The future of high value E-Commerce

ISSE

The Future Of High Value E-Commerce

High value e-commerce is projected to rapidly shift from proprietary Electronic Data Interchange (EDI) technology and paper-based transactions and more towards the Internet and open digital signature-based solutions.

PETER WILLIAMS

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 exchanging 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, and more towards an open Internet infrastructure.

Request for an open EDI

So why the dramatic change, when current EDI systems support procurement efficiencies, enable savings by automating tasks, increase visibility of information among vendors plus provide stronger links to customers, partners, and suppliers? 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 plus enhanced procurement efficiencies.

Extranet and security

Yet the extranet environment also poses new challenges. By far the most important, is the need to protect the high-value transactions typical of B2B commerce, financial services and related areas. 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? Or a higher-value purchase like an airline ticket or a personal computer? One way or another, the average transaction will likely fall below — probably well below — the US-$ 1000 mark. Yet 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 protects consumers engaging in e-commerce, there are no such guarantees in place for B2B e-commerce.

Legal-grade protection

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. The following examples offer an insight into potential fallout from unprotected B2B transactions:

- An insurance company transfers confidential medical information to an associated medical facility. An unauthorised medical facility staff member receives the communication and – 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?
- In Europe, a high tech manufacturer accepts a contract from a supplier in the US and begins to market and manufacture product. But when the required parts fail to appear on time, the supplier disavows the contractual agreement. Because communication occurred online and the necessary evidence is unavailable, the company has no legal recourse. Meanwhile, major customers are lost and the after-effects ripple throughout the company's supply chain.
- Finally, a company 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.

Such examples only serve to illustrate that legally binding electronic commerce is critical to support high-value transactions. In order to achieve widespread acceptance of such high-value e-commerce, a level of integration and enhancement of legal protections similar to the ones that EDI offers, must also be made available within the Internet environment. Achieving legal-grade e-commerce, however, involves several complex issues. Some relate to security, others to the law, while additional issues relate to operational practices in place at 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 do legally binding contracts get formed between entities transacting business.

Test of Contracts

When two parties engage in business, they mutually agree to a set of assurances to each other. For any transaction exceeding four hundred dollars, law requires that the parties put their agree-

ment 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. From a legal standpoint, a contract's use in a court of law as evidence of the agreement between the parties conducting business is its most important function.

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 are:

- Authentication: Is the contract an original document?
- Signature: Have the parties involved signed it? 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?
- Effectiveness: Is the contract "in force" now?
- Record: Have the parties kept a copy of the record safely?
- Registration: if required, have they recorded the document in a registry?

When a court however 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, who he says he is?

– Verification

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?

– Security

Can the parties demonstrate that they both kept a copy of the contract in a tamper-proof and secure manner? Can the parties 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?

Digital contract system

The concerns about the validity and enforceability of a traditional contract are similar to the concerns regarding a digital contract. 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 encrypting and signing data transmissions, detecting network intrusions and authenticating user identity with digital certificates. Yet 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. If enterprises are therefore 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 indeed deal with the legal uncertainties and the relative newness of digital contracts? To address such questions and build legal-grade e-business systems enterprises must make important technology choices combined with the implementation of essential operations procedures:

Technology Choices

Choice of CA

Use digital certificates for authenticating the identity of the individuals involved in

business transactions. Specifically, select digital certificates issued by members of well-accepted digital identity consortiums such as the Identrus set of banks or certificate issuers recognised as "licensed" by state and federal governments.

Validation

Build 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.

Long Term Archiving

Enterprises should 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, tamper-proof storage. Enterprises should build e-business applications that retain records of transactions and contracts along with digital certificates for prespecified records retention periods as required by the type of transaction and by transaction-specific laws.

Document Standards

Transactions seeking the benefits of trust infrastructure services should be in an industry standard form (such as PDF) as far as possible. Transaction documents representing contracts should be in as standard a form as possible to conform to traditional writing requirements.

Operations Procedures

Personnel

Retain and hire personnel who are familiar with security operations procedures and have personal knowledge of how a system is both supposed to operate security and how it actually operated during creation or storage of a record. Alternatively, outsource key security and trust operations to a dedicated provider of trust and security systems so that the sanctity of the transactional system can be maintained with minimal specialised expertise.

Software Quality and Trust

Certain software components in a legal-grade e-business application are specifically geared towards providing the trust and security requirements. Such systems – 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 a claim of integrity and, therefore, authenticity and admissibility of a record as evidence. The functions and systems of Trust Providers systems should be documented in a formal "security target" documentation format that 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.

Audit

Legal grade e-business applications or their subcomponents specifically targeted at trust and security should be subject to periodic security audit 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.

Liability

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.

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 life cycle, 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 who 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, as well as 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,

Zusammenfassung

Die Zukunft des High Value E-Commerce

High Value E-Commerce wird sich schnell von proprietärer EDI-Technologie (Electronic Data Interchange) und papiergestützten Transaktionen hin zum Internet und zu offenen Lösungen auf der Basis digitaler Signaturen verlagern. Anders als beim E-Commerce im Verbraucherbereich, der schnell zum Trend wurde, wird HighValue E-Commerce für verschiedene Anwendungen wie Supply Chain Management, Handelsfinanzierung, Darlehensbearbeitung, Gesundheitsfürsorge und Informationszugriff normalerweise durch grosse Unternehmen abgewickelt. Diese tauschen Daten entweder über proprietäre Netzwerke in EDI-Formaten oder durch papiergestützte Mechanismen aus. Auf dem Markt ist nun aber eine neue Änderung feststellbar, nach der sich die Unternehmen von proprietärer EDI-Technologie und Papier wegbewegen, mehr hin zu einer offenen Internet-Infrastruktur. Für die Zukunft des High Value E-Commerce ist es wichtig, dass Unternehmen offene und neutrale Sicherheitslösungen annehmen, die eine E-Transaktion in allen Phasen ihres Lebenszyklus schützen, unabhängig von Zertifizierungsstellen, Zahlungsabwicklern und Anwendungen.

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. [4]

For more information about ValiCert Inc:
Dan Chappell
Andrew Lloyd & Associates
+44 1273 675100
dan@ala.com

Peter Williams *joined ValiCert as security architect in 1998, after leaving VeriSign, Inc where he was Chief Architect responsible for the company's Internet debut in 1995. Previously, he worked at University of London as a security architect and research fellow from 1989. Whilst working at NASA Ames Research (via Sterling Software in 1991), he was involved in a series of high-profile EEC, NASA, USPS, IRS, DOD/NSA projects to apply digital signatures to government services. Peter Williams is a computer science graduate of University College London, and is currently preparing to submit a doctoral dissertation on trusted transactions to the same university. He will be speaking at ISSE 2001 – Information Security Solutions Europe – from 26-28 September 2001 at QEII Conference Centre, London. This article has been written as part of a series for ISSE 2001.*

Web-Engpässe

Der Internet-Software-Hersteller Mercury Interactive stellt fest, dass 35% der Performance-Engpässe im Internet ausserhalb der Firewalls zu suchen sind. Mittels verschiedener Tests haben die Experten von Mercury Interactive vier häufige Ursachen für Engpässe im Internet festgestellt: Datenbank-Tuning, Netzwerk-Flaschenhälse und die Konfiguration von Anwendungs-Servern beziehungsweise Web-Servern. Die Schwachstellen ergeben sich hauptsächlich daraus, dass Router, Gateways und Switches schlecht aufeinander abgestimmt sind. Mercury betont, dass Performance-Probleme in praktisch jedem Teil der Web-Infrastruktur auftreten können. Auch wenn die Server, Datenbanken und Applikationen einer Website für sich sehr robust sind, können sie teilweise die volle Leistung nicht erbringen, wenn sie miteinander kombiniert werden. So treten 98% der Performance-Probleme deshalb auf, weil die Infrastrukturkomponenten für eine bestimmte Anwendung nicht optimiert oder nicht richtig konfiguriert sind.

Homepage: www.mercuryinteractive.ch

Optische Silizium-Saphir-Chips

Der US-Chiphersteller Peregrine Semiconductor will mit seiner auf Saphir basierenden Technologie in den Markt für optische Netzwerktechnologie einsteigen. «Wir wollen für die Telekomindustrie dasselbe erreichen, was Intel für die Computer-Industrie getan hat», erklärte Ron Reedy, Chefentwickler von Peregrine. Bisher hat sich das Unternehmen vor allem auf die Erzeugung von Telekommunikations-Prozessoren für Satelliten- und Mobilfunk-Anwendungen konzentriert. Der neue Netzwerk-Chip übersetzt optische Signale in elektrische Daten und ermöglicht Übertragungsraten von 3 Gbit/s. Mit der weiteren Miniaturisierung der Prozessoren will das Unternehmen bis zum Jahr 2003 eine Übertragungsleistung von 40 Gbit/s erreichen. Gleichzeitig soll die Reichweite der optischen Elemente gesteigert werden. Dazu soll die Produktionsanlage bis 2003 für 0,13-µ-Technologie aufgerüstet werden. Peregrines Silizium-Saphir-Technologie wurde ursprünglich für die US-Navy entwickelt. Saphir hat gegenüber anderen Halbleitern wie Silizium und Germaniumarsenid den Vorteil, dass es keine Energie absorbiert. Damit kommen Silizium-Saphir-Chips mit weniger Energie aus und erlauben gleichzeitig höhere Taktraten.

Homepage: www.peregrinesemi.com

Internet-Betrug

Das grösste Risiko betreffend Betrug im Internet geht von den eigenen Mitarbeitern aus, heisst es in der globalen «e.fr@du»-Studie von KPMG Forensic Accounting. Da Führungskräfte diese Tatsache oft unterschätzen, fehlen die entsprechenden Sicherheitsvorkehrungen. Oft werden beim Reparieren des angegriffenen Systems wichtige Beweismittel vernichtet. «Die meisten Sicherheitsverletzungen werden von Personen begangen, die mit den Systemen, die sie angreifen, bestens vertraut sind», erklärt Norman Inkster, Vorsitzender von KPMG Investigation & Security Inc. sowie des International Forensic Accounting Committee von KPMG. 79% der befragten Führungspersonen sind jedoch der Meinung, dass in ihr E-Commerce-System höchstwahrscheinlich über das Internet oder über andere externe Zugangsmöglichkeiten eingebrochen wird. Dementsprechend werden Sicherheitsvorkehrungen in Angriff genommen. Weniger als 35% der befragten Führungskräfte gaben an, dass an ihren E-Commerce-Systemen Sicherheitsprüfungen durchgeführt werden. Davon verfügt wiederum nur die Hälfte über entsprechende standardisierte Sofortmassnahmen, wenn eine Verletzung vorliegt. «Das Erste, das angegriffene Unternehmen tun, ist, den Schaden möglichst schnell zu beheben, damit das System wieder in Betrieb genommen werden kann», erklärt Peter Cosandey, Leiter Forensic Accounting. «Dabei ist ihnen nicht bewusst, dass sie auf diese Weise Beweismaterial vernichten und es fast unmöglich machen, Vermögenswerte zurückzuholen oder rechtliche Schritte einzuleiten.» Die Ergebnisse der Studie basieren auf 1253 Antworten der grössten öffentlichen und privaten Unternehmen in Australien, Belgien, Kanada, Dänemark, Deutschland, Hongkong, Indien, Italien, Südafrika, der Schweiz, Grossbritannien und den Vereinigten Staaten. Sie kann ab Freitag im Internet abgerufen werden.

Homepage: www.kpmg.ch