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 payload, process through translation software, return functional acknowledgement, inspect flat file
3. Send non-encrypted payload, process through translation software, return functional acknowledgement, inspect flat file, return GISB EDM non-encrypted message response
4. Encrypt same payload, 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 payload, 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 payload 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 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 Administrator.

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 email that handshake file was received	ERCOT confirms receipt via email.
ST196	0			CR or TDSP	ERCOT	[handshake file]	CR or TDSP sends an UN-ENCRYPTED handshake file. CR	Un-encrypted, plain text file, or send a file not encrypted with the ERCOT

							or TDSP emails ERCOT results of successful posting from their GISB log. No FA required.	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