

Final – Version 1.0

UIG Internet EDI Work Group

**Dave Darnell
Work Group Leader**

Data Transport Alternatives for Electronic Business Transactions

White Paper – Version 1.0 Final

June 7, 2000

Final – Version 1.0

1. Background and Executive Summary

The Internet EDI Work Group of the UIG was formed to gather and disseminate information on the various Internet EDI transport mechanisms and technologies. The first task undertaken by the work group was to put together this white paper based on as many inputs as was possible in the time allocated. In addition to several task group meetings, E-mail solicitations were generated many times and open conference calls were held to facilitate the information gathering,

This white paper will not attempt to recommend, but rather it will delineate facts about the various technology alternatives for EDI transport, focusing on advantages and disadvantages of each. In order to leverage our time, the work of various PUC sponsored EDI groups will be utilized as key inputs to this document. Please note that the various sections of this report were “donated” by several members of the UIG, with little editing by the Internet EDI Work Group leader. Document references are listed in the Appendix of this paper. What follows is an executive summary of the available transport technologies for electronic business transactions.

A VAN (Value Added Network / Value Added Service Provider) uses a commercially provided secure mailbox system to store and forward electronic business transactions, similar to the US Post Office. It is considered a trusted third party service. It has been the traditional mode of EDI (electronic data interchange) transaction transport.

Internet email data interchange has been defined in the IETF EDIINT (Internet Engineering Task Force EDI over the Internet) Work Group AS1 (Applicability Statement). With this methodology, Internet email attachments can be secured with encryption and digital signature technology, making this a workable alternative for transport of EDI (electronic data interchange) or Electronic Business Transactions (EBT). CommerceNet has assisted in adoption of this methodology by certifying interoperability of software products that have implemented AS1.

FTP (File Transfer Protocol) is a possible alternative; however, traditional FTP did not provide for security of user logins. Today FTP is considered the most efficient protocol for file transport. It has recently been secured for the Internet using SSL (secure sockets layer)/TLS (transport layer security) technology. This makes it a workable protocol for Internet transport of EDI/EBT.

GISB EDM (Gas Industry Standards Board Electronic Delivery Mechanism) and the IETF EDIINT AS2 specification are standardized alternatives utilizing HTTP. GISB EDM has a significantly large installed base and has been a “production proven” protocol for a number of years. The AS2 specification, being a newer effort, has the advantage of incorporating the newest security and electronic business technology features. There has recently been a move to converge these two methodologies, which has resulted in a revised AS2 specification with the key features and advantages of both technologies. GISB has shown interest in endorsing the new AS2 specification, leading the way to achieving interoperability between GISB EDM software products and AS2 software products.

Extranets are another alternative. An Extranet has been defined as an intranet that allows controlled access by authenticated outside parties. Typically an extranet will link the intranets of distributed organizations for the purpose of conducting business. This secure electronic consortium usually consists of an enterprise and its key trading partners, customers, dealers, distributors, suppliers, or contractors.

The data transport methodology selected by an electronic business transaction trading partner community may vary according to the needs and business requirements of the group. Careful study and reading of the following document will be of assistance in making an educated and successful implementation decision.

Final – Version 1.0

2. Status

Electronic commerce is the use of integrated information technologies to streamline external business procedures and facilitate trade. EDI, XML/EDI and other tools are "enablers" of electronic commerce. The exponential growth of the Internet and the subsequent evolution of WEB-based commerce has focused attention more on the use of an all encompassing global network and away from the traditional structure of dedicated data lines between two parties and Value Added Networks. As a result, much emphasis is placed on "emerging" Internet technologies. The current state of electronic commerce affords a multitude of technological and business choices for conducting business. Thus, the dilemma faced by utility industry market participants is not limited to the decision to use EDI, XML/EDI or other formats, but rather which data transmission mechanism should be employed. Technology is in a great state of flux - developing and changing so rapidly that today's workable solutions may well be obsolete in the near future.

Rather than focus on current products or available technology in structuring this white paper, the UIG Internet EDI Work Group chose first to define a set of critical success factors. We believe these factors will be more enduring and, therefore, should be used as criterion in evaluating and making electronic commerce choices in the near term.

3. Critical Success Factors

Although the Subgroup considered several factors, we believe the following are the critical factors in evaluating and selecting a data transfer mechanism and the related standards and practices. The two most prevalent data transfer mechanisms currently available for EDI are private Value Added Networks (VANs)¹ and the Internet. We considered each in terms of the critical success factors.

3.1 Security

The characteristics of a secure transaction are:

- a) Privacy - no one other than the parties involved will know the details of the transaction;
- b) Authentication - all parties to the transaction will know at the outset who they are dealing with;
- c) Integrity - messages cannot be changed enroute between parties; and
- d) Non-repudiation - a party cannot deny having engaged in the transaction.

VANs and the Internet address security concerns in different ways as shown by the table below. In the case of the VAN it is the operator who has responsibility for complying with the listed requirements. The Internet is a public network with no central network operator; the individual users are responsible for implementing measures to enable compliance with the listed requirements.

¹ A VAN is typically a privately owned network that provides or performs specific services for a fee. VAN customers typically purchase telecommunications services (dial-up, leased lines, etc.) that connect them to the VAN.

Final – Version 1.0

Characteristic	VAN requirements	Internet requirements
Privacy	Private network – ability to establish direct connections	Encryption
Authentication	User names and passwords	Digital Signature / Digital Certificate (self-certified or commercial authority)
Message Integrity	Contractual relationship/private network	Digital Signature / Message digest algorithm (MIC/MAC)
Non-repudiation	Logging	Digital signatures, logging

3.2 Reliability

To be characterized as reliable, the data transfer mechanism and related processes must be available as required. Reliability is a relative concept measured in degrees, not in absolute terms. Minimum operational requirements for the data transfer mechanism are 24 hours per day, 365 days per year with scheduled maintenance activities that do not affect service.

Virtually all of the major EDI VAN operators offer 24 hours per day, 365 days per year operations, and manage their scheduled maintenance activities without affecting service. The Internet is considered to operate 24 hours per day, 365 days per year and was specifically designed for network reliability, even though random parts of the network may be inherently unreliable. The Internet uses a robust communications protocol (TCP/IP) that is mature and stable. With this protocol, data packets can be re-routed dynamically to their eventual destinations should there be an outage in a portion of the Internet.

3.3 Performance

The data transfer mechanism and processes must demonstrate dependable and consistent operation under varying, but typical, conditions within a required timeframe. For example, these conditions include transmission of large files, varying degrees of network traffic, and transmission at different times of day. Performance requirements must be ensured initially through testing and over time through an established track record of on-line performance.

3.4 Recovery & Re-Transmission

This refers to the ability to support automatic re-transmission for up to a certain number of working days, after which requests for special processing and handling would be required.

3.5 Archiving and Auditing

The creator of the EDI outgoing message is able to archive or recreate the actual record in accordance with the particular rules governing each transaction. An adequate audit trail must exist to provide records of activity (logs).

3.6 Interoperability

This refers to the ability to operate and exchange information in a heterogeneous network. For parties using VANs, interoperability must be offered at the communications level, and the parties' VAN must be able to communicate with other VANs. Inherent in the Internet is the universal TCP/IP communications protocol.

Final – Version 1.0

4. Discussion of Current EDI Transport / Data Transfer Alternatives

4.1 Value Added Networks (VANs)

A VAN is a private network owned and operated by an organization responsible for its reliable and secure operation. It can be distinguished from a public data network (i.e. Internet) by the array of ancillary services that are included or offered as "value added" services. Such services include a wide variety of access mediums (regular telephone modem connections, leased telephone line connections, Internet connections) available to its customers, secure message management including a network user logon procedure, digital signatures and encryption capabilities, maintenance of transaction logs and audit trails, translation of varying non-EDI data sources to/from EDI standard transactions, and the capability of facilitating electronic communication between partners with dissimilar EDI formats, communications protocols, or technology platforms.

- The VAN uses a "store and forward" mail boxing system to manage all transfer of information from the sending party to the receiving party's mailbox. This type of process offers the added benefit of having an independent 3rd party acting as the "always available exchange point". This allows either party (trading partner) to process its data without the necessity of the other party's (trading partner) computer system being coincidentally available.
- Charges for VAN services typically include various fixed fees (monthly mailbox fees, interconnect fees - to connect to other VAN providers, and an initial 'set up' fee) plus several variable fees based on data transmitted (per transaction fees, and per character volume fees).
- VANs are likely to continue to exist since many market participants already use VAN services, they: have a high degree of reliability; are readily accessible; and can accommodate a wide variety of protocols.

In addition, VANs have added the Internet Protocol (IP) to their capabilities, thus becoming capable of allowing Trading Partners direct access to their other trading partners' EDI networks without the need for mailboxing (avoiding the accompanying VAN charges). VANs are providing Internet gateways which open up EDI document trading with those smaller trading partners with Internet access who do not wish to incur VAN costs. Some of these VAN Internet gateways offer a robust form of Secure File Transport Protocol (S/FTP), which utilizes Secure Sockets Layer (SSL)-Transport Layer Security (TLS) to protect and secure FTP connections from the Internet to VAN mailboxes. Other protocols that provide Internet capabilities are also being provided by VANs.

4.2 Internet

The Internet is a worldwide network of computers communicating with the universal TCP/IP protocol and is used by millions of users. The Internet is considered a public network with no sole owner or operator. The architecture and protocols associated with the Internet were specifically designed for network reliability, even though random parts of the network may be inherently unreliable. Outages to portions of the Internet cause data packets to be routed dynamically through the Internet to their destinations.

There are three primary transfer protocols used to transfer files over the Internet: File Transfer Protocol (FTP); Simple Mail Transfer Protocol (SMTP); and Hypertext Transfer

Final – Version 1.0

Protocol (HTTP). Unlike the VAN, there are no monthly mailbox, transaction or volume-based fees for Internet transmission of data. However, using an Internet protocol will require some incremental investment by market participants to install and maintain the type of infrastructure necessary to provide internally certain functionality now included in the price of VAN services. These are the "value added" services provided by the VANs and include functionality such as security via similar encryption capabilities, an adequate level of reliability, a similar level of authentication, message integrity, transaction logging and archiving. Further, parties who choose this option would have to absorb the cost of keeping their systems current and maintaining interoperability with a wide variety of trading partners.

4.3 Internet E-mail

There are a number of possibilities for using e-mail protocol (Simple Mail Transport Protocol: SMTP) to transport EDI. S/MIME (Secure/ Multipurpose Internet Mail Extensions) or Pretty Good Privacy (PGP) can be utilized to provide security-related features required for electronic commerce transactions: privacy, authentication, integrity, non-repudiation (P.A.I.N.). The Internet Engineering Task Force's (IETF) EDIINT Work Group has published a standard for utilizing Internet E-mail for EDI. This document is called "AS1". AS1 describes how to implement existing IETF standardized protocols to create a secure Internet e-mail protocol for EDI.

Products that have implemented EDIINT AS1 all currently utilize S/MIME to encrypt and digitally sign EDI files. Some interoperability problems have been noted with the S/MIME implementations in commercial e-mail software packages (MS Outlook, Netscape Mail, etc.) This has been documented in a paper called "Characteristics and Attributes that affect S/MIME Product Interoperability" by Jerry Mulvenna, Larry Keys, Dale Walters, Srinivas Gantac, Sarbari Guptac. The abstract of this paper reads:

S/MIME is based upon the popular MIME standard, and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The S/MIME specification was designed to promote interoperable secure electronic mail. However, because the specification allows multiple interpretations and implementations, and is sometimes silent about key aspects that affect interoperability, a number of "S/MIME Enabled" products are available on the market that are incapable of fully interacting with one another. In this paper, we present a set of characteristics that affect the interoperability profile for a given S/MIME application, and illustrate how they may be used to achieve a higher level of interoperability within the family of S/MIME compliant products.

The concluding summary of the paper states:

In conclusion, we would like to point out that it is heartening to see the widespread adoption of the S/MIME secure electronic mail standard, and the availability of commercial products based upon the standard. Despite the fact that public key infrastructure technology is still in its infancy, and the standards are continuously evolving, the S/MIME vendors are making considerable progress in resolving the existing barriers to interoperability. In the near future, users will find that security services will be integrated into most e-mail applications.

It should be noted, however, that the authors of this paper did not evaluate any EDIINT products for this paper.

4.4 Internet FTP (File Transfer Protocol)

Final – Version 1.0

FTP is considered the most efficient Internet protocol for transfer of files. However the original IETF standards for FTP did not provide for security of user logins. User IDs and passwords are passed over the network “in the clear” and thus unprotected from a “sniffer” security threat. In addition, FTP is considered an unsafe service to make available to users via the Internet. FTP file creation and deletion capabilities could wreck havoc on an internal network (Intranet) if a hacker were to gain “Admin” level security through “spoofing” (impersonation). Thus almost no Corporate Security support personnel will allow FTP access to internal Intranet FTP services through their Internet Firewall.

Additional security has to be applied to the original FTP protocol in order to make it secure and reliable for EDI. One such security protocol is KERBEROS, which allows for encrypted passwords and user identification as well as a number of other network and network client/server security features.

FTP has also been implemented with SSL (Secure Sockets Layer)/TLS recently. Netscape originally developed SSL for Web server and browser security utilizing PKI (Public Key Infrastructure) encryption and digital signature at the “session” level. A proposed draft from the IETF (WG) defines this “S/FTP” protocol, and at least one product has been successfully implemented.

Currently, the IETF EDIINT work group has not worked on a standard for “S/FTP”.

4.5 Internet Web (HTTP: Hyper Text Transport Protocol)

4.5.1 GISB EDM

The Gas Industry Standards Board (GISB) is a voluntary, independent organization comprised of, and supported by, all segments of the natural gas industry. GISB is a non-profit, autonomous organization with three main goals:

- (1) Develop and maintain voluntary standards governing electronic communications for business transactions within the natural gas industry,
- (2) Serve as a forum for reaching market-responsive solutions, and
- (3) Enhance the reliability of gas service through easy access to information standards needed for critical business transactions.

The GISB business requirements call for tight bidding windows, transaction revisions and nomination deadlines. The move toward EDI in this instance required the preservation of the interactive nature of the electronic bulletin boards already in place while addressing the divergent user interface issues the bulletin boards created for shippers nominating to multiple pipelines prior to a daily nomination deadline. To meet these needs, GISB adopted a server-to-server based model using then available Internet-based tools. Use of the GISB data transfer mechanism model (EDM/Electronic Data Mechanism), which utilizes HTTP transport, has been mandated by FERC for interstate gas pipelines. Some states are also considering the use of the GISB Internet based data transfer model (EDM) for the retail electric marketplace. GISB EDM uses PGP 2.6.2 for encryption and digital signature. PGP 2.6.2 is not PKI compliant, utilizing a proprietary digital certificate (not the PKI X.509v3 standard certificate).

The “GISB Future Technology Task Force Pilot Team Report - September 17, 1996” sections 1 and 2 (Executive summary and Test Experience and Results) is included in the appendix as a reference for more details on the GISB EDM Pilot.

4.5.2 Potential Convergence of GISB EDM and IETF EDIINT AS2

The IETF EDIINT AS2 (HTTP) standard is in draft form and under development. Initial discussions between IETF, GISB and CommerceNet have begun in order to determine the feasibility of seeking a solution within the EDIINT AS2 proposed standard to provide inclusion and backward compatibility for the GISB EDM standard. Although discussions are underway,

Final – Version 1.0

no commitments at present exist between the groups to change or combine their respective standards into a single converged standard. Numerous benefits accrue to all parties if the convergence effort is successful. For example:

- Existing investments in GISB implementations will be preserved.
- The GISB EDM standard will have international and cross industry support via its incorporation in EDIINT AS2.
- There are GISB products available today in the marketplace.
- The EDIINT AS2 standard will, like GISB, utilize HTTP, removing the SMTP related concerns about the present EDIINT AS1 standard.

To summarize the potential value of this convergence, GISB EDM is a secure, mature and proven standard for exchanging mission critical business-to-business EDI transactions via the Internet. If the developing EDIINT AS2 standard can include the GISB EDM standard and handle backwards GISB compatibility, many of the concerns raised under both standards will be resolved.

4.6 Extranets

According to Deborah Bayles, in the book Extranets, an Extranet is defined as “an intranet that allows controlled access by authenticated outside parties. Typically an extranet will link the intranets of distributed organizations for the purpose of conducting business. This secure electronic consortium usually consists of an enterprise and its key trading partners, customers, dealers, distributors, suppliers, or contractors.”

One form of Virtual Private Network (VPN) technology utilizes encryption at the network layer to form protected “tunnels” between defined nodes on a network, thus allowing a “private network” to “virtually” exist over the Internet. The IETF IPsec Work Group was formed to standardize this technology for the Internet. Today interoperable software is available and has been successfully used to form EDI Trading Partner “Extranets” on the Internet. One such successful network in operation today is the automotive industry’s (AIAG) ANX Extranet. In order to be a part of the ANX, qualified trading partners must have ICISA (International Computer Security Agency) certified VPN software. Although this technology has been successfully implemented, initial pilot studies have shown the necessity of substantial trading partner financial and time investment in order to be successful.

Other protocols and technologies utilized to form secure Extranets over the Internet involve the use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to provide security at the session layer. Software and standards have been developed for Secure File Transport Protocol (S/FTP) and Secure HyperText Transport Protocol (HTTPS) that provide the transaction security necessary to achieve many of the benefits of a trading partner Extranet. Experience has shown that Extranets utilizing this technology have been formed in a cost effective manner conducive to attracting widespread SME (Small to Medium Sized Enterprises) involvement.

The UIG Internet EDI Work Group is actively investigating the possibility of the UIG forming an Extranet for the utility industry.

5. Guidelines for Data Transfer Mechanism Testing

Set forth below are the minimum proposed data transfer mechanism testing guidelines. The Subgroup acknowledges that further comprehensive EDI testing guidelines will need to be developed by the Testing and Training Subgroup.

Final – Version 1.0

In order to assure that specific implementations of the recommended data transfer mechanism are reliable and robust enough to handle peak traffic periods and larger than normal file sizes, testing between each pair of trading partners must be conducted prior to use in the actual business process of retail access. This testing should also be conducted whenever any trading partners significantly modify their existing data transfer mechanism infrastructure. The test plans should verify compliance with the critical success factors, discussed in Section 6 of this report, as described below.

5.1 Security

- Confirm that file integrity was not compromised (file content received was file content sent)
- Verify control totals on received file against sender's file control totals
- Determine that message is only readable by authorized individuals
- Send and receive encrypted files
- Confirm that contents are successfully decrypted
- Non-repudiation. Confirm that:
 - An acknowledgement of origin is generated, logged, saved and easily retrieved.
 - An acknowledgement of receipt is generated, logged, saved and easily retrieved.
 - A mechanism exists to highlight when an acknowledgement of receipt or origin is not received.
 - A means exists to verify that the sender and/or receiver is whom they profess to be
 - Verification that file sequence integrity has been maintained (i.e. FIFO, first in – first out)
 - Simultaneous receipt of files from multiple senders (could be multiple transaction 'sends' from the same sender or different senders)
 - Maintenance of processing order via transaction date/time stamps of receipt

5.2 Reliability

- Transmission medium and software work properly with minimum downtime.
- File set is received intact and complete.
- Transmission processing is completed with minimal interruptions.
- Transmission medium is stable.
- Transmission process can be automated, allowing minimal manual intervention.
- Accommodation of the following levels of acknowledgement:
 - Means to notify the receiver that the file was sent;
 - Means to notify the sender that the sent file was received correctly; and
 - Means to notify the sender that the file was not received correctly.

5.3 Performance

- Transmission medium works consistently under various conditions (i.e. different times of day, different volumes of data, critical time periods).
- Capability to send, receive and process representative amounts of data within a time schedule that successfully supports the business process.
 - Throughput - assure that files are sent and received with the necessary speed to process all transactions within the required schedule.

Final – Version 1.0

- Capability to send and receive files between multiple participants (one to many; many to one).

5.4 Recovery and Re-Transmission

- Confirm that a re-transmitted file matches the originally transmitted file, in both directions.
- Re-transmit files from each of the past five days.

5.5 Archiving and Auditing

- Confirm that a history of transactions, which are sent, delivered, and processed is available.

5.6 Interoperability

- Verify that trading partners are able to exchange files - both directions
- Transmit a file with the full ASCII character set in it to ensure that the receiving end properly interprets all characters - both directions.
- Successfully send/receive files to and from servers with different hardware & software configurations.

6. EDI Transport Technology Matrix

	Technology	Advantages	Disadvantages
1	SMTP (EDIINT/ S-MIME)	<ul style="list-style-type: none"> • Documented as Internet Draft ² • Commercial products have certified interoperability • Avoids need for server & firewall • X.509/PKI compliant ³ 	<ul style="list-style-type: none"> • No guarantee of timely delivery • Possible performance problems related to large file sizes – dependent on infrastructure • No data compression • SMTP “store-and-forward” allows for more “points of failure” for transport of EDI files
2	SMTP (EDIINT/ PGP-MIME)	<ul style="list-style-type: none"> • Documented as Internet Draft • Commercial products have certified interoperability • Avoids need for server & firewall 	<ul style="list-style-type: none"> • No guarantee of timely delivery • Possible performance problems related to large file sizes – dependent on infrastructure • Not X.509/PKI compliant • SMTP “store-and-forward” allows for more “points of failure” for transport of EDI files

² Standards such as EDIINT build on other standards that are listed elsewhere in this table but that are not repeated for the high-level standards. For example, EDIINT using SMTP is documented as an Internet Draft but builds on standard-level RFCs 821 and 822, draft/ proposed standard RFCs 1767, 1847, 1892, 2015, 2045 to 2049, and 2298, and informational RFC 2311.

³ References to PGP are to version 2.6 because this is the version incorporated in existing standards

Final – Version 1.0

3	SMTP/ S-MIME (RFCs 821, 822, 1847, 1891, 1892, 2045 - 2049, 2311)	<ul style="list-style-type: none"> • Low cost, easy implementation • Wide availability of low cost software • RFCs 821 and 822 are full Internet standards; RFCs 1847, 1891, 1892, and 2045 - 2049 are standards-track 	<ul style="list-style-type: none"> • No Message Disposition Notification (MDN) • Requires custom programming
4	HTTP Post (EDIINT/ S-MIME))	<ul style="list-style-type: none"> • Documented as Internet Draft • X.509/PKI compliant 	<ul style="list-style-type: none"> • Limited commercial implementation • No data compression
5	HTTP Post (EDIINT/ PGP-MIME)	<ul style="list-style-type: none"> • Documented as Internet Draft 	<ul style="list-style-type: none"> • Limited commercial implementation • Not X.509/PKI compliant
6	HTTP Post (GISB)	<ul style="list-style-type: none"> • Open standard, flexible implementation • Established for use in wholesale gas transactions 	<ul style="list-style-type: none"> • Distribution of PGP certificates (not X.509 compliant), no provision for other encryption methods • Complex setup
7	HTTP Post (SSL/ TLS) (RFCs 2068 & 2246)	<ul style="list-style-type: none"> • Widespread implementation • Standards-track RFCs 	<ul style="list-style-type: none"> • Turn-key implementations do not incorporate digital signature • Doesn't provide non-repudiation (MDN)
8	HTTP Put (SSL/ TLS) (RFCs 2068 & 2246)	<ul style="list-style-type: none"> • Currently used by PG&E, which has provided free client software 	<ul style="list-style-type: none"> • Nonstandard for EDI • Doesn't provide non-repudiation (MDN) • Doesn't provide digital signature of documents/files/transactions
9	HTTP Put/ Get (S-MIME)	<ul style="list-style-type: none"> • Simple implementation • X.509/PKI compliant 	<ul style="list-style-type: none"> • Nonstandard for EDI • Doesn't provide non-repudiation (MDN)
10	FTP (RFC 959)	<ul style="list-style-type: none"> • Full Internet standard • Widespread implementation 	<ul style="list-style-type: none"> • Security is not inherent (needs to be applied to files on server) • Allows non-encrypted user id and passwords
11	FTP (RFC 2228)	<ul style="list-style-type: none"> • Standards-track RFC • Kerberos-level security 	<ul style="list-style-type: none"> • Limited implementation
12	FTP/ SSL	<ul style="list-style-type: none"> • Documented as Internet Draft 	<ul style="list-style-type: none"> • Limited implementation
13	X12.58	<ul style="list-style-type: none"> • ANSI X12 Standard 	<ul style="list-style-type: none"> • Security mechanism, not transport
14	Extranet/ VPN	<ul style="list-style-type: none"> • Provides for security of file transfer 	<ul style="list-style-type: none"> • Method of interconnectivity, not a protocol that enables data transfer
15	VAN/ Service Bureau (as intermediary)	<ul style="list-style-type: none"> • Flexibility among protocols, because VANs can handle protocol conversion 	<ul style="list-style-type: none"> • Ongoing cost of service fees based on a per character charge (not bandwidth pricing as with the Internet)

Final – Version 1.0

7. EDI Transport Technology Comparison Matrix

ALTERNATIVE	SPAM susceptibility	Difficulty / ease of implementation	Certified interoperability	Avoid need for server and firewall	X.509 / PKI compliant	Provides data compression	Good performance with large file sizes	Guarantee of timely delivery	Provides MDN	Provides authentication and non-repudiation	Security is inherent	Ongoing cost: for sender, for receiver	Cost of entry scalable	High-level security (how should security be rated?)	Widespread implementation 1-5 (5=max)	Level of standardization for EDI 1-5
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
SMTP (EDHINT/ S-MIME)	Y	L	Y	N	Y	N	?	N	Y	Y	Y	L	Y	H	3	3
SMTP (EDIINT/ PGP-MIME) not implemented in products	Y	L	N	N	N	Y	?	N	Y	Y	Y	?	?	H	0	0
SMTP/S-MIME	Y	L	Y	N	Y	N	N	N	N	Y	Y	N	N	H	5	1
HTTP Post (EDHINT/ S-MIME AS2)	N	L	N	N	Y	N	Y	Y	Y	Y	Y	L	Y	H	1	1
HTTP Post (EDHINT/ PGP/MIME)																
HTTP Post (GISB)	N	H	N	N	N	N	Y	Y	Y	Y	Y	L	Y	H	3	2
HTTP Post (SSL/ TLS) (RFCs 2068 & 2246)	N	M	N	N	Y	N	Y	Y	N	Y	Y	L	Y	H	2	4
HTTP Put (SSL/ TLS) (RFCs 2068 & 2246)	N	M	N	N	Y	N	Y	Y	N	Y	Y	L	Y	H	2	4
HTTP Put/ Get (S-MIME)	N	M	N	N	Y	N	Y	Y	N	Y	Y	L	Y	H	2	4
FTP (RFC 959)	Y	L	Y	N	N	N	Y	Y	N	N	N	L	Y	L	4	3
FTP (RFC 2228)	Y	L	Y	N	N	N	Y	Y	N	N	N	L	Y	L	4	3
FTP/SSL	Y	L	Y	N	Y	N	Y	Y	N	Y	Y	M	Y	L	4	3
X12.58	N	M	Y	N	Y	Y	Y	N/A	N	Y	Y	M	Y	Y	3	5
Extranet/ VPN	Y	H	Y	Y	Y	N	Y	Y	N	Y	Y	M	Y	Y	3	5
VAN/ Service Bureau (as intermediary)	Y	L	Y	Y	N/A	N	Y	Y	Y	Y	Y	H	Y	Y	Y	Y
VAN/ FTP from Internet	Y	L	Y	Y	Y	N	Y	Y	Y	Y	Y	H	Y	Y	Y	Y

APPENDIX I

Additional Information

A. Traditional VAN EDI

In today's global economy, businesses need to remain competitive. In order to accomplish this, the need to re-evaluate the way business is conducted is essential. With the growing popularity of the Internet and computers on every desktop, businesses are looking for new approaches to integrate their current EDI technology with the ease of use of the Internet.

Traditionally, the exchange of electronic information is provided by a service or system called a VAN (Value Added Network). The VAN enables the transfer of electronic information through the use of communication protocols and line speeds that are compatible to different systems. The VAN uses a secure "store-and-forward mail boxing system" to manage all transfer of information from the sender's mailbox into the receiver's mailbox. VANs can ease the process of exchanging the electronic information by providing services that become an asset to the users of EDI.

- **Access:** Depending upon the VAN, many different access methods are used such as dial-up, toll-free lines, Internet/Intranet, satellite, leased line, frame relay, ISDN, and Internet Browser.
- **Communication Exchange:** The majority of VANs provide the ability to exchange data between other VANs, VABs and ADMDs both domestically and internationally. In addition, there are gateways to Proprietary e-mail in place for RFC 822 standard, Internet, Microsoft Mail, cc:Mail, Notes, Novell MHS, DEC, Office Vision, HP, and MS Exchange
- **Communication Protocols:** Multiple transport options such as SMTP, S/MIME, HTTP, SSL, POP, MAPI, and TCP/IP are available.
- **Communications Audit Trail:** This provides the trading partners with a log detailing the transmission of each interchange. The trail includes times, dates, identifiers, acknowledgments, errors encountered, etc.
- **Compliance Checking:** Standards and IC compliance checking are available through some of the VANs.
- **Digital Signatures:** The VAN provides the ability to use digital signatures that cannot be opened except by the recipient.
- **Encryption:** Depending on the VAN selected; various encryption options are available such as RSA, DES, RC2, MDS, AUTACK, X.509, SSL, and NT.
- **Security:** The VANs provide secure message management for Internet, enabling EDI and non-EDI communication. Various data securities such as data encryption, Public

Final – Version 1.0

Key, Private Key, DES, Message authorization, G-2 level, Firewalls, User authentication, S/MIME, and PKI may be available.

- **Standards:** VANs support many standards including ANSI X12, UN/EDIFACT, WINS, VICS, TDCC, Tradacoms, Odette, NACHA, SWIFT, GENCOD, UCS, SEDAS, and ELFE.
- **Support:** By subscribing to a VAN's service, knowledge and expertise with ANSI X12 and EDIFACT is provided. Moreover, many VANs provide training, support, and documentation.
- **Volume:** VANs provide the ability to manage high volumes of transactions from a diverse amount of trading partners.
- **Additional Benefits:** Many VANs provide on-line services such as Tier1/Tier 2 Supply Chain, document conversion, Internet access, bulletin boards, on-line directories/catalogs, Java-based Web EDI, electronic forms, and imaging on the Internet.

However, this clearinghouse for electronic transactions provides these value-added benefits not without a cost to the trading partners.

- **Access:** If a telephone line or the VAN's network is down, transactions are not received or sent. Although most VANs provide a toll free number, some VANs that require trading partners to make long distance calls.
- **Communication Exchange:** Some VANs are not interconnected; therefore, the software must be capable of communication to multiple VANs. Moreover, some of the trading partners may not be using a VAN service, resulting in the user's EDI system being able to support a direct connection.
- **Networking Complexity:** With EDI, a large investment in computer networks is needed for the telecommunications capability.
- **Price:** VANs are known for their high initial startup cost, software cost, transmission cost, and annual maintenance cost. Subscribers normally pay per-transaction charges and a pro-rated charge based upon data volume. If additional resources are needed, the VAN provides consultants based upon various fees.
- **Proprietary Software:** Some VANs require that the users use their proprietary communications software.
- **Standards:** Currently, there are no set standards for communication between VANs. Therefore, a script that is developed for one VAN may not work with another VAN.
- **Usability:** Maintaining the translators can be cumbersome and restricting.

As businesses begin to look at other alternatives apart from the VANs, Internet EDI may offer a cost-effective and easy to use solution. Through the use of Web browsers, the user is provided an easy to use interface that converts the HTML (HyperText Markup Language) into the EDI format.

Final – Version 1.0

- **Flexibility:** The ability to exchange documents during business and non-business hours
- **Cost:** Reduced business transaction cost

B. WEB EDI

There are many ways to send EDI over the Internet. One can use Browsers like Netscape or Microsoft Internet Explorer and send (push) files as e-mail attachments. More security can be achieved by using WEB forms to send files using HTTP/HTML. One can use FTP and “post” or put your files to a server or a URL. One can also use dedicated Gateways or public ISP Gateways. The methods are incredibly varied. Part of the purpose of this white paper is to begin to explain the various systems with their advantages and disadvantages.

The cost benefits and speed of using the Internet for transmission have to be weighed against the cost of added systems, both hardware and software, that must be added to provide the necessary security and data management requirements. Also, once the system is in place, interoperability becomes an issue. Will another trading partner’s system be able to recognize, validate, and receive/retrieve data sent using an Internet solution? Standards, once established, would alleviate this problem of being able to communicate with one another.

TCP/IP and HTTP, the standard protocols for the Internet today, were not designed to offer secure communication services. The problem for WEB EDI then becomes how to protect the privacy of communications in store-and-forward applications such as email and in real time applications such as the data flowing between a Web client and a Web server.

Cryptography technology is one solution embodied in industry-standard protocols such as SSL (Secure Sockets Layer), SET (Secure Electronic Transactions) and S/MIME (Secure Multipart Internet Mail Encoding). These standards provide the foundation for a wide variety of security services, including encryption, message integrity verification, authentication and digital signatures. These methods and their application will be addressed in another section of this paper.

For a real education on the topic of EDI over the Internet, the following documents are recommended reading:

Gas Industry Standards Board Electronic Delivery Mechanism Related Standards
www.gisb.com

AIAG Guideline for Electronic Commerce Message Routing on TCP/IP Networks
www.aiag.org

Secure AS/400 Transactions over Intranets and the Public Internet
<http://www.inetmi.com/products/whitepg.html>

B.1 WEB EDI DICTIONARY

Final – Version 1.0

Digital Signature - Binds a document to the possessor of a particular key and is the digital equivalent of a paper signature.

CGI - Common Gateway Interface.

FTP - File Transfer Protocol is used to transfer files from one system to another across an IP network.

HTML – Hypertext Markup Language

HTTP - Hypertext Transfer Protocol has immediate request and response capabilities for documents that are time-sensitive in nature and require immediate acknowledgement of receipt.

EC - Electronic Commerce

MAC - Message Authentication Codes

MIME - Multipurpose Internet Mail Extension. MIME permits the identification and concatenation of message parts (called body parts) into a single message that can traverse the Internet using one of the application level protocols (like HTTP).

Push technology – A method of communicating transactions, which involves automating delivery of electronic documents to the receiver as they become available rather than storing them at the sender's facility until the recipient initiates a session to obtain them. SMTP and FTP can be used in a push model. Pull technology requires the receiver to access a URL or server to retrieve the posted documents.

Public Key - A method of cryptography whereby each person gets a pair of keys, a public key and a private key. Each person's public key is published, while the private key is kept secret. The sender encrypts using the public key of the recipient, and the recipient decrypts using the recipient's private key.

Public Key Certificates - Also called digital certificates, digital IDs, digital passports, or public-key certificates, they are defined by an ITU standard called X.509. An X.509 certificate is a small file that contains information on the owner of the certificate, the issuer's name, the owner's public key (512-bit RSA key), the issuer's digital signature (RSA encryption, not human readable), the validity period, and the serial number.

RSA - Rivest, Shamir, Adleman. A type of data security

SET - Secure Electronic Transactions, a security protocol that uses public and symmetric-key algorithms.

SME - Small and Medium Enterprises

S/MIME - Secure Multipart Internet Mail Encoding, uses public and symmetric-key algorithms for encrypting and signing email messages in a store-and-forward mode.

SMTP - Simple Mail Transfer Protocol. A mail protocol (push technology) that can be used by most Email software for sending and receiving messages for situations in which a store-and-forward scenario is required due to dial-up connections or other non-persistent links to a network.

SSL - Secure Sockets Layer. A SSL handshake includes exchange of client and server certificates and corresponding signatures.

Web Form - an application format for enveloping transmission of messages or files over the Internet. Methods include HTML. Anyone with a Web server for publishing HTML documents can create forms, since the form definition tags are just HTML tags. There are many companies offering forms generators. For a tutorial on Web Forms go to

Final – Version 1.0

www.webcom.com/html/tutor/forms/intro.shtml

TCP/IP - Transmission Control Protocol/Internet Protocol, a common standard for transport of electronic information

XML - Extensible Markup Language, offers a mechanism that allows data to be transmitted with human-readable semantics

C.1 GISB EDM – Secure EDI over the Internet

The Gas Industry Standards Board (GISB) is a voluntary, independent organization comprised of, and supported by, all segments of the natural gas industry. The GISB mission is to take the lead in developing standards across the industry to simplify and expand electronic communication, and to streamline business practice. Industry participants are encouraged to exceed minimum standards through provision of value-added services and customized arrangements.

The Gas Industry Standards Board business EDI requirements call for tight, time-sensitive bidding windows, and scheduling requires that all demand be known, hence demand requirements must be in place before scheduling can occur. GISB's adoption of EDI required the preservation of the interactive nature of the electronic bulletin boards (EBBs) already in place, while addressing the divergent user interface issues the EBBs created for shippers nominating to multiple pipelines prior to a daily nomination deadline. Rather than implementing costly real-time EDI systems, GISB instead adopted the GISB EDM (Electronic Delivery Mechanism). The GISB EDM is a server-to-server based model using Internet based tools.

The following are some key technical aspects of the GISB EDM:

- Original purpose of GISB EDM: Transport EDI X12 and other business transaction formats securely and reliably over the Internet
- Requirements: Need to address authentication, integrity, non-repudiation; guaranteed delivery of data; binary and arbitrary data sizes sometimes > 100MB; immediate reporting of errors; interoperability across industry; meet time sensitivity requirements
- Time synchronization: Time-stamping important, e.g., to “prove” that a transaction was received before a deadline
- Technical requirements: Must be implemented with off-the-shelf browser; must use Internet; must be firewall-friendly; HTML-based real-time acknowledgement; must use RSA public key crypto system; must be compatible with PGP 2.6; time synchronization with NIST; clear error reporting; follow RFC 1867 (now 2388) = multipart/form-data MIME type; support for interactive and batch modes
- Redundancy: Due to the fact that the files are pushed from the sender directly to the receivers' server, redundant servers are in many cases implemented in order to ensure that transactions are not lost

As a result of deregulation, some states (PA, Maryland, New York) are evaluating the use of the GISB Internet based data transfer model as an alternative to the VAN for the retail electric utility marketplace. While GISB EDM has been recognized for implementing standardized EDI files, which addressed long-standing user interface issues created by the EBBs mandated by the FERC, the applicability of the data transfer mechanism to the deregulated electric industry has not been assumed.

Final – Version 1.0

The following are the key drawbacks and advantages of the GISB EDM, which have been noted by participants studying the applicability of the transfer mechanism to electric industry use:

Drawbacks:

- Lack of broad vendor support
- Issues related to PGP/RSA licensing: platform support, single source vendor
- Undetermined costs
- Only in use in the gas industry, limiting opportunity for broader electronic commerce use
- Non ANSI X.509 compliant security certificate management scheme with no external authority option (potential resolution with PGP 6.0)

Advantages:

- Open architecture
- In production 2+ years
- Standards-based, rather than product-specific solution
- Specifies use of HTTP protocol, which may offer more robust support of transfer of large-sized files, as are expected to be exchanged between electric distribution companies and generation suppliers per deregulation
- Use of positive acknowledgements

Potential Convergence of GISB EDM and AS2

Initial discussions have begun to determine the feasibility of seeking a solution within the IETF's EDIINT HTTP AS2 draft standard that may provide inclusion and backwards compatibility for the GISB EDM standard. This EDIINT HTTP AS2 converged standard is in draft form and under development. There are no commitments at present between GISB and the EDIINT group to change their standards or combine their standards into a single converged standard.

There are numerous benefits for all parties if this effort is successful. For example:

- Existing investments in GISB implementations will be preserved
- The GISB standard will have international and cross industry support via its incorporation in EDIINT
- There are GISB products available today in the marketplace.
- The converged standard will, like GISB, utilize the HTTP protocol, thus removing the SMTP-related concerns about the present EDIINT standard

Associated issues, constraints, concerns with convergence:

- Numerous GISB implementations are in production which are used daily and cannot be simply “thrown away”.
- The installed GISB base is not motivated to change; functionality must be extended without adversely impacting standards and interoperability.

To summarize the potential value of this convergence, the GISB EDM is a secure, mature and proven standard for exchanging mission critical business-to-business EDI transactions via the Internet. If the developing EDIINT HTTP AS2 convergence can incorporate the GISB standard and handle backwards GISB compatibility, many of the concerns raised under both standards will be resolved.

C.2 GISB Future Technology Task Force Pilot Team Report

Final – Version 1.0

1. Executive Summary

The pilot test of GISB Future Technology Task Force (FTTF) standards was accomplished in two Phases. Phase I, complete as of July 26, 1996, addressed basic Internet connectivity and performance along with HTTP (HyperText Transport Protocol) protocol functionality. Phase II, ending August 14, 1996, was designed to test the security architecture and to refine procedures for implementing and administering public key cryptography for secure electronic commerce. A set of standard test files was created to simulate nominations transactions of various sizes. These files were used by all parties throughout both phases of the test.

In Phase I, six companies provided server facilities for receiving transactions via the Internet. Eight companies participated as transaction senders, including the six receivers. Approximately one month was required for the participants to develop, install, and test the basic client and server components targeted for the first phase. This process was facilitated by information sharing between companies. Most of the difficulties encountered were the result of local environmental constraints and differing interpretation of the GISB FTTF specifications. This afforded the opportunity to further refine and document the standards and related implementation procedures.

In Phase II, the same six servers were used, however there was one additional company posting transactions. HTTP basic authentication or realm security and PGP public key encryption with digital signatures were added to the architecture model that was tested in phase I. An additional month was necessary to add these features.

Throughout the testing the performance of the HTTP protocol and the public Internet infrastructure remained reliable and consistent. Minor variances were experienced; these are not significant for the transaction volumes expected by the industry. Performance of peak transaction loads during the nomination deadline period appeared acceptable. However, it must be pointed out that universities are a significant segment of the Internet user community, and all testing to date has been conducted during the summer recess. Continued implementation work by the task force will ensure that the impact of Internet traffic patterns is properly documented over a longer period of time.

Limited concurrency tests were conducted in which the effect of single input from a large number of trading partners was simulated by repeated simultaneous transmission of test files from the nine test participants. The role of receiver was rotated to allow for verification of this scenario against different platforms and configurations. Based on this testing, it is anticipated that today's public Internet and current commercially available server technology can handle projected transaction loads. Scaling the environment to handle an actual volume of business will be the responsibility of the individual companies during implementation. The architecture selected by the FTTF is extremely flexible. For a small company an average desktop computer might be adequate whereas a large corporation would need an industrial-strength server. Scalability, along with the fact that Internet access and related technologies have become a commodity, makes the solution accessible to large and small companies alike.

2. Test Experience and Results

2.1. Issues

2.1.1. Participation and Industry Involvement

Participation in the pilot test was less than anticipated and involved mostly pipelines and third party providers. Because of the time constraints on completing the proof of concept for the architecture, significant segments of the industry declined to participate. However the participation and intensity of testing were sufficient to prove the viability of

Final – Version 1.0

the technology. The concurrency testing that was conducted simulated high data volumes from a small number of participants. While this demonstrated the ability of the Internet and the receiving site to handle a significant amount of data in a specific time period, the transaction arrival patterns will necessarily differ in a real-world production environment. This may present other concerns that did not arise during the test. However, those issues are most likely to involve a single site's specific implementation rather than the performance of the Internet and its protocols.

2.1.2. Technical Skill Requirement

The companies which implemented the HTTP client and server components for the pilot test assigned dedicated Information Technology staff members to the pilot project. It took approximately two months for those companies to develop those components to the point where they could provide all the functions required for the test. All participants needed a high level of understanding of Internet technologies, and frequent communication was necessary to exchange site-specific information. Certain issues arising from differing interpretation of the standards frequently had to be worked out between individual participants. For this reason, the solution proposed by the FTTF is not considered to be a trivial implementation. However, it is the objective of the pilot test team to standardize and document the technical details so that the industry can implement the solution more easily.

2.1.3. Impact of Internet growth

The current rate of growth in Internet access has prompted industry watchers to make dire predictions about the lack of adequate transmission capacity in the future. Today, telecommunications providers are upgrading their backbone networks to ensure that this capacity will remain available. With the development of multimedia applications and the entry of cable TV companies and others into high bandwidth data services, there is great commercial incentive for new providers, protocols, and technologies to extend the infrastructure. This process is expected to continue as demand escalates. It is recognized that this growth will not be entirely smooth and may at times have business impact. At this time, however, the growth of Internet use appears to present no risks greater than those associated with today's methods of communication using VANs (Value Added Networks) and proprietary EBBs. Implementers of GISB standards are expected to design their processing environments to provide a level of redundancy and fault tolerant appropriate to business needs.

2.1.4. Bi-directional Communications Capability

The HTTP file upload model implemented by the FTTF requires all trading partners to function as both a client and a server. The client component initiates the upload of the transaction dataset and the server is required in order to receive any transactions including functional acknowledgments. Maintaining a dedicated server on-site may entail considerable expense, which has given rise to many questions about the cost of installing and supporting the solution for small companies. The FTTF's mission has been to define and validate an open architecture for the electronic delivery of transactions. As such, the task force cannot presume to determine the cost to an individual company to implement the solution. Nor can the task force anticipate factors that might influence a company's selection of specific platforms for implementation. However, FTTF will identified a number of options for both client and server configurations and will provide detailed explanations of the alternatives in the implementation guide.

2.1.5. Server Side Software Development

All server implementations require a custom-written program using the Common Gateway Interface (CGI) or other Application Programming Interface (API) to store the

Final – Version 1.0

uploaded file and to format and return the HTTP response. During the testing, several versions of this processing program were created for a variety of computing platforms using a number of programming languages. The fruits of this effort are a library of programs that could be made available to the rest of the industry as a starting point for implementation. However, this code would be distributed without warranties of any kind.

2.1.6. Custom Software Requirement for Fully Automated Batch Client

The original objective of the FTTF was to select technology that could be implemented using commercially available shrink-wrap software. While the file upload can be manually invoked with a standard, off-the-shelf World-Wide Web browser, the FTTF adopted a working assumption that it should be possible to initiate the transmission in an unattended, automatically scheduled batch mode. As of the time of the pilot test, this required the development of custom software or modification of readily available, public domain programs. During the testing, several versions of this "batch browser" were created for a variety of computing platforms using a number of programming languages. The fruits of this effort are a library of programs that could be made available to the rest of the industry as a starting point for implementation. However, this code would be distributed without warranties of any kind.

2.1.7. Single Points of Failure

A dedicated connection to the Internet is potentially a single point of failure that can cause a site to become inaccessible due to an outage caused by the Internet Service Provider or telecommunications provider. Redundant dedicated connections are an expensive proposition, although dial access to the Internet is a readily available and inexpensive commodity. Individual companies must weigh cost and benefits of providing alternate access. It is expected that communications procedures and alternatives will be detailed in the trading partner agreement.

2.1.8. Internal Network Security

Any connection to the public Internet mandates tighter network security for an organization as a whole. The FTTF proposed standards state that this is a site specific issue, since it depends on a company's own network use policy as well as the way in which a site is connected to the Internet. However, because of these differences, it is expected that those sites employing firewall machines to protect their internal networks will have to coordinate closely with trading partners to work out configuration details for the HTTP protocol and socket numbers that may affect transmissions.

2.1.9. Increased Security Administration

Coordination of security measures such as HTTP Realm I Security (also referred to as Basic Authentication) and PGP (Pretty Good Privacy) encryption keys will require administrative overhead beyond that which is needed for the current EDI trading partner arrangements using VANs. A common industry "trust model" is desirable to assure authenticity of transactions and verify the identities of trading partners. In order to fully implement a trust model for electronic commerce, the industry should utilize an external authority that will certify PGP keys. At this point in time there is no commercial source for this service. Until such source is available, the industry should develop a process that includes self-certification of keys. At a minimum, key exchanges should be handled directly between individual trading partners. This is the recommendation of the EDI working subgroup of the Internet Engineering Task Force (IETF), an international body which sets standards for Internet services and protocols.

2.1.10. Security Management using Third Party Providers

Companies may elect to use third party providers as their "designated site" for EDM

Final – Version 1.0

transactions. According to this definition, transmissions handled by the third party on behalf of the company will follow the FTTF standards, but the back end interface between the company and the third party is outside the scope of the standards. Thus it will be necessary for the company and the third party to define roles and responsibilities regarding data transfer, encryption, digital signatures, and security management.

2.2. Progress and Expectations

2.2.1. Performance of Transmission via the Internet

The public Internet infrastructure with existing traffic loads successfully accommodated transmission of several megabytes of nominations transactions during the concurrency test in the 10 minute interval from 11:20-11:30 Central Clock Time (CCT). This time period was chosen because it represents both a peak activity time on the Internet and the daily nominations deadline under the GISB standards. This will allow companies to meet the nominations and confirmations deadlines based on anticipated volumes as indicated by responses to the pilot test survey. Each individual company must scale its Internet connection and processing environment to provide sufficient capacity to meet the deadlines. Ongoing efforts of the Implementation Team will be aimed at further evaluating the impact of performance factors such as university-related traffic and the long-term growth of Internet use.

2.2.2. Timeline for Implementation

It is reasonable to expect that the industry will be able to implement the proposed FTTF standards for data transmission via the Internet by the target dates identified in FERC Order No. 587. The FTTF will publish detailed specifications for the HTTP request and response formats as part of an implementation guide designed to assist the industry.

2.2.3. Clarification and Refinement of Standards

The communications methods and formats were selected because of their flexibility and portability as open standards. It is expected that these standards will be well-positioned to evolve with changes in technology and business practices. The FTTF and the Pilot Test Subgroup developed and published clear specifications of the required formats for the pilot test. Nevertheless, several incomplete and inaccurate implementations surfaced during the test. The FTTF must therefore design its implementation guide to specify all details of the architecture and its data elements in a way that cannot be misinterpreted. It will be critical for all companies adopting the standards to follow the specifications exactly.

2.2.4. Site-Specific Decisions

Successful use of the public Internet for data transmission depends heavily on the way in which a company interfaces with the Internet; specifically, the use of a reliable Internet Service Provider (ISP), the proper selection and sizing of hardware and software components, and the implementation of appropriate security measures.

2.3. Conclusions

2.3.1. Reliability of Public Internet and HTTP Protocol

Test experience indicated that the Internet and the HTTP protocol were reliable for the delivery of X12 transactions during the entire test period. The overall transaction error rate, exclusive of problems related to initial startup, was 1.4%. It should be noted that errors caused by program defects that were identified and fixed during the test period were not included in this figure. Of those that were reported in the final statistics (see the error transaction chart under Test Results from Phase II, Summary by Client and Server), the majority appear to be related to the method that was used to simulate

Final – Version 1.0

multiple concurrent transmissions from different trading partners and would not occur in a production environment. This level of reliability is considered comparable to those of current EBB communications and VAN based EDI.

2.3.2. Implementation Time Frame

It is reasonable to assume that the industry should be able to implement the FTF solution in the required time frame even though this will not be a trivial task.

2.3.3. Cooperation and Communication During Implementation

Successful implementation of the EDM architecture requires a great amount of direct communication between individual trading partners. In this respect the current effort parallels the industry's initial implementation of EDI.

2.3.4. Scalability

The architecture proposed by FTF can be implemented using a variety of configurations ranging from a desktop workstation to a multiprocessing server. During Testing, the client component ran on desktop PC and server alike. A wide range of server platforms was used for the pilot test. For the server component, it possible to provide the "designated site" HTTP server through an ISP or external web hosting company. The standard web browser client was tested repeatedly during the pilot using a 486 PC. Server implementations with a 486 PC would only handle a very small transaction load. Memory appeared to be a limiting factor, especially on the server. The scenario of using an ISP hosting service for the server component has not yet been tested, but is targeted as one of the next activities for the Implementation Subgroup.

2.3.5. Strategic Aspect of FTF Standards

The technologies chosen by FTF and the work accomplished by the pilot test team have laid the groundwork for the next phase of standardization in the gas industry. HTTP and World-Wide Web technologies can be employed to make information available in formats other than ANSI X12 and can be used to develop interactive applications. Companies that are using web servers today for a corporate Internet presence can implement the FTF architecture with minimal additions to existing infrastructure. Those who are considering such a presence should be able to share the resources installed for this implementation with other business functions.

2.3.6. Need for Further Refinement and Testing

Because of the short period of time allowed for the pilot test, a number of procedural items have not been completely defined. For these items, the Pilot Test Subgroup has adopted a set of "working procedures" that have been used during the test phase but are not recommended as part of the final implementation. Further experience with the architecture will be needed to refine those procedures and document them in the implementation guide. Additional standards may be proposed to the FTF and Business Practice Subcommittee (BPS) if necessary.

2.4. Recommendations

2.4.1. Implementation Subgroup

The Pilot Test Subgroup recommends that further deployment of the architecture proceed continuously as the industry moves towards a production implementation. The Pilot Test Subgroup would be chartered as an Implementation Subgroup which would immediately address the following goals:

1. Involve other participants to benchmark the proposed FTF implementation guide.

Final – Version 1.0

2. Establish a common process for PGP key certification.
3. Develop a set of procedures for PGP key distribution and maintenance.
4. Test the interfaces with X12 translation and identify related implementation issues.
5. Develop a cost and technology model for using a dial-up ISP account to establish a “designated site” as defined in the GISB standards.

2.4.2. Implementation Assistance

The FTTF should identify a strategy for assisting the industry with the technical aspects of implementation. The Implementation Subgroup would be a primary resource for such assistance. The creation of private newsgroups, and scheduled conferences and training sessions under GISB auspices is being pursued.

2.4.3. Refinement of Formats and Standards

Several changes to the FTTF's HTTP transaction formats have been considered by the Pilot Test Subgroup as a result of test experience and were accepted the FTTF at the meeting on August 20, 1996. These changes are intended to add functionality and flexibility to the architecture. Any changes which affect the proposed BPS standards must be returned as comments to the BPS standards prior to September 5, 1996, so as to be incorporated for the Executive Committee vote on September 12-13.

D. “PGP” or “PKI”?

Today's EC/EDI Manager/Coordinator is faced with a formidable decision in choosing the software to provide transaction security and reliability over the Internet: “Should I select PGP or a PKI based product for encryption and digital signature.”

What is “PGP”?

PGP is an acronym that stands for “*Pretty Good Privacy*”. It is a software product, developed by Phil Zimmerman about seven years ago, that provides encrypted security, authentication, and integrity for computer files and messages. It has been used by millions of Internet users and is to this day, legally free for non-commercial use.

What is “PKI”?

PKI stands for “*Public Key Infrastructure*”, a term used to collectively describe all the parts of a security structure that is enabling Electronic Commerce and Electronic Data Interchange over the “mother of all mothers” open public network - the Internet. It is being used today for virtually all Internet World Wide Web secure transactions and most Internet EDI exchanges. It is strongly based on X.500 and X.509 standards for Public Key Certificates and Directory Services.

Before going further, some background information on security and encryption technologies will prove helpful.

What are the Security Requirements for Commerce?

There are five fundamental security concepts with requirements that must be understood and must be adhered to in order for commerce to take place, electronic or not:

1. Confidentiality - information is not revealed to those unauthorized

Final – Version 1.0

2. Authorization or Access Control - only authorized entities can view or modify the protected information
3. Integrity - altering of data can be detected allowing for voiding of the transaction or information
4. Data Authentication - proof is readily available showing the origin of the information or transaction
5. Non-repudiation - provides proof that every entity that was originally part of the transaction cannot deny being a party to the origination or receipt of the transaction

Everybody can think of ways these requirements have been met in the paper world of manual transactions, but how do we do it electronically? Encryption technologies have provided the answer to this.

Encryption Technology provides the answers for Secure and Reliable EC

Encryption technology can provide all the five requirements for secure electronic commerce and forms the basis of the PKI. The basic encryption technology found in PKI is found in the product PGP.

Encryption technology can be classified into two categories:

1. Symmetric Cryptography - the same key (this key is like a password) is used to encrypt and decrypt. This was the only method widely available in the 1970's when DES (Data Encryption Standard) became popular and a standard. The major problem with this method is that you must distribute the single key to the encryption to all parties of the transaction. This key distribution is in itself a risky procedure. An unauthorized party intercepting the symmetric key would have the ability to decrypt any information encrypted with this compromised key.
2. Asymmetric Cryptography - also known as "public-key" cryptography, uses key pairs, "public" and "private". This is the technology basis for PKI. An algorithm operating in a software program generates this pair of keys. The private key is held in a secret secure file that is protected with the owner's password or "passphrase". The corresponding public key is freely distributed to any that wish to use it to encrypt data meant for the public key's owner.

The advantage of Asymmetric Cryptography's public key distribution is obvious. However, Symmetric Cryptography has a 10-20X-speed improvement and processing advantage over Asymmetric Cryptography.

Both PGP and PKI based products employ both these technologies in optimizing the design and function of their products. PGP, like PKI products, utilize Asymmetric Cryptography to encrypt and protect a one time randomly generated symmetric key. This symmetric key is used to encrypt and decrypt the bulk of the data. The only data that receives the Asymmetric encryption is the part that contains the Symmetric encryption key. The decryption process is initiated when the receiving party uses their private Asymmetric key to decrypt the Symmetric encryption key, which in turn is used to decrypt the entire bulk of the message or encrypted data. The Symmetric key, to reiterate, is only used once and is generated by a random process.

It is this random process that generates the single use symmetric key that has proven a challenge to the software manufacturers. If the generation of this symmetric key is not very close to random then the software leaves a huge hole for hackers and cryptanalysts to exploit. Non-random generation of this key means it

Final – Version 1.0

becomes much easier to “guess” and to have the encryption broken by “brute force”.

“Brute Force” attacks on encryption are very common and merely consists of trying each bit combination that could make up the key that will “unlock” the decryption. This is analogous to trying combinations on a safe until you guess the right one that unlocks the safe.

PGP has been around for years and no problems have been found with PGP’s random selection of the single use symmetric key for the “bulk encryption” of the messages or data. PKI products, however, are mostly newer and not as proven as PGP. Netscape’s early history of their application of PKI is a good example of how logic flaws in this area can cause security problems.

PGP gets the nod here for long-term proven reliability.

Digital Signature

The public key's owner uses the corresponding private key of the "public key pair" to generate "digital signatures" on data that must have authentication, integrity, and non-repudiation. Anyone that has the public key of the digital signature originator can perform a "check" using the appropriate computerized encryption algorithm. This signature check can be done by anyone, anytime and will confirm the authentication, integrity, and non-repudiation of the data or transaction.

An understanding of how integrity is insured with the digital signature is only developed through an understanding of the digital signature process.

The first step in the digital signature process is the application of a “hash function” to the bulk of the message or data that will receive the digital signature. This hash function will calculate a fixed length “hash total” that is also called a “Message Integrity Check (MIC)” or a “Message Digest” for the message or data. This binary number is fixed in length, always being the same length regardless of the size of the message or file. Some common hash functions are:

- MD5 (Message Digest 5) function that produces a 128 bit hash value
- SHA (Secure Hash Algorithm) is a 160-bit hash. Considered more secure than MD5
- MD2 & MD4 are earlier versions of MD5, both considered less secure than MD5 and SHA

This “hash” number is protected inside the digital signature process by encrypting it with the originator's asymmetric private key. The only way to decrypt this number is to apply the originator's public key to the encryption algorithm. Before doing this, however, the receiver of the message or data will calculate (automatically through software) a hash total on the data that has been received. Then the decrypted hash number is compared to the receiver's calculated hash number. If the two are the same, then the software will indicate a successful digital signature check. Integrity of the message or data is insured, as well as the authentication of the identity of the sender.

PGP and PKI based products are almost identical in their application of Digital Signature, and I do not view one as being better than the other.

Final – Version 1.0

Digital Certificates

Digital Certificates have been likened to "driver's licenses for the Information Superhighway". They are an integral part of PKI, without which there would be chaos in PKI based electronic commerce. Think of the chaos we would have if we did not have a licensing system for automobile drivers - the same level of chaos would exist in electronic commerce if we did not have the concept of Digital Certificates. A digital certificate is simple in concept and structure - it ties the identity of an individual to the individual's public key and is made available to the participants in the PKI. This identification information is secured in the Digital Certificate by a trusted third party's digital signature on the Digital Certificate. This trusted third party is known as a "Certificate Authority".

It is in this area of Encryption technology that PGP and PKI products differ the most. PGP relies on a so-called "web of trust" and not on a designated "Third Party" to provide this signature and guarantee of identity to the public key.

Also, in PKI, the Digital Certificate format has been formally specified in the "X.509" standard, while PGP does not have a standard linked directly to its digital certificate format.

The X.509 standard is extremely important since all software security products that follow it can utilize the same certificate no matter who the manufacturer is. This means that a person need only have one X.509 certificate for all transactions and for all software used now and in the future.

Also, with the latest enhancements to the X.509 standard, it is now possible to include biometrics in the certificate. Biometrics is an important addition for future Electronic Commerce transactions that require stringent high-level authentication.

Certificate Authority

A Certificate Authority (CA) in the PKI structure issues digital certificates, verifies digital certificates, and revokes digital certificates. The revocations are handled through maintenance of a Certificate Revocation List or "CRL". The CA must be trusted and reliable with its certification coming from a higher level within the CA hierarchy. State governments around the US are just now formalizing the Public Key Infrastructure CA hierarchy and corresponding regulations. Leading the way is California's Digital Signature Law and Regulations (see <http://www.ss.ca.gov/digsig/regs.htm>) .

Again, PGP differs greatly from PKI products in this category. The certificate authority for PGP products is an informal, non-standardized function left entirely up to the users of PGP to implement.

Directory Services

One problem facing both PGP and PKI based security products is the distribution of the Public Key Certificates to any qualified parties that wish to interchange data with another.

To be effective the public keys (in X.509 certificates) should be easily and readily available to those who need to initiate a "trading partner" relationship.

Final – Version 1.0

Directory Services offer the answer. With a Directory Service available, one can simply query the Directory Service for all the information required for communication with another party. This includes, of course, obtaining the Public Key Certificate.

A new standard has emerged call LDAP (Lightweight Directory Access Protocol). This standard was developed by the Internet Engineering Task Force as the Internet's implementation of a standard directory service closely patterned after a sub-set of the X.500 standard for directory services.

Since the focus in Directory Services is on standards, PGP looses out to PKI in this area due to the widely accepted IETF standards that are based on X.500 and X.509.

Certificate Revocation Lists

Another important aspect of a workable EC/EDI system utilizing encryption technologies is the availability and maintenance of lists of Certificates (X.509, of course) that have been revoked or cancelled. This operates much like a black list of stolen credit card numbers that must be widely published. As in credit cards, Asymmetric private keys might become compromised forcing one to revoke the key/number. These lists are only effective if software is utilized that checks the Certificate Revocation List (CRL) often.

Again, the widely accepted standard for certificates and the CRL is based on X.509 and not PGP. Another edge to PKI based software products.

I use my Public Key to do what?

In order to understand the workings of all components of the Public Key Infrastructure; let's clarify PKI with an example:

Oscar Scott, owner of "Oscar Pet Supply" in Tempe, Arizona wants to send "Big D Dog Food's" sales person, Lucy in Dallas Texas, an EDI purchase order for 1000 bags of "Xtra Healthy Brand" dog food. Oscar wants to use the Internet because it is the most cost-effective means of communication at his disposal, but he also knows the risks of using the open network for confidential business. Oscar uses his electronic commerce security software to encrypt the EDI purchase order, using Big D's public key from Big D's Public Key Certificate. We know that this Public Key contained within the Public Key Certificate is authentic since it has been digitally signed by "VERI-TEX", a top-notch Certificate Authority located in Texas. This encryption will keep the pricing and quantity details of what he is ordering secret from his competitor - just in case his competitor has a good Internet hacker snooping around the Internet. Only Big D will be able to decrypt the EDI purchase order so authorized access to the information is properly controlled. Oscar also wants his EDI purchase order transaction to have integrity, authentication, and non-repudiation, so he has his software apply a digital signature, using his secret private key. Oscar's software also handles creating and sending an e-mail file attachment of the encrypted, digitally signed EDI purchase order (PKI based standard, S/MIME : Secure / Multipurpose Internet Mail Extensions)

Lucy at Big D Dog Food logs onto her Internet account and receives the e-mail file attachment of the encrypted, digitally signed EDI purchase order. Lucy decrypts the file attachment using her encryption software and her private secret key. Her software (different manufacturer, but PKI - S/MIME compatible) also automatically

Final – Version 1.0

detects the digital signature and uses Oscar's public key to confirm that the entire file was transmitted without error by Oscar - providing proof of data integrity, data authentication and non-repudiation. Since Oscar's public key was obtained from a valid digital certificate from the "VERI-TEX" Certificate Authority, Lucy knows she can trust the results of her software that has successfully decrypted and analyzed the digital signature of Oscar's EDI purchase order. Also Lucy knows that her software has automatically checked the Certificate Revocation List (CRL) to make sure that Oscar's Public Key Certificate (X.509) has not been revoked. Lucy now has a trusted, unencrypted EDI purchase order from Oscar for 1000 bags of "Xtra Healthy Brand" dog food, ready for automatic EDI processing into Big D Dog Food's order entry system.

PGP could have been used for the above scenario, but all parties would have to purchase PGP for commercial use, and be locked into this one product for EC security without the advantages of the X.509 Digital Certificate.

Note: This article was written in September 1998 for EC Forum Magazine (issue published March 1999) before PGP version 5 was released. PGP version 6.5 now has X.509/PKI capability. Some application systems and standards still, however, require the use of the earlier PGP version 2.6.2 which is not X.509/PKI capable.

Final – Version 1.0

E. Summary of EDIINT Working Group “Requirements for Interoperable Internet EDI”

Draft-ietf-ediint-req-06.txt, December 1999

Jim Price, CPUC/ORCA, 6/2/99

Functional Requirement	Description	Needs	Issues	Recommendations
<p>Standard Encryption Algorithms and World-Wide Encryption (3.2) ⁴</p>	<p>Encryption turns otherwise readable text into something that cannot be read and understood, and conveys confidentiality to the EDI Interchange. Encryption is based on two components: an algorithm and a key. An algorithm is a mathematical transformation that takes plain-text or other intelligible information and changes it into unintelligible cipher text. In order to encrypt the plain text, a key is used as input in conjunction with an encryption algorithm. An algorithm can use one of any of a large number of possible keys. The number of possible keys each algorithm can support depends on the number of bits in the key. An encryption algorithm is considered "secure" if its security is dependent only on the length of its key.</p> <p>With symmetric encryption algorithms, two trading partners must use the identical key to encrypt and decrypt the EDI Interchange. If a trading partner has n trading partners, then n secret keys must be maintained, one for each trading partner. Symmetric encryption schemes cannot prove origin or destination authenticity (non-repudiation of origin, and receipt), since any EDI Interchange encrypted with a symmetric key, could have been sent by either of the trading partners. By using public key cryptography,</p>	<p>In order to provide confidentiality for EDI Interchanges on the Internet, a standard encryption algorithm(s) and key length(s) must be specified. For inter-operability to occur between two trading partners, the encryption algorithm and key lengths must be agreed upon either before hand, or within an individual transaction.</p>	<p>How secure the algorithm is; how fast implementations of the algorithm are; whether the algorithm is available for international as well as domestic use; the availability of APIs and tool kits in order to implement the algorithms; and the frequency of the use of the algorithm in existing implementations.</p> <p>Sufficient key lengths must be chosen with regard to the value of the EDI Interchange so that brute-force attacks are not worth the time or effort compared to the value of the Interchange.</p>	<p>There are many encryption algorithms that are secure and can provide confidentiality for an EDI Interchange. For most commercial applications a key length of at least 75 bits is recommended. For more valuable EDI interchanges, use of Triple-DES, IDEA, or 128 bit length RC2 or RC5 is recommended. DES, Triple-DES, and RC2 should be used in CBC mode, and RC5 in CVC Pad mode. A key length of 128 bits would make a brute force attack on RC2 or RC5 not feasible</p> <p>Indications are that IDEA is a secure algorithm and its use in PGP makes it the most widely used encryption algorithm for Internet electronic mail. IDEA's 128 bit key-length provides more than adequate security.</p>

⁴ Numbers refer to sections of the EDIINT Working Group's "Requirements for Interoperable Internet EDI", <http://www.ietf.org/internet-drafts/draft-ietf-ediint-req-06.txt>, December 1998. In all areas, the EDIINT Working Group's Internet Draft provides more detail than is contained in this summary.

Final – Version 1.0

	<p>management of symmetric keys can be simplified to use a symmetric key not only for each trading partner, but for each exchange between trading partners</p> <p>Public-key cryptography is based on a key pair associated to one, and only one, trading partner. Each half of the pair (one key) can encrypt information that only the other half (one key) can decrypt. One part (the private key) is only known by the designated trading partner; the other (the public key) is published widely but is still associated with the designated trading partner. For digital signature, Trading Partner A encrypts part of a message (a Message Integrity Check) with its private key, and if Trading Partner B can decrypt it using A's public key, B knows it could only have been with A's private key. For confidentiality, A encrypts a message with B's public key, and only B's private key can decrypt the information. Public key cryptography can thus unambiguously establish non-repudiation of origin and receipt.</p> <p>Since DES (a symmetric key algorithm) is 100 times faster than software encryption using the RSA asymmetric encryption algorithm and hardware encryption using DES is anywhere from 1,000 to 10,000 times faster than hardware encryption using RSA, public-key encryption algorithms are used in practice to encrypt the exchange of symmetric encryption keys.</p>			
<p>Key Management – Symmetric Keys (3.3)</p>	<p>The use of symmetric encryption is based on a shared secret. Two trading partners using a symmetric encryption algorithm must be able to do the following; generate a random symmetric key and agree upon its use; securely exchange the symmetric key with one another; set up a process to invalidate</p>	<p>A method to manage the symmetric encryption keys used in encrypting EDI Interchanges on a transaction basis. The method should simplify the generation, maintenance, and distribution of the symmetric encryption keys, and also provide a secure channel for distributing the symmetric encryption keys between trading partners.</p>	<p>Agreement by trading partners to use public-key cryptography to manage symmetric keys, and to generate a symmetric key for each EDI transaction.</p> <p>Issues affecting the choice of public-key encryption algorithms and key lengths are those listed under "Standard Encryption</p>	<p>RSA is a public-key encryption algorithm that has become a de facto standard in its use for symmetric key management. Its use is recommended in managing and distributing symmetric encryption keys when doing EDI over the Internet.</p>

Final – Version 1.0

	<p>a symmetric key that has been compromised or needs changing.</p> <p>Using public-key cryptography simplifies management of symmetric keys such that a "session key" can be used for each exchange between trading partners. Since a unique symmetric key is generated for each EDI transaction, trading partners do not need to invalidate compromised or expired keys; in the unlikely event that one of the symmetric keys is compromised, only one EDI transaction is affected, not every transaction in the trading partner relationship. Since only the receiving trading partner has knowledge of its private asymmetric key, only it can decrypt a symmetric key encrypted with its public asymmetric key and is thus the only one who can use the symmetric key to decrypt the EDI Interchange.</p> <p>To impart confidentiality to an EDI Interchange using public key cryptography for symmetric key management, the following steps would be performed: (1) the EDI Translator outputs the EDI Interchange, (2) a random symmetric key of the specified length is generated, (3) the EDI Interchange is encrypted using the randomly generated symmetric key with the chosen encryption algorithm, (4) the random symmetric key is then encrypted using the receiver's public asymmetric key, and (5) the encrypted symmetric key and encrypted EDI Interchange are then enveloped and sent to the trading partner. On the receiving side, (1) the symmetric key is decrypted using the receiver's private asymmetric key, (2) the decrypted symmetric key is then used to decrypt the EDI Interchange, and (3) the decrypted EDI Interchange is then routed</p>		<p>Algorithms and World-Wide Encryption".</p>	
--	--	--	---	--

Final – Version 1.0

<p>Key Management – Public and Private Keys (3.4)</p>	<p>to the EDI translator.</p> <p>The use of public-key cryptography to simplify the management of symmetric encryption keys presents the user with two problems: protecting the private key, and binding a trading partner's identity to his public key. The software generates a random private key, encrypts it, and stores it in a file or database, for access indirectly by the user through access to the software. User access to the software is generally controlled by a password, pass-phrase, and/or certain access rights. These are internal security policies, and are company specific. It is important to control the access to the private key, since any unauthorized access can lead eventually to the revocation of the corresponding public key.</p> <p>The mathematics of public key cryptography is complicated, but are based on mathematical manipulations of large numerical quantities. In the case of RSA, deriving the private key from the public key is based on the difficulty in factoring large numbers. The RSA key length is configurable, but as the cost of computing power decreases (e.g., a decrease in computing costs by a factor of ten every 5 years) then by the year 2030, a 512 bit public key can be "broken" for \$10. When using the RSA encryption algorithm to encrypt symmetric keys, support of 512 bit to 1024 bit variable key lengths is required. In general, asymmetric algorithms require longer keys to provide the same level of security as their symmetric key cousins. For example, a 512 bit RSA encryption key is equivalent to a 64 bit symmetric key, and a 768 bit RSA encryption key is equivalent to an 80 bit symmetric key. It is recommended that for EDI transactions requiring the use of RSA encryption to</p>	<p>Adoption of a trust model, or the use of certification authorities for issuing commercial grade/class 3 certificates. Each trading partner must choose a trust model. For instance, trading partners can self-certify one another, or they could use certification authorities acceptable to their other trading partners.</p> <p>Formats and protocols for requesting, revoking, and exchanging certificates and certificate revocation lists between certification authorities and trading partners, as well as between the trading partners themselves need to be agreed to and standardized.</p>	<p>The lack of wide-spread use of certification authorities in real world commercial applications, and the need to do additional profiling of X.509v3 certificates and standards for requesting, revoking, and exchanging certificates and certificate revocation lists.</p>	<p>Near Term Approach: Since a trust relationship between EDI trading partners already exists, it is recommended that the trading partners "self-certify" each other as part of the process of establishing a trading partnership, if an agreed upon certification authority is not used, until use of certification authorities become more established. The UA and/or EDI application interface must maintain a database of public keys used for encryption and authentication, in addition to mapping between the trading partner and e-mail address. It is still highly recommended that trading partners acquire a X.509v3 certificate from a certificate authority trusted by both trading partners. Trading partners should exchange certificates using the formats and protocols specified by "certificate-only" PKCS7 when using S/MIME, and GPG certificate formats and protocols when using PGP/MIME.</p> <p>Long Term Approach: Additional Internet-EDI standards will need to be developed to simplify the process of establishing a trading partnership, including the acquisition, revocation, exchange, and third party authentication of certificates. PKCS7 and PKCS10 as well as the standards being developed by the IETF-pkix (public key infrastructure X.509 work-group) need to be evaluated and adopted as standards for Internet EDI</p>
---	--	---	--	--

Final – Version 1.0

	<p>protect "session keys", that at least a 768 bit RSA encryption key be used. For very "high" value EDI transactions, at least a 1024 bit or higher key should be used.</p> <p>When using public key cryptography, there a "trust" issue arises: how can one trading partner be sure that the public key of another trading partner is bound to that trading partner, and is valid? Trading partners must exchange public keys or be able to access each other's public key in a manner that is acceptable to each of the trading partners. One method by which trading partners can exchange public key information is through the use of public key certificates. Public key certificates come in many different formats, and the trust model on which they are based also come with different underlying assumptions. Public key certificates based on the X.509 standards however are becoming prevalent in their use. The X.509 certificate is a binding of an entity's distinguished name (a formal way for identifying someone or something in the X.500 world, in our case it would be a trading partner) to a public key. A certificate also contains the digital signature of the issuer of the certificate, the identity of the issuer of the certificate, and an issuer specific serial number, a validity period for the certificate, and information to verify the issuer's digital signature. Certificate issuers are called certification authorities, and are trusted by both trading partners. In essence, a certificate is a digitally notarized binding of a trading partner to its public key.</p>			
Content Integrity (3.5)	Content integrity guarantees that the receiving trading partner gets the EDI Interchange in its originally sent state, and assures that no modifications (additions,	Choice of a one-way hash algorithm to calculate the hash value required to insure content integrity.	The one-way hash algorithm should be secure, publicly available, and should produce hash values of at least 128 bits.	The Secure Hash Algorithm, SHA-1, produces a 160-bit hash value that makes a brute-force attack infeasible. It is being recommended by most e-mail security programs and other security specifications, as

Final – Version 1.0

	<p>deletions, or changes) have been made when it is in transit between trading partners. Content integrity is achieved if the sender includes a message integrity check (one-way hash function), computed to "fingerprint" the EDI Interchange and MIME content headers, and the receiver calculates a matching hash value. One-way hash functions are constructed so the probability is infinitely small that some arbitrary length piece of plain-text can be hashed to a particular value, or that any two pieces of plain-text can be hashed to the same value. One-way hash values are usually from 112 to 160 bits long. The longer the hash value, the more secure it is. Unlike encryption algorithms, one-way hash functions can't be reversed or "decrypted", and don't require a key. The algorithm used must be agreed upon by the trading partners. MD5 produces a 128 bit Message Digest and is currently widely used by most e-mail security programs, such as PEM, PGP, and S/MIME.</p>			<p>weaknesses are being found in MD5.</p> <p>It is recommended that all new implementations use SHA-1 for outgoing messages, but to continue to accept MD5 incoming (SHA1 as well) as there already exist many MD5 implementations.</p>
<p>Authentication and Non-Repudiation of Origin (3.6)</p>	<p>Both authentication and non-repudiation of origin guarantee the identity of the sender of the EDI Interchange. Non-repudiation of origin identifies the original sender, and is the same as authentication when the EDI Interchange is sent point-to-point, i.e., when there is no forwarding involved. Both authentication and non-repudiation of origin are accomplished using digital signatures, which is another application of public-key cryptography. In contrast to using a receiving trading partner's public to encrypt a symmetric key, which could only be decrypted by the receiving trading partner's private key, for a digital signature the roles of the private and public keys are reversed, so that encryption is done with the</p>	<p>Choice of a digital signature algorithm</p>	<p>Issues affecting the choice of public-key encryption algorithms and key lengths are the same as those listed under "Standard Encryption Algorithms and World-Wide Encryption".</p>	<p>The RSA public-key algorithm is recommended for digital signatures as well as to encrypt symmetric keys. The recommended key lengths when using the RSA encryption algorithm for signature are the same as when using RSA encryption for managing symmetric keys: a 768 bit RSA encryption key should be used for most EDI transactions requiring digital signatures, and at least a 1024 bit or higher key for very "high" value EDI transactions.</p>

Final – Version 1.0

	<p>private key, and decryption is done with the public key. Encryption with a private key therefore uniquely identifies the person or entity doing the encryption, and non-repudiation of origin is achieved. The sender cannot deny applying the encryption, since only it knows the private key. Public-key encryption algorithms are not meant to encrypt something very large, but a one-way hash value is usually only between 112-160 bits long, so it is a natural choice for what can be digitally signed. If the message integrity value is signed with a private key, then not only is authentication and non-repudiation of origin guaranteed, but message integrity as well.</p>			
<p>Signed Receipt and Non-Repudiation of Receipt (3.7)</p>	<p>The term "receipt" is used for both the functional activity and message for acknowledging receipt of an EDI/EC interchange if the acknowledgment is for an interchange resulting in a receipt which is NOT signed. The term "signed receipt" is used if the acknowledgment is for an interchange resulting in a receipt which IS signed. "Non-repudiation of Receipt" (NRR) refers to a legal event which occurs only when the original sender of an interchange has verified the sender and content of a "signed receipt". NRR is not possible without signatures. The signed receipt is an acknowledgment sent by the receiver to the sender to (a) address the lack of wide-spread RFC mailbox delivery notification implementations within the Internet mail infrastructure; (b) provide the equivalent of VAN mailbox delivery notification, VAN mailbox pick-up notification, and VAN mailbox authentication, and (c) detect the situation where EDI Interchanges are maliciously deleted, or are not delivered by the transport. By having the receiver sign the receipt, it</p>	<p>Define the format and protocol for the signed receipt so that it provides: (1) implicit acknowledgment of mailbox delivery to the recipient, (2) explicit acknowledgment that the receiver has authenticated the sender and verified the integrity of the sent EDI Interchange, (3) provides non-repudiation of receipt, (4) provide information in the signed receipt for tracking, logging, and reconciliation purposes. The re-transmission timer, and retry count to detect lost Interchanges should be configurable.</p>		<p>The results of the IETF receipt working group shall be the basis for implementing signed receipts. When a signed receipt is used by trading partners, the message integrity check that is verified by the receiving trading partner must be returned to the originating trading partner in the signed receipt. The time-out and retry values for the signed receipt should be configurable. Duplicates should be checked by the UA and discarded. The signed receipt must be implemented using a MIME message disposition notification. A MIC is then calculated over the message disposition notification, and this MIC is digitally signed.</p>

Final – Version 1.0

	<p>authenticates that the intended receiver verified the integrity of the EDI Interchange and the identity of the sender. By returning the original message id and the one-way hash value of the received contents back in the signed receipt, the sender can reconcile the acknowledged EDI Interchange with what was sent.</p>			
<p>Syntax and Protocol for Specifying Cryptographic Services (3.8)</p>	<p>Once cryptographic services are applied to EDI Interchanges, then specification of the formats and protocols used for the cryptographic information (encryption algorithm, one-way hash algorithm, symmetric keys, initialization vectors, one-way hash values, and public-key certificates) needs to be enveloped and sent along with the EDI Interchange.</p>	<p>A syntax and protocol for specifying EDI Interchanges that have had cryptography applied to them. Several suitable standards already exist.</p>	<p>Several standards appear to fulfill the security requirements needed by this work group, including S/MIME and PGP/MIME. S/MIME can accommodate many different security algorithms and key lengths. PGP 4.5 is less flexible, but PGP 4.5 is more than adequate to insure confidentiality, non-repudiation of origin, and message integrity.</p>	<p>Either S/MIME or PGP/MIME fulfill the requirements of the EDIINT work group.</p>
<p>Transmission Successfully Translated from Internal Format to Standard EDI Format (4.2)</p>		<p>A facility to assure the sender that the EDI transmission was correctly translated and prepared for outbound transmission.</p>		<p>This is standard functionality for EDI translators and must not be required functionality of an EDI UA.</p>
<p>Transmission Successfully Encoded, Encrypted, Signed and Sent (4.3)</p>		<p>A facility to assure the sender that an EDI transmission was successfully encoded, encrypted, signed, and sent.</p>		<p>The EDI UA must maintain tracking of the success or failure of security services, and be able to identify the transmission by its message id, and a calculated MIC value if desired.</p>
<p>Transmission Successfully Delivered to the Recipient's Mailbox (4.4)</p>		<p>A facility to assure the sender that an EDI transmission was successfully delivered to a recipient's mailbox</p>		<p>This type of tracking information should be kept by the UA and is returned to the sender as a Delivery Status Notification, as specified in RFC 1894.</p>
<p>Transmission Successfully Received (4.5)</p>		<p>A facility to assure the sender that the transmission was correctly received by the intended receiver.</p>		<p>The EDI UA must track this information and return it as a signed receipt. The X12 997 message can also provide the equivalent of an acknowledgment, but the signed receipt is still recommended because the 997 applies to a control ID only and not to the actual data.</p>
<p>Transmission Successfully Translated by Receiver (4.6)</p>		<p>A facility to assure the sender that the receiver could "understand" (in EDI terms) the transmission.</p>		<p>The functional acknowledgment 997 serves this exact purpose and should be tracked by the EDI translator.</p>
<p>Detection and Recovery of Delayed or Lost Transmissions (4.7)</p>		<p>A facility by which a sender can detect sent transmissions that have not been acknowledged as correctly received, by a configurable period of time, and act accordingly.</p>		<p>The receipt or signed receipt (Message Disposition Notification as specified in RFC 2298) return the original message ID. Actions based on a failure to receive a receipt or signed receipt may include re-transmitting or alerting the operator. If re-transmitted, the receiving UA must be able to</p>

Final – Version 1.0

				detect the second transmission as a duplicate and discard it.
Detection and Handling of Duplicate Transmissions (4.8)		A facility allowing the receiver to detect duplicate transmissions.		Translator initiated duplicates should not be halted. Re-transmission in attempts to deliver transmissions quickly should allow a UA to identify and discard duplicates generated by the sending UA.

E. “Push vs. Pull”

One issue that must be determined in any exchange of data is whether the data is “pushed” or “pulled.” Either means can work for EDI. However, experience in California, plus general business principles suggest that “pushing” may be preferable.

“Pushing” refers to the situation in which the party that provides the data sends the data to the party receiving the data. The “pusher” initiates the transaction and is responsible for ensuring that the recipient either receives the data or is notified that the data is available. A simple example would be a utility sending a bill by U.S. Mail. The utility prints the bill and mails it. In this case, the utility has fulfilled its responsibility for ensuring that the receiving party has access to the data, because the U.S. Mail is responsible for delivering any item submitted with proper postage. Sending e-mail is another example of “pushing” data.

“Pulling” refers to the situation in which the party receiving the data must retrieve it from a specified location (real or virtual). A simple example would be picking up dry-cleaning: the customer comes to the store and picks up his or her cleaning when it is ready. The store is not responsible for the customer receiving the dry-cleaning if the customer does not come to the store. In California’s competitive electric market, meter data is now handled this way. The data is posted to a server in the recipient’s “mailbox,” and it is the recipient’s responsibility to check the mailbox each day for the data.

In California, the “pull” system has been in use for about a year. There have been a number of issues in exchanging metering data in California (most of which have been or are being resolved), but the largest seems to be data matching. This refers to situations in which the Meter Data Management Agent (MDMA) has processed and posted data but the parties receiving the data do not receive it because they were not looking for it (in one type of example, there may be a list of customers, so the recipient retrieves the data file but is unaware that some customers that should be in the list are not; in another example, the recipient fails to retrieve the data, because the recipient did not know it had a file available). Such errors have occurred relatively equally whether the utility or a non-utility is the MDMA.

A “push” system would likely have reduced the errors. In that approach, the MDMA would be sending files to the recipients, who would then know they were responsible for processing it. The situations described above would not occur.

A “push” system has the general benefit of being similar to the way in which most business is conducted. In almost all cases, when a company wants payment for a product or service it has delivered, the company sends a bill. The recipient knows they have to deal with the bill, whether they received the product or service or not. Similarly, even if the recipient knows they received the product, the company would not rely on the recipient to come back to the company on its own to pay the bill without having sent the bill to the customer.

In general terms, our economy and business laws - and electricity meter reading systems - have developed around the “push” system. The service provider is responsible for notifying the customer that the service has been provided and how much the customer owes and when. In electricity, the service provider does so by obtaining the meter read, calculating the bill, and sending it to the customer. The meter reading service provider should do so by reading the meter, then sending the product (the reads) to the customer (the billing provider). Such a “push”

Final – Version 1.0

approach is far less prone to errors and, for this and the other reasons discussed above, should be preferred for EDI.

F. CommerceNet

CommerceNet is a global non-profit membership organization addressing the evolving needs of companies doing electronic commerce. Since its founding in 1994, CommerceNet's mission has been to promote and advance interoperable electronic commerce to support emerging communities of commerce. Today, CommerceNet serves over 500 corporate members worldwide, providing a global perspective on electronic commerce.

CommerceNet, among other activities, certifies the inter-operability of software developed and based on the Internet Engineering Task Force's (IETF) EDIINT standard. To date the EDIINT AS1 standard utilizes an SMTP (e-mail) protocol to accomplish data transfer; however, the IETF is developing an HTTP-based protocol (EDIINT AS2).

Final – Version 1.0

Appendix II Glossary

ASCII

Computer coded data in accordance to the American Standard Code for Information Interchange.

Authentication

The process of identifying a principal (for example, a user or a process running on another computer) by something that the principal knows, such as a password, something the principal has, like a physical token or certificate, or by the location of the principal, like being at a secured terminal.

Certificate

A credential that is tamper-proof and forgery-proof enough to be used for authentication. A certifying authority, usually issued by an independent third party, issues certificates to individuals, servers, and process that need to identify themselves.

CommerceNet

A global non-profit membership organization addressing the evolving needs of companies doing electronic commerce.

Digital Signature

Extra data appended to a message which identifies and authenticates the sender and message data using public-key encryption.

EDI

Electronic Data Interchange

EDIINT

Abbreviation/acronym used to identify reference to the EDI over the Internet standards set promoted by the IETF and CommerceNet

EDIINT AS1

Abbreviation/acronym used to identify reference to the specific EDI over the Internet standard promoted by the IETF and CommerceNet based on SMTP

EDIINT AS2

Abbreviation/acronym used to identify reference to the specific EDI over the Internet standard promoted by the IETF and CommerceNet based on HTTP

Encryption

An algorithm based process that turns a message (plain text) into a scrambled string (ciphertext), that is intelligible only to someone/process with an encryption key

FTP

File Transfer Protocol. One of several communications protocols used in Internet based communications. Method of transferring files where the receiving party gives sending party some level of physical control over it's computer.

GISB

Gas Industry Standards Board

HTML

Hypertext Markup Language. A computer programming language used to create Internet WEB pages

Final – Version 1.0

HTTP

Hypertext Transfer Protocol. One of several communications protocols used in Internet based communications. The basis for the WEB.

IETF

Internet Engineering Task Force. An international non-profit voluntary group who set standards for the Internet

MDN

Message Disposition Notification. Process used in eMail (SMTP) based processes to notify sending party that message was received at destination

Message Digest

A large single number, usually 128 to 256 bits in length, created from a string of text. Even a slight change in the text results in a different number being generated. These values ensure that a message isn't changed en route from the sender to the recipient.

Non-repudiation

Term meaning that a party to a transaction can not reasonably deny its participation in the transaction

PKI

Private Key Infrastructure. Used to manage the creation, revocation, and management of public keys used in encrypted applications.

Public and Private Keys

An encryption scheme, introduced by Diffie and Hellman in 1976, where each person gets a pair of keys, called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his private key. The need for sender and receiver to share secret information (keys) via some secure channel is eliminated: all communications involve only public keys, and no private key is ever transmitted or shared.

SMTP

Simple Mail Transfer Protocol. One of several communications protocols used in Internet based communications. The basis for eMail systems.

TCP/IP

Transmission Control Protocol/Internet Protocol. The de facto standard developed for internetworking heterogeneous computer systems. It encompasses both network layer and transport layer protocols. While TCP and IP specify two protocols at specific protocol layers, TCP/IP is often used to refer to the entire protocol suite..

VAN

Value Added Network. A privately owned network that provides specific services for a fee. A VAN usually offers some service or information that is not readily available on public networks. VAN customers typically purchase telecommunications services (dial-up, leased lines, etc.) that connect them to the VAN.

X12

An abbreviation/acronym used to refer to the Accredited Standards Committee (ASC) X12, Electronic Data Interchange or its published standards. The Accredited Standards Committee X12 is a chartered committee of the American

Final – Version 1.0

National Standards Institute (ANSI) responsible to develop uniform standards for electronic interchange of business transactions.

XML

Is a subset of the Standard Generalized Markup Language (like HTML). It is a generalized markup language that is computer platform independent and extremely flexible. It can be used to specify presentation of a document (font size, indentation, etc.) or to specify structure of the document (paragraph, section, chapter, etc.).

Y2K

Year 2000. The century beginning on January 1, 2000.

Final – Version 1.0

APPENDIX III

References and Information Sources

Note: Ordered by Sequence of Contribution

1. CPUC Internet EDI Meeting Notes, by Jim Price. April 1, 1999
2. CPUC Internet EDI Meeting Notes, by Jim Price. March 1, 1999
3. Comments On EDI Data Communications Connectivity Options, by Richard Shiffer, PECO Energy. 7/7/98 Version 2.0
4. Electronic Transmission Recommendation, Maryland Electronic Data Interchange Subteam, March 14, 1999.
5. SCE Internet EDI Infrastructure Flow Diagram, Ray Wenzel, April 1, 1999.
6. Minutes – March 25, 1999 Regional Meeting – Reno , Deregulation Group, Brian McFaden.
7. NYPSC Case No. 98-M-0667, Data Xfer Mechanisms Sub-Group Meeting, PSC Offices - NYC; 03/4/99 9:00AM - 5:00PM, Notes Prepared by Fran Hart
8. Gas Industry Standards Board - Electronic Delivery Mechanism Related Standards, Ver. 1.3, July 31, 1998
9. Automotive Industry Action Group (AIAG) E-5 Standard, Guideline for Electronic Commerce Message Routing on TCP/IP Networks, March 10, 1998.
10. Guideline for Electronic Commerce Message Routing on TCP/IP Networks, AIAG Publication E-5 FAQ
11. Internet Engineering Task Force (IETF) documents: draft-ietf-ediint-as1, draft-ietf-ediint-as2, draft-ietf-ediint-hl7, draft-ietf-ediint-req-06
12. PGP or PKI – What is the Best Answer for Internet EDI?, by Dave Darnell, EDI FORUM, March 1999.
13. PA-PUC - EDEWG Internet EDI Protocol Test Plan
14. “Push vs. Pull” by Chris King, e-mail March 8, 1999.
15. “Traditional VAN EDI” by Dee Sutphin, e-mail March 12, 1999:
Etzel, Klaus. “EC Provides the Key” Electronic Commerce World, September 1998, p39.

GE Information Services Web site. “The Business of EDI” [Online] Available March 1999, <http://www.support.geis.com/edi/edip03.html>.

GE Information Services Web site. “The Tools of EDI” [Online] Available March 1999, <http://www.support.geis.com/edi/edip05.html>.

GE Information Services Web site. “The Traditional Definition of EDI” [Online] Available March 1999, <http://www.support.geis.com/edi/edip01.html>.

McGarr, Michael S. “Traditional EDI Not Going Away Anytime Soon” Electronic Commerce World, November 1998, p44-70.

National Institute of Standards and Technology Web site. “[Communication Audit Trail](http://www.nist.gov/itl/div896/ipsg/eval_guide/subsubsection3_6_3_9.html)” [Online] Available March 1999, http://www.nist.gov/itl/div896/ipsg/eval_guide/subsubsection3_6_3_9.html.

National Institute of Standards and Technology Web site. “Direct Trading Partner Connection” [Online] Available March 1999, http://www.nist.gov/itl/div896/ipsg/eval_guide/subsubsection3_6_3_5.html.

National Institute of Standards and Technology Web site. “Multiple VAN Support” [Online] Available March 1999, http://www.nist.gov/itl/div896/ipsg/eval_guide/subsubsection3_6_3_4.html.

National Institute of Standards and Technology Web site. “VAN Script Files” [Online] Available March 1999, http://www.nist.gov/itl/div896/ipsg/eval_guide/subsubsection3_6_3_3.html.

Final – Version 1.0

Oakland Electronic Commerce Resource Center Web site. “Access Methods” [Online]
Available March 1999, <http://ecrc.org/selectvan.html>.

Sterling Commerce Web site. Glossary [Online] Available March 1999,
<http://www.sterlingcommerce.com/gloss/index.html#>.

Thomas EC Resources Web site. “Benefits of EDI Outsourcing” [Online] Available March 1999,
<http://www.ecresources.com/presentations/croom/tsld008.htm>.

16. WEB EDI and WEB EDI DICTIONARY by Diane Watson, March 04, 1999.
17. New York PUC Data Transfer Mechanism Subgroup supplied by Dale Austin on June 8, 1999.
18. GISB section contributed by Chris Navadauskas, May 27, 1999.
19. EDIINT matrix contributed by Jim Price, CPUC/ORR, 6/2/99
20. GISB documentation
21. State of Pennsylvania EDEWG documentation
22. The Handbook of EDI
23. State of Maryland Electronic Data Interchange Sub-Team documentation
24. Vendor presentations
25. IETF documentation
26. UIG documentation
27. February 1999 edition of e-Business Advisory -- Secure Transactions: Getting Started by Dan Sullivan
28. Pennsylvania PUC hearing on Data transfer mechanisms held 4/28/99 in Harrisburg, PA.