NEW JERSEY RETAIL CHOICE
INTERNET EDI PLAN
FOR ELECTRIC AND GAS

Version 1.02

August 21, 2001

Executive Summary

This document defines the business processes and rules that will be followed by participants in the deregulated Electric and Gas marketplace in New Jersey with regard to the accepted transportation protocol when sending and receiving Electronic Data Interchange (EDI).

This document does NOT supercede any New Jersey Board of Public Utilities (BPU) orders or Utility settlements. Associated documents (Gas Test Plan, Electric Test Plan, Electronic Data Exchange and Protocol Process Flows for Gas Deregulation in the State of New Jersey, Electronic Data Exchange and Protocol Process Flows for Electric Deregulation in the State of New Jersey) will be updated after the BPU approves this document.

Migration plan from Value Added Network (VAN) to Internet EDI (Gas Industry Standards Board ("GISB") Electronic Delivery Mechanism (EDM)):

Electric

- PSE&G– Requires mandatory migration for EDI transport from VAN to GISB after Competitive Account Services (CAS) implementation and before Gas Certification testing.
- Conectiv – Plans to support optional use of GISB 3rd quarter 2001. Will require mandatory migration for EDI transport from VAN to GISB by the end of 1st quarter 2002.
- GPU Energy – has supported optional use of GISB since 3rd quarter 2000. Will require mandatory migration for EDI transport from VAN to GISB by the end of 1st quarter 2002.
- Rockland Electric – upon implementation of EDI, will require mandatory use of Internet EDI via GISB.

Gas

The *Electronic Data Exchange and Protocol Process Flows for Gas Deregulation in the State of New Jersey*, which the BPU approved by Order dated August 16, 2000, documents the data exchange method and business rules used by the various gas utilities. The rules contained in this document describe the transport protocol requirements when using EDI.

- PSE&G – upon implementation of EDI for Gas, will require mandatory use of Internet EDI via GISB.
- South Jersey Gas – Will require implementation of GISB Internet EDI in place of VANs and is prepared to support and implement GISB EDI in accordance with the current Natural Gas EDI Implementation Plan timetable of testing by January of 2002 and Implementation by March 15, 2002.
- New Jersey Natural Gas – Will require mandatory implementation of GISB in accordance with the current BPU stated Natural Gas EDI Implementation Plan timetable.

- Elizabethtown Gas – Will require mandatory implementation of EDI via the Internet using GISB in accordance with the current BPU stated Natural Gas EDI Implementation Plan timetable.

Document History

Date/Version	Summary of Changes
July 20, 2001 Version 1.0 Draft	Initial Draft version
July 27, 2001 Version 1.01 Draft	Incorporate changes suggested at state level meeting held on 7/26/01
August 21, 2001 Version 1.02	Incorporate Elizabethtown gas comment Added comments to section Internet Test Plan

New Jersey Assumptions

1. As used herein, "Utility" means a New Jersey electric or natural gas utility, "Supplier" means a New Jersey licensed electric or natural gas supplier, "party" means either a Utility or Supplier.
2. Where Utilities and Suppliers are sending EDI transactions to conduct Retail Choice business, the default and only acceptable transport protocol will become GISB. The implementation schedule will vary by Utility as defined in the Executive Summary.
3. Some Utilities will require trading partner agreements.
4. Utilities will notify current Suppliers of the availability of testing and the method to schedule testing.
5. All Utilities and Suppliers will complete internal tests of their Internet EDI systems, including the tests defined in Appendix A.
6. All Utilities are recommended to host daily teleconferences with the Suppliers in testing. At a minimum, feedback from the Utility to the supplier regarding testing feedback is required.
7. Internet EDI exchanges will follow rules for exchanging EDI data as defined in the sections of the GISB EDM Version 1.4 outlined in Appendix B, unless explicitly stated in this document.
8. Each Utility and Supplier is required to send transactions according to state defined timelines. A back office failure (e.g., an FTP from the mainframe to the GISB server fails) does not change this requirement.
9. All Utilities and Suppliers are encouraged to resolve Internet EDI problems with their trading partners. A dispute is a problem where the two trading partners cannot agree on who is responsible for the problem and/or how to fix the problem. Any unresolved disputes over Internet EDI performance will be presented to the BPU for resolution.

10. All EDI transactions are to be treated as confidential, and must be encrypted when sent across the Internet. Receipt of un-encrypted 'clear-text' transactions should be treated as an exchange failure that needs to be fixed. Clear-text exchange failures should not be ignored! See Appendix B.
11. Suppliers utilizing utility Consolidated Billing with Bill Ready utilities need to understand the risks associated with Exchange failures and should plan appropriately. The Utility will be responsible to extend the invoice due date in exchange failure situations that are the utility's responsibility that reduce the bill window to below the period required by the utility's applicable tariff or other document. This may be due to an EDI 867 transaction being sent late, or the unavailability of the system when an EDI 810 transaction is being returned.
12. Under Supplier Consolidated Billing, the supplier will be responsible to extend the invoice due date in exchange failure situations that are the supplier's responsibility that reduce the bill window to below the period required by the utility's applicable tariff or other document.
13. Continued exchange failures will not be considered normal business.
14. It is expected that parties are only required to respond to exchange failures during regular business hours.
15. Each party is required by New Jersey BPU approved EDI rules to retain copies of X12-compliant transactions.
16. Each party should maintain one production Uniform Resource Locator (URL) and one test URL, at a minimum.
17. Parties will continue to send EDI X12 997 functional acknowledgements. The GISB HTTP response only indicates that some file was received at a specified time. It does not verify that the file could be decrypted, and is a valid readable EDI X12 file with regard to content and structure, as does the 997. They serve two separate purposes, and both are used.
18. The same timestamp anchor as currently used for New Jersey Retail Choice EDI transactions will be used for GISB-based exchanges. (Eastern Prevailing Time: EST, utilizing Daylight Savings Time). See Appendix B.
19. GISB encryption
    - Depends on the Pretty Good Privacy (PGP) versions used by each trading partner being compatible. The recommendation is to use the most current version. However both parties do not require the same version, as newer versions provide backward-compatibility.
    - The GISB EDM requires the use of the RSA algorithm. See Appendix B.
    - GISB recommends use of 1024-bit public key. See Appendix B.
    - Public keys should be changed annually. Notice should be given to a trading partner when changing keys. It is recommended that regularly scheduled non-emergency public key changes should include a 30-day notice.

20. Security

- Each party shall use those security procedures specified in the applicable sections of the GISB EDM.
- Security Key Exchanges. Each party shall maintain a public key used to facilitate secure electronic communication. The trading partners will determine the manner in which public encryption keys are to be changed and/or exchanged. However, in emergency situations in which it is necessary to change a key immediately, each party shall provide the other party with immediate notice of the change. Each party shall provide to the other its public key by either: (a) a certified or receipt mail service using a diskette with the public key contained in an ASCII text file; or (b) an electronic simple mail transfer protocol ("SMTP") mail message with the public key contained in the body. The public key shall be verified by the party to whom it is sent by validating the fingerprint of the public key by phone or by other comparable means.
- Signatures. Each party shall apply its private key as its signature, which signature shall be applied to each Document transmitted by such party ("Digital Signature"). Such Digital Signature, when decrypted by the receiving party, will be used to authenticate the identity of the sender.

21. Transmissions

- Proper Receipt at the receiving party's Receipt Computer shall be evidenced by the receipt by sending party of an Hyper Text Transfer Protocol (HTTP) response initiated by receiving party. The HTTP response shall specify the date and time of receipt of a Document at the receiving party's Internet server (also called "time-c" in the GISB EDM documents). No Document shall have any effect if the HTTP response is not received by sending party, or if the HTTP response indicates an error.
- The "Receipt Computer" shall be identified by the receiving party's URL. The URL points to the appropriate Internet server locations and resources. Where the Trade Partners employ the services of outside GISB transmission providers to transmit and receive Documents, the receiving party's Receipt Computer shall be defined as the URL provided by the receiving party's Provider.
- Digital Signature Verification and Decryption. Upon Proper Receipt of any Document, the receiving party shall attempt to decrypt the Document and verify the Digital Signature of the sending party. If the Document is verified and the decryption is successful, the receiving party shall transmit a Functional Acknowledgment in return. If the Document is verified and the decryption is unsuccessful, the receiving party shall send the applicable error message to the sending party. The sending party shall attempt to correct the error and promptly retransmit the Document or otherwise contact the receiving party.

22. Parties are required to communicate GISB server maintenance schedules to their trading partners. This could be done via e-mail and/or web server.

Summary of Failures

1. A **protocol failure** occurs any time a sending party's GISB server cannot connect to the receiving party's GISB 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.
2. An **exchange failure** is when a sending party's GISB server has had continual protocol failures over a two-hour period. Each party is required to try at least 3 times over the two-hour period before flagging an exchange failure.
3. E-mail will be used to notify partners of exchange failures and of resolution of the problem. This will assist in rectifying and documenting problems.
4. When a protocol failure occurs, it is recommended that the sending party wait 60 minutes, then retry the GISB transfer. If a second protocol failure occurs, the sending party should wait another 60 minutes, then retry the GISB transfer. For example, the first protocol failure happens at 1:00 am, the second happens at 2:00 am, and the third happens at 3:00 am.

Example

For example, at 1 am my GISB server tries to post a file on your GISB server, but your server is down. I note a protocol failure at 1 am. I wait some period of time and try again. If your server is still down, I note another protocol failure. I continue trying (at least 3 times) for two hours. If I still cannot connect after two hours, I note an exchange failure.

As soon as I note an exchange failure, I send an exchange failure e-mail to your specified GISB administration mailbox. This gives the receiving party a notification that there is a problem, and initiates any manual or automated processes to rectify the problem.

INITIAL INTERNET EDI TEST PLAN

This section is only applicable to the initial electric implementation of Internet EDI. The existing Electric test plan will be updated at some future date to include ongoing Internet EDI testing and will supersede this section at that time.

The testing plan for Gas will be incorporated into the "New Jersey Gas Certification Testing Plan" document.

Testing Assumptions

1. For this section "trading partners" means utilities and suppliers who are, or plan to, exchange EDI transactions.
2. This abbreviated Internet EDI test is for trading partners that have already completed Certification testing with each other over the VAN. Initially, Internet EDI testing will be conducted with existing trading partners (i.e., trading partners who are already trading via the VAN).
3. This Test Plan does not replace the full certification test plan that must be conducted to test the business processes behind the transaction exchange.
4. The full test plan for Certification will be modified to reflect use of the Internet for future testing between parties that have not completed Certification testing with each other.
5. The Internet EDI will be performed with a sample of one outbound production file per trading partner.
6. Each Utility can define batches to help facilitate testing.
7. Each Utility will communicate to current Supplier trading partners its Internet EDI test plan, any trading partner agreements, and Internet EDI testing batch schedule dates.
8. Each party will provide a contact and an email address to which manual and automated protocol and exchange failure messages are sent.
9. Each Supplier will maintain the pace of the test batch as published by the Utility, or risk being removed from the test batch.
10. Each Utility will add Internet EDI items to their FAQ, including protocol and exchange failure process and contacts, and test exceptions.

Testing Goals

1. Establish Internet EDI connectivity between trading partners, including HTTP connections and encryption compatibility.
2. Validate that normal production EDI files can be sent.
3. Validate that X12-compliant transaction data payloads are being delivered after decryption.

4. Validate that HTTP and X12-compliant 997 functional acknowledgements are being delivered.
5. Validate that protocol failures are handled properly.
6. Validate that exchange failures are handled properly.
7. Validate that encryption/decryption failures are handled properly.

Testing Process

1. The Utility will notify the Supplier with the date on which the Utility and Supplier will begin testing.
2. The Utility will conduct a kickoff testing discussion. The kickoff discussion should include identification by each party of what production exchanges will be captured and sent for testing. The test should be completed in approximately one week.
3. Each trading partner will identify which files will be/were captured for testing purposes. Each party will modify their production file by changing the ISA information to indicate that this is a test file, including the sender and receiver information, and the ISA13 production/test flag. Each party will indicate how the file will be modified in the initial kickoff meeting and the testing profile.
4. Each party will send these files to the other party through Internet EDI, and notify the testing contact of the trading party that the files were sent.
5. Each trading partner should run these files through their translator to confirm that the files were not corrupted. The files may be processed further. However, this is not required
6. Each trading partner will simulate a protocol failure, triggering the appropriate automated notices to the identified trading partner contacts.
7. Each trading partner will simulate an exchange failure, triggering the appropriate automated and manual notices to the identified trading partner contacts.
8. Each trading partner will simulate an encryption/decryption failure, triggering the appropriate automated and manual notices to the identified trading partner contacts.
9. Each trading partner will send a formal notice via e-mail to the trading partner when Internet EDI capability is certified.

Appendix A – Recommended Internal Tests

This is a list of tests that should be conducted by each party prior to testing with a trading partner.

1. Stress Test – Ability to receive large production files from a trading partner.
2. Failure test – Test any automated processes triggered by a protocol or exchange failure.

Appendix B – Relevant Sections of the GISB EDM Version 1.4

The following sections of the GISB EDM Version 1.4 are determined to be relevant and controlling for New Jersey's Retail Choice implementation of GISB:

1. The Section entitled BUSINESS PROCESS AND PRACTICES, Subsection C. Electronic Delivery Mechanism Related Standards, the Sub-Subsection entitled Standards: Standards 4.3.7 through 4.3.15 inclusive.
2. The Section entitled TECHNICAL IMPLEMENTATION - INTERNET EDI/EDM & BATCH FF/EDM, subject to the following modifications and clarifications:
   - 2.1 - Ignore all references to "BATCH FF/EDM", "FF/EDM", "deadlines", "pipelines", and "nominations".
   - 2.2 - In the Data Dictionary For Internet EDI, the Format of the Business Name transaction-set refers to specific 8-character codes, which are not relevant for New Jersey purposes. The Internet EDI Subgroup will develop a list of relevant codes.
   - 2.3 - Under the Subsection entitled SENDING TRANSACTIONS, Sub-Subsection entitled Client Specifications, the reference to Central Time (Central Standard / Central Daylight) should be changed to Eastern Time (Eastern Standard / Eastern Daylight).
   - 2.4 - Under the Subsection entitled RECEIVING TRANSACTIONS, the Sub-Subsection entitled URL/CGI Implementation Guidelines is informational in nature only and has no force and effect. This Sub-Subsection shall not be construed as to impose any requirements on any utility or supplier.
   - 2.5 - Under the Subsection entitled RECEIVING TRANSACTIONS, Sub-Subsection entitled Server Specifications, the reference to Central Time (Central Standard / Central Daylight) should be changed to Eastern Time (Eastern Standard / Eastern Daylight).
3. Appendix A of GISB EDM.
4. Appendix B of GISB EDM.

The GISB EDM Version 1.4 is available at http://www.gisb.org.

Appendix C – Sample Test Script

This appendix includes a sample test script. It is provided for information only and should not be viewed as mandatory.

Tests to be conducted after the trading partners (identified as Host and Trading Partner) have exchanged URL, PGP private key, and X12 ISA/GS information. The test sequence can be initiated from either the utility or supplier, as agreed by the partners.

Test Event and Acceptance Criteria	Completion Date	Status (Pass/Fail)
1.0 Successful transfer of outbound data from Host's translator to Host's GISB EDM server (Optional test, at the discretion of the testing party)		
1.1 Back end system successfully places translated outbound X12 data in the outbound directory on the GISB EDM system. *Compare file in outbound directory to file sent from backend system to validate that they are the same.*		
2.0 **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 Timestamped response received from Trading Partner. *Verify that the file was sent and the timestamp was received.*		
3.0 Successful receipt of upload from a Trading Partner to the Host's GISB EDM 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.*		
4.0 Successful transfer of inbound data to backend system (Optional test, at the discretion of the testing party)		
4.1 Backend successfully retrieves file		
4.2 Inbound file successfully run through translator		
4.3 Backend system deletes file on GISB EDM system after successful transfer		
5.0 Successful delivery of GISB 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 HTTP header.*		
5.2 Trading Partner sends X12 file encrypted with wrong key. *Verify that a GISB standard error file was sent. Contact Trading Partner and verify that they received the error file.*		
6.0 Proper processing of GISB 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 HTTP 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*		

Test Event and Acceptance Criteria	Completion Date	Status (Pass / Fail)
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 GISB standard error file was received.*		