# Challenges of implementing public key infrastructure in Netcentric enterprises

*Sunil Hazari*

**The author**

**Sunil Hazari** is Faculty Research Associate in the Office of Information Technology and Adjunct Professor in the Robert H. Smith School of Business, University of Maryland, College Park, Maryland, USA.

**Keywords**

Information management, Security, Computer security, E-commerce, Encryption, Wireless technology

**Abstract**

The explosive growth of e-commerce has resulted in organizations sharing data over the Internet with other Netcentric organizations. Advances in telecommunications and networked applications are forcing dramatic changes in corporate functions, such as supply chain management, enterprise resource planning and customer relationship management. Online transactions with business partners and customers has prompted e-businesses to re-evaluate their security strategy, to avoid network downtime and being unable to connect to upstream partners and suppliers. Presence of a robust security architecture is essential to the success of netcentric organizations. Public key infrastructure (PKI) is one such technology that may offer benefits to Netcentric organizations, being a system of services, technology, protocols and standards that can be used as a solution for providing secure transactions. There are many factors that make PKI implementation difficult. This paper provides an overview of PKI technology, insight into challenges, as well as impact of implementing PKI in Netcentric organizations.

**Electronic access**

The research register for this journal is available at
**http://www.emeraldinsight.com/researchregisters**

The current issue and full text archive of this journal is available at
**http://www.emeraldinsight.com/0957-6053.htm**

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · pp. 385–392
 · ISSN 0957-6053
DOI 10.1108/09576050210447073



## Introduction

Over the past few years, businesses have realized advantages of facilitating computer-to-computer communications to drive e-commerce activities. The Internet has become a business innovation with the power to transform corporate processes and functions such as procurement, logistics and order management. Effective use of the Internet has increased productivity and revolutionized business models (Kosiur, 1997; Ghosh, 1998). As Web presence of organizations has shifted from brochures and static marketing content to transaction-enabled Web sites, complexity of integrating sales, production, delivery processes and systems electronically among a company, its customers, and its supply chain and demand chain partners has also increased (Deise *et al.*, 2000). Legal documents such as contracts, requisitions, purchase orders and invoices can now be sent online to enable electronic transactions completely. The Internet has also become a pivotal tool to gain market share and revenue, cut costs and improve supply chain efficiencies. The primary goal of Internet-based supply chain management is for organizations to link all business processes into a seamless flow of information across global borders. Large organizations have begun to utilize supply chain automation technology to share logistics, transportation and other data over the Internet while trading with business partners located at various distribution and manufacturing plants across the world. Smaller organizations previously limited by costs incurred under proprietary EDI systems, can now use the Internet to compete in the global marketplace. These "Netcentric" organizations leverage connectivity to eliminate transaction processing lag times and enable faster management decisions that result in cost-effective and agile organizations which respond quickly to market shifts, customer needs and supplier inquiries, which in turn enables higher efficiencies and strategic advantage in every aspect of business. Globally-integrated virtual solutions with easy-to-use Web-based front ends, and the ability to tie together geographically distributed data have now become a reality. However, for all the connected processes to work efficiently, a strong information security

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · 385–392

infrastructure is needed to facilitate, support and safeguard business processes.

## Information security

The four important components of information security are authentication, authorization, non-repudiation and privacy. "Authentication" deals with identity verification of users accessing computing resources. Once the user is authenticated, proper access privileges can be granted to the user. These privileges can be validated at any time during the transactions by using digital tokens such as certificates or signatures. Tools that help with authentication process include passwords ("what you know"), smart cards ("what you have") and biometrics ("what you are"). The type of authentication used will depend on degree of security required. A combination of techniques using mutiple-factor authentication will provide a more robust mechanism for authenticating users and prevent masquerade attacks, replay attacks and identity interception. Business enterprises are also increasingly considering the use of smart cards for authentication purposes. Smart cards have a chip that stores digital certificates and the user's private key which are used for proper identification. Once users have been authenticated, proper "authorization" must be in place to grant access to only those resources which the user is authorized to access. Use of access control lists at the application, document, form or field level may be used to provide multiple levels of authorization. Proper authorization allows only validated users to access the resources and offers user accountability of those resources. "Non-repudiation" prevents validated parties in a transaction from denying the actions have taken place. Secure systems are able to provide proof that communication between parties was done by authenticated users who were authorized to use the resources and the message was transferred unaltered between the sender and receiver. In addition, privacy of individuals must be maintained in electronic environments to protect sensitive or privileged information from being seen by other users or alternately be intercepted and tampered with. E-businesses are particularly vulnerable to privacy of consumers being compromised, and systems must be in place to prevent this from occurring. Encryption techniques (such as symmetric key and asymmetric key encryption explained later) can be used to change the data to un-readable format during transmission. When the message is received at the destination, data are decrypted to the original readable format. Cryptography techniques can also be applied to ensure data integrity which provides assurance that the original data were not altered en route. Strong security measures must support e-business transactions of Netcentric organizations, and controls must protect business-critical data at all costs.

Businesses realize the need for improved security after evolving from small environments, in which transactions are done with trusted partners, to the global marketplace, where business transactions between unknown entities is common. While in small environments basic security of passwords and SSL encryption technology usually suffice, in a larger marketplace, transactions that provide an extra layer of security by validating and authenticating identities of business partners is needed. Although e-business can be done without a public key infrastructure (PKI), robust enterprise architecture can flourish with use of technologies and standards that provide the highest form of security.

## Public key infrastructure

PKI is a system for encrypting, authenticating and validating network transactions through certificate authorities and digital certificates. Although there are many ways of developing security infrastructure for organizations, PKI offers a scalable security solution that maintains all four aspects of security to support authentication of users, confidential communication of employees using encryption, verification of data integrity in e-commerce applications, and use of digital signatures used to ensure enforceability of contracts. Certificate authorities, digital certificates and signatures and directory services form the technical building blocks of PKI. They provide verification to authenticate legitimacy of all parties and applications engaged in a transaction, and offer a foundation on which secure Internet transactions can be carried. According to RSA Security (1999, p. 19), "public key

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · 385–392

infrastructure consists of protocols, services, and standards supporting interoperable applications of public key cryptography". Benefits for enterprises using PKI include the ability to use secure mail that ensures integrity, origin, and confidentiality of e-mail message, development of secure company Web sites that use certificates to control user rights and permissions for Web resources. Other advantages of PKI technology include support for use of secure sockets layer (SSL) and transaction layer security (TLS) protocols for transactions that must be based on authenticated servers and/or users, software code signing which uses certificates and digital signing technology to ensure integrity and authorship of software that is developed for distribution on the Internet, smart card logon process to authenticate users, and other custom security solutions to provide authentication, authorization, non-repudiation, and privacy for the enterprise. The use of digital signatures and digital certificates are important issues in development and implementation of PKI.

There are two types of algorithms used for encryption. These are: symmetric (secret-key) or asymmetric (public-key). In systems that use symmetric key encryption, a single key is shared between the sender and receiver. Data to be sent are encrypted with a secret key, which is used to convert a message to ciphertext before being sent to the receiver. To decrypt the message, the receiver uses the same secret key to return the ciphertext to its original readable format. Although this system may work for small number of users, the number of keys required for large user population becomes difficult to manage. As an example, only one key is shared between two users, 45 keys are required for ten users, and approximately 500,000 keys are required for 1,000 users. (The number of keys required can be calculated by using the formula $(n^*(n-1)/2)$ where $n$ is the number of users.) To overcome the main problem of distributing keys securely, asymmetric key encryption provides a greater advantage. Two keys, one private and one public, are used in this system. The sender and receiver of a message each have a pair of keys. These two keys are different and mathematically unrelated with each key being used for encryption or decryption. The public key of every user is published and accessible to any user. To send a message, the sender accesses the receiver's public key and encrypts the message using this public key. On receiving the encrypted message, the receiver decrypts it using a private key that is the only way the message can be decrypted. In practice, to achieve performance gains, this approach is modified by using a hybrid approach that uses symmetric as well as asymmetric algorithms. In this approach, the sender uses a "session key" generated at random to encrypt the receiver's public key and sends both the encrypted key and encrypted message to the receiver. The receiver uses private key to decrypt the random symmetric key, and then uses this key to then decrypt the message. Use of this hybrid method optimizes operational performance of secure transactions.

Digital certificates supply required components for building end-to-end trust and privacy by guaranteeing tamperproof communication between suppliers and users, eliminating the need for multiple passwords, and also incorporating non-repudiation of business transactions in enterprisewide security solution. To obtain a digital certificate, users first register their public keys with a certificate authority (CA). The CA is a trusted entity which distributes certificates that include public keys carrying the digital signature of the CA. PKI is based on open standards recommended by the PKT for X.509 certificates (PKIX) working group of the Internet Engineering Task Force (IETF). Essentially the CA binds the user's identity with a public key and other relevant information. For certificates issued under X.509 standard, identifier of digital signature algorithm, validity period (start and end date), name of user, public key of user, and identifier of public key algorithm are included as part of the certificate (Summers, 1997).

PKI provides reliable means of assuring that the private key used electronically to sign a transaction is done so by the rightful owner of the key. Digital signatures use public key methods to verify identity of the sender and also prevent the sender from repudiating the message. These electronic signatures work towards maintaining authenticity and integrity of the message. With the sender and receiver each having a pair of public and private keys, when using digital signatures, senders use their private key to encrypt the message. Thus the message now has the sender's stamp or "digital signature" that can be verified by using the sender's public key

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · 385–392

when decrypting the message. As in public key cryptography, to achieve performance gains, the sender does not sign the message directly but generates a "hash" (which is a unique fingerprint of total characters in the document) from the message that is encrypted by the private key. Since the hash function is generated from the message and the private key, digital signatures are unique to each message cannot be transferred to another document. Because of its secure nature, digital signatures have a potential for playing an important role in e-commerce transactions. The Electronic Signatures in Global and National Commerce Law which has been in effect since 1 October 2000, was designed to provide a framework for making digital signatures binding and legal, thereby creating new models of conducting business electronically. Although the law makes digitally signed electronic documents legally acceptable, it does not specify how these digital signatures can be created, nor does it set a standard for what exactly is acceptable in digital format. For digital signatures to be widely accepted, a framework that integrates legal and technical procedures must be established. This can also be achieved by integrating PKI in the network infrastructure of an enterprise.

Since digital signatures form a large component of PKI, Netcentric businesses are well positioned to leverage PKI technology to be an enabler for online transactions. As businesses establish trusted relationships with vendors and customers, use of digital certificates and signatures is expected to grow considerably since it offers a reliable method of binding identity and end-to-end trust and privacy to a transaction before, during and after it occurs. Also, it guarantees tamperproof communication between suppliers and users, eliminates need for multiple password, and includes non-repudiation of business transactions in enterprise-wide security solution.

## Wireless security

PKI also has implications for wireless security. Wireless devices have become widespread in today's Netcentric environment because of advantages such as portability, compact size and the ability to access networked resources remotely. The same security issues that apply to wired transactions can also be applied to wireless devices. IT managers remain reluctant to deploy wireless access technologies because of seemingly weak authentication and authorization tools at the handheld level (Chen, 2001) therefore strategies for efficiently managing wireless devices need to be developed. Owing to limited processor capabilities and memory resources, these devices present unique security challenges but are increasingly favored by employees needing to access corporate data (such as e-mail, phonebooks, calendar, groupware) remotely and gain full access to resources and services of the corporate network. Lack of wireless security standards has not stopped some companies from deploying applications that need security to survive. Examples of electronic wireless stock trading, online banking, and bill-payment are in place using weaker security, which further reinforces the need for PKI to provide a robust wireless infrastructure.

With the availability of local area networks (*LAN*s) powered by IEEE 802.11 wireless standard, a common solution for wireless LAN access is based on the IEEE 802.11b standard which focuses on the two lowest (physical and datalink) layers of the OSI/ISO model. This standard includes data encryption capability for mobile devices by having the access point issue an encrypted challenge packet and expecting the client to use its key and encrypt a correct response to authenticate itself for network access. Although wireless products can be installed relatively quickly with minimum configuration, the default installation of wireless access points allows open access into the network. Therefore proper planning is necessary to secure the wireless network. Taking steps to prevent broadcasting of wireless access point extended service set identification, using access control lists on these access points, deploying wireless encryption protocol on 802.11b access points, will ensure only legitimate users are accessing a company's wireless network. Other technologies such as personal area networks using Bluetooth technology, and wide area networks that incorporate palm devices are being used by enterprises interested in providing remote access to a mobile workforce. These technologies can also

potentially benefit from PKI in similar manner to wired devices.

For cell phone type devices, the wireless application protocol (WAP), developed by WAP forum defines a set of framework for bringing Internet Web application programming model to handheld devices. WAP is a standard created by wireless infrastructure companies in collaboration with computer industry vendors. Included in WAP is the wireless transport layer security (WTLS), which is similar to IP-based SSL. WTLS enables use of server and client certificates on mobile devices for authentication and non-repudiation. It also ensures data integrity, privacy, and denial-of-service protection. One of the major weaknesses for wireless devices accessing the Internet has been the "WAP gap". An intermediary device is usually needed to convert between the wireless and Internet protocols. When a device accesses corporate data using WAP, encrypted data leaving the corporate firewall is decrypted at the wireless gateway of the wireless carrier from WTLS protocol to secure IP protocol (such as SSL). The lag time between this conversion makes data vulnerable during that time and creates a security hole. Digital certificates need to be coupled with data that are in the WAP format. In theory, security features of PKI can be implemented into WAP. The traditional X.509 certificates in WAP must be replaced by smaller certificates that have a finite life span to make management easier. Owing to the inherent nature of wireless devices, PKI encryption needs to be offered under comparatively slower processing speeds and reduced bandwidths. Although under current WAP standards, integration of digital certificate storage and use has high latency time, companies involved in the development of WAP protocol are developing standards to support better security for WAP-enabled devices including integration of PKI.

## PKI implementation issues

Integrating PKI into corporate networks is a complex issue. In the past, PKI has been used mostly by government and financial sectors which have a need to provide more secure solutions than offered by traditional username/password authentication methods. As an example, Illinois State Government in their effort to put more government services online, has been using digital certificates to authenticate users for electronic transactions. With many different agencies within the state there is a need for a central certificate authority to issue and manage certificates. Certain policy decisions also impact PKI deployment. In the Illinois state example, these decisions refer to moving the issuance of digital certificates to an entirely online Web-based system without citizens being physically present to receive the certificate, revocation of certificates by agencies, cross-certification with other states, and use of certificates by the private sector to enable commercial transactions (Frank, 2001). New Jersey Government is also deploying PKI on an outsourced basis for a court application at the state's Department of Labor. In this approach attorneys will be required to apply for digital certificates so they can track cases online and exchange documents electronically. This government-to-business approach provides for a controlled environment in learning about the advantages and limitations of PKI before larger extending government services to citizens of the state. This partial implementation option can also be modeled by Netcentric organizations looking to migrate to PKI environment. Large e-commerce vendors such as business-to-business exchanges and portals have come to realize advantages offered by PKI systems and are moving toward deploying PKI in their operations.

Since there are only a few vendors of PKI products, managers are confronted with "buy-versus-build" solutions for PKI infrastructure. For a business deciding to develop in-house PKI, careful attention must be focused on directory services and associated hardware and software that must be in place to support issuance, management and revocation of digital certificates. One of the biggest dilemmas for businesses is whether to develop a certification system in-house or use third-party verification. Internal development of such a system will produce cost savings for companies that have large number of users since third-party options usually charge a fee that is based on per-user fees. Building a technical infrastructure in-house to support PKI will require companies to setup up a registration authority (RA) to sign up users, setting up a database to store digital certificates, and plan the management

of user certificates. The company next has to purchase vendor software that allows it to serve as its own certificate authority for certificate registration, issuance and revocation. Commercial CA would be one option for companies interested outsourcing that portion of services. Another alternative would be to keep the RA in-house but outsource the CA portion. Advantage of such an approach would be that the certificate branding is done at the RA stage with the company name instead of the service provider's generic service name.

Another option for businesses is to outsource the security portion to application service providers (ASP) and managed service providers (MSP). ASPs offer packaged application software to customers from centrally managed data facilities. The software applications can range from simple applications such as e-mail, word processing, Web hosting, to complex applications such as data mart, enterprise resource planning, sales force automation, and customer relationship management (Deise *et al.*, 2000). In the past, PKI vendors provided their products for use on networks, but lately vendors, whose core business is in the issuance, management and applications of digital certificates, are finally realizing market opportunities to secure Web sites on which applications are hosted. A new class of ASPs called management security service providers (MSSP) are now making their services available to businesses. Solutions offered by these organizations are limited to security which may include: baseline measures such as authentication, firewalls, intrusion detection systems, penetration testing and virus scanning; value-added security such as content inspection, secure hosting, Web application security; and advanced protection such as enterprise security, e-risk management and policy development. Initially companies are overwhelmed by security needs and choose to outsource the operation to get a head start while e-business is being conducted. Outsourcing PKI is similar to outsourcing other common services being handled by ASPs and MSPs in which all aspects of application installation, management, maintenance and backups are handed to the service provider. Advantages of this solution include high availability of operations, scalability, robust infrastructure operation (usually at the vendor's site), backup, revocation management, directory standards, and interoperability disaster recovery plans and independent auditing of certification procedure. Businesses should be aware of security risks associated with ASP and MSP. In having many types of customers, ASP/MSP/MSSPs may not take the highest amount of precaution and try to balance risks by taking "middle of the road" approach. For businesses requiring hosting of mission critical applications, this approach could jeopardize security. Also, many ASP/MSP/MSSPs are outsourcing operations to other specialized service providers. This introduces additional vulnerabilities in the value chain since company data may be maintained in a shared environment that may be more susceptible to risks of data loss.

Application integration may also cause hurdles in user-acceptance of PKI technologies. Security is most effective when used correctly. Technology acceptance models such as Rogers (1995) innovation diffusion theory, Davis (1989) technology acceptance model, and reasoned action and planned behavior (Mathieson, 1991; Ajzen, 1985) models have been studied widely by information systems researchers in terms of human factors and IT adoption. Since these models and theories have also been researched in context of Internet technologies and e-commerce applications (Gefen, 1997; Gefen and Straub, 2000), it is reasonable to extrapolate that these theories can be applied to security applications in terms of user acceptance. Whitten and Tygar (1999) posit that effective security requires a higher usability standard that cannot be achieved through the user interface design techniques appropriate to other types of consumer software, therefore the development of a domain-specific user interface design principles and techniques is needed. Since not many applications are PKI ready today, integrating PKI would require additional development efforts not only to make it work, but also to have it be widely adopted in business functions.

Threats to wireless networks should not be taken lightly. Vulnerabilities that were previously unheard of in wired devices have taken new forms that are endemic to wireless devices. For example, Timofonica, a variant of the Love Letter virus was written specifically for cell phones that have text capabilities. A Palm Pilot Trojan horse

Logistics Information Management
Volume 15 · Number 5/6 · 2002 · 385–392

program called Liberty crack virus was disguised as a Game Boy application. The need for mobile digital certificates has never been greater. Moving from mobile device browsing to mobile transaction capabilities, PKI-based transactions at this time appear to be the most robust solutions for in providing a secure e-business environment. IT managers should look at wireless technologies not as a separate entity, but as part of the infrastructure that is integrated into e-business strategy. As a result, IT managers are looking for a single framework in which to offer PKI-based security to wired and wireless devices. Stringent password management techniques on wireless devices, internal security audits, user awareness, isolation of access points, implementation of media access control address tracking, access log monitoring etc. are some of the techniques that can be used to secure wireless networks in absence of PKI integrated wireless networks.

Although PKI holds much promise for e-businesses, its implementation remains a challenge due to lack of standardization and high deployment costs. For a robust PKI architecture there must be features such as documentation of key history, key backups, secure time stamps and adherence to the online certificate status protocol that checks a certificate's validity online. Farrow (1999) reports that a vendor calculated study showed five-year cost of installing a PKI product for 5,000 users including support and life cycle management is approximately $3 million. For most organizations today, due to limited time, cost and personnel resources, there is more focus on warding off viruses, and denial of service attacks first which are capital-intensive expenditures taking priority over long-term projects such as PKI. Future implementations of PKI are expected to become easier to use and more affordable since competition among mass market vendors will put pressure on the market to reduce cost and complexity of certificate authorities and directory services products. Vendors of PKI technologies are striving to make their systems interoperable in order to accelerate adoption of this type of security framework. A consortium of vendors has been established to work on common standards for exchanging information about certification revocation lists. Vendors are working to create an industry-standard implementation of public key technology, which standardizes not only certificate types, but also principles used for recognizing and managing a certificate authority. PKI therefore holds promise for offering a more secure Internet over which Netcentric organizations can conduct e-business transactions.

## Conclusions

Companies must safeguard business critical data at all costs. Security is key enabler of successful Internet-based transactions and costs associated with mitigating risks are included as component of business operations. As businesses have increasingly to comply with security laws and regulations governing privacy and data confidentiality (such as the Health Insurance Portability and Accountability Act imposed on the health care industry), compliance will become a business requirement. If used correctly, the Internet supported by PKI architecture can offer a common physical communications infrastructure, guaranteed user authentication and data integrity, along with secure message transport. As organizations deploy in-house PKI solutions, the costs for deployment are becoming clearer. However further research is needed into the types of organizations, development factors, infrastructure requirements, and policies that are needed to provide an enterprise wide PKI. On the heels of banking industry push for strong global encryption standard and wide acceptance of e-commerce will soon create the need for additional laws that mandate secure e-commerce by using electronic signatures and PKI systems for validating transactions across borders and conducting business securely with supply chain partners.

## References

Ajzen, I. (1985), "From intentions to actions: a theory of planned behavior", in Kuhl, J. and Beckmann, J. (Eds), *Action Control: From Cognition to Behavior*, Springer-Verlag, Berlin, pp. 11-39.

Chen, A. (2001), "M-commerce security: a moving target", *eWeek*, Vol. 18 No. 2, pp. 45-60.

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, pp. 319-40.

Deise, M.V., Nowikow, C., King, P. and Wright, A. (2000), *Executive's Guide to E-business: from Tactics to Strategy*, Wiley, New York, NY.

Farrow, R. (1999), "Public key infrastructure", *Network Magazine*, January, available at: www.networkmagazine.com/article/NMG20000517S0061

Frank, D. (2001), "Illinois unifying PKI program", *Federal Computer Week*, January, available at: www.civic.com/civic/articles/2001/0122/web-pki-01-24-01.asp

Gefen, D. (1997), "Building users' trust in freeware providers and the effects of this trust on users' perceptions of usefulness, ease of use, and intended use", doctoral dissertation, Georgia State University, Atlanta, GA.

Gefen, D. and Straub, D. (2000), "The relative importance of perceived ease of use in IS adoption: a study of e-commerce adoption", *Journal of Association for Information Systems*, Vol. 1 No. 8, available at: http://jais.aisnet.org/articles/default.asp?vol=1&art=8

Ghosh, A. (1998), *E-commerce Security: Weak Links, Best Defenses*, John Wiley & Sons, New York, NY.

Kosiur, D. (1997), *Understanding Electronic Commerce*, Microsoft Press, Redmond, WA.

Mathieson, K. (1991), "Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior", *Information Systems Research*, Vol. 2 No. 3, pp. 173-91.

Rogers, E.M. (1995), *Diffusion of Innovations*, 4th ed., Free Press, New York, NY.

RSA Security (1999), *A Guide to Security Technologies: A Primer for IT Professionals*, RSA, Bedford, MA.

Summers, R.C. (1997), *Secure Computing: Threats and Safeguards*, McGraw-Hill, New York, NY.

Whitten, A. and Tygar, J. (1999), "Why Johnny can't encrypt: a usability evaluation of PGP 5.0", *Proceedings of the 8th USENIX Security Symposium*, available at: www.cs.cmu.edu/~alma/johnny.pdf