Memorandum

Date: 05/29/98

To: Ms. Rae McQuade, Executive Director of the Gas Industry Standards Board

CC: Mr. Mike Bray, Chair of the Executive Committee

From: Susan P. Croley, Chair of the Future Technology Task Force

RE: Revisions to the Electronic Delivery Mechanism Related Standards

---

The Future Technology Task Force has identified several items in the Electronic Delivery Mechanism Related Standards Manual over the past several months that need to be rectified. FTTF has deemed these items as errata. Each item was voted on and approved at the last Future Technology Task Force meeting held April 24, 1998. Please present these before the GISB Executive Committee for approval. Listed below are the corrections, the voting results, and reason for each correction or group of corrections.

Note: New text is represented in **bold**. ~~Strikethroughs~~ represent deleted text.

Miscellaneous subjects

To be inserted as a second paragraph under Throughput Considerations on p. 6.1.20:

> **Implementers of Internet EDM sites should review and evaluate Domain Name Server (DNS) cache refresh intervals so as to ensure trading partner address changes are recognized on a timely basis. A refresh interval of 24 hours or less is common.**
>
> **FTTF Vote:** Passed unanimously.
>
> **Reason:** Serves as a technical tip for evaluation by the individual implementer.

To be inserted as a new bullet sentence below the other bullets on p. 6.1.12:

- Each data element should have \r\n\r\n (c notation) before the start of the data.
- **In the receiving program, all tag values in the HTTP header should be evaluated in a case insensitive manner.**

  FTTF Vote: Passed unanimously.

  Reason: To prevent users of the manual from taking the examples in the manual too literally. This serves also to remind implementers to code in a case-insensitive fashion to provide interoperability with multiple trading partners.

Replace “transaction set” with “EDI data” in an appropriate manner wherever used.

Replace one instance of “a transaction set” with “EDI data” on p. 3.1.

Replace one instance of “transaction set” with “EDI data” on p. 3.1.

FTTF Vote: Passed unanimously.

Reason: To remove confusion over plurality in the trasmission of EDI transaction sets. It should be clear that one or more transaction sets (X12 documents) may be transmitted within one encrypted file.

Series of changes for RSA algorithm used for key generation

Replace the sentence appearing on p. 4.5 with the following:

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.

Insert this sentence in the second paragraph under Undersstanding PGP on p. 6.1.19:

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.

Under PGP File Encryption on p. 6.1.21, please replace the second sentence with the following:

The encryption software employed is required to be compatible with PGP 2.6 ~~at a minimum~~ or greater **(using keys generated with the RSA algorithm).**

Insert the following as a third sentence under number item 4 on p. 6.1.26:

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. …

FTTF Vote: All RSA-related items passed unanimously.

Reason: To prevent implementers from purchasing the wrong version of PGP with regard to the key generation algorithm. The ramification of purchasing the wrong key generation type is that their trading partners will not be able to decrypt the files they receive from implementer not using RSA key generation. Once discovered, the implementer has to purchase, after the fact, the RSA key generation version. Understandably, this will cause delay of testing and implementation. **To alleviate unnecessary purchasing errors, we strongly suggest this additional language. This revision does not limit the implementer to any particular vendor offering PGP products.**