The Impact of IETF's EDI over Internet Recommendations on World-wide Electronic Commerce

By Rik Drummond
Chair, IETF "Internet EDI over Internet" Workgroup (IETF EDIINT WG)
Email: drummond@onramp.net

Introduction

Where is Electronic Commerce? The press has hyped electronic commerce ever since the WEB took off three years ago. An IETF "Internet EDI over Internet" Workgroup (IETF EDIINT WG), with over 400 national and international members, is addressing how to transmit EDI documents, between businesses, in a secure and reliable manner. Our objective is: Secure, International, Inter-operable EDI over Internet -- Now!

Status Update

To date, the workgroup has produced three papers in various stages of review. The first is a discussion of the detailed technical security requirements for EDI. A second is a detailed matrix comparing the four major security technologies: MOSS, S/MIME, PGP and MSP. The last is a technical paper describing how to conduct secure EDI over SMTP. Interoperability Tests

Since the IETF does not pilot recommendations or standards, CommerceNet is sponsoring an interoperability pilot between interested vendors to test the recommendations of the IETF EDIINT WG. Eleven companies from around the world are participating. Vendors such as: Digital Equipment Corporation, AT&T, Sterling Electronic Commerce, Harbinger, Premenos, Actra, CyberPath, Atlas Products, US Department of Defense, Electronic Data Systems, and DanNet. The completion of the pilot test will be a major step forward towards our objective of inter-operable, secure EDI over SMTP NOW.

The pilot started October 14, 1996, and focuses on testing the EDI over SMTP recommendations. It has three phases, each phase building on the previous phase. Phase 1 is the basics -- testing that the vendor products can transfer data over SMTP using MIME with RFC 1767 -- the MIME EDI body part. Phase 2 deals with a secure EDI over Internet. Phase 3 focuses on Signed-receipts/ Non-repudiation of Receipts. All three phases should be complete by early next year. At that time interoperable EDI over Internet will be a reality in several vendor products.

What is standing in the way?

Most professionals agree that there are four broad categories stalling the implementation of business to business electronic communications. They are: 1) business process integration, 2) sovereignty issues (cross border secure exchanges), 3) reliability, and 4) security. The IETF EDIINT WG has discussed three of these categories: sovereignty, reliability and security, in an effort to reach our objective. The first is beyond the scope of our effort. Sovereignty issues while not solvable by the IETF WG are interesting in that they give one a view of the issues involved with world-wide electronic commerce. Reliability is an operational issue, NOT a technical issue. The Internet protocols are as reliably constructed as any of the ISO protocols. They are currently not always operated in a reliable manner in many parts of Internet. Our focus will be on sovereignty and security.

Sovereignty issues

The recommendations focused on international, interoperable security issues, such as: encryption, signature, and certificate distribution across the international arena. Internationalizing the issues becomes complex because of ITAR Encryption Control laws in the USA, and similar laws in several other G7 nations.

G-7 Nations and the International Encryption Hindrance

The transmittal of tightly encrypted electronic data is problematic to most governments, including the USA. Most government believe they must be able to ready, eavesdrop, on electronic communications to protect they constituents from the criminal elements. Because they believe this is one of their purposes many will continue to push for easily breakable and/or the escrow of keys, slowing world-wide usage.

Law Enforcement Examples

The general theme of governments seems to be that governments must balance the privacy needs of the citizen with the investigative requirements of law enforcement. No one knows where the balance will finally rest.

The tone at the "Joint Australian/OECD Conference on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure Conference" in February 1996 was distinctly in favor of mandating security and encryption methods that are breakable by security and law enforcement agencies.

As an example, at the International Cryptography Institute in September, 1995, FBI Director Louis Freeh reported that encryption had been encountered in a terrorism investigation in the Philippines involving an alleged plot to assassinate Pope John Paul II and bomb a U.S. airliner. The law enforcement issues are real. These issues of how to secure electronic commerce in the international environment, across sovereign international boundaries are slowing the introduction of secure electronic commerce. How will it be resolved? Some believe the only solution is by the introduction of wide scale key escrow systems managed by government or government accessible entities. Without these systems we will be required to use "weak" easily breakable keys -- which are not sufficiently secure for many types of EC.

Security - Identity of Participants and key management How does one know with whom they are doing business, and that the person has the authority and financial resources to purchase or negotiate terms of the purchase? With the general anonymity afforded participants on Internet, one does not know, with assurance, with whom they are dealing, without the use of additional technology and services. The technology is the public/ private key technology used to create digital signatures. The holder of a private key, which is kept secret, may be uniquely identified by that key. Software from several vendors and standards may uniquely generate the public/ private key pairs. However, this is not the current problem with implementation. Hindrances are two fold: 1.) how to manage the records of hundreds, thousands , or millions of electronic signatures and 2.) how to know the signature truly represents the entity. This is true especially in the consumer world, where purchases are made infrequently from specific merchants -- maybe only once in a lifetime. So, the management of signature records and identity verification is problematic. The signature records must be shared widely between all participating consumers and merchants to ensure "safe" transactions. This is hundreds of millions of entities.

In closed communities, as is the case of EDI trading partners "today" (this will change over the next couple of years), the problem of signature management and entity identity verification is not as much an issue. Trading partners already have contacts in place and have verified that other trading partners are who they say they are, and have resources to buy and sell products and services. So the primary issue holding back general electronic commerce is not a problem for EDI over Internet.

Security Protocols

A lot of the workgroup's time has been spent defining the requirements and discussing upon which existing security protocols to base general EDI product interoperability. Discussion has ranged over four protocols: PGP, S/MIME, MOSS and MSP which meet all or most of our requirements. The two which are best for both the domestic and

international environments are PGP V3.0 and S/MIME. The CommerceNet Pilot is currently focused on S/MIME. In the near future PGP interoperability test should commence.

Conclusion

The IETF EDIINT Workgroup is recommending the technical standards to facilitate interoperable, secure, world-wide, EDI. CommerceNet is sponsoring a test of these recommendations by over 10 vendors. Finally we all wait on various governments to allow encrypted data to across their boarders in a uniform manner so that world-wide, secure electronic commerce will be realized.