



Internet EDI Plan

Version 2.0

Pennsylvania Electronic Data Exchange
Working Group (EDEWG)

February, 2006

1 – EXECUTIVE SUMMARY

This document presents pertinent technical standards and a migration plan for the Pennsylvania Electronic Data Exchange Working Group [‘EDEWG’] Internet Electronic Transport [‘ET’], the Internet-based electronic transport of electronic data interchange [‘EDI’] in support of the Pennsylvania retail electric marketplace.

In 2005 the Pennsylvania Public Utility Commission [‘PA PUC’] ordered the migration from Gas Industry Standards Board [‘GISB’] Electronic Delivery Mechanism [‘EDM’] Version 1.4 to North American Energy Standards Board [‘NAESB’] Internet ET, and directed EDEWG to develop a transition plan and a schedule for testing and implementation. This document comprises EDEWG’s response and replaces the EDEWG Internet EDI Plan Version 1.3.

This document should be used as a supplement to the business practices as ratified by NAESB for electronic delivery of data, and should be used in conjunction with the “PA-NJ-DE-MD Implementation Guidelines for EDI” and the “EDEWG Revised Plan”.

2 – VERSION HISTORY

Date/Version

Nov 30, 2008

Feb 26, 2006

Version 2.0

June 8, 2005

July 23, 2001

Version 1.2

October 12th, 2000

Version 1.1

May 18th, 2000

Version 1.0

Summary of Changes

- Made support of DSS keys mutual by both parties.
- Revised to reflect PA PUC Order at Docket M-00960890, F0015 entered May 19, 2005, made effective by Order entered October 5, 2005, including:
 - Elimination of all VAN and AS2 references
 - Change from GISB 1.4 to NAESB Internet ET and compatible standards
 - Addition of OpenPGP
 - Reformat to mirror NAESB documents
 - Removed Appendix B
- As directed by the May 19, 2005 PA PUC Order M-00960890 F0015, Removed Paragraph 3 from the High-level Summary of PA PUC EDEWG Internet EDI Orders section on page 2.
- As recommended by the May 12, 2004 IET Report, Removed Paragraph 2 and 22 from the Additional EDEWG Assumptions section on pages 3 and 5.
- Updated all former “puc.paonline.com” links to the current PA PUC link.
- Updated PA PUC contact email address from the Testing Process section on page 7.
- Updated NAESB link in the EDEWG Internet EDI Test Plan on page 8.
- In Appendix B, moved link from <http://choice.imark-it.com/1dot4.htm> to http://puc.paonline.com/electric/data_exchange.asp
- Added assumption regarding expectations for support of exchange failures
- Change ‘Summary of PA PUC Orders’ to reflect 7/13/2000 PA PUC orders
- Added wording to further detail the risks associated with Bill Ready billing and the Internet
- Version 1.0 finalized on EDEWG teleconference
- Removed ‘Final Draft’ Indicator

- Inserted page numbers
- Inserted this Document History section

3 – INTRODUCTION

In 2005 the PA PUC ordered that EDI transactions exchanged after 1/1/2007 must be transported using NAESB Internet ET or a compatible standard. The PA PUC Order can be found by clicking on “EDI over the Internet” at the URL below. Previous EDEWG Internet EDI documents are also maintained here:

http://www.puc.state.pa.us/electric/electric_electronic_data_exchange.aspx

After 1/1/2007, EDEWG transactions must be transported using NAESB Internet ET or a compatible standard. Internet Engineering Task Force [‘IETF’] EDI Internet [‘EDIINT’] standards (e.g. AS1/AS2/AS3) and older versions of GISB/NAESB electronic delivery mechanisms [‘EDM’] (version 1.5 and prior versions) are excluded as compatible standards.

EDEWG recognizes the similarity of NAESB WGQ EDM versions 1.6 and higher with the NAESB Internet ET standard and has adopted practices to maximize compatibility, outlined in Section 6 “Technical Implementation”.

The test plan outlined in this document is meant as a supplement to the testing and certification process that is required to participate in the marketplace.

The Migration Plan in Appendix A details the 2006 cutover from EDEWG Internet EDI Plan v1.3 (based on GISB 1.4) to EDEWG Internet EDI Plan v2.0 (based on NAESB Internet ET).

Table of Contents:

1 – Executive Summary	2
2 – Version History	2
3 – Introduction	3
4 – Business Processes and Practices	4
4.1 – Principles	4
4.2 – Definitions	4
4.3 – Standards and Practices	5
5 – Related Standards	6
6 – Technical Implementation	7
7 – Test Plan	7
Appendices	11
Appendix A – 2006 V2.0 Migration Plan	11

- Deleted: 3
- Deleted: 2
- Deleted: 4
- Deleted: 2
- Deleted: 4
- Deleted: 2
- Deleted: 4
- Deleted: 2
- Deleted: 5
- Deleted: 2
- Deleted: 6
- Deleted: 2
- Deleted: 7
- Deleted: 2
- Deleted: 7
- Deleted: 2
- Deleted: 11
- Deleted: 2
- Deleted: 11
- Deleted: 2

4 – BUSINESS PROCESSES AND PRACTICES

4.1 – Principles

No principles are defined.

4.2 – Definitions

- 4.2.1 'Bill-Ready Consolidated Billing'. A process in electric and gas markets that requires a timely exchange of business transactions between EGS and EDC to achieve a consolidated bill sent to the customer.
- 4.2.2 'EDC'. Pennsylvania jurisdictional Electric Distribution Companies.
- 4.2.3 'EDM'. 'Electronic Delivery Mechanism', the name GISB and NAESB WGQ used on EDM versions 1.7 and prior. Generally, EDM refers to a broader set of standards used by the wholesale gas industry, rather than the Internet transport standards used in many electric markets.
- 4.2.4 'EDEWG'. The Pennsylvania stakeholder group "Electronic Data Exchange Working Group" comprised of Electric Generation Suppliers, energy service providers and Pennsylvania jurisdictional Electric Distribution Companies.
- 4.2.5 'EGS'. Pennsylvania jurisdictional Electric Generation Suppliers. By definition, EGS also includes brokers, marketers and third-party service providers.
- 4.2.6 'Exchange failure'. An exchange failure occurs when a sending party's NAESB server has had continual protocol failures over a two-hour period. The NAESB Internet ET 'exchange failure' standard requires that you attempt to send a package at least three times over a 30- to 120-minute period. At minimum, this means 30 minutes has elapsed between your first protocol failure and your third protocol failure. At maximum, 120 minutes has elapsed between your first failed attempt and your third failed attempt. For example, if you make your first attempt at time 00:00:00, and your third attempt at time 00:30:00, your second attempt can occur any time between the first and third. If the third attempt fails, you have an 'exchange failure' and should notify your trading partner.
- 4.2.7 'GPG'. GnuPG, the open-source, free implementation of the OpenPGP standard.
- 4.2.8 'NAESB'. North American Energy Standards Board. See <http://www.naesb.org>.
- 4.2.9 'NAESB Internet ET'. The name of the NAESB standard that replaces the WGQ EDM for retail marketplaces.
- 4.2.10 'OpenPGP'. An IETF open standard for PGP encryption. See RFC 2440 and <http://www.openpgp.org>.
- 4.2.11 'Package'. The name for the electronic stream of information that includes the NAESB HTTPS transport header and the encrypted Payload.
- 4.2.12 'Payload'. The confidential content that is being sent over the Internet using Internet ET. EDEWG content sent using these standards consists only of EDI X12-formatted transaction files.

- 4.2.13 'PGP'. A proprietary software product from Network Associates for PGP encryption. See <http://www.pgp.com>.
- 4.2.14 'Protocol failure'. A protocol failure occurs when a sending party's NAESB server cannot connect to the receiving party's NAESB server. For example, if a server tries to connect to a server and fails, or tries to post a file and fails, this is a protocol failure.
- 4.2.15 'WGQ'. 'Wholesale Gas Quadrant', the name of the quadrant of NAESB that was the original GISB group that developed the GISB EDM, including versions 1.5 and prior.
- 4.2.16 'X12'. An ANSI international standard for EDI transactions.

4.3 – Standards and Practices

- 4.3.1 Parties will send transactions according to timelines identified in Section 3L of the EDEWG Revised Plan. An internal failure of the EDEWG Internet ET solution (e.g. an FTP from the mainframe to the NAESB server fails) does not change this requirement.
- 4.3.2 Parties should resolve EDEWG Internet ET problems directly with their trading partners. Disputes - where two trading partners cannot agree on who is responsible for the problem and/or how to fix the problem - that cannot be resolved by trading partners should be escalated to the PA PUC.
- 4.3.3 Parties will treat all EDEWG data Payloads as confidential, and will encrypt those Payloads when sent across the Internet. Receipt of un-encrypted 'clear-text' Payloads should be treated as an exchange failure that needs to be fixed. CLEAR-TEXT EXCHANGE FAILURES SHOULD NOT BE IGNORED!
- 4.3.4 Parties using Bill-Ready Consolidated Billing need to understand the risks associated with EDEWG Internet ET failures and should plan appropriately.
- 4.3.5 Parties should not consider continued exchange failures normal business practice.
- 4.3.6 Parties will respond to exchange failures during regular business hours.
- 4.3.7 Parties will retain copies of X12-compliant transactions, as required by the EDEWG Revised Plan.
- 4.3.8 Parties should maintain at least one production URL and one test URL.
- 4.3.9 Parties will send X12 997 functional acknowledgements. The NAESB response only indicates that a file was received at a specified time. It does not verify that a valid, readable (content and structure) X12 file was received, as does the 997. The NAESB response and the 997 serve two separate purposes, and both are required.
- 4.3.10 Parties will use Eastern Prevailing Time 'EPT' (Eastern Standard Time 'EST' using Daylight Saving Time 'DST') as the default time zone for EDEWG transactions.
- 4.3.11 Parties can send transactions encrypted using either PGP 6.5 or higher, or OpenPGP. Both parties do not require the same version, as newer versions provide backward-compatibility. If using OpenPGP, parties will use specific settings in OpenPGP as outlined in Section 6 "Technical Implementation". The RSA algorithm and 1024-bit public keys are required.
- 4.3.12 Parties should give a 30-day notice to trading partners when changing keys.

- 4.3.13 Parties will communicate EDEWG Internet ET server maintenance schedules to their trading partners.
- 4.3.14 E-Mail will be used to notify trading partners of exchange failures.

5 – RELATED STANDARDS

5.1 – EDEWG Retail Choice Standards

The EDEWG Internet ET standards define transportation and delivery standards for the transactions used in the retail electric marketplace defined by EDEWG standards. A complete list of EDEWG-related documentation can be found here:

http://www.puc.state.pa.us/electric/electric_edewg_download.aspx

5.2 – NAESB Standards

EDEWG Internet ET standards are built on the NAESB Internet ET and WGQ EDM standards. NAESB standards define standards for wholesale and retail electric and natural gas markets. The NAESB Internet ET, WGQ EDM V1.6, and WGQ EDM V1.7 specifications can be obtained at the NAESB website (members only):

<http://www.naesb.org>

When this document refers to “maximizing compatibility”, it refers to EDEWG efforts to maximize compatibility between the NAESB Internet ET standards and the NAESB WGQ EDM v1.6 and later of the NAESB standards. There IS NO COMPATIBILITY with GISB EDM v1.5 and prior standards.

5.3 – Encryption Standards and Products

EDEWG Internet ET relies on PGP and OpenPGP standards encryption:

<http://www.openpgp.org>

<http://www.pgp.com>

The ERCOT marketplace has compiled a GPG PGP User Guide that outlines PGP and GnuPG/OpenPGP implementation in NAESB environments. Contact the PA PUC or ERCOT for a copy.

http://www.ercot.com/Participants/Committees/Documents/TDTWG_KeyDocs/EncryptionGuide.doc

5.4 – PA PUC Gas Marketplace Standards

PECO, PPL, UGI retail marketplaces for natural gas currently use GISB 1.4. The PUC order does not apply to these markets.

PECO

PECO will upgrade both gas and electric to the NAESB Internet ET protocol.

PPL

PPL is not currently in production with retail gas suppliers using GISB. When/if this production begins, PPL will evaluate the EDI transport requirements in use at that time and define PPL's position with respect to the GISB/NAESB protocol to be employed for retail gas operations.

UGI

UGI will continue to use the GISB 1.4 protocol for gas partners while the NAESB 1.6 protocol will be used for electric partners.

6 – TECHNICAL IMPLEMENTATION

Technical implementation of EDEWG Internet ET is as defined in the NAESB Internet ET standard with the following conventions and practices:

- 6.1.1 Parties will NOT USE the optional 'time-c-qualifier' header data element to maximize backwards compatibility. EDEWG Internet ET packages will have a default time zone of Eastern Prevailing Time (Eastern Standard Time using Daylight Savings Time).
- 6.1.2 Parties will only use the 'input-format' data dictionary element equal to 'X12' to maximize backwards compatibility.
- 6.1.3 Parties will not require signed receipts. Parties are free to implement signed receipts on a mutually-agreed-upon basis.
- 6.1.4 Parties will use DUNS/DUNS+4 codes for the 'to' and 'from' NAESB Internet ET Common Code ID data dictionary elements. These values should match the values used within EDEWG EDI transactions, or notify trading partners when Common Code values do not match EDI codes.
- 6.1.5 Parties will NOT USE the optional 'refnum-orig' header data element to maximize backwards compatibility.
- 6.1.6 Parties will use ~~the RSA key generation algorithm with 1024 bit encryption to maximize compatibility with OpenPGP. Parties may, by mutual agreement, use alternative keys or encryption (DSS, DSA, higher encryption, etc).~~

Deleted: agree that they

Deleted: RSA keys or DH/DSS keys with cipher other than IDEA

7 – TEST PLAN

The EDEWG Internet ET test plan is designed to complement the EDEWG Certification process. Prior to sending any transactions for certification, EDEWG Internet ET testing assures that electronic transactions can be delivered to trading partners.

7.1 – Testing Assumptions

- 7.1.1 THIS TEST PLAN DOES NOT REPLACE THE FULL CERTIFICATION TEST THAT MUST BE CONDUCTED TO TEST THE BUSINESS PROCESSES BEHIND THE TRANSACTION EXCHANGE.
- 7.1.2 Parties will complete internal tests of their EDEWG Internet ET systems, including a stress test of large files (1MB or bigger).
- 7.1.3 Parties will provide feedback to trading partners during testing.
- 7.1.4 Each EDC can group EGS trading partners into test flights or batches to help facilitate testing of large volumes of EGS trading partners.
- 7.1.5 Each EDC will communicate to EGS trading partners their EDEWG Internet ET test plan, any trading partner agreements, and testing flight dates.

- 7.1.6 Parties will provide a contact and an SMTP address to which manual and automated exchange failure messages are sent.
- 7.1.7 Each EGS will maintain the pace of the test flight as published by each EDC.
- 7.1.8 Parties may make exceptions or additions to test plan scripts, however they should be mutually-agreed with their trading partners.
- 7.1.9 Each EDC will add EDEWG Internet ET items to their Frequently Answered Questions, including URL's, protocol and exchange failure processes and contacts.

7.2 – Testing Goals

- 7.2.1 Establish EDEWG Internet ET connectivity between trading partners, including HTTPS connections and encryption compatibility.
- 7.2.2 Validate that normal production EDI files can be sent.
- 7.2.3 Validate that X12-compliant transaction data Payloads are being delivered after decryption.
- 7.2.4 Validate that the HTTPS gisb-acknowledgement and the X12-compliant 997 functional acknowledgements are being delivered.
- 7.2.5 Validate that protocol failures are handled properly.
- 7.2.6 Validate that exchange failures are handled properly.
- 7.2.7 Validate that encryption/decryption failures are handled properly.

7.3 – Testing Process

- 7.3.1 The EDC will notify the EGS with the date they will begin testing.
- 7.3.2 The EDC will conduct a kickoff testing conference call. The kickoff should include identification by each party of what production exchanges will be captured and sent for testing.
- 7.3.3 Parties will send files to the other party through EDEWG Internet ET, and notify the testing contact of the trading party that the files were sent.
- 7.3.4 Parties should run received files through their translator to confirm that files were not corrupted.
- 7.3.5 Each trading partner should simulate an exchange failure and an encryption/decryption failure, triggering the appropriate automated and manual notices to the identified trading partner contacts. Parties should confirm receipt of the failure notifications.
- 7.3.6 Parties will send a formal notice via e-mail to their trading partner when EDEWG Internet ET capability is certified, with a copy being sent to the PA PUC at annmarino@state.pa.us.

7.4 – Sample Test Scripts

These sample test scripts are provided for your information and are not required.

Test Script Sample #1

1. Include certificate generation / set-up / expire / gen new / re-import / as part of testing.

2. Include password generation / set-up / expire / gen new / re-import / as part of testing.
3. Include testing of manually-initiated batch browser. This can help debug initial set-up and may be needed for exception processing.

Testing in following sequence makes debugging a lot easier:

1. Encrypt EDI message / decrypt / into translator, 997 back, Flat file inspected, return HTML message response encrypted
2. Sign & Encrypt same EDI message / Check signature / decrypt / into translator, 997 back, Flat file inspected, return HTML message response encrypted & Signed
3. Send 5 above with errors in the EDI file Make sure can recon 997 (not garbled) and check in bound HTML response manually
4. Test automated parsing of HTML response codes and notifications sent & application action taken
5. Inspect internal log files to make sure properly recording sequence of events and timestamps
6. Check timestamps and Transaction Id are what was expected
7. Queue multiple files at once to test for race conditions with timestamp granularity

Also test following negative test cases:

1. Bad URL destination
2. Bad User ID
3. Bad password
4. Wrong time-zone timestamp
5. Wrong encryption key
6. Bad signature
7. Expired certificate
8. Session timeout waiting for HTML response
9. Processing a negative HTML message response code

Test Script Sample #2

- 1 Successful transfer of outbound data from Host's translator to Host's NAESB server
 - 1.1 Back end system successfully places translated outbound X12 data in the outbound directory on the NAESB EDM system. Compare file in outbound directory to file sent from backend system to validate that they are the same.
- 2 Successful send of large production X12 file from the Host to the Trading Partner
 - 2.1 Valid X12 test file signed, encrypted, and sent to Trading Partner. Place the test file in the Host's outbound directory and send the file. Verify with Trading Partner that the file was received and correctly decrypted.
 - 2.2 Time-stamped response received from Trading Partner. Verify that the file was sent and the timestamp was received.
- 3 Successful receipt of upload from a Trading Partner to the Host's NAESB server
 - 3.1 X12 file received, decrypted, authenticated, and placed in inbound directory. Look in the Host's inbound directory and verify that the file was received and correctly decrypted.
 - 3.2 Trading Partner received timestamp with correct status information. Verify with Trading Partner that they received the timestamp.
- 4 Successful transfer of inbound data to backend system
 - 4.1 Backend successfully retrieves file
 - 4.2 Inbound file successfully run through translator

- 4.3 Backend system deletes file on NAESB EDM system after successful transfer
- 5 Successful delivery of NAESB standard error message to Trading Partner
 - 5.1 Trading Partner sends X12 file with wrong DUNS number in "to" field. Verify that a timestamp was sent indicating an error in the HTTPS header.
 - 5.2 Trading Partner sends X12 file encrypted with wrong key. Verify that a NAESB standard error file was sent. Contact Trading Partner and verify that they received the error file.
- 6 Proper processing of NAESB standard error messages received from Trading Partner
 - 6.1 Send file to Trading Partner indicating wrong DUNS number in the "to" field. Verify receipt of a timestamp indicating an error in the HTTPS header.
 - 6.2 Send file encrypted with wrong PGP key to Trading Partner. Encrypt a test file with a key other than the Trading Partner's public key. Send a test file using the bad key. After the test, make sure to replace the Trading Partner's key.
 - 6.3 Receive error file from Trading Partner indicating decryption failure. Verify that a NAESB standard error file was received.

APPENDICES

Appendix A – 2006 V2.0 Migration Plan

The EDEWG marketplace will migrate to the EDEWG Internet ET v2.0 environment between 7/1/2006 and 10/31/2006. This migration plan appendix focuses on execution of that migration.

A.1 – Version 2.0 Migration Plan Assumptions

- A.1.1 Each EGS that wants to remain EDI Certified must be ready to test EDEWG Internet ET v2.0 by 7/1/2006, and to implement EDEWG Internet ET v2.0 with each EDC trading partner by 10/31/2006.
- A.1.2 Each existing certified EGS that is inactive may be required by the EDC to do the full Certification test after the Internet ET test and prior to going live in the marketplace.
- A.1.3 Each new EGS that is not certified will be required by the EDC to do the full Certification test after the Internet ET test and prior to going live in the marketplace.
- A.1.4 Each EDC will post rules for new EGS entry and schedules for testing, including a two-month blackout period for cutover to the new version.
- A.1.5 Each EDC will notify their EGS trading partners if Trading Partner Agreements need to be changed and/or re-signed.

A.2 – Version 2.0 Migration Plan Milestones

Milestone	Date*
Initial V2.0 notifications sent to TP's	12/31/2005
Impact Analysis on Gas (PECO, UGI, PPL) completed	12/31/2005
EDC 2006 schedule published, if any	1/15/2006
EDC Testing Begin/End/Cutover Dates Set	1/15/2006
EDEWG EDM Subcommittee Meeting	1/18/2006
Publish report to EDEWG list	1/20/2006
EDEWG Internet EDI v2.0 Final Draft to EDEWG	2/2/2006
EDEWG Internet EDI v2.0 Published	3/31/2006
Testing Window Opens	7/1/2006
AP Testing Begins	8/1/2006
AP Testing Ends	10/1/2006
AP Testing Cutover	10/15/2006
Duquesne Testing Begins	7/1/2006
Duquesne Testing Ends	10/1/2006
Duquesne Testing Cutover	EGS by EGS after Successful Test
PECO Testing Begins	8/1/2006
PECO Testing Ends	9/1/2006
PECO Testing Cutover	10/1/2006
Penn Power / PennElec / MetEd Testing Begins	7/1/2006
Penn Power / PennElec / MetEd Testing Ends	10/31/2006
Penn Power / PennElec / MetEd Testing Cutover	11/30/2006
PPL Testing Begins	9/11/2006
PPL Testing Ends	10/31/2006
PPL Testing Cutover	EGS by EGS after Successful Test
UGI Testing Begins	7/1/2006
UGI Testing Ends	8/31/2006
UGI Testing Cutover	EGS by EGS after Successful Test
Testing Window Closes	10/31/2006
Compile Post-Implementation Debrief & Cost/Benefit Study	12/15/2006

*NOTE: An EDC is permitted to advance its stated implementation dates only if performed in a nondiscriminatory manner and if the EDC and its respective trading partners mutually agree.