Is PKI the Solution to HIPAA Security?

by Michelle Dougherty, RHIA

Public key infrastructure (PKI) has been called the only technology currently available that will comply with the HIPAA proposed security rules. If you have heard of PKI but have yet to understand it, keep reading. This article will give you a nuts-and-bolts look at the technology and how it works.

PKI is a method of encryption and authentication that uses "keys" to convert encrypted information into a readable format, plus identify the author. The technology seems new to healthcare but has been used for 20 years, primarily in government and finance. As healthcare organizations move toward Internet-based medical record access and transactions, PKI technology is being recognized as a way to tackle security concerns. PKI offers the ability to protect confidential information moving through fiber-optic cables, across extranets, or sitting in Web servers by protecting it from end to end (the point where a message originated to the point where it is received). Further, the technology is not limited to only Web-based applications; it can also be used on closed networks as well.

In healthcare organizations, information technology systems tend to be fragmented by different departments using disparate software applications. The Internet, a Web browser, and PKI can bring these different applications together into one independent system that centralizes access to all data and security administration. This platform streamlines the security administration process by eliminating the need for separate, built-in security systems unique to each application.

What's the Key?

PKI software uses a string of numbers (the keys) to encrypt documents to protect them from unauthorized access, then decrypts them for authorized users. In a public key infrastructure, a third party called a certificate authority (CA) manages the creation and use of key pairs and digital certificates for each user. The digital certificate is often compared to a digital passport or driver's license because it verifies a user's identity. The CA that issued the keys and digital certificates is considered the root of trust in a transaction because it vouches for the identity of the user presenting the certificate. A state drivers' license bureau is similar to a CA because it's an independent party that issues licenses used for identification purposes. There is a strong assurance that the person holding the driver's license issued by the state is who he or she claims to be.

When establishing a digital certificate, the user receives a public key and a private key certificate combination and two mathematically related numbers (each is usually a minimum of 1,024 bits long). The public key is a code used to encrypt information and verify digital signatures and is readily available to anyone. It can be stored on a directory, sent with an e-mail, or posted on a Web site. The private key is unique to an individual and must be kept secure. It is used to decrypt information and generate a digital signature. A user's private key can be kept on a smart card, a portable token, or inside a computer.

Management of the digital certificates is critical to PKI success. This can be done by the healthcare organization itself or through a third-party CA. PKI vendors have recognized the trend of companies' managing their own certificates and have been partnering with IS vendors, firewall manufacturers, and telecommunications companies to produce integrated PKI solutions.

A Glossary of PKI terms

authentication: confirms the identity of the parties involved in a transaction and verifies that a person really is who he says he is. Prevents unauthorized users from accessing data

encryption: a device or method that ensures only authorized users access data/information and unintended recipients can't compromise or intercept data

access control: a system or process that controls and manages which parts of the record are "visible" to different users

certificate authority (CA): a trusted third party that vouches for the identity of an individual. A CA issues digital certificates that validate the identity of an individual for online transactions.

certificate policy: a document that explains exactly how much responsibility the certificate authority undertakes to those who rely on its certificates

digital certificate: an advanced form of authentication that contains a serial number, the owner's name, and the public key information of the owner. It can be used to absolutely prove or disprove a person's electronic identity

digital signature: an electronic ID used to identify a particular user

message integrity: the message sent by a user is the same is the one received

nonrepudiation: assurance that the message came from a particular sender

public key infrastructure (PKI): a method of encryption and authentication that uses a key pair (a public key and a private key) to convert encrypted information into a readable format and also identify the author. PKI uses a certificate authority to issue the keys and a digital certificate to verify the identity of an individual

private key: a string of numbers that is part of a key pair (public key) unique to an individual and must be kept secure. The private key decrypts information and generates a digital signature

public key: a string of numbers that is part of a key pair (private key) that is exported to a public server or to another user. The public key is used to encrypt information and verify digital signatures

What Does PKI Have to Do with HIPAA?

HIPAA requirements for security have pushed PKI to the forefront. Although HIPAA does not require any specific technology, PKI has been touted as one of the only technological solutions to meet the security requirements of HIPAA by providing for access control, authentication, confidentiality, message integrity, and nonrepudiation. More information on each of these components follows:

• access control: in establishing a user, PKI gives a healthcare organization the ability to establish privileges to access the network and has the capability to allow access to select information and maintain detailed audit trails. Once a digital certificate is issued, it can be customized to restrict what data the user has the right to access, change, or transmit

• authentication: PKI technology provides a systematic way to authenticate users from in-house or remote stations. Through the digital certificate, the user's digital identity is attached to any encrypted data that is accessed or transmitted, providing solid authentication

• confidentiality: because the user's identity can be attached to data that is accessed or transmitted, there is definitive proof of who has accessed what and when. The encryption process also allows authorized individuals to view or use the information

• message integrity: PKI is able to ensure, usually through the message authentication code, that the message received is the same as the message sent

• nonrepudiation: PKI offers strong evidence of the identity of an individual signing a message and the integrity of the message. It will be difficult for a party to deny the content of a message or deny creating and submitting it

Although PKI seems to be the answer to many technology concerns, there are still challenges to consider. PKI can be difficult to customize, challenging to manage, and costly to implement. Yet, knowing the downside of PKI implementation and possible delays in HIPAA security mandates, the healthcare industry continues to see it as a security solution to meet ongoing business needs. Organizations are looking for ways to keep confidential information secure but provide access to staff, physician, patients, and payers. PKI seems to be the most promising technology available today. u

References

Berry, Gretchen. "Is PKI the Key to Your Information Security Needs?" Advance for Health Information Professionals 9, no. 15 (1999): 18-20.

Elrod, Elliott. "Data Encryption: What It Is & How It Works." E-Mail & More 8, no. 7 (2000): 59-61.

Hayes, Bill. "Virtual Private Networks Secure Communications." Guide Series: Computing: 50 Hot Technologies 8, no. 1 (2000).

Herrmann, Stacy. "I Sign, Therefore I Am." Healthcare Informatics 17, no. 9 (2000).

Hemmings, Terry. "PKI: Up Close and Personal." Health Management Technology 21, no.9 (2000): 20-23.

Levine, Diane, R. "Public Key Infrastructure Adds Security to E-Business." InformationWeek no. 787 (2000).

Levitt, Jason. "What is Public Key Infrastructure?" InformationWeek no. 771 (2000).

Tabar, Pamela. "If You Don't Know What PKI is Yet, You'd Better Find Out." Healthcare Informatics 16, no. 7 (1999).

Wilde, Candee. "Public key Infrastructure Gets Easier to Install." InformationWeek no. 776 (2000).

Michelle Dougherty *is an AHIMA practice manager. She can be reached at michelle.dougherty@ahima.org.*

Article citation:
Dougherty, Michelle. "Is PKI the Solution to HIPAA Security." *Journal of AHIMA* 72, no.2 (2001): 22-23.
