GISB EDM PLAN

Texas Data Transport Work Group (TDTWG)

Version 1.1

January 19, 2001

Executive Summary

This document defines the Internet Data Transport protocol and rules for point-to-point transactions as defined by the Texas Data Transport Work Group (TDTWG) for the deregulated Electric marketplace in Texas.

This document does NOT supercede any PUC orders

Document History

Date/Version	Summary of Changes
January 19, 2001 / 1.1	Removed references to X.509 Specified time change synchronization Specified PGP parameters Grammatical clean-up

High-level Summary of Texas PUC GISB EDM

1. The acceptable TDTWG transaction data transport protocol platform for point-to-point transactions between Competitive Retailers (CRs) and Transmission and Distribution Service Providers (TDSPs) is Gas Industry Standards Board Electronic Delivery Mechanism (GISB EDM) standard version 1.4.
2. All CRs and TDSPs are required to be GISB EDM Internet ready for testing and certification by 1/29/01 or otherwise required by the Independent Third Party Testing Administrator (ITPTA) with completion of testing and certification prior to transaction scenario testing.

Additional TDTWG Assumptions

1. This document is intended to be consistent with the proposed Texas Transaction Test Plan.
2. All TDSPs shall allow GISB EDM exchanges for CRs prior to a TDSP service agreement being signed.
3. ERCOT shall publish testing procedures for point-to-point (between CRs and TDSPs) transactions using GISB EDM.
4. The ITPTA retained by ERCOT shall administer testing for point-to-point (between CRs and TDSPs) transactions using GISB EDM.
5. After successful testing has been completed the ITPTA shall approve CRs and TDSPs as GISB EDM capable.
6. All CRs and TDSPs shall complete internal tests of their GISB EDM systems, including the tests defined in Appendix A.

7. GISB EDM exchanges shall follow rules for exchanging transaction data as defined in the sections of the GISB EDM Version 1.4 outlined in Appendix B, unless otherwise explicitly stated in this document.
8. Each party is required to send transactions according to timelines identified in the Texas Transaction Test Plan.
9. All CRs and TDSPs are encouraged to resolve GISB EDM problems with each other. A dispute is a problem where the two CRs and TDSPs cannot agree on who is responsible for the problem and/or how to fix the problem.
10. Transaction disputes that cannot be resolved between CRs and TDSPs shall be brought to the attention of the ITPTA for resolution.
11. If CRs and TDSPs argue that the transaction dispute is not adequately resolved by the ITPTA the dispute shall be raised to the ERCOT Technical Advisory Committee (TAC).
12. All GISB EDM TX SET transactions are to be treated as confidential and must be encrypted when sent across the Internet (except when sent for test purposes only). Receipt of un-encrypted TX SET '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.
13. Each party can obtain copies of TX SET compliant transactions from **www.ercot.com**.
14. Each party should maintain one production URL and one test URL, at a minimum.
15. Parties shall continue to send transaction 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 or is a valid readable transaction file with regard to content and structure.
16. It is mandatory to use PGP encryption software (version 6.5 or later) or other software compliant with OpenPGP/RFC 2440 .
17. PGP Parameters and Options:
    - Public Keys are generated using the RSA algorithm
    - Key expiration must be set at 2 years
    - User ID must be in format "name (organization) <email address>"
    - All GISB EDM payloads (transactions) will be encrypted with digital signatures applied
    - PGP compression option must be used.
18. Key Management
    - Market Participant's public key should be self-signed and sent to all Market Participants that they wish to do business with in the Texas Market. The recommended procedure for sending the self-signed public key is via email attachment sent to the appropriate authority designated by each party.
    - The received public key shall be verified by comparing the fingerprint of the public key by verbal communication.
19. Parties are required to communicate GISB EDM server maintenance schedules to their trading partners. This could be done via e-mail and/or web server.

20. Each Market Participant's GISB EDM administrator's E-mail address and contact information are required to be identified to the ITPTA. This E-mail address will be used for communicating protocol and exchange failures and other related communications.
21. Clocks shall be rolled forward and backward at 2:00AM Central Prevailing Time to accommodate daylight savings time changes.
22. Encrypted data can be in binary form.

Summary of Failures and Fail-over Standards

The following procedure is the minimum recommendation:

1. A **protocol failure** occurs any time a sending party's GISB EDM server cannot connect to the receiving party's GISB EDM 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 EDM 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 shall be used to notify partners of protocol and exchange failures. This shall 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 EDM transfer. If a second protocol failure occurs, the sending party should wait another 60 minutes, then retry the GISB EDM 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.
5. Automatic fail-over systems are recommended but not required by this plan at this time.

Example

For example, at 1:00 AM a GISB EDM server tries to post a file to the receiver's GISB EDM server, but the server is down. Note a protocol failure at 1:00 AM. Wait some period of time and try again. If you're the receiver's server is still down, note another protocol failure. Continue trying (at least 3 times) for two hours. If it still cannot connect after two hours, note an exchange failure.

As soon as the protocol failure is noted, send a protocol failure E-mail to the specified GISB EDM administration E-mail address. This gives the receiving party a notification that there is a problem and could be used to troubleshoot and fix the problem prior to an exchange failure.

As soon as the exchange failure is noted, send an exchange failure E-mail to the specified GISB EDM administration E-mail address. This gives the receiving party a notification that there is a problem, and initiates any manual or automated processes to rectify the problem.

TDTWG GISB EDM TEST PLAN

GISB EDM Testing Assumptions

1. The GISB EDM test shall be performed with a sample of one outbound transaction file per CR or TDSP.
2. The ITPTA shall coordinate timing and transactions with Market Participants to facilitate testing.
3. Each Market Participant's GISB EDM administrator's E-mail address and contact information are required to be identified to the ITPTA. Each party shall provide contact information and an E-mail address to which manual and automated protocol and exchange failure messages are sent.
4. Each CR and TDSP shall maintain the pace of the test as published by the ITPTA.
5. Each party may make exceptions or additions to this test plan. However, the exceptions must be presented to ITPTA prior to testing implementation in the Testing Sign-off Worksheet.
6. Each CR and TDSP shall add GISB EDM items to their FAQ, including URLs, protocol and exchange failure processes and contact information, and test exceptions.

GISB EDM Testing Goals

1. Establish GISB EDM connectivity between CRs and TDSPs, including Internet connections and encryption compatibility.
2. Validate that normal production transaction files can be sent.
3. Validate that TX SET compliant transaction data payloads are being delivered after decryption.
4. Validate that GISB EDM time-stamp and TX SET compliant 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 and digital signature failures are handled properly.

GISB EDM Testing Process

1. The ITPTA shall notify the CRs and TDSPs with the dates to begin testing.
2. Each bi-lateral test should be completed in approximately one week.
3. The ITPTA shall conduct a kickoff testing discussion. The kickoff discussion should include identification by each CR or TDSP of what production exchanges shall be captured and sent for testing.

4. The ITPTA shall identify which files shall be used for testing purposes.
5. Each CR or TDSP shall send these files to the other party through GISB EDM, and notify, through E-mail, the ITPTA and receiving test party that the files were sent.
6. Each CR or TDSP should run these files through translation software to confirm that the files were not corrupted.
7. Each CR or TDSP shall simulate a protocol failure as defined in GISB EDM PLAN under the Summary of Failures and Fail-over Standards (1), triggering the appropriate notices to the identified Market Participant contacts.
8. Each CR or TDSP shall simulate an exchange failure as defined in GISB EDM PLAN under the Summary of Failures and Fail-over Standards (2), triggering the appropriate notices to the identified Market Participant contacts.
9. Each CR or TDSP shall simulate an encryption/decryption failure, triggering the appropriate notices to the identified Market Participant contacts.
10. Each CR or TDSP shall send a formal notice of successful certification completion to the PUC with copies to the Market Participant and the ITPTA.

Appendix A – Recommended GISB EDM Internal Tests

This is a list of tests that should be conducted by each CR and TDSP during testing.

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

Appendix B – Relevant Sections of the GISB EDM Version 1.4

Based on TDTWG's review of the GISB EDM Version 1.4, the following sections were determined to be relevant and controlling for TDTWG's implementation of GISB EDM:

1. In 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 - GISB EDM/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 GISB EDM, the Format of the Business Name transaction-set refers to specific 8-character codes that are not relevant for our purposes. The TDTWG shall develop a list of relevant codes and transaction name descriptions based on the TX SET scenarios (e.g. "810_02", TDSP Invoice).

2.3 - 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 CR or TDSP.

3. Appendix A
4. Appendix B

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

Appendix C – Sample Test Scripts (subject to review)

This appendix includes two sample test scripts submitted by different parties. They are provided for your information, and should not be viewed as required.

Test Script Sample #1

1. Include certificate importation.
2. Include password generation.
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 is recommended.

1. Send non-encrypted text message (for initial testing purposes only)
2. Send non-encrypted TX SET transaction, process through translation software, return functional acknowledgement, inspect flat file
3. Send non-encrypted TX SET transaction, process through translation software, return functional acknowledgement, inspect flat file, return GISB EDM non-encrypted message response
4. Encrypt same TX SET transaction, send to receiver, return GISB EDM encrypted message response, decrypt, process through translation software, return functional acknowledgement, inspect flat file
5. Sign and encrypt same TX SET transaction, send to receiver, check signature, return GISB EDM encrypted and signed message response, decrypt, process through translation software, return functional acknowledgement, inspect flat file
6. Send 5 above with errors in the TX SET transaction file, assure that functional acknowledgement can be sent and received successfully, and check in- bound GISB EDM response manually
7. Test automated parsing of GISB EDM response codes and sending of notifications
8. Inspect internal log files to ensure proper recording sequence of events and timestamps
9. Check that timestamps and Transaction Id are correct
10. Queue multiple files at once to test for proper handling and timestamp assignment

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 GISB EDM response
9. Processing a negative GISB EDM message response code

Test Script Sample #2

Tests to be conducted after the CR and TDSP (identified as Sender and Receiver) have exchanged URLs and transaction header information. The test sequence can be initiated from either the CR or TDSP, as specified by the ITPTA.

Test Event and Acceptance Criteria	Completion Date	Status (Pass/Fail)
1.0 Successful transfer of outbound data from Sender's translation software to GISB EDM server (Optional test, at the discretion of the testing party)		
1.1 Back end system successfully places translated outbound TX SET data in the outbound directory on the GISB EDM system. *Compare file in outbound directory to file sent from back-end system to validate that they are the same.*		
2.0 Successful transmission of large (e.g. 5MB or larger) production TX SET file		
2.1 Valid TX SET test file signed, encrypted, and sent to Receiver. *Place the test file in the Sender's outbound directory and send the file. Verify with Receiver that the file was received and correctly decrypted.*		
2.2 Time-stamped response received from Sender. *Verify that the file was sent and the timestamp was received.*		
3.0 Successful receipt of transmission from a CR or TDSP to the GISB EDM server		
3.1 TX SET file received, decrypted, authenticated, and placed in inbound directory. *Look in the Receiver's inbound directory and verify that the file was received and correctly decrypted.*		
3.2 Received timestamp with correct status information. *Verify with Receiver that timestamp was received.*		
4.0 Successful transfer of inbound data to back-end system		
4.1 Inbound file successfully processed through translation software.		
4.2 Back-end system successfully retrieves file.		
4.3 Back-end system successfully deletes file on GISB EDM system after successful transfer		
5.0 Successful delivery of GISB EDM standard error message returned to Sender		
5.1 GISB EDM software sends TX SET file with wrong DUNS number in "to" field. *Verify that a timestamp was sent indicating an error in the HTTP header.*		
5.2 GISB EDM software sends TX SET file encrypted with wrong key. *Verify that a GISB standard error file was sent. Contact Receiver and verify that the error file was received.*		
6.0 Proper processing of GISB EDM standard error messages		
6.1 Send file 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. *Encrypt a test file with a key other than the Receiver's public key. Send a test file using the bad key. After the test, make sure to replace with the correct key.*		
6.3 Receive error file from Sender indicating decryption failure. *Verify that a GISB standard error file was received.*		