

This month's column represents installment two of five in our on-going series about security architectures and systems needed to support electronic commerce¹. I had intended to cover the requirement for trusted operating systems, which are a core foundation level security element for any e-commerce site. However, as is quite normal with the Internet today, recent events in the security area have conspired to change my plans. (Just like the typical Internet CEO, authors writing on the Internet must also to be able to change direction on a dime, it seems.) As a result, this quarter's column will cover some timely developments in the area of secure on-line authentication of identity of which you should be aware.

In traditional commerce, authenticating the identity of an individual is relatively straightforward. If you know a counterparty and can physically see him, you can authenticate him. The likelihood of someone creating a physical double for someone well-known to you, requires *Mission Impossible*-like capabilities that few criminals possess. In cases where the individual is physically present but not well-known (e.g. airline check-in, cashing a check at a grocery store), photo-id's such as driver's licenses or passports, or a combination of cards and personal identification numbers (PINs) as are used in debit cards, can validate an individual's identity. This system, while acceptable for most- day-to-day commerce, is not perfect and certainly not acceptable for large-value or high security transactions, as attested to by the number of James Bond movies scripts and spy thrillers that use forged identities as the basis for a plot. Thus, financial institutions and other organisations have made good business creating trust mechanisms, like letters of credit, that reallocate the risks inherent in limitations of time, distance, and lack of identity information in business transactions.

It was recognised as early as the 1960's by the academic community that secure authentication of identity on-line was a security issue for commerce². It was only with the advent of the Internet 30 years later that the problem became more than an interesting academic exercise. Moreover, it is only in 1999 – due to the skyrocketing

¹ See (provide reference to last issue's article please)

² In a September 13, 1999 conversation with Whitfield Diffie, the co-inventor of public key cryptography, I learned that the NSA claims to have recognized the need for secure on-line authentication of identities as early as 1959. Whit was somewhat skeptical of this claim, as am I. However, we do agree that academic and commercial recognition of the problem began in the late 1960's.

growth of business-to-business electronic commerce, with its potential for fraud/theft of large-value transactions – that large scale deployments of systems/networks for secure authentication of identity have become economically feasible. Forrester estimates that the business-to-business e-commerce market will swell from \$48 billion in 1998 to more than \$1 trillion by 2003. Compare this figure to the consumer market. Business-to-consumer e-commerce is only expected to grow from \$7.8 billion to \$108 billion during the same period³. It is the awakening of this “sleeping giant” that has suddenly made on-line authentication of identity critical to you and your customers.

Until recently, most on-line authentication of identity has involved the use of electronic “one-time pads.”⁴ This process involves giving the user a card that generates a unique, secure passcode valid for each on-line session/transaction. The code generated usually has a time-stamp and expiration – so that if the code is not entered in a specific time (e.g. 45 seconds), the code is automatically invalid and the session terminates. The card is unique to the individual, and can only become functional if the user enters an appropriate login sequence onto the card. Thus, the card becomes a secure physical extension of an individual’s identity. Card security is relatively hard to break, since a thief would have to steal both the card and its secure login sequence without the owner’s knowledge.

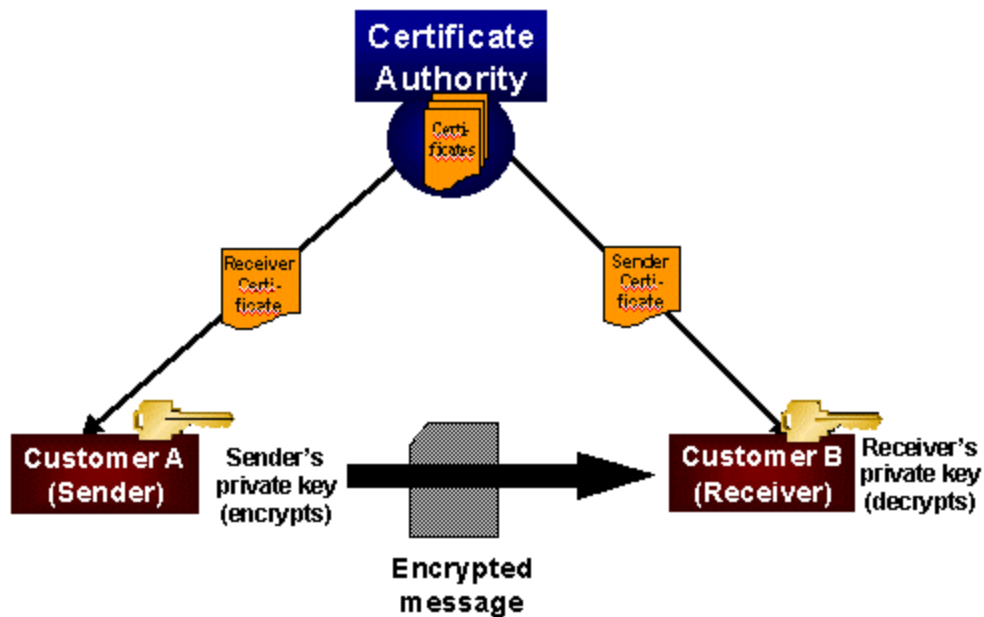
The problem with these electronic one-time pad systems is that they are based on a series of single “private” keys. Private key systems can be used relatively easily in closed systems where a single organization controls the deployment of cards to users and servers to authenticate. However, these systems do not conform themselves well to open buying systems like the Internet, where there is no centralized control between buyers and sellers. Even in coordinated environments, such as on-line supply chains, private-key systems still require a level of IT coordination between parties in the chain that makes private-key systems unwieldy.

³ S. Bell, S. Dolberg, S. Cheema, and J. Sharrard, “Resizing On-Line Business Trade.” The Forrester Report. Forrester Research, v.2, no. 5, November, 1998, page 13 and Sun internal estimates.

⁴ The name “one time pad” is descriptive of the original form of secure messaging. In this form, both sender and receiver have a thick pad of pages. The pads are exactly identical. Each page contains a different algorithm for encrypting/decrypting a message. The receiver encrypts using the current page of the pad; the receiver decrypts. After a single use, both sender and receiver destroy the current page and move onto the next. Thus the name “one-time pad.”

The budding security community recognized these problems with single, “private” key identity systems (also known as asymmetric systems) 25 years ago. As a result they created a new approach based on dual keys and publicly-published algorithms known as “public key cryptography”.⁵ Public-key systems (also known as Public Key Infrastructure or PKI systems) for secure authentication of identity have been used on the Internet almost since it’s inception. If you are using an Internet browser from Microsoft or Netscape, you have a public key (known as a digital certificate) on your computer today. This digital certificate is used to encrypt secure messages you send, as well as to securely authenticate your machine identity (e.g. when you make a stock purchase on-line).⁶

FIGURE 1
How a 3-Corner PKI-Based Digital Certificate System Works



⁵ See B. O’Higgins, “Real World PKI,” Proceedings from the Burton Group: Next Generation Infrastructure Conference, July 28, 1998. For a more thorough technical overview see, B. Schneier, Applied Cryptography, 2nd Edition. (New York, J. Wiley, 1996).

⁶ I say “securely authenticate your machine’s identity because this certificate really cannot authenticate you. But the combination of a recognized machine identity, plus your login name and PIN-code, provide a reasonable degree of certainty of your on-line identity.

Current PKI systems operate on what is known as a three-corner model (Figure 1). A sender requests the digital certificate of someone he wants to send a message to. The sender uses the certificate and his secret private key to encrypt the message. The recipient decrypts the message with the sender's public certificate and the recipient's secret private key. This combination of certificates and private key assures the identities of sender and receiver, prevents anyone from eavesdropping, and guarantees the integrity of communication.

However, current three-corner PKI systems have inherent limitations which make them unlikely to be deployed in large scale for business-to-business e-commerce:

- **X.509 Certificates Interoperate Poorly.** X.509 digital certificates are rarely interoperable, despite the fact that x.509 is the open, industry-developed standard for PKI certificates. This is because x.509 certificates may have customized fields and/or customized procedures for challenge-response that make certificates unrecognizable between systems.
- **No Mandate of a Hardware Token.** Recent articles have shown that digital certificates residing on hard disks are vulnerable to breach by brute-force attacks.⁷ Yet, no legal system is in place today that mandates that a digital certificate must reside on a hardware token – such as a smart card.
- **Businesses Must Manage Hundreds of Public Certificates on their Own.** A traditional three-corner model for PKI is fine when the receiver must only keep a single public key. However, once a supply chain is opened up to large numbers of companies, each receiver must now maintain a consistent database of current public keys for all other members of the network. This becomes both difficult and costly to do, and most companies perceive this as too burdensome a requirement for implementing a PKI solution.
- **Real-time Validation of Certificates Difficult and Has Risks.** Not only must someone maintain the database of public keys, but the keys must be current and there must be a real-time mechanism for checking that a

⁷ A. Shamir and N. van Someren, “Playing Hide and Seek with Stored Keys,” (Santa Clara: RSA Corporation, September 22, 1998)

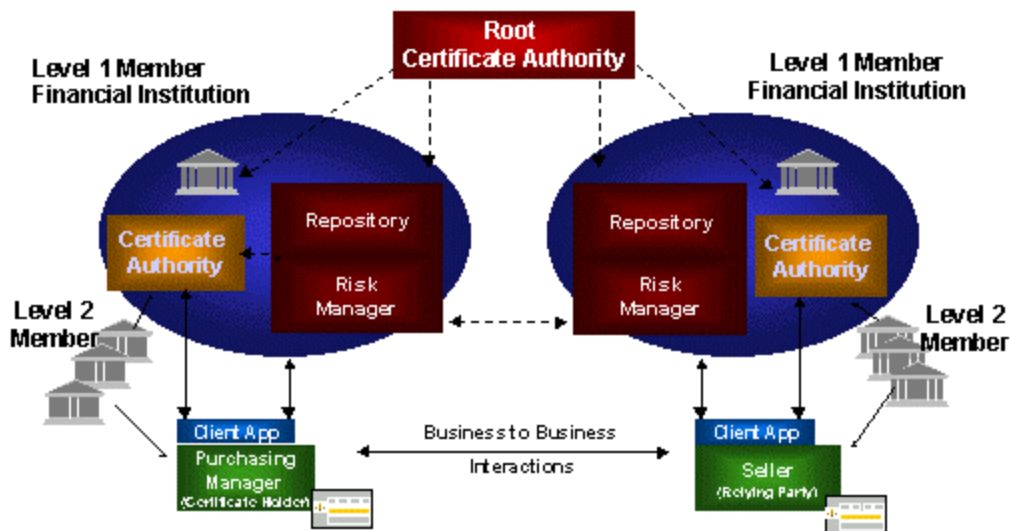
certificate is still “valid.” Companies neither want the burden nor risk associated with maintaining real-time certificate validation.

- **Current Solutions Lack Consistent Legal and Risk Management Framework.** A digital certificate must have legal standing. Each country or trading region has implemented its own legal and risk management framework for digital certificates. Whatever PKI system is in place, it must be able to ensure that a digital signature generated by that system is both legal and recognized as a valid contract worldwide.
- **No Existing Entity Provides Signature Warranties.** When a transaction goes bad, who is liable? Today that question has no clear answer, and there is no entity that will provide warranties for any losses incurred when a document is signed with a fraudulent digital signature.

Recognizing these limitations, ten global financial institutions (ABN AMRO, Barclays, Bank of America, Citibank, Chase, Deutsche Bank, CIBC, Hypovereinsbank, IBJ, Nat West, Sanwa) have come together to form a membership organization, named Identrus, whose sole purpose is to overcome these business and technical limitations to secure identity authentication for business-to-business Internet commerce. Identrus serves as both a root certificate authority (CA) and policy approval authority. Identrus will issue certificates to participating financial institutions—enabling them to offer real time validation, risk-metering and warranty services⁸. These financial institutions, in turn, will act as certificate authorities and issue smart cards holding digital certificates to approved employees at their corporate customers. This certificate (incorporating a digital signature) essentially represents a passport for engaging in trusted e-commerce. The certificate authenticates the sender and enables the recipient to verify the integrity of the message.

⁸ While there are only ten founding members of Identrus, the plan is that several thousand will join this core group in the next 36 months.

FIGURE 3
How the Identrus Four-Corner Model Works



In order to minimize the need for corporate customers to maintain complex certificate management systems and track public keys for thousands of relationships, Identrus has adopted a “four corner” model (Figure 3) that works as follows:

1. Acting as the certificate authority, a financial institution issues digital certificates on smart cards to authorized employees of subscribing corporate customers.
2. The authorized employees use the smart card issued by the financial institution to acquire a secure connection and to generate digitally signed transaction requests intended for a relying party (i.e. the seller).
3. The seller sends the buyer’s digital certificate to the seller’s financial institution. The relying party (seller) must maintain some simple Identrus-enabled systems that allow it to isolate the Identrus-enabled signature from the subscribing customer (buyer) and forward it to their financial institution. But unlike traditional three-corner PKI systems, the relying customer does not need to maintain any public keys or complex systems for key validation.
4. The seller’s financial institution forwards the certificate to the buyer’s financial institution, which either validates or denies the buyer’s identity and authority to make a purchase. This authorization is sent back to the seller via his financial institution.

The advent of Identrus is a major step forward in making business-to-business e-commerce a reality on a global scale. It not only creates the technical and business infrastructure needed to allow secure authentication of identity on-line, but it also makes the process painless for the business customer relative to previous options. This simplicity becomes especially important as business-to-business e-commerce moves into mainstream companies that are not early adopters of technology.

Let's take an example. Let's say General Motors moves to an on-line buying system in order to reduce its cost of processing purchase orders. GM now needs its vendors to convert to an on-line process. How does it accomplish this? Before Identrus, it would work with a value added network provider (VAN) and establish specific EDI standards/interfaces which its vendors would use to interact with its systems. The VAN would provide specific security/identity authentication procedures as part of this service. The cost/effort to establish this system, since it sits on a "private" communications system, would be significant. Each of the vendors would also need to make extensive adaptations to its systems to interface with GM's specifications. Moreover these investments would be GM-specific. If Bosch wanted to sell spark plugs to Daimler-Chrysler, it would need to set up a separate set of standards/interfaces and identity authentication procedures for this new electronic relationship, possibly through a different VAN. Very quickly, complexity would outweigh the benefits, which is why technologies like EDI never have enjoyed resounding commercial success.

With Identrus, the underlying communications medium is the Internet. As a subsidized communications medium, the Internet makes the cost of deploying much lower to begin with. If GM wishes to convert to an on-line purchasing process, it now goes to its bank and makes a request to do so. The bank, working with technology providers like Sun, places some simple technology, known as a gateway, "in-front" of the corporations accounting and ERP systems that Identrus-enables these systems. The bank then issues digital certificates on smart cards (along with card readers) to each individual GM has identified as having authorization to make purchases. GM directs its vendors to their banks (anywhere in the world), who perform a similar service. At this point, both GM and its vendors are ready to undertake buying and selling on the Web with secure authentication of identity, at a very reasonable cost with minimal effort. Moreover the system is totally open. If Bosch now wants to sell electronically

to Daimler-Chrysler, Bosch directs Daimler-Chrysler to its bank to sign up. Daimler-Chrysler goes through the process with its bank, receives its smart cards, and is ready to go.

Next issue: Sun's architectural approach to PKI systems.