EDI: Business on the Internet

HP World '96 Conference and Expo
Presentation #: 4017
by Steve Botts
Premenos Corp
1000 Burnett Avenue
Concord, CA 94520
+1 510-602-2000

Electronic Commerce

There are a number of commercial activities being conducted on the Internet today. All of these constitute Electronic Commerce. This paper addresses EDI, or the application to application exchange of highly structured messages in a standard format, such as purchase orders, invoices, shipping notices and the like, and how these messages may be transmitted securely over the Internet.

EDI is a Beneficiary of Internet Growth

The use of EDI in the US has been growing steadily since its early deployment back in the 1980s: from approximately 4,500 companies in 1987 to over 100,000 in 1995. Although the implementation of EDI is significant, even today only about 5% of US businesses use it. By any measure the growth and popularity of the Internet dwarfs the growth of EDI.

In early 1996 there were over 10 million hosts connected to the Internet on over 100,000 networks. The driving force behind this growth is primarily the World Wide Web, which is growing so fast that any statistic reported today is virtually meaningless within a week.

Nevertheless, EDI is a beneficiary of the explosive growth of the Internet, because this ubiquitous connectivity makes doing EDI easier, faster, and less expensive than anything experienced to date.

Why do EDI?

EDI takes advantage of the fact that 75% of all data input into a business computer system is the output of another computer system. In general businesses use EDI because it decreases cost, increases speed, and improves the quality of business processes. The following table summarizes some of the efficiencies and benefits of doingEDI.

Why Do EDI?

Decreases Cost	Increases Speed	Improves Quality
Personnel efficiency	Throughput	Data Integrity
Storage (Inventory)	Collections/cash flow	Reconciliations
Interest Expense	Inventory Turns	Error elimination
Postal and telephone	Deliveries (enables QRS/JIT)	Responsiveness
Office Supplies	Automatic Processing	Customer Service

Who benefits from EDI?

Many companies currently doing EDI are reluctant participants in the process, not realizing its many benefits. Generally those businesses which are proactive in their implementation of EDI realize the greatest benefits. Forrester Research reported the following: "EDI...has long been the only way to automate billing and inventory between business partners. But it has been an ugly 30-year struggle whose high costs have benefited only the biggest firms." Many smaller companies who have implemented EDI under duress will agree with this assessment. EDI may have added costs to the way they do business.

VAN's Share of EDI Transmissions is Declining

One of the high costs of EDI is an on-going cost: that of VAN communications. Since its inception, most EDI has been transmitted using the services of Value Added Networks. They typically invoice for services, based on formulas which invariably include charges for connect time, document counts, and character counts. This fee structure has resulted in very high charges for transmission services. Because of their high costs, in recent years the VANs share of EDI traffic has been declining. Some companies have opted to use direct connections with high volume trading partners to reduce their VAN charges. Direct connects, however, increase the complexity of communications management which is itself an additional cost.

The rise of Internet EDI represents a major paradigm shift

Internet savvy companies have discovered that the Internet solves problem of high cost associated with VANs and the expensive communications management associated with direct connections. They recognize that the Internet is not without its problems, however. Inasmuch as it is an open network, they need to be much more concerned about security issues. Fortunately these security concerns are easily addressed with existing security protocols. Forrester Research says: "There has been a lot of hype about the potential for break-ins, but now with recent [product] developments, the Internet is viable." Nevertheless, there are legitimate questions that should be addressed before using the Internet for EDI.

Internet EDI Security Issues

- How do I know who sent it?
- Did it arrive exactly as sent?
- Can the sender deny sending it?
- Can the receiver deny having received it?
- Can anyone else read it?
- Who provides tracking and auditing?

Internet EDI Security Requirements

The forgoing questions identify requirements, which are typically labeled as follows.

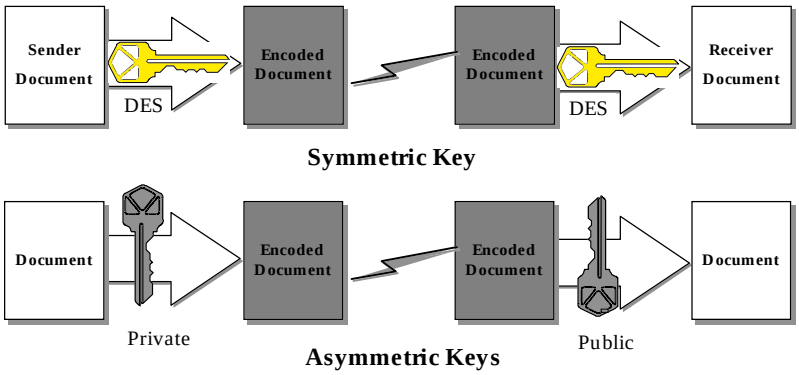
- Authentication
- Integrity
- Non-Repudiation
  - Origin
  - Receipt
- Confidentiality

Standard security mechanisms, protocols, and other controls exist today to answer all of these security concerns and conduct EDI with complete confidence over the Internet. Public key cryptography as implemented in S/MIME provides confidentiality, data integrity, authentication, and non-repudiation of origin.

Cryptography 101

To understand how the technology works, it's necessary to know a little bit about cryptography. Some encryption algorithms, like DES, RC2, or RC4, use the same key to encrypt and decrypt the data. These symmetric algorithms are extremely fast, but for purposes like EDI require that both parties to a transaction know the secret key. Public key technology on the other hand, involves the use of key pairs, a private key, kept secret and used only by the owner, and a corresponding public key which may be published to the world. Data encrypted with either key can only be deciphered by the other key. Public key algorithms, like RSA, allow each party to keep his private key secret and distribute or publish his public key to trading partners.

Cryptography Concepts

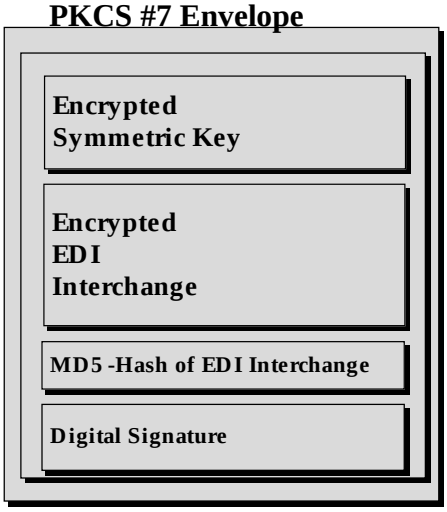


A Digitally-Signed Message

Following is a description of how this technology may be implemented in a messaging environment. It is described here as various steps, which in actual practice are completely automated for transparency. The EDI interchange is encrypted using a randomly generated symmetric key. The symmetric key itself is then encrypted using the recipient's public key. This means that only the recipient, who holds the private key can decrypt the symmetric key that unlocks the Interchange. This makes the EDI Interchange confidential.

To assure the data integrity of the interchange, a message digest of the interchange is created, using MD5, a one-way hashing algorithm. The message digest it creates, like a fingerprint, is unique, but cannot be used to recreate the interchange itself. Finally, the message digest is digitally signed by the sender using his private key and everything is sent per the PKCS #7 enveloping standard and S/MIME.

Send EDI Securely with S/MIME

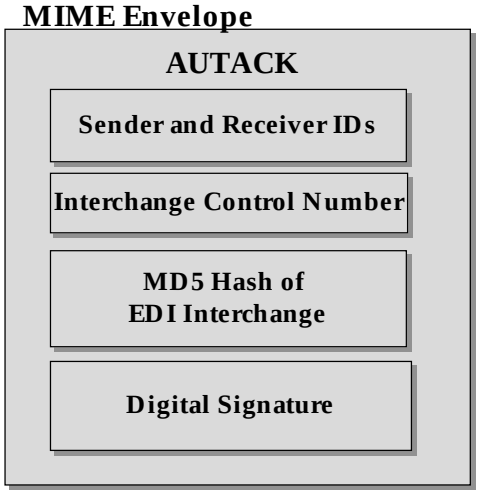


When the recipient gets the message he applies the sender's public key to expose the message digest and he applies his private key to decrypt the EDI interchange. Then, using the MD5 algorithm, he calculates his own message digest of the interchange. If the two message digests are identical, he has established that the interchange arrived intact. Also, since the sender applied his private key to sign the message digest, the sender cannot deny having sent the message. The recipient is assured of the sender's identity and of the interchange's data integrity.

A Digitally-Signed Receipt

To provide the sender with the assurance that the recipient got the message exactly as it was sent, the recipient now signs the message digest using his private key and returns it to the sender as per ISO 9735, which specifies the application level syntax rules for a Secure Authentication and Acknowledgment Message, commonly known as the EDIFACT AUTACK message. This completes the loop and provides non-repudiation of receipt.

Templar Acknowledges Receipt



In actual practice, using *Templar* software from Premenos with dedicated Internet connections, an EDI interchange is sent, a signed receipt is transmitted back to the originator, and the interchange and its receipt notification are automatically reconciled within a few minutes total elapsed time. A retransmission/notification policy, which provides that an interchange will be automatically retransmitted if it is not acknowledged within a user-specified time period, generation of e-mail, or a pager alert to an administrator upon certain occurrences, and tracking capability round out the requirements

Security at the Application Level

It is significant to note that security is applied at the application layer of the communications stack. When applied in this manner, the secured interchange may be transmitted in any manner as agreed by the parties, since the security is independent of the layers below it, so it is easy to send as mail, file transfer, using HTTP, over x.400, etc.

Templar uses Standards to Enable Secure Internet EDI

All of the forgoing security services rely on existing standards:

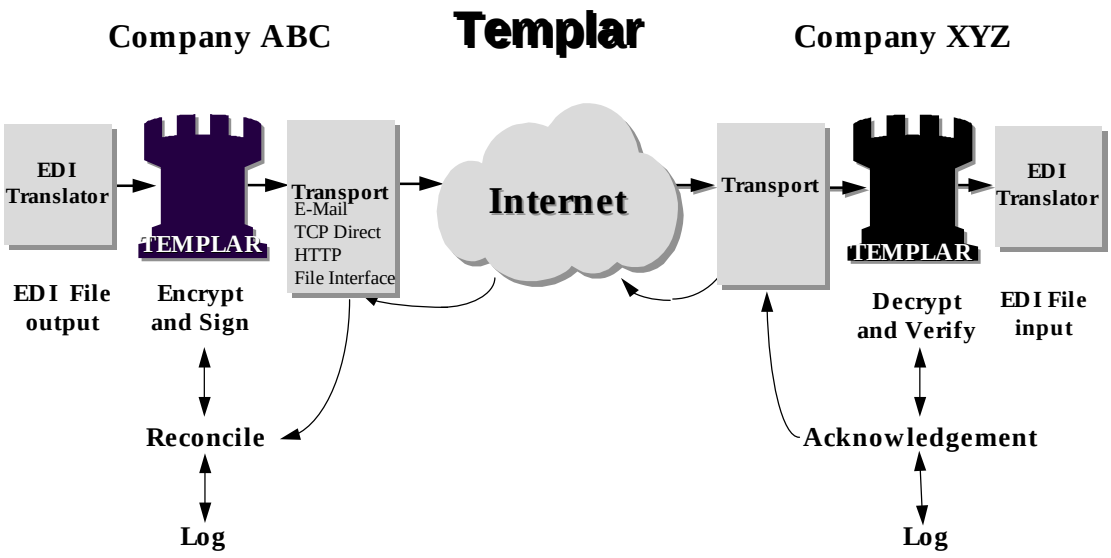
- **MIME:** And more specifically, MIME/EDI as defined in RFC 1767, which specifies ANSI X12, EDIFACT, and consent content types.
- **S/MIME:** Which specifies the use of RSA Public Key cryptography, PKCS #7 security enveloping, DES, RC2, RC4 symmetric cryptographic algorithms, and MD5 a one-way hashing algorithm.

- **AUTACK:** The ISO Authenticated Acknowledgment which returns a digitally signed receipt containing the message digest of the EDI interchange, trading partner IDs, and interchange control number, etc.

Templar Security Fits Between the EDI Translator and Message Transport System

The diagram below illustrates the relationship of various system components. Business applications output data to the EDI translator, which converts the data to Messages within Interchanges conforming to EDI syntax. Next *Templar* applies the security policy established for the appropriate trading partnership and envelopes the entire Interchange so that it is ready to be transmitted as an object attached to an Email message. The mail system, or alternatively some other transport, transmits the message to the trading partner.

Upon delivery, the recipient's *Templar* system removes the security enveloping, authenticates the message and its data integrity, then returns a signed receipt to the sender. This acknowledgment is automatically reconciled by the originator's *Templar* system. Using dedicated connections, this entire process occurs in a matter of minutes.



Savings are Significant

Since Internet access is based on a fixed price for bandwidth rather than a formula based on character counts, savings can be significant compared to using a VAN. Although Internet access charges have dropped considerably since it was published in March, 1995, the following table shows the savings as estimated by BIS:

Characters/month	VAN	Internet	Savings
10-20K	$1,580	$400	75%
150-200K	$1,880	$400-$746	60-79%
500-2M	$2,788-$6,530	$412-$758	85-88%
10M-30M	$24,875-$47,792	$9,290	63-81%

Source: BIS

Certification of Keys or Key Exchange is a Requirement of Internet EDI

In order to use the security services of *Templar*, key pairs must be generated and public keys exchanged. *Templar* generates key pairs and facilitates exchange of the public key by means of X.509 Certificates. Even in the absence of a formal government or commercial infrastructure to manage and certify these public keys, EDI users are able to conduct EDI securely on the Internet. This is because of the apriori relationship which exists between trading partners. They know each other, and have already exchanged a lot of information just to be able to do EDI. The bi-lateral exchange of their public keys is just another part of the trading information which needs to be communicated between partners. This is accomplished within *Templar* by e-mailing the X.509 certificate as an attachment to a mail message.

As Certifying Authorities like Verisign, the United States Postal Service, and perhaps banking institutions begin issuing signed X.509 certificates, ad hoc relationships between trading partners, who have no prior knowledge of one another, will be facilitated.

Internet access is a commodity and EDI users are the beneficiaries

Today, all of the Fortune 500 companies have Internet access at T1 or greater speed. In effect they have connectivity to a wide area network of unprecedented proportions. Millions of small and medium size enterprises also have access to the Internet. The competitive nature of Internet service provider business has driven access prices to extremely low price points. AT&T and some other long distance telcos have gone so far as to offer 5 hours per month of free Internet access to their long distance customers. Unlimited dial-up access at 28.8 bps is generally available throughout the US for under $20.00 per month.

Low cost or free access has resulted in millions of new Internet subscribers who fuel the demand for increased bandwidth. As with other so-called "free" services, take television for example, advertisers will pick up the tab or subsidize the cost for access. Small businesses who use the Internet for legitimate business purposes, like EDI, are beneficiaries of this ubiquitous access.

Benefits of EDI on the Internet

The benefits of using the Internet for EDI are numerous and compelling.

- Single reliable and robust network access protocol and communications connection (TCP/IP) for EDI, e-mail, file transfers, host access, WWW, etc.
- High speed data transmission
- Fixed low cost bandwidth pricing
- Global access and availability
- End-to-End EDI
- Connectivity to millions of businesses
- Open, standards based, and platform independent

Summary

Early users of the Internet from research organizations, universities, and the military, could scarcely have guessed how the Internet would evolve to become what it is today. Although still widely used for non-commercial purposes, today, commercial activities comprise a large portion of all traffic on the Internet, from on-line banking and shopping, to delivery of news and stock quotations, to the delivery of e-mail and EDI business documents. All of these commercial activities make Internet access highly desirable.

Sensitive information like credit card numbers, bank account numbers, and some business documents need to be digitally signed, so that they may be relied upon as authentic and binding, and encrypted for confidentiality, so that they are not available to someone other than the parties involved. Fortunately, as the Internet has evolved, standards to support these security services, have been implemented in software products like *Templar*. Today, as a result of *Templar*, EDI may be conducted safely and securely on the Internet.