

NAESB EDM v2.2 Discussion / 2014 Internet ET review – 9/4/2014

**Purpose:** Annual plan action item to review Internet ET

**History**:

In November 2013, the Texas Data Transport Working Group (TDTWG) filed System Change Request 776 to request the TX marketplace to upgrade to NAESB EDM v2.2. The PA EDEWG leadership decided to monitor and as part of the annual Internet ET deliverable would make a recommendation to PUC staff if PA should consider such an upgrade.

**Current Internet Protocol in PA:** NAESB EDM v1.6

**NAESB EDM v2.2 – new features/functionality**

The TDTWG presented four business cases in their formal change request:

**Issue 1**

Risk currently exists where an unauthorized party could intercept and respond to a data transmission since the current NAESB EDM v1.6 standard does not allow for sufficient repudiation for EDM responses. This means that there is a risk for a party outside the intended receiver to represent themselves as the authorized party on a connection and successfully intercept and/or manipulate the response data to the sender.

**Resolution**

The risk is significantly minimized with the implementation of NAESB EDM v2.2 which mandates the use of digital signature for EDM responses. These responses support the public-private key structure to encrypt EDM responses to verify sender. A public key is shared amongst retail market participants using NAESB as data transport. A private key is a unique key and is only known to an individual party.

The addition of digital signature will ensure:

* Validation of the sender is accomplished through the use of public/private key infrastructure.
* Near real time identification of any compromised data by authorized receiving party.
* Preventative actions can be taken immediately by authorized receiving party.

**Issue 2**

Since the implementation of the NAESB EDM v1.6 standard in 2004 the ERCOT retail market has implemented multiple new file types to accommodate various retail market processes (in addition to the standard X12 Texas Standard Electronic Transactions (TX SETs). The NAESB EDM v1.6 standard does not accommodate the identification of these file types.

**Resolution**

Implementation of the NAESB EDM v2.2 accommodates these new file types in transaction-set header data elements will allow files to be identified at the transmission level to allow for enhanced tracking and processing. These file types include:

* *Electronic Data Interchange (.edi)*
	+ The predominant format used to send and receive Texas Standard Electronic Transactions (Texas SET) in the retail market.
* *CBCI Files (.csv)*
	+ These are used to communicate Customer Billing Contact Information to be used in a Mass Transition Event.
* *Demand Response Files (.csv)*
	+ These files contain information about ESIIDs participating in a Demand Response program.
* *Advanced Meter Interval Data Format and Submission Files (.lse)*
	+ These are 15 min interval CSV formatted files for daily meter usage.

**Issue 3**

The current NAESB EDM v1.6 standard does not support the identification of a failed file transmission event. This situation has continually created significant delays in file processing, causing system degradation and negatively impacting any MARKET PARTICIPANT and/or ERCOT reporting as required by PUCT Subst. rule 25.88 Retail Market Performance Measure Reporting and/or Service Level Agreement (SLA).

**Resolution**

NAESB EDM v2.2 accommodates the identification of file retransmissions through the implementation of header data elements to identify files that have been previously attempted. This provides the ability for the receiver to expeditiously identify subsequent attempts of the same original transmission which would aid in troubleshooting and resolution with NAESB system issues.

**Issue 4**

NAESB EDM v1.6 does not specify decryption error response time following a previously accepted EDM response transmission. This gap causes delays in identifying missing files impacting customers and retail business file processing.

**Resolution**

Implementation of NAESB EDM v2.2 requires decryption errors be sent within one hour of receipt of a file transmission. This allows the sender to know the files were not processed and resolution efforts shall commence.

**EDEWG Recommendation:**

## Leadership

Brandon Siegel discussed PA’s consideration of a NAESB EDM v2.2 upgrade with the EDEWG leadership during multiple leadership team meetings. Upon review of the above issues outlined in the TX upgrade request the following discussion took place: Item 1 while adding security, there has never been a known breach of EDM v1.6. Item 2 does not apply as the EDM is only used for EDI in PA. Items 3 and 4 have never been reported to EDEWG as areas of operational constraint or concern. In addition, ERCOT’s Technical Advisory Committee never ruled on SCR 776 because the TDTWG withdrew the upgrade request. Some TX market participants raised concerns regarding cost benefit of such an upgrade. It should also be known EDM v1.6 and EDM v2.2 are incompatible with one another and therefore may require additional implementation costs. Upon taking all of this into consideration, the EDEWG leadership does not recommend an upgrade to EDM v2.2 as part of the 2014 annual review.

## EDEWG discussion

## Brandon Siegel reviewed this document during the September 4, 2014 EDEWG meeting. There were no objections to leadership’s recommendation. The consensus then being EDEWG does not recommend upgrading to NAESB EDM 2.2 under the 2014 annual Internet Electronic Transport review.