Chapter
10

Trust in Business-to-Business Marketplaces

Business-to-consumer (B2C) Net marketplaces pioneered the use of the Internet as a platform to conduct commerce, but the emerging business-to-business (B2B) marketplaces will be the main beneficiaries of all the earlier innovations. B2B e-commerce is growing beyond comprehension. Gartner Group predicts that 7,500 to 10,000 B2B marketplaces will emerge by 2002 and estimates that businesses will spend $7.2 trillion by 2003 on Internet-based business relationships.

What is the risk-management system behind these emerging Net marketplaces? What is the accountability and assurance infrastructure? What is the legal framework? What are the responsibilities and liabilities of the buyers and the sellers? How do we ensure the integrity of electronic commerce systems? The answers are simple, although the structures that implement the solutions are extremely complicated and are still evolving. This chapter investigates trust—the common thread to all the above questions—in B2B Net marketplaces.

B2B Net Marketplaces

A **B2B Net marketplace** is a commerce site that enables communities of buyers and sellers to meet on the Internet and to conduct trade. B2B marketplaces eliminate the inherent inefficiencies in traditional markets by improving the relationship between buyers and suppliers, reducing supply chain costs, and promoting price discovery. When its total purchase volume crosses a threshold, a B2B marketplace becomes extremely efficient and converges toward the most perfect trading structure ever developed in the history of commerce [ARIB00].

The B2B Internet business model has come a long way since the early days of electronic data interchange (EDI), which creates one-to-one relationships between businesses that have well-established trading practices. EDI systems are costly and cannot leverage implementations across various trading partners, even though a lot of effort has gone into standardizing EDI transactions. Business-to-consumer (B2C)

marketplaces, such as Amazom.com, represented a major shift away from the EDI paradigm and revolutionized the Internet as a platform for conducting commerce. The B2C business model generally creates one-to-many relationships between one distributor and many buyers. Because a single distributor does not typically aggregate all the suppliers in an industry, B2C marketplaces are not very efficient and do not meet the requirements of corporate procurement. Buyers are responsible for comparing prices across various B2C marketplaces in order to find the most attractive purchase costs.

Meanwhile, enterprise resource planning (ERP) vendors have extended their legacy purchasing systems to the Internet. End users invoke ERP processes from their Web browsers, view supplier catalogs, and procure products; the back-office ERP systems conduct the transactions and update accounting information. Web-based ERP systems lower transaction costs by improving the end user experience, eliminating the need for fat ERP clients, and extending functionality to external business partners. Such systems are not, however, very efficient trading structures. Corporate procurement must set up and maintain catalogs for each supplier and does not benefit from the supplier liquidity, owing to the size of the supplier base.

B2B marketplaces represent the most efficient trading structures because they support many-to-many relationships between buyers and suppliers. The aggregate of suppliers injects liquidity into a marketplace; the aggregate of buyers pushes the marketplace total purchase volume over the threshold, where economies of scale kick in and the marketplace becomes an ultimate trading platform. Pricing models, such as auctions, become dynamic, further increasing market efficiency.

Trust

Trust is the bedrock of commerce systems. As they reshape B2B commerce relationships and replace traditional commerce structures—which took centuries of legal proceedings to mature—B2B marketplaces must address how they intend to provide trust, enforce contracts, and establish a legal framework.

Distributed Trust Management

Pioneers of Internet electronic commerce created the first secure electronic environments for selling goods and services and receiving payments. The Secure Socket Layer (SSL) protocol and Web server SSL digital certificates were the technological advancements that secured the electronic trading environments. The SSL protocol uses server certificates to authenticate a merchant to customers and to securely transmit payment information, such as credit card numbers, over the Internet. The padlock that appears in a browser reminds a customer that the SSL protocol is in effect and that all the network communications with a merchant are encrypted.

Customers have now embraced the Internet B2C business model and trust these electronic trading environments. When they connect to a secure merchant site, customers trust the identity of the site and are willing to send private information to the party on the other side of the network connection. Trust seems to be the common thread woven through the entire fabric of the Internet business model. But what is the nature of this trust, and what is its source? What is the most fundamental problem that the notion of trust attempts to address?

Risk management and integrity are the essence of trust. Secure electronic commerce systems are a complex web of processes and software programs operating on a framework of accountability and assurance. Public key infrastructures (PKIs) provide the accountability and assurance structure needed to conduct commerce electronically. Certification authorities (CAs) authenticate merchants and manage their credentials; CAs assume liability for the quality of their authentication processes and adhere to their Certificate Practice Statements (CPS). Software vendors prepackage a set of public trust points for customers and merchants to help them automate their trust-based buy and sell policies. Customers are responsible for protecting their private keys and may have to assume liability for compromised keys. Merchants should distinguish between legitimate shoppers and fraudulent users in real time to reduce their liability for unpaid goods and services. In secure electronic commerce systems, every participant has responsibility for the integrity of a subsystem and assumes liability for it. When every subsystem has integrity, the overall commerce system has integrity and manages the risk by distributing it to all the participants.

What gives a secure electronic subsystem integrity? Secure transactional systems rely on a set of underlying trusted security services to ensure their reliable and correct operations; these security services in turn rely on a set of security mechanisms, cryptographic algorithms, and keys for their trusted functioning. If security algorithms are reliable, a system's trustworthiness and integrity ultimately boil down to the trustworthiness of the underlying cryptographic keys.

What is the measure of trust for keys? Keys are trustworthy if the system that distributes them is trustworthy. In other words, trustworthiness of a key distribution system translates into the trustworthiness of distributed keys, which ultimately translates into the trustworthiness of a secure electronic commerce system. Secure key distribution systems play a critical role in establishing trust for Net marketplaces. These systems authenticate marketplace participants, bind their identities to cryptographic keys, seal the keys and all the relevant identity information in tamperproof data structures called certificates, transport the certificates in public networks, and deliver the certificates to clients, enabling them to make trust-related decisions.

How trustworthy is a key distribution system? Key distribution systems are as trustworthy as the certification authorities that operate them, create keys, and manage the life cycle of keys. The trustworthiness of a certification authority directly

translates into the trustworthiness of the key distribution system that it operates and ultimately determines the integrity of an electronic commerce system. Certification authorities create trust in Net marketplaces and operate the accountability and assurance framework necessary for automating the rule-based transactional polices.

How trustworthy is a certification authority? Certification authorities have a Certificate Practice Statement (CPS) that clearly states their polices and practices for issuing and maintaining certificates, their liabilities toward relying certificate-using systems, and the obligations of their subscribers and the systems that rely on their certificates. Eventually, a CA's employees operate the computer stations and approve certificate enrollment requests; management must ensure that the operators abide by the stated practices. Accounting firms perform accreditation, audit, and arbitration processes to ensure that certification authorities adhere to their stated policies and detect violations from standard practices. Certification authorities are, therefore, as trustworthy as their certification practices and the accounting firms that ensure their accreditation. "By assuring the process of issuing and managing digital certificates, particularly by assuring the distribution of trust points, we obtain a trusted public key certification system that engenders accountability of communicating parties and the operational status of transactions" [FEGH98], p. 271.

Because they have to support many-to-many relationships between buyers and suppliers transacting in extremely dynamic trading structures, B2B marketplaces require a great deal of flexibility from trust management systems. Sellers want to know who the buyers are and whether they can afford to pay for purchased goods and services; buyers want to know who the sellers are and whether they can deliver the advertised goods and services. The trust management system must reliably and correctly identify the selling and buying agents, specify their organizational affiliations, and specify reasonable limits on the transactions they can conduct.

Stakes are higher in B2B transactions. The average B2C transaction value is $75; the average B2B transaction value is $75,000 [ARIB00]. Once a seller and a buyer negotiate on a transaction, the trust management system must provide assurance that they will not later repudiate the transaction. Gathering and archiving audit trails are crucial, as disputes will arise. The trust system must support all phases of the customer experience—selection, purchase, delivery, and support—and must also ensure the privacy of transactions.

Monolithic trust systems cannot function in B2B marketplaces. Trust must be distributed but chained to global trust networks, to increase the number of buyers and sellers and to maximize the total purchase volume. Businesses should be in charge of authenticating their own buying and purchasing agents and may also want to authenticate their business partners. These local networks of authenticated users must interoperate with other local networks in B2B marketplaces. It should not matter which local authority has authenticated a buyer or a seller; that a buyer can pay and that a seller can deliver goods are relevant factors. Global trust net-

works integrate these local trust networks and supply a framework for accountability and assurance.

Real-time identity verification of B2B marketplace participants is critical. Purchasing agents who leave their organizations must not be able to buy from the moment they lose their affiliations. The distributed trust system must supply such vital information to all the marketplace players in real time; any latency weakens the assurance framework and decreases the efficiency of the marketplace. B2B marketplace players must be able to roam and to submit buy and sell orders from their office computers, home computers, and airport computer kiosks. The distributed trust system must allow them to roam and to deliver their credentials over public networks to them.

Such a distributed trust system provides transparency in a B2B marketplace and promotes its efficiency. Buyers and sellers engage in commerce and trade with parties that they may not have transacted with before. Local networks of authenticated business agents plug into global trust networks and transparently access the marketplace. The distributed trust infrastructure provides real-time identity verification information for all network users and allows agents to roam, providing integrity for transactions and managing the risk by distributing it among all the players. With the increased level of trust, more buyers and sellers join the marketplace; usage increases and total purchased volume goes beyond the threshold. The marketplace becomes a perfect trading structure and operates with maximum efficiency.

Verifiable Trust

Public key infrastructures provide trust for B2B marketplaces. But to be effective, trust must be verifiable, and electronic commerce transactions must be nonreputable. If a seller agrees to deliver goods or services, the buyer must be able to seek damages if the seller later repudiates the transaction; the seller must be able to litigate if the buyer refuses to pay for the delivered goods or services. The trust infrastructure must create and maintain an electronic paper trail for e-commerce transactions in order to resolve disputes and to enable litigation.

Statutes and court rulings have established legal precedents for commercial relationships to govern commerce and to enforce contracts. The Statute of Frauds, embodied in the Uniform Commercial Code, requires an enforceable contract to be in writing, signed by the party against whom enforcement is sought. Writing is defined to include printing, typewriting, or any other intentional reduction to tangible form; signed is defined as any symbol executed or adopted by a party with present intention to authenticate a writing. Traditional commerce systems generate paper-based documents, such as signed contracts, invoices, payment receipts, and settlement records, that can be used in litigation when disputes arise.

A fair amount of legal confusion has existed ever since the judiciary began to view electronic records as intentional reduction to tangible form. Witnesses and juries did

not fully understand electronic paper trails, which do not have the same tangible look and feel of a traditional paper trail. Judges had to reexamine the laws and to reinterpret them in a new context. The confusion, however, is lessening, and clarity is emerging as the legislative and judicial systems are catching up with the technology. Most jurisdictions today consider electronic records to qualify as writing for the Statute of Fraud purposes. Furthermore, electronic records, such as e-mail, which evidence directly or circumstantially the sender's assent and self-identification, have generally been considered as signed for the Statute of Frauds purposes. The recently signed electronic signature bill set a national legal standard for electronic signatures and records. The bill gives electronic signatures the same legal authority as signatures written with pen and ink. The electronic medium now has the same legal effect and enforceability as the medium of paper.

Digital signatures are the building blocks for verifiable, nonreputable trust in electronic commerce systems. The asymmetric nature of public key technology allows users to share their public keys with the outside world while keeping their private keys to themselves. An e-commerce transaction digitally signed by a private key strongly binds the owner of the private key to the signed transaction. Digital signatures can later be verified to ascertain the bindings, if disputes arise, and to enforce contracts.

Digital signatures must be time stamped to ensure that they last forever. Reliance on a digital signature is permitted if the private key used to generate the signature was in its operational period at the moment of use. Private keys cease to be operational when their corresponding public key certificates expire or when the issuing certification authorities revoke their corresponding public key certificates. Signatures that are not time stamped expire when private keys expire and become invalid when private keys are revoked. Time stamping, however, prevents dishonest users from repudiating a transaction on the grounds that their private keys were expired or revoked when the transaction was signed. Time-stamped signatures last well beyond the expiry or revocation of keys.[1]

The trust infrastructure must archive all the relevant electronic records for years. The archival system must be redundant and provide for disaster recovery. The trust infrastructure must provide authenticated access to data repositories to aid the litigation process.

B2B Trust Services

We provided an overview of security management solutions in our book on digital certificates [FEGH98] and covered a number of PKI vendors that offer certificate

1. Note that the trust infrastructure must ensure that private keys are operationally valid when they are used to generate signatures.

toolkits, certificate servers, certificate management workstations, and outsourced certification services. Many of these vendors have now enhanced their products to enable secure communications and transactions in B2B marketplaces. These enhancements range from point solutions, such as supplying real-time revocation information or supporting time stamps, to a portfolio of comprehensive B2B trust services. Because most of these PKI vendors are still defining their B2B solutions and are in early phases of integration testing, we will not attempt to analyze the B2B trust services deployed in the marketplace. Instead, we identify authentication, payment, and validation as three broad categories of B2B trust services and provide a brief description of each category, using VeriSign as a third-party trust provider.

Authentication

VeriSign Authentication services [VERIA] provide identity establishment, credential management, identity validation, and directory services for B2B Net marketplaces. These services address the authentication issues for B2B environments, such as establishing polices for unknown organizations and individuals, implementing delegated authentication, minimizing risk and liability, devising security and auditing process, and providing around-the-clock availability.

The OnSite service provides managed PKI and delegated control over trust polices, enabling organizations to issue digital certificates to partners, customers, employees, servers, routers, and firewalls. The Roaming service provides a network-based credential distribution system by securely storing private keys on the network and delivering them to users who roam and need to access their profiles from any computer terminal attached to the network. The Online Certificate Status Protocol (OCSP) [MYER99] service supplies real-time revocation information for high-value B2B transactions.

Payment

VeriSign Payment services [VERIB] address the fragmented Internet payment systems that connect on-line merchants to banks via privately operated, point-to-point networks. The Payment services provide an Internet payment gateway that supports multiple payment instruments, connects to all relevant back-office payment processors, offers uniform interface access to payment functions, and allows merchants to switch between alternative financial instruments and payment processors.

The Payflow Internet payment service supports all major consumer credit card, debit card, electronic check, purchase card, and automated clearinghouse (ACH) transactions. Additional Payment services include functionality for fraud detection and risk management, and application integration with back-office and B2B payments systems through an Extensive Markup Language (XML) application integration layer.

Validation

VeriSign Validation services [VERIC] support digital notarization, digital receipts, digital records, and dispute resolution for Net marketplaces. In digital notarization, VeriSign acts as a third-party witness to an e-commerce transaction and archives electronic bookkeeping records needed to later prove that a transaction has taken place. The Digital Notarization service creates an electronic time stamp of a transaction,[2] notarizes the transaction by adding a digital signature to the time-stamped transaction to create a digital receipt, and delivers the receipt to the transacting parties.

Digital receipts provide nonreputable proof of transactions by linking authentication, validation, and Internet payment processing. The digital receipt repository securely archives the digital receipts, provides an authenticated access mechanism to retrieve the receipts, and supports a mechanism to determine their validity.

Summary

A B2B Net marketplace is a commerce site that enables communities of buyers and sellers to meet on the Internet and to trade. B2B marketplaces eliminate the inherent inefficiencies in traditional markets by improving the relationship between buyers and suppliers, reducing supply chain costs, and promoting price discovery.

Trust is the bedrock of commerce systems. As they reshape B2B commerce relationships and replace traditional commerce structures, B2B marketplaces must address how they intend to provide trust, enforce contracts, and establish a legal framework. The trustworthiness and integrity of an electronic commerce system ultimately boil down to the trustworthiness of the underlying key distribution system, which is as trustworthy as the certification authority that operates it. Certification authorities are as trustworthy as their certification practices and the accounting firms that ensure their accreditation.

Trust must be verifiable, and electronic commerce transactions must be nonreputable. The digital signature bill gives electronic signatures the same legal authority as signatures written with pen and ink; the electronic medium now has the same legal effect and enforceability as the medium of paper. Digital signatures are the building blocks for verifiable, nonrefutable trust in electronic commerce systems. Digital signatures, however, must be time stamped to ensure that they last forever.

---

2. The Public Key Infrastructure Working Group of IETF (PKIX) [http://www.ietf.org/html.charters/pkix-charter.html] is developing standards for a time-stamp protocol for the Internet X.509 public key infrastructure.

References

[ARIB00] Ariba, "B2B Marketplaces in the New Economy," white paper, 2000. (http://www.ariba.com/com_plat/white_paper_form.cfm)

[FEGH98] Feghhi, J., J. Feghhi, and P. Williams. *Digital Certificates: Applied Internet Security,* (Reading, MA: Addison-Wesley, 1998). (http://cseng.awl.com/bookdetail.qry?ISBN=0-201-30980-7)

[MYER99] Myers, M., R. Ankney, A. Malpani, S. Galperin, and C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP,* Request for Comments (RFC) 2560, June 1999. (http://www.ietf.org/rfc/rfc2560.txt)

[VERIA] VeriSign, "VeriSign Authentication Services," white paper (http://www.verisign.com/rsc/wp/auth_srv/index.html)

[VERIB] VeriSign, "VeriSign Payment Services," white paper (http://www.verisign.com/rsc/wp/pmt_srv/index.html)

[VERIC] VeriSign, "VeriSign Validation Services," white paper (http://www.verisign.com/rsc/wp/valid_srv/index.html)