In order to achieve widespread acceptance of high-value transactions, legally binding B2B e-commerce is critical and must be made readily available by large corporations within the internet arena.

Legalising B2B e-commerce

Alex Garcia-Tobar

High-value e-commerce is projected to shift rapidly from proprietary electronic data interchange (EDI) technology and paper-based transactions, towards the internet and open digital signature-based solutions. Unlike consumer electronic commerce (which is quickly moving into the mainstream) high-value e-commerce for very diverse applications (such as supply-chain management, trade finance, loan processing, healthcare delivery, and information access) is typically conducted by large corporations. These organisations will exchange information either over proprietary networks using EDI formats, or using paper-based mechanisms. But now a new market shift is underway where enterprises are moving away from proprietary EDI technology and paper, towards a more open internet infrastructure.

Considering that current EDI systems support procurement efficiencies, enable savings by automating tasks and increase visibility of information among vendors — while providing stronger links to customers, partners, and suppliers — why the dramatic change?

The reality is that the scope of EDI has always been limited intentionally to ensure controlled activity within a closed environment. However, as a result of heavy overheads associated with the EDI infrastructure, many small, medium and even large businesses have been shut out. In direct contrast, an open internet infrastructure opens doors to an expanded supply chain, while at the same time enabling lower operational costs and enhanced procurement efficiencies.

New challenges

But the extranet environment also poses new challenges. By far the most important is the need to protect the *high-value* transactions typical of B2B. These high-value transactions require much greater security and management than most online consumer transactions. Consider a typical consumer e-commerce transaction. Is it a book from amazon.com for US$21.99 (€25) or higher-value purchases like an airline ticket or a personal computer? One way or another, the average transaction will likely fall below the US$1,000 (€1,077) mark. But with mission-critical applications like electronic bill payment, insurance policy management and claims processing — in addition to regulatory compliance and supply chain management being conducted over extranets — a B2B transaction is routinely in the thousands, millions, or even hundreds of millions of dollars. Moreover, while a credit card maximum liability cap of a US$50 (€54) protects consumers engaging in e-commerce, there are no such guarantees in place for B2B e-commerce.

With so much money at stake, failure to provide robust protection can prove massively expensive. Financial repercussions can be astronomical, legal entanglements limitless, and the effect on business partners incalculable.

Let's look at some hypothetical companies which could run into some very real difficulties if B2B e-commerce is not legally binding. Take, for example, an insurance company which transfers confidential medical information to an associated medical facility. An unauthorised medical facility staff member receives the communication and then for malicious or monetary reasons, threatens to release subscriber information to employers and other interested parties. The authorisation breach occurs within the confines of the medical facility, but the insurance company is accused of liability. How many thousands of lives could be affected in this single incomplete transaction? How many lost customers? What price in customer confidence and reputation? And how many ensuing legal battles?

Let's also imagine that a high-tech manufacturer based in Europe accepts a contract from a supplier in the US. It then [MH1]begins to market and manufacture its product. But when the required parts fail to appear on time, the supplier disavows the contractual agreement. This is because communication occurred online and the necessary evidence is unavailable. The company has no legal recourse. Meanwhile, the major customers are lost and the after-effects ripple throughout the company's supply chain.

And finally, what about a company who accepts a contract from a supplier internationally and supplies a letter of credit, but the supplier rejects the letter of credit because it's communicated digitally, and neither the supplier nor his bank has the means to verify its authenticity or legal validity?

Legally binding e-commerce

Such examples only serve to illustrate that legally binding electronic commerce is critical to support high-value transactions. Achieving legal-grade

Reprinted with permission of TELECOMMUNICATIONS, from the March 2001 issue
©2001 Horizon House® Publications, Inc.

e-commerce, however, involves several complex issues. Some relate to security — others to the law — while additional issues relate to operational practices in place for the parties engaging in the high-value e-commerce. But to really understand what it means to be legal-grade, it's first important to understand the more basic issue of how legally binding contracts are formed between entities transacting business.

It is important for the future of high value e-commerce that enterprises adopt open and neutral security solutions designed to protect all phases of the e-transaction lifecycle.

When two parties engage in business, they mutually agree to a set of assurances with each other. For any transaction exceeding US$400 (€430), law requires that the parties put their agreement in the form of a written contract. The contract can then be used as evidence by a court of law or an arbitrator in resolving any disputes between parties.

The concerns about the validity and enforceability of a traditional contract are similar to the concerns regarding a digital contract (*see sidebar*). The question that confronts us now is how do we put an effective means in place, which allows enterprises to implement a legally enforceable digital contract system? The computer industry has, until now, focused on creating security, encryption, and trust technologies for concealing and signing data transmissions, detecting network intrusions, and authenticating user identity with digital certificates. But without an effective means for businesses to put all these technologies together, enterprises are still unable to rely on the internet for high-value business transactions. So if enterprises are to proceed with confidence they must first address three issues.

Firstly, what security and trust technologies are needed by parties doing business with each other to satisfactorily meet the tests of evidence required for a digital contract? Secondly, what business practices must the enterprise conform to in order to meet the tests required by the laws of evidence? Finally, how should enterprises deal with the legal uncertainties and the relative newness of digital contracts?

Testing a contract

A contract's most important function in a court of law is that of being used as evidence of an agreement between the parties conducting business. When a court examines a contract, it applies several tests to determine whether or not a contract was properly formed between the parties. Specifically, these tests include:

- *authentication* — is the contract an original document?
- *signature* — have the parties involved signed it and can we demonstrate that they indeed intended to sign a contract?
- *writing* — is the contract in the 'proper' form that one might expect a contract to be in?
- *validity* — are the terms legal?
- *operational* — were the signing parties authorised to do so at the time they did?
- *effective* — is the contract 'in force' now?
- *record* — have the parties kept a copy of the record safely?
- *registered* — if required, have they recorded the document in a registry?

When a court examines a contract in digital form, these tests need to be changed appropriately:

- *Authentication*

Can the digital contract be truly verified as the original that the two parties agreed to? In other words, can there be assurance that its content is complete and unaltered? Is there proof that the electronic communications involved in the business transactions actually came from the parties that they purport to come from?

- *Signature*

Can we be sure that the two parties involved intended to sign the document and indeed did so? Can we be sure that the individual that signed had the authority to commit his organisation to the transaction? Did the system for exchange and signing of digital contracts enable each recipient to determine who really sent the message, and if that individual is, in fact whom he says he is?

- *Writing*

Did both parties sign an identical version of the contract? Is the contract in a standard digital form? Can we be sure that each party when signing the contract submitted their signatures to the other and was sure of delivery? Do we have proof of the content of the transaction, namely the communications that actually occurred between the parties during the contract formation process?

- *Validity*

If the contract called for the terms to be confidential (as many do) then did the system for implementing digital contracts ensure prevention of disclosure of the transaction to unauthorised persons?

- *Operational*

Is the contract properly time-stamped? Can it be verified that the individuals that signed digitally had the authority to sign at the time they did?

- *Record*

Can the parties demonstrate that they both kept a copy of the contract in a tamper-proof and secure manner? And can they demonstrate that they took measures to reduce the possibility of deliberate or inadvertent alteration of the contents of the electronic record of the transactions?

- *Registration*

If required, was the digital contract recorded at a digital notary service?

[MH1] Chini — "Asia" OK? There was nothing here to indicate where the supplier was located.

Reprinted with permission of TELECOMMUNICATIONS, from the March 2001 issue
©2001 Horizon House® Publications, Inc.

Technology choices

To address such questions and build legal-grade e-business systems, enterprises must make important technology choices, combined with the implementation of essential operation procedures.

Certificate authority (CA) can be chosen by determining the use of digital certificates for authenticating the identity of the individuals involved in business transactions. An example of this is the Identrus set of banks, or certificate issuers, recognised as 'licensed' by the state and federal governments.

> There is now a new market shift underway where enterprises are moving away from proprietary EDI technology and paper, towards a more open internet infrastructure.

Validation can be achieved by building a set of e-business applications in such a way that all digital certificate transactions and digital signatures are validated in real-time prior to acceptance.

Secure delivery and receipt transactions, authenticated using trust infrastructure services, must be properly 'received'. The recipient should formally acknowledge error-free delivery of data and also formally accept responsibility for handling the transaction.

Enterprises should also build their e-business applications in such a way that all business communication is acknowledged with a tamper-proof digital receipt that can be stored in long-term, secure, and tamper-proof storage. Enterprises should also retain records of transactions and contracts, along with digital certificates for pre-specified records and retention periods. This is required by the type of transaction, and by transaction-specific laws.

Finally, transactions seeking the benefits of trust infrastructure services and transaction documents (representing contracts), should be in an industry standard form (such as PDF) as much as possible.

Operational procedures

Companies should retain and hire personnel that are familiar with security operation procedures and have personal knowledge of how a system can operate securely, and how it actually operated during creation or storage of a record. Alternatively, they should outsource to a dedicated provider of trust and security systems, so that the sanctity of the transactional system can be maintained with minimal specialised expertise.

With regard to software quality and trust, certain software components in a legal-grade e-business application are specifically geared towards providing trust and security requirements. Such systems, known as trust provider systems, should be supported (or purchased) from vendors that support trusted software engineering processes that leave a trail of design decisions for each stage in the manufacturing process. The trail support proves the reliability of a records system, which in turn supports the claim of integrity, authenticity, and admissibility of a record as evidence. The functions and systems of trust provider's systems should be documented in a formal 'security target' documentation format. This supports evaluation and certification that an implementation satisfies the formalised security requirements. The target should document the functions of the system, and label each as either security critical or security enforcing.

Legal grade e-business applications or their sub-components, specifically targeted at trust and security, should be subject to periodic security audit. This is according to criteria laid down either by state licensing authorities or by mutual consent of the parties. These checks should measure the effectiveness of the management, operational, and technical controls of all trustworthy systems.

A provider of legal-grade e-business systems, either directly or through outsourced trust service provider relationships, should be able to demonstrate financial responsibility for the amount of liability that it explicitly accepted.

In conclusion, it is important for the future of high-value e-commerce that enterprises adopt open and neutral security solutions designed to protect all phases of the e-transaction lifecycle — regardless of which certificate authorities, payment vendors, or applications are used. To protect themselves before conducting a transaction, enterprises must validate the identification credentials presented to them. Without validation, fraudulently obtained or revoked digital certificates can be used to access confidential information or infiltrate to the heart of a business. In addition, enterprises may not be able to trust certificates from business partners and customers that use other security systems. Organisations must have a secure, fast, and reliable way to send sensitive data over the internet. Enterprises must also be able to securely generate, exchange, archive and reconstruct e-transactions in an auditable manner. They should also make electronic contracts and transactions legally binding by providing all the essential elements of non-repudiation. Finally, as the world of commerce moves towards a paperless environment, issues of delivery documentation, transaction integrity, and dispute resolution will increase in frequency and importance. Digital receipts will offer proof that an e-transaction occurred at a specific time and date, in accordance with government regulation, and with proper authorisation, while preserving the audit trail in a safe and secure location. This is the necessary infrastructure, which must be in place, securing e-transactions from end-to-end to conduct high-value and legal grade e-commerce. ▼

Alex Garcia-Tobar, *vice president, international operations, ValiCert*

Reprinted with permission of TELECOMMUNICATIONS, from the March 2001 issue
©2001 Horizon House® Publications, Inc.