EDI Transaction Electronic Delivery Mechanism

Prepared by Mary Do, NAESB Executive Committee

Current Situation

- Current Standard is GISB version 1.4. This standard has been deprecated in August 2001. The GISB v1.4 underlying components have been hacked and the customer data is susceptible to “man-in-the-middle” attacks, along with several other vulnerabilities.

- NY EDI Standards reference using NAESB version 1.6. This standard was deprecated in December 2003.

- The Wholesale Natural Gas Industry uses the same Electronic Delivery Mechanism, referenced as “WGQ/RMQ Internet Electronic Transport” , and are currently on version 2.0 with movement to version 3.0. Their are no differences between version 2.0 and 3.0 in the WGQ/RMQ Internet Electronic Transport standard.

- The JU attestation states “All Confidential Utility Information is encrypted in transit utilizing industry best practice encryption methods.”

GISB/NAESB Version Progression

- V1.6 Added SSL
- V1.7 No change
- V1.8 Digital Signature of Response on EDM – Mutually Agreed
- V1.9 Digital Signature of Response on EDM – Mandatory
- V2.0 No Change
- V3.0 No Change

What are Best Practices?

- Most retail electric markets use NAESB version 1.6, even though it has been retired since 2003 on the wholesale natural gas segment.

- With recent cyber attacks, ERCOT (Texas) is considering moving to current standard version 2.0 in 2019.

- Version 2.0 requires a digital signature for the receiver response and Version 1.6 does not.

- Version 2.0 requires a few more header elements than 1.6

- Encryption key size should move from 1024 to 2048 or 4096. Every market participate needs to do this to avoid compatibility issues.

- PGP Version 6.5 or greater

- GPG Version 2.8 or greater

- Basic Authentication (username/password)different from test and production.

PAIN

Data **P**rivacy
Authentication
Data **I**ntegrity
Non-repudiation

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.

Data **P**rivacy 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:

OpenPGP, defined by (IETF RFC 2440) with modifications described in this specification

OR

PGP 2.6 (minimum) or higher (strongly encouraged), with RSA keys can be used on a mutually agreed basis

Internet ET uses base64-encoding and 128-bit SSL to protect username and password.

Authentication

Authentication is the assurance to one entity that another entity is who he/she/it claims to be. Basic authentication is the required standard to prevent intruders from connecting to Internet ET Web sites. Internet ET uses 128-bit SSL-protected usernames and passwords to establish authentication. Optional techniques such as firewall security enable further authentication.

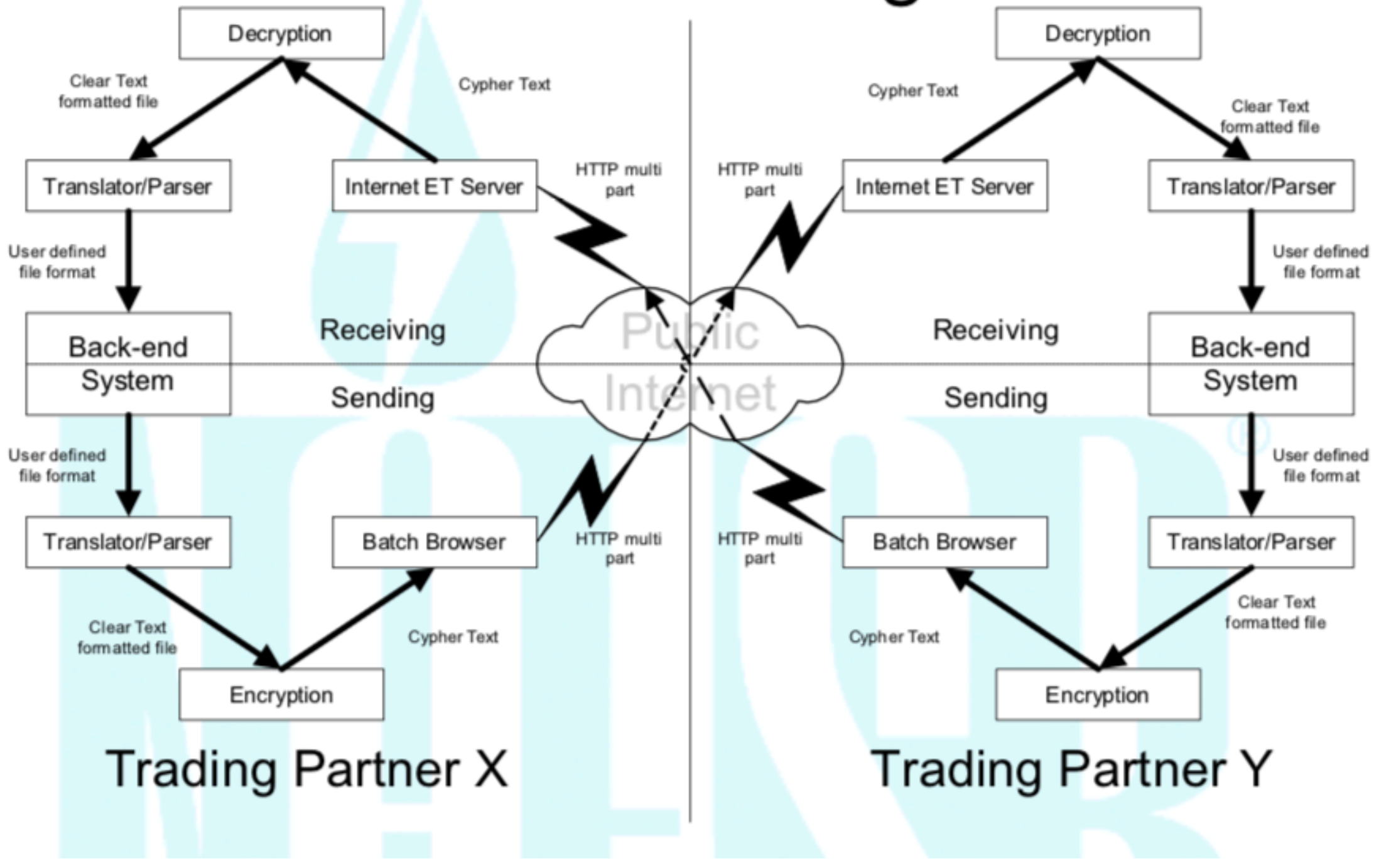
Integrity

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 OpenPGP/PGP 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 will include 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.

Batch Flow Diagram



Upgrade to V1.6 or V2.0?

- Does NY want to join the other states at V1.6
- Does NY want to lead the other states to V2.0
- What does the “Best Practices” attestation require

NAESB

- NAESB is a member driven standards organization

- NAESB has a copyright on all Internet Electronic Transport versions.

- All users of the version 1.4 or version 1.6, or version 2.0 must purchase the standard for $250, if they are not a NAESB member.