Gas Industry Standards Board
Future Technology Task Force
Duke Energy, Houston, Texas
April 24, 1998 9:00am - 4:00pm
Draft Meeting Minutes

Antitrust guidelines were read to the meeting participants.

Facilities were described to the group.

Pete Whatley from Natural Gas Clearinghouse volunteered secretary for minute-taking.

Adoption of agenda-
Item number 6 removed due to the fact that the standard requiring this action was voted down in IL&F. It is noted that this item may reappear pending the action of the EC meeting on May 15.
Request for standard enhancement concerning RSA algorithm use in key generation. Added as agenda item # 10.
Objected to by Steve Hinton from TransCapacity. TransCapacity feels it inappropriate to address this issue without a triaged request.
Sub group will submit request for standard enhancement.
May 7, 1998 deadline for Implementation Guide changes. Therefore Implementation Guide Issues will be motion to accept
second by me

Meeting particpants were introduced.

Review, revision, and adoption of minutes of the prior meeting.
The list of participants was missing and needed to be included.
Changed the wording of Item 6, 3rd paragraph to read:

"A motion was made to recommend to the appropriate GISB process that the first sentence of Standard 4.3.15 be changed as follows:"

Identify and discuss new implementation issues.
Donald Richardson brought up the fact that PGP SDK 5.5. does not support RSA for key generation in the automatic mode? but does in the command line mode. . Susan Croley has discussed the issue with PGP and PGP has verified that there will be continued support of RSA for key generation in automatic mode?

Due to difficulties encountered in testing at different levels of development, Richard Hamilton suggested that GISB FTTP develop or provide:
A test transaction for use in development.
Suite of utilities for testing & development.
Develop accepted procedures for testing.

Review of Internet Look and Feel Task Force.
Review of happenings at IL&F. See minutes of that meeting for details.
Brief discussion of the impact of FERC RM587-G insued.

R97126 Develop standard EDM error messages for problems occurring beyond decryption but before the generation of a 997. Significant discussion identified a number of categories of messages and resulted in the following:

EEDMxxx:Standard Text;Variable Text

Checks for association between EDM tags and ISA sender and receiver
EEDM code : EEDM701
Standard text : EDM party not associated with EDI party
Variable text : optional and open
Passed unanimously

X12 Compliance
EEDM code : EEDM702
Standard text : Data Structure Error
Variable text : optional and open
Passed; 12 for ; 1 opposed

Trading Partner errors for X12
EEDM code : EEDM703
Standard text : Data set exchange not established for Trading Partner
Variable text : optional and open
Passed; 12 for; 1 abstained

Additional Standards Proposals to Business Practice Subcommittee
EEDM997 to be reserved and unused to avoid confusion.

System Errors
Sender System Error
EEDM code : EEDM980
Standard text : System error - sender
Variable text : optional and open
Passed; 12 for; 1 opposed

Receiver System Error
EEDM code : EEDM981
Standard text : System error - receiver
Variable text : optional and open
Passed; 12 for; 1 opposed

System Error (existing)

System unavailable
System unavailable due to scheduled outage - transaction accepted
WEDM code : WEDM901
Standard text : System unavailable due to scheduled outage
Transaction queued
Variable text : Expected availability as a courtesy
Passed; 9 for; 1 opposed

System unavailable due to scheduled outage - transaction rejected
EEDM code : EEDM901
Standard text : System unavailable due to scheduled outage
Transaction rejected
Variable text : Expected availability as a courtesy
Passed; 12 for; 1 opposed

System unavailable due to unscheduled outage
WEDM code : WEDM902
Standard text : System unavailable due to unscheduled outage
Transaction queued
Variable text : Expected availability, if available, as a courtesy
Passed; 9 for; 1 opposed

System unavailable due to unscheduled outage
EEDM code : EEDM902
Standard text : System unavailable due to unscheduled outage
Transaction rejected
Variable text : Expected availability, if available, as a courtesy
Passed; 12 for; 1 opposed

Passed unanimously

Implementation Guide Changes
Mike (Williams) asked if it was appropriate to address standard 4.3.4 dealing with the retention period for EDI data in order to pull GISB standards in line with FERC regulations for interstate pipelines. Consensus did not think so.

The following changes to implementation guide language regarding security stem from a standards initiation request covering the requirement to use keys generated with the RSA algorithm.

Implementation Guide References to PGP

Pages 4.4 - 4.5

Security
Though many decisions as to overall security measures are left to each trading partner and their environment, several security measures were established as standards to ensure a minimum level of confidence in conducting business over the Internet and to provide some uniformity in the implementation of security. Four primary security aspects were considered as vital in providing the level of protection of transactions needed for gas industry commerce: data privacy, data integrity, authentication, and non-repudiation. The FTTF found that these concerns are addressed by the use of encryption and digital signature capability of the Pretty Good Privacy (PGP) security application. Any process used for encryption and decryption compatible with PGP 2.6 using keys generated with the RSA algorithm meets the minimum standard to be applied to files transmitted over the Internet. To prevent unwanted intruders from connecting to the Web sites, basic authentication is the required standard. Additional issues such as firewall security are discussed in the standards, but are considered implementation issues to be addressed by each organization.

Page 4.11

4.3.15
Trading partners should implement all security features (secure authentication, integrity, privacy, and non-repudiation) using a file-based approach via a commercially available implementation of PGP 2.6 or greater (or compatible with PGP 2.6 using keys generated with the RSA algorithm). Trading partners should also implement basic authentication. This should be regarded as an interim solution since this technology is not an open standard. This technology supports all of the above security features while providing independence of choice of Web servers and browsers. Encryption keys should be self-certified and the means of exchange should be specified in the trading partner agreement.

In general, these needs are met by using the Basic Authentication capability of the Web server and the encryption and digital signature capability of the PGP security application for securing transactions.

Understanding PGP

Pretty Good Privacy (PGP) is the name of the chosen security application. See the GISB home page for information on software packages to implement the PGP security application. PGP utilizes a public key/private key pair to accomplish secure file transfers. The private key must be known only to the company which generated it. The public key counterpart is shared with trading partners.

Each company must generate its public key and private key pair. The RSA key generation algorithm should be chosen for versions of PGP which offer alternatives. The public keys will be distributed using a secure method (eg., courier mail) to the company's trading partners. You must use the utmost care in protecting your private key. If it is compromised, the security is broken. It is recommended that a key size of 1024 be chosen when generating the key pair. This provides a significantly secure transaction.

When a company wishes to send transactions to its trading partner, it will use the partner's public key to encrypt the file. Encryption provides data privacy. Only the private key counterpart can decrypt this file. Hence, the need to guard your private key.

When the sending party encrypts the file, it also uses its own private key to "sign" the transaction. The receiving party can use the sender's public key to verify the signature. The digital signature provides non-repudiation.

Encryption / Digital Signature

Encryption and signatures are applied to files already translated to a GISB standard data format. (Use of internal encryption such as X12.58 encryption is outside the scope of GISB encryption standards but does not conflict with PGP.) Encryption and signatures can be accomplished manually for each file using the on-line PGP software, or in an automated (or "batch") fashion using programs to encrypt and sign. Whether encrypting in a manual or automated fashion, it is essential that the correct public key of the trading partner be used to encrypt and just as essential that the correct sender's own private key be used to digitally sign the file.

Decryption / Signature Verification

After a transaction is received and processed by the CGI program, it is ready to be decrypted and have its signature verified. PGP will utilize the appropriate key pair when encrypting, signing, and decrypting if given the correct userID in the keyring identifying the trading partner. Upon request for signature verification, the PGP software will return a human-readable company name. It is recommended that all implementors create a process where the name is used to look up the ID of the company in a database table. If the ID is passed along with the decrypted file, a process could be created to verify that the company which sent the transaction corresponds to the company identified within the file, once the data has been translated.

Throughput Considerations

Encryption, digital signing, decryption and signature verification are all very CPU intensive. It is not recommended that decryption or signature verification be performed within the CGI that receives and processes the file. In fact, it would not be a good idea to have these steps performed on the same computer that is attempting to receive transactions at a time close to a deadline. Therefore, it is recommended that the secured or to-be-secured transaction be passed to a separate computer for security processing. This "passing" would likely be accomplished by using the File Transfer Protocol (FTP). The security processing computer should be optimized for CPU and memory.
Because decryption and signature verification are not handled at the time the file is received, the sender will get an HTTP response of successful transfer but doesn't know if the file can be decrypted by the receiver. Guidelines for communicating the status of the decryption step have been developed. See Section "Sending Error Notification Transactions" and Table A, "Internet EDM Standard Error Codes and Messages".

Security Requirements

Basic Authentication

Basic authentication, also known as realm one security, has been defined as one of the security standards for transmission on the Internet. The userid and password will be assigned by the server party according to site standards. The trading party agreement must identify the userid and password for this security as well as procedures for changing the password, if applicable.

PGP File Encryption

File encryption of the EDI file is also selected as a security standard for transmission on the Internet. The encryption software employed is required to be compatible with PGP 2.6 at a minimum or greater (or compatible with PGP 2.6 using keys generated with the RSA algorithm).. Those companies who wish to conduct business across the Internet in an unsecure fashion may do so by mutual agreement.

1 Install an interactive browser. Identify an existing Web server from among GISB compliant servers offering interactive upload for test. See the GISB home page for a list of organizations willing to act as testing partners. These organizations should have a URL complete with the CGI program name to which a tester may send test files. File content does not need to be X12 or other GISB standard format to accomplish this step in testing.

2 Develop or acquire a batch browser that uses multipart for the encoding methodology. Transfer the same test file as in step 1 to the URL not requiring Realm One security.

3 Add Realm One security to your file transfer, and change the URL to the secure URL. Continue transfer tests with your batch browser.

4 Acquire and install PGP software. Generate your public and private key pair. Make sure to choose the RSA key generation algorithm. Download the test server's test public key. Encrypt your data file using this key. Modify your file transfer to send the encrypted file. Continue transfer tests. Request that the test server contact decrypt your file.

Minor references ignored on pages 6.1.27, 6.1.28, 6.1.30, 6.1.32, 6.1.34

Passed unanimously
Add to implementation guide in the appropriate area:

"Implementers of Internet EDM sites should review and evaluate DNS cache refresh intervals so as to insure trading partner address changes are recognized on a timely basis. A refresh interval of 24 hours or less is common."

Passed unanimously.
Add to implementation guide in the appropriate area:

"In the receiving program, all tag values in the HTTP headers should be evaluated in a case insensitive manner."

Passed unanimously
Y2K

FTTF standpoint is that there is no EDM standard that wouls preclude a company from implementing a Year 2000 compliant system

Passed unanimously
Add to implementation guide in the appropriate area:

"In the receiving program, all tag values in the HTTP headers should be evaluated in a case insensitive manner."

Passed unanimously
Replace "transaction set " with "EDI data" in all appropriate locations in the Implementation Guide in order to remove confusion over plurality in the transmission of EDI transaction sets. It should be clear that multiple transaction sets may be transmitted within one encrypted file.

Passed unanimously
Prior meeting implementation issues.
Assignments and further research.
Determine requirements and schedule for the next FTTF meeting.
Election of chair(s) to be at next meeting
Date and time of next meeting be determined (May 29th?)

Summarize progress and action items

Adjourn at 15:45

Attendance List:

Donald Richardson*	EDI Works
Susan Croley	Duke Energy
Terry Lehn	Enron/EDS
Richard Hamilton	The Williams Companies
Mike Stender	El Paso Energy
Dick Brooks	Group 8760
Pete Whatley	NGC Corp.
Leigh Spangler	Latitude Technologies
Michael Bencal	NGC Corp.
Christopher Phillips	Columbia Gas Transmission
Rick Hawley	Latitude Technologies
Andy Sicignano	Enron Capital and Trade
Jim Keisler	Transco
Steve Hinton**	Transcapacity

*left early
**attended via telephone

Gas Industry Standards Board
Future Technology Task Force
Duke Energy, 5400 Westhiemer Court, Houston, Texas
April 24, 1998 09:00 - 16:30
Draft Minutes