transfers and process according to NAESB WGQ standards. Test transfers to your CGI using your batch browser.
- Transfer a X12 or other NAESB WGQ standard format dataset to your server and process it through your translator or other appropriate processes.
- 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.
- 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.
- Once your site security is established, contact a trading partner to test transfers against your server.
- Test with various file sizes to ensure that your CGI can process small and large files.
- 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.
- Test application with various simulated errors in both file transfers and in PGP or OpenPGP decryption.

~~TAB~~ 8 – TABLES

TABLE A – INTERNET ET STANDARD ERROR CODES AND MESSAGES

These errors and warnings are strictly related to problems found in the Receiving program 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 Receiving program or decryption. Numbering schemes and descriptions should aid in this distinction.

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 ET Standard Error Codes and Messages

Validation Code	Description	Data Element	Data Element Required or. 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 (OPEN ISSUE 016)	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	Data Element Required or. 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	file itself	required - security
EEDM699	Decryption Error		required for general decryption errors not specifically identified by PGP or OpenPGP messages or exit codes
EEDM701 (OPEN ISSUE 017)	EDM party not associated with EDI party		required
EEDM702 (OPEN ISSUE 017)	Data Structure Error		required if the translator does not handle this exception
EEDM703 (OPEN ISSUE 017)	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

TABLE B – FREQUENTLY ASKED QUESTIONS

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

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

Q: NAESB EDM / AS2 Compatibility. What is the status of NAESB compatibility with AS2?

A:

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

A: As often as necessary to ensure synchronization to within +/- ?? seconds of the atomic clock.

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

A: 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 without operator intervention.

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

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

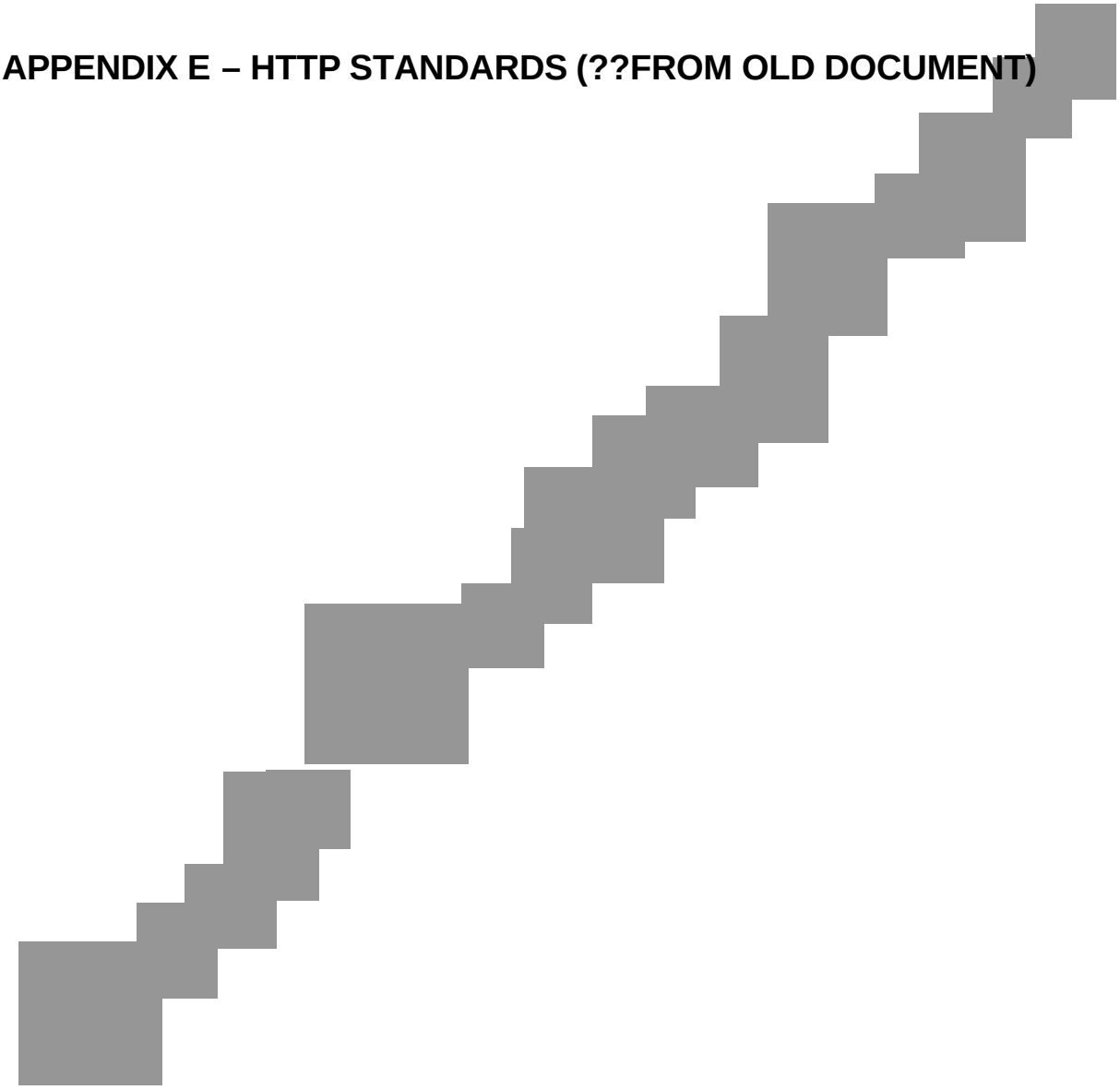
TABLE C – GLOSSARY OF INTERNET ELECTRONIC TRANSPORT TERMS

The following terms and conventions are used throughout this document.

Term	Definition or Convention
Batch Browser	A Browser that can be run with little or no manual operation or intervention. See "Browser"
Browser	A software program capable of generating HTTP Requests, including HTTP POST requests.
Client	The computer hardware and software used by the Sender to transmit an Electronic Package to the Receiver's Server. A Client can be fully-automated or manual.
COTS	Commercial Off-The-Shelf; software that can be purchased that requires little or no customization.
Electronic Package	A data stream sent via HTTP POST that contains header information and Payload File(s). The Payload Files are encrypted using defined Internet ET encryption techniques.
Error Notification	Errors that are trapped after the IET receipt is sent are communicated via an Error Notification package from the Receiver of the original data to the Sender.
HTTP Request	The stream of data sent from the Client to the Server that includes header information and payload data.
HTTP Response	The stream of data sent from the Server to the Client in response to an HTTP Request.
HTTP Server	A computer capable of receiving HTTP Requests and responding with HTTP Responses.
IETF	Internet Engineering Task Force; a body of technical experts that set standards, known as Requests for Comments (RFC) for the Internet.
Interactive Browser	A Browser that requires manual operation or intervention. See "Browser".
Internet EDM	The GISB and NAESB WGQ standards up to and including Version 1.7. The "Internet ET" and "QEDM" standards were derived from these EDM standards.
Internet Electronic Transport, ET	The NAESB standards for the secure transport of electronic information between trading partners.
Package	See "Electronic Package."
Payload Files	The data contents inside of an electronic package. NAESB Internet ET does not care what the contents of ET Electronic Packages contain.
QEDM	Quadrant-specific Electronic Delivery Mechanism; the set of standards for each NAESB quadrant that define the business policies, practices and processes for that quadrant. The QEDM excludes electronic transport practices and standards. The QEDMs were derived from the Internet EDM from GISB and NAESB WGQ.
Quadrant-Specific Electronic Delivery Mechanism	See "QEDM".
Receipt	The HTTP Response sent from the Receiver to the Sender that includes a timestamp and OK/error status.
Receiver	The party that receives an electronic package.
Secure Electronic Package	See "Electronic Package"

~~Term~~	~~Definition or Convention~~
~~Sender~~	~~The party that sends an Electronic Package.~~
~~Server~~	~~The computer hardware and software used by the Receiver to receive an Electronic Package from the Sender's Client. The Server is an HTTP/Web Server.~~
~~Web Browser~~	~~See "Browser"~~
~~Web Server~~	~~See "HTTP Server".~~

APPENDIX E – HTTP STANDARDS (??FROM OLD DOCUMENT)



Tab 4 Change Notes: [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" or "NAESB REQ"
[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

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

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 format	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
HTTP Response, Request		Capitalized all references to HTTP Response, Request
“—8760”	Changed all “—8760” boundary values to generic boundary value