

■ KENNETH E. KENDALL, Feature Editor, School of Business-Camden, Rutgers University

IT HAS BEEN OVER FIVE YEARS SINCE THE *NEW YORKER* MAGAZINE PUBLISHED A CLASSIC Peter Steiner cartoon that shows a large dog sitting at a keyboard and telling a smaller dog, "On the Internet nobody knows you're a dog." Still, most of us simply assume that we are communicating with the person or company we picture at the other end. We accept software updates, email, and information in general without thinking twice about whether it contains a virus or simply incorrect information. As we transact more business in the ecommerce world, we will need to depend on ID certification. Although there are established ways to certify the sender's identification, the acceptance of a digital ID system has been slow to catch on. This month's ecommerce column by Eric Turner explains how public key infrastructure is having an identity crisis of its own.

Public Key Infrastructure: Is This Digital ID System Having an Identity Crisis of Its Own?

Eric C. Turner, School of Business and Public Management, The George Washington University

Security is a paramount concern in the world of electronic commerce, or electronic business, as conducted over the Internet. In a 1999 survey, Ernst and Young reported that CEOs identify trust, privacy protection, and authentication as the most serious barriers to e-commerce. More recently, the U.S. Internet Council's "State of the Internet 2000" report states that more people will purchase products and services as they feel their identity is secure (Ernst&Young, 1999) (USIC, 2000). But as Ken Kendall reminds us in the July 2000 issue of *Decision Line* (Kendall, 2000), ecommerce is broader than simply what is bought or sold on the Web. This implies that ecommerce security is not only necessary for online retailing, but for every electronic transaction, whether it is business-to-consumer (B2C) or business-to-business (B2B).

You may not realize that public key infrastructure (PKI) technology using digital certificates has been around for approximately 20 years and appears to meet the requirements for confidentiality and integrity of data, access control, authentication, and non-repudiation. On the other hand, you might be familiar with Verisign, the best known company providing a managed PKI service, because one of its security messages occasionally pops up when you

are viewing a Website. You probably also realize that encryption alone is not satisfactory because it does not provide proof of a person or company's identity. That is, in essence, why PKI is needed—to attest to a person's true identity. Why then, given its promise, has PKI been so slow to spread?

What is PKI and Why Isn't It More Broadly Accepted?

PKI technology has been available for approximately 20 years and includes many capabilities including encryption, client identification, and digital signatures that would seem to be particularly useful in facilitating e-commerce over the Internet. I offer a simplified definition of PKI as a software-based infrastructure developed with public key technology that uses digital certificates and encryption algorithms to secure data transmitted over public networks such as the Internet.

Although many technologies never emerge from the cycle of potential, hype, and ultimate disillusionment, it would appear that PKI meets an immediate need and has the technical merits to become an essential and productive business tool. Enterprises are increasingly integrating IT systems with trading partners over the



Eric C. Turner

is a doctoral student at The George Washington University. He is currently employed at the Federal Reserve Board in Washington, D.C., as a manager in the Division of Information Technology. He

holds an MBA in MIS/Finance and a BS in mechanical engineering from the University of Maryland at College Park. His research interests include electronic commerce, information security, telecommunications, and human computer interfaces. Mr. Turner is a member of the AIS, ACM, IEEE, and CMG professional societies.

turnere@frb.gov or turnere@gwu.edu

Web. The growing importance and complexity of business-to-business application integration projects requires security that addresses authentication, confidentiality, authorization, integrity, nonrepudiation, and availability.

Given this reality, why is it that PKI has not been universally implemented? Which factors have prevented the widespread deployment of PKI technology in B2B and other areas of electronic commerce? How will these factors play out in the future? This column attempts to offer a brief review of some of the elements that have contributed to the slow rate of PKI implementation.

What is Security?

Any comprehensive security solution must address authentication, confidentiality, authorization, integrity, and nonrepudiation. A brief definition of each of these areas is provided below.

- **Authentication:** Ensuring that users or applications are uniquely identified to the application environment.
- **Confidentiality:** Ensuring that only those people who have a need to see information are able to see it.
- **Authorization:** Ensuring that a correctly authenticated user can access only those resources for which the resource owner has given approval.
- **Integrity:** Ensuring that a transaction does not change somewhere between the sender and the receiver.
- **Nonrepudiation:** Ensuring that both the sender and receiver of the information can unequivocally prove that business transactions have occurred and with whom they have occurred.

PKI is of value because it provides a framework to address all of the areas of security defined above. However, there still remain a significant number of practical issues that have not been adequately addressed to facilitate pervasive and broad-based adoption of PKI. These issues include vendor interoperability, Certificate Authority (CA) policy, operational and support infrastructures, cost, government regulation, and the availability of complementary or alternative solutions.

Why Are There PKI Interoperability Issues?

To date, competing vendors have apparently determined that it is more profitable to offer proprietary solutions that on the face appear to be based on open standards than to provide solutions that would easily interoperate with other vendor's products. Theoretically, public key standards have been created to ensure the integrity of the key and key exchange process; however, in practice, maintaining the integrity of the key through effective management of the certification process across vendor products is still a major concern.

Almost all vendor products support implementations that are based on the same standard Internet Engineering Task Force (IETF) X.509 version 3 digital certificate recommendations, but they are still incompatible with each other because of independent interpretations of actual implementations and the use of proprietary extensions. Solving the cross-vendor problem of ensuring that a public key in use is valid and belongs to the claimant rather than someone else is essential in developing the needed trust relationships to facilitate B2B commerce.

Unfortunately, until recently, few of the major PKI vendors have appeared serious about supporting a standard interface based on open protocols. Still, the future is not entirely bleak. Several groups, such as the PKI Forum, are tackling the interoperability issues among the major PKI vendors.

What's Behind the Complexity of CA Policy and Operational Issues?

The X.509v3 standard defines two methods for joining CAs: hierarchical signing and cross-certification. Due to problems with interoperability in the application methods for cross-certification, as well as liability concerns with both methods, many vendors have opted to use access control lists. Access control lists, while easy for administrators to use, open up vulnerabilities that are unacceptable to many users transmitting sensitive information. In the typical access control lists implementation, the client defines—in many cases errone-

ously—the community of trust versus the community in which the client has membership. In practice, this can lead to the imprecise granting of privileges that can then compromise the entire security framework. Thus, hierarchical signing and cross-certification are viewed as offering more robust methods for controlling trust (Moskowitz, 2000).

Many current PKI implementations employ a hierarchical scheme wherein the principles public key is included and signed by an authority, and the authority may hold a certificate issued by a super authority, and so on up the hierarchy. This is how many people commonly define the public key certificate management infrastructure, or public key infrastructure. In practice, however, hierarchical PKIs are typically only implemented in narrowly defined administrative domains. The complexity of the interaction methods between the registration authority (RA) to Certificate Authority (CA) on the one hand, and CA to CA on the other, has been a challenge to the few that have attempted to tie together CAs. Of particular concern are the legal implications of certificate practice statements and the process for timely and effective management of certificate revocation lists.

Why Have Attempts to Implement a PKI using IETF Standards Failed?

One of the design goals of the X.509v3 standard was to add CA cross-certification. Although this appears in the specifications, in practice the difficulty of building a PKI using CA cross-certification has meant that some groups have delayed or pulled back designs built around it. In 1998 the federal government decided to abandon its plans to use a hierarchical model due to its complexity and instead moved toward a structured cross-certification PKI model. Again, despite the apparent demand, vendors have been slow to provide workable cross-certification solutions. Although the IETF standards include CA cross certification in the Certificate Management Protocol (RFC2510), to date there have not been many real world implementations demonstrating the interoperability of the CCR (cross-certificate request) and CCP (cross-certificate response) capabilities of RFC 2510 (Moskowitz, 2000).

The National Institute of Standards and Technology (NIST) PKI technical working group has spent a significant amount of resources addressing the cross certification issue. Much of what has been developed are heavily customized solutions with a multitude of extensions that could not easily be applied across multiple CAs operating in domains outside of the federal government. Other user groups have given similar reports at the PKI Open Forum's first meeting (see www.pkiforum.org). Although CA cross-certification poses a high technological hurdle, it appears that the PKI forum and other groups are attempting to address the problem and there are signs of progress. Until then, handcrafting of proprietary CA cross-certifications will continue until certification through a standard certification process truly works.

Is the Cost of PKI a Factor?

Public key infrastructure project costs can reach into the \$1 million range, thus obviating the cost advantage of using the Internet. Although prices are continuing to come down, it is very difficult to compare total cost of ownership for various vendor bids. The number of options presented to potential users in response to competitive solicitations often makes direct 'apples to apples' comparisons difficult.

For example, the two leading PKI vendors, VeriSign and Entrust, generally take two fundamentally different approaches for implementing their solutions. One vendor (VeriSign) offers an outsourced service model providing hybrid certificate authority services and other services to essentially manage and run the infrastructure; the other vendor (Entrust) sells PKI software products and services with the goal that the PKI would be operated by the enterprise. Yet another vendor, GTE CyberTrust, will provide either implementation approach (Wheatman, 1998).

As such, vendor pricing generally excludes project management or other recurring administrative and technical costs incurred by the enterprise in managing a PKI. Professional service and systems integration work including consulting can add significantly to overall project costs. The hope for the future is that the resolution of other issues will increase the number of

PKI implementations causing a shake out in the industry and better pricing.

What Are Governments Doing to Support PKI?

Following in the footsteps of many states, Congress recently passed digital signature legislation that recognizes digital signatures to be as legally binding as handwritten ones. In addition, a number of countries from Singapore to Brazil have recently implemented electronic signature bills. Non-repudiation is an important attribute offered by PKI-based electronic signatures. Non-repudiation means that the party that signed an order to purchase supplies, for example, cannot later deny the fact. There is a contract. However, many businesses will still not ship product unless it is prepaid, despite a signature or binding purchase contract. Nonetheless, the notion of accepting digital signatures as being legally binding to the same extent as a written signature is a major step toward overcoming the psychological and cultural obstacles of acceptance of PKI.

Does PKI Have a Future?

As with any security solution, there are always trade-offs between making a system user-friendly versus making a system secure. In the (now seemingly distant) past, systems provided mainframe-based SNA network accessible services built around the principle of a centrally controlled, closed-end, point-to-point infrastructure. In this environment, the provision of robust security was enhanced by certain physical-like location sensitive access barriers and thus was seemingly easier to defend.

By contrast, today's distributed, open-ended, anywhere-to-anywhere-networked services world provides a multitude of new vulnerabilities and, hence, opportunities for exploiting the very openness that is celebrated by users. The virtual nature of the internetworked world means that system location is no longer a controlling factor. In an annual study performed by the FBI and Computer Security Institute, participants reported that 57 percent of intrusions into their networks came through the Internet. This is, alas, the price we pay for freedom.

The promise of an effective public key infrastructure where data can be transmitted securely anywhere at anytime with no predetermined communication or setup still seems like a future goal. However, the concept of a phone book-type model for looking up, initiating, and establishing secure transmissions has tremendous implications for the future growth of electronic commerce over the Internet. With the potential for this technology one would expect quick resolution of existing barriers to implementation. Governments appear to be knocking down some of the legal and legislative barriers, and with knowledgeable people addressing these and other issues, this author is projecting (and hoping) that the technical barriers are ready to fall as well.

References

- Ernst & Young. (1999). Third annual global information security survey. Available at www.ey.com, 4.
- Kendall, K. (2000). Ecommerce: Thou shall not steal. *Decision Line*, 31(4), 12.
- Moskowitz, R. (2000). PKI at the CrossRoads. *Network Computing*, May 1, 45.
- USIC (2000). US Internet Council, State of the Internet Report 2000. Available at www.usic.org.
- Wheatman, V. (1998). Pricing public key infrastructures. Gartner Group, September 8. ■

Kenneth E. Kendall
School of Business-Camden
Rutgers University
Camden, NJ 08102
(856) 225-6586
fax: (856) 424-6157
ken@thekendalls.org
<http://www.thekendalls.org>