NAESB EDM PLAN

Texas Data Transport Work Group (TDTWG)

Version 2.01

October 4, 2002

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
June 25, 2002 / 2.0	

High-level Summary of Texas PUC NAESB EDM

1. The acceptable TDTWG transaction data transport protocol platform for transactions between Competitive Retailers (CRs), Transmission and Distribution Service Providers (TDSPs), and ERCOT is North American Energy Standards Board Electronic Delivery Mechanism (NAESB EDM) standard version 1.6.
2. All CRs, TDSPs, and ERCOT are required to be NAESB EDM Internet ready for testing and certification by.

Additional TDTWG Assumptions

1. This document is intended to be consistent with the proposed Texas Market Test Plan.
2. All TDSPs shall allow NAESB EDM exchanges for CRs prior to a TDSP service agreement being signed.
3. ERCOT shall publish testing procedures for transactions using NAESB EDM.
4. The Testing Authority retained by ERCOT shall administer testing for point-to-point (between CRs and TDSPs) transactions using NAESB EDM.
5. After successful testing has been completed the Testing Authority shall approve CRs, TDSPs, and ERCOT as NAESB EDM capable.
6. All CRs,TDSPs, and ERCOT shall complete internal tests of their NAESB EDM systems, including the tests defined in Appendix A.
7. NAESB EDM exchanges shall follow rules for exchanging transaction data as defined in the sections of the NAESB EDM Version 1.6 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 Market Test Plan.
9. All CRs, TDSPs, and ERCOT are encouraged to resolve NAESB EDM problems with each other. A dispute is a problem where the two CRs, TDSPs, or ERCOT 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, TDSPs, and ERCOT shall be brought to the attention of the Testing Authority for resolution.
11. If CRs, TDSPs, and ERCOT argue that the transaction dispute is not adequately resolved by the Testing Authority the dispute shall be raised to the ERCOT Executive Management.
12. All NAESB 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 NAESB 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. OpenPGP Parameters and Options:
    - Public Keys are generated using the El Gamal algorithm
    - Key expiration must be set at 2 years
    - User ID must be in format "name (organization) <email address>"
    - All NAESB EDM payloads (transactions) will be encrypted with digital signatures applied using the DSS standard
    - OpenPGP compression must be used.
18. Key Management
    - Market Participant's public key should be self-signed and sent to all Market Participants and ERCOT 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 NAESB EDM server maintenance schedules to their trading partners. This could be done via e-mail and/or web server.

20. Each Market Participant's NAESB EDM administrator's E-mail address and contact information are required to be identified to the Testing Authority. 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.
23. All NAESB EDM 1.6 required functionality must be implemented by all Texas Market Participants and ERCOT.

Failure Procedures

The following procedure is the minimum recommendation:

1. A **protocol failure** occurs any time a sending party's NAESB EDM server cannot connect to the receiving party's NAESB 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 NAESB 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 NAESB EDM transfer. If a second protocol failure occurs, the sending party should wait another 60 minutes, then retry the NAESB 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.
6. It is recommended that exchange failures be monitored closely, and the appropriate internal Trading Partner escalation procedures put in place in the event they occur.

Example

For example, at 1:00 AM a NAESB EDM server tries to post a file to the receiver's NAESB EDM server, but the server is down. Note a protocol failure at 1:00 AM. Wait one hour and try again. If 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 NAESB EDM administration E-mail address and include the protocol failure error message. This gives the receiving party a notification that there is a problem and could be used to trouble shoot 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 NAESB 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 NAESB EDM TEST PLAN

NAESB EDM Testing Assumptions

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

NAESB EDM Testing Goals

1. Establish NAESB EDM connectivity including Internet connections and encryption compatibility between all parties (CRs, TDSPs, ERCOT).
2. Validate that payload data files can be sent.
3. Validate that payload data files can be decrypted.
4. Validate that the NAESB EDM time-stamp is being delivered and verified by both parties
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.

NAESB EDM Testing Process

1. The Testing Authority shall notify the CRs, TDSPs, and ERCOT the dates to begin testing.
2. The Testing Authority shall conduct a kickoff testing discussion.
3. Each participant's connectivity test plan should be completed in approximately one week.
4. The Testing Authority shall identify which payload files shall be used for testing purposes.

5. CRs, TDSPs, or ERCOT shall send these files to the other party through NAESB EDM, and notify the Testing Authority and receiving test party via E-mail that the files were sent.
6. CRs, TDSPs, or ERCOT shall simulate a protocol failure as defined under the **Failure Procedures** section of this document, triggering the appropriate notices to the identified Market Participant contacts.
7. CRs, TDSPs, or ERCOT shall simulate an exchange failure as defined under the **Failure Procedures** section of this document, triggering the appropriate notices to the identified Market Participant contacts.
8. CRs,TDSPs, or ERCOT shall simulate an encryption/decryption failure, triggering the appropriate notices to the identified Market Participant contacts.
9. Successful completion of NAESB EDM testing allows CRs, TDSPs, or ERCOT to proceed to the next testing frame for market certification, as required.

Appendix A – Recommended NAESB EDM Internal Tests

This is a list of tests that should be conducted internally by the CR,TDSP, or ERCOT 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 – Texas Electric Industry Implementation of NAESB EDM Version 1.6

Based on TDTWG's review of the NAESB EDM Version 1.6, the following sections were determined to be relevant and subject to the following modifications and clarifications to the TDTWG's implementation of NAESB EDM 1.6:

1. 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. Section entitled TECHNICAL IMPLEMENTATION - NAESB 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 NAESB EDM, the Format of the Business Name transaction-set refers to specific 8-character codes that are not relevant for our purposes.

   Based on the definitions of best practices, in the future, the TDTWG may develop a list of required transaction-set 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 CRs, TDSPs, or ERCOT.

3. Appendix A
4. Appendix B

The NAESB EDM Version 1.6 is available to NAESB members at http://www.NAESB.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 NAESB EDM non-encrypted message response
4. Encrypt same TX SET transaction, send to receiver, return NAESB 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 NAESB 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 NAESB EDM response manually
7. Test automated parsing of NAESB 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 NAESB EDM response
9. Processing a negative NAESB EDM message response code

Test Scipt 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 Testing Authority.

Script ID	Fr.	Date	Sim Date	From	To	Trans	Description	Expected Result
ST196	0			CR or TDSP	ERCOT	[Tech Wksht]	CR or TDSP emails completed Technical Worksheet to ERCOT.	Worksheet received by ERCOT
ST196	0			ERCOT	CR or TDSP	[Tech Wksht]	ERCOT emails Technical Worksheet to the CR or TDSP GISB Communication Contact with Scheduled Testing Date to the CR or TDSP.	Worksheet received by CR or TDSP
ST196	0			ERCOT	CR or TDSP	[Encryption Keys]	ERCOT emails public keys to CR or TDSP	Keys sent to CR or TDSP
ST196	0			CR or TDSP	ERCOT	[Encryption Keys]	CR or TDSP emails public keys to ERCOT	Keys sent to ERCOT
ST196	0			ERCOT	CR or TDSP	[handshake file]	ERCOT sends an encrypted file containing the handshake file . ERCOT emails CR or TDSP results of successful posting from their GISB log. No FA Required.	Encrypted and digitally signed file sent via GISB EDM; Receipt received by ERCOT
ST196	0			CR or TDSP	ERCOT	[Email]	CR or TDSP notifies ERCOT via email that the handhake file was received.	CR or TDSP confirms receipts via email
ST196	0			CR or TDSP	ERCOT	[handshake file]	CR or TDSP sends an encrypted file containing the handshake file. CR or TDSP emails ERCOT results of successful posting from their GISB log. No FA required.	Encrypted and digitally signed file sent via GISB EDM; Receipt received by CR or TDSP
ST196	0			ERCOT	CR or TDSP	[Email]	ERCOT notifies CR or TDSP via	ERCOT confirms receipt via email.

							email that handshake file was received	
ST196	0			CR or TDSP	ERCOT	[handshake file]	CR or TDSP sends an UN-ENCRYPTED handshake file. CR or TDSP emails ERCOT results of successful posting from their GISB log. No FA required.	Un-encrypted, plain text file, or send a file not encrypted with the ERCOT public key. **This may need to be optional.**
ST196	0			ERCOT	CR or TDSP	[GISB ACK]	ERCOT returns GISB Error (601 for public key invalid, or 602 for file not encrypted) indicating the CR or TDSP file was not encrypted.	ERCOT server sends back error message to CR or TDSP server
ST196	0			CR or TDSP	ERCOT	[GISB ACK]	CR or TDSP confirms receipt of GISB Error EEDM999 from the ERCOT server.	CR or TDSP confirms GISB server received Error Message
ST196	0			ERCOT	CR or TDSP	[handshake file]	ERCOT sends an UN-ENCRYPTED handshake file . ERCOT emails CR or TDSP results of successful posting from their GISB log. No FA Required.	Un-encrypted, plain text file, or send a file not encrypted with the CR OR TDSP public key. **This may need to be optional.**
ST196	0			CR or TDSP	ERCOT	[GISB ACK]	CR or TDSP returns GISB Error (601 for public key invalid, or 602 for file not encrypted) to the ERCOT server indicating the ERCOT file was not encrypted.	CR or TDSP Server sends back error message to ERCOT server
ST196	0			ERCOT	CR or TDSP	[GISB ACK]	ERCOT confirms receipt of GISB Error 601 or 602 from the CR or TDSP server via email	ERCOT confirms GISB server received Error Message
ST196	0			CR or TDSP	ERCOT	[Test Fail]	ERCOT tests CR or TDSPdefined process for an exchange failure	CR or TDSP calls/emails ERCOT; waits for feedback
ST196	0			ERCOT	CR or TDSP	[Test Fail]	CR or TDSP tests ERCOT defined process for an exchange failure	ERCOT calls/emails CR or TDSP; waits for feedback