Bridging E-Business and Added Trust: Keys to E-Business Growth

Do you trust the Internet enough to send your life’s savings to your business partner electronically? How much would you be willing to risk? Are you sure of who you are communicating with at the other end of the line? For electronic commerce to flourish, consumers must be comfortable with the answers to these questions.

What can we do to encourage the continued growth of e-commerce? Legislation passed more than two decades ago—the Electronic Fund Transfer Act, effective 1979 (15 US Code)—forced the credit card and ATM industry to limit a user’s personal financial risk. This limit is usually a maximum of $50 if cards are used fraudulently. Because users did not fully trust the technology, this approach focused on reducing risk.

Limiting risk compensates for a lack of trust. Many, however, consider this approach a Band-Aid for the real issue: How do you increase user trust? Can the technical community now assure the public of higher trust in transactions? If the direct relationship between risk and trust holds true, then the more trust offered, the less businesses need to pay to cover a user’s financial risk. So, if there is a means to increase trust, e-commerce should grow even more rapidly than it has now, when legislation minimizes the risk. Trust is key.

As a consequence of new federal and state legislation in the US (the Electronics Signatures in Global and National Commerce Act, 30 June 2000) and the e-commerce evolution occurring globally, the legal issues of electronically signed documents have taken on a new and more realistic form. US law now recognizes documents transferred electronically over global networks and digitally signed by agreeing business partners as legally binding. International acceptance of digital signatures is following, and in some countries, digital signature acceptance is leading the way toward a paperless society.

Routine Web communications (such as for Internet credit card transactions) are implementing a limited form of digital signatures. In this scenario, your credit card identifiers let a willing business partner (such as a merchant) perform a legal transaction that includes a note for money exchange, either through the credit card company or a bank. Of course, because legislation forces credit card and ATM banking organizations to limit liability, many consider the limited risk to compensate for the lack of trust.

Similarly, banks now let clients electronically access accounts, pay bills, and transfer funds for both minor and major business transactions, including stock purchases and sales. Buyers and sellers must trust each other for the process to work. Buyers must trust that sellers are who they say they are. In turn, sellers must trust that buyers have the valid credit card or bank account...
they claim to have and that buyers will make the payments agreed to.

The risk associated with electronic check or cash transfers has limited the growth of these types of transactions. However, if technology could offer a method that increases the illusive trust factor, it could kick this buyer-seller process into high gear.

**DIGITAL SIGNATURE/AUTHENTICATION**

Currently, the approach most popular with banks is simply authenticating the user based on a password. The bank then takes action for the user in making a bank-to-bank transaction. Real-time, person-to-person transactions do not yet occur without the bank serving as an intermediary.

Currently available public-key processes can help business systems build trust between business partners and clients. An information sender can digitally sign information with his private key, and/or he can encrypt it with the recipient’s public key. Digital signatures provide authentication and information integrity; encryption ensures the information’s confidentiality. After receiving this information, the recipient can authenticate and validate the information’s integrity by using the sender’s public key. The recipient can also ensure the information’s confidentiality by using his private key to decrypt the information. This public-key infrastructure, shown in Figure 1, provides a verifiable method for securing information—all in a single process.

In addition, properly applied PKI methods can support nonrepudiation of information transfers—that is, the sender cannot deny that he sent the information or performed the transaction. Correspondingly, a system can invoke PKI to ensure that a specific recipient does not deny receiving the information or transaction (Carlisle Adams and Steve Lloyd, *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*, New Riders Publishing, Indianapolis, Ind., 1999). By providing support for nonrepudiation, PKI applications offer a significant step forward in adding trust to the current business infrastructure.

One fundamental principle that makes public-key technology work is that users distribute public keys openly but need not distribute or expose private keys, as was the case in symmetric-key approaches.

Although public keys are openly available, they also must be protected to ensure their integrity—that is, people do not modify public keys without authorization or detection. Problems preventing the public key’s distribution or damaging its integrity could contribute to a form of service denial and prevent user authentication. To alleviate these problems, early PKI proponents proposed certificate structures (L., Kohnfelder, *Towards a Practical Public-Key Cryptosystem*, bachelor’s thesis, Massachusetts Institute of Tech., May 1978). Certificate authorities issue, distribute, and maintain the integrity of a certificate that binds the public key to a user’s or entity’s name, private key, and any desired user attributes. To accomplish this function, several forms of certificates have evolved. These include Pretty Good Privacy (PGP), basic attribute, Simple Public Key Infrastructure, and the generally accepted X.509 Public Key certificates (Carlisle Adams and Steve Lloyd, *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations*).

**Why PKI?**

A majority of business systems require personal identification numbers (PINs) or passphrases to access their services. Many argue that PINs and passphrases are doing the job. Why does business need PKI?

Before answering this question, let’s review the identification/authentication approaches shown in Table 1. In the first approach, a PIN and passphrase identifies individuals. The user is generally (though not entirely) responsible for managing his user names and PINs or passphrases, which could possibly vary from service to service. This requirement places too much of a burden on users who have multiple sets of user names with PINs or passphrases.
In the second approach, the user accesses a certificate with a passphrase stored on a removable device (such as a smart card) or on a terminal. The certificate represents the individual as his personal identity throughout the session. Because users must remember only a passphrase, this approach is less of a burden for them than having to remember both a PIN and a passphrase.

The third approach requires users to access a certificate with biometric data. Users need not remember a passphrase, so this system imposes very little burden on them. However, users will have to remember which biometric (iris scan, fingerprint, or so on) to use. This should be a minimal burden because users will standardize on only a few biometric identifiers. For example, a user would primarily use his right thumbprint for identification and his right eye as a backup.

Table 2 highlights key characteristics of PIN-passphrase and PKI approaches. Based on these characteristics, a business could select the approach that best suits its needs.

Typically, a central location manages PIN-passphrase combinations. The user must obtain and store the PIN and passphrase at a central location. Using a PIN and passphrase for access to only one particular service limits this method's system scalability.

On the other hand, an individual can obtain a PKI certificate from any registration/certification authority. With the appropriate policy established, the certificate provides a stronger bonding between the individual and itself. Ideally, the users of PKI-based systems could use a single certificate from one service provider for several different services.

**INDUSTRY STATUS**

PKI-based systems are being installed at the enterprise level and at outsourcing facilities. However, these systems rely on individual certification authorities to issue public keys. Establishing the certificate authorities has been challenging. For example, should there be one or several authorities? Through the lessons learned from credit card vendors, multiple certification authorities are a likely solution that the PKI industry could adapt. The next question becomes, “How should certificate issued by one authority be trusted by another authority?” This problem is similar to that of using one bank’s credit card to pay another bank’s debt.

Today, many companies have started PKI-based programs. These programs generally have four phases to ensure that any PKI user can conduct a business transaction with any other PKI user or system. These phases test operation

- within a local PKI pilot program,
- with selected business partners,
- with all business partners, and
- with all global e-commerce participants.

During the local PKI pilot program, companies learn the functions and features of PKI technology and determine

---

**Table 1. Identification/authentication approaches.**

<table>
<thead>
<tr>
<th>Approaches</th>
<th>Authentication</th>
<th>User burden</th>
<th>Security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users access the system directly, using a PIN or passphrase for identification.</td>
<td>User ID and password</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Users access a certificate using a passphrase; the certificate identifies users to the system.</td>
<td>Certificate</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Users access a certificate using a biometric identifier; the certificate identifies users to the system.</td>
<td>Certificate</td>
<td>Low</td>
<td>Higher</td>
</tr>
</tbody>
</table>

**Table 2. Comparison of PIN-passphrase systems and PKI.**

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>PIN-passphrase</th>
<th>PKI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Centralized</td>
<td>Distributed</td>
</tr>
<tr>
<td>Features</td>
<td>None</td>
<td>A PKI system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• maintains data integrity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• provides authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• supports nonrepudiation</td>
</tr>
<tr>
<td>Personal identity</td>
<td>Moderate</td>
<td>Strong</td>
</tr>
<tr>
<td>Interoperability</td>
<td>None</td>
<td>Evolving</td>
</tr>
<tr>
<td>Management/operation</td>
<td>Local</td>
<td>Global</td>
</tr>
</tbody>
</table>
its usefulness in their business environment. Identifying and developing PKI-enabled applications are this phase’s main effort. When the pilot satisfactorily meets these objectives, a company will probably select a suitable business partner and start a two-way e-commerce experiment. The selected business partner may or may not use the same PKI system and may tend to run its PKI system autonomously. For automatic electronic transaction exchange, the company and its partner must establish a trusted (electronic) relationship. The process and procedures learned in this phase will help expand the system to accommodate other PKI-enabled business partners.

In later phases, the technologies identified in the first phase can have problems scaling to accommodate additional partners. In a global e-commerce environment, a customer could obtain a certificate from an independent registration authority and use it to carry out a trusted electronic transaction with any participating business.

When an entity is ready for the second through fourth phases, it should consider three possible PKI interoperability approaches:

- **Root anchor**, which establishes a trusted relationship through the trusted anchor. The root anchor is a certificate authority (CA) that must certify each business entity’s certificate before such entities can carry out a business transaction. A root CA exists for the organization and issues certificates to all CAs and users beneath it in the hierarchy. As long as a business can trust the root CA, it can trust any certificate that it traces back to being issued from the root CA. However, the root anchor approach leaves very little room for interconnection with other PKIs. A system based on a root anchor is essentially on an island unless it can connect with other PKI systems.

- **Cross-certification**, which is a technology that builds a bilateral trusted relationship between business entities. The trust model for the cross-certificate approach assumes that as long as two business entities trust each other, they can conduct business transactions. There is no need for three parties to institute the trusted relationship, as in the root approach.

- **Bridge system**, which arises as more PKIs use cross-certification to interconnect, there will be a rapidly increasing number of cross-certification agreements. A bridge architecture becomes necessary. CAs wishing to cross-certify merely cross-certify once with the bridge’s CA or one of the bridge’s authorities. These bridge systems are beginning to feature service levels that let users validate a trust path at a predetermined level, where the path itself has been subject to a rigorous check for integrity.

Through the interconnection with a bridge, users at one organization can create complete certificate chains to users at another organization attached to the bridge. A certificate chain is the collection of certificates that constitutes the CAs between sender and receiver. The bridge approach minimizes the cross-certification required and optimizes the operation and management effort.

**GLOBAL E-COMMERCE**

The provisioning of certificate interoperability capabilities is now a rapidly expanding e-commerce field. Several well-known, emerging trust models offer interoperation among the numerous CAs that arise daily. These models can be strictly hierarchical, distributed, Web oriented, or simply user-centric.

A global e-commerce world will combine a variety of bridging architectures such as the CA islands, root anchors, cross-certification, and bridge user configurations shown in Figure 2. The challenge is how to interconnect these distinct user communities so they can interact cohesively. For example, a user of any platform should be able to exchange and verify an electronic transaction sent by another user. The certificate trust path should be validated regardless of the sender and receiver systems.
A centralized database can facilitate the process. When you want to validate the trust path, your PKI-based system sends a request with a distinguished name to a database system. The database’s response should include path information and the path’s policy. The requester will, based on the path information, send out queries to each directory system or status responder for the certificate status. In other words, the architecture uses a centralized database but distributes the path processing.

This process is very much like the Internet domain name server (DNS). When a router cannot resolve a host name, it sends a domain name to DNS, which returns the domain name’s IP address. The local DNS usually services this request—an example of distributed operation. Only when the local DNS fails to translate the given name into an IP address will the router query a centralized database.

The PKI path validation process should work in a similar way. For example, commonly used domain name information can be stored in a local space. But, when the given name is an IP address will the router query a centralized database.

The number of services available to users continues to increase, so will the need to maintain the user’s identity in a secured, trusted manner. The user name and password concept has worked thus far but lacks the portability and scalability that global e-commerce demands. An interoperable PKI system that offers trust services between users will become a common industry practice. We envision that the future global e-commerce system should work with various devices, from desktops to handheld computers. Eventually, one certificate will represent an individual across multiple services and devices.

Hsiao Su Hsiung is president and CEO of ComCert Inc., an information security development firm located in McLean, Virginia. Contact him at hsiung@yahoo.com.

Scott Scheurich is vice president of product development for ComCert Inc. Contact him at sscheurich@yahoo.com.

Frank Ferrante is president of FEF Group LLC and an associate editor-in-chief for IT Pro. Contact him at fferrante@ieee.org.