



# Is PKI the Answer

---

## to the HIPAA question?

July 14, 2000

### What is PKI?

Public Key Infrastructure (PKI) is an information security infrastructure that can be used to secure the transmission of information. Through the use of two related encryption keys, the technology can ensure the confidentiality of transmissions, verify the integrity of that data, authenticate the identities of both parties to the transaction, and provide assurances that neither party can deny that the transaction took place. The technology consists of the two related keys, one of which is widely known (the public key) and one of which is kept secret (the private key). This usage of two different keys is called asymmetric encryption and provides an easy-to-use, secure method for protecting information. The two keys are assigned, and the identities of the key holders is validated by a certificate authority (CA). A trusted third-party issues digital certificates, the heart of which is the user's private key. Certificates function as digital identification and may also be used to grant access rights.

### How can PKI be used for HIPAA compliance?

Hospitals and health systems looking to employ cost-effective, user friendly methods to transfer data through an intranet, extranet, and especially the Internet should give serious consideration to PKI.

PKI's largest roles in HIPAA compliance relate to electronic signatures and message integrity. HIPAA regulations call for signatures to be digital and to ensure the following:

- **Integrity:** "Ensuring, typically with a message authentication code, that a message received matches the message sent."
- **Authentication:** "The corroboration that an entity is the one claimed."
- **Non-repudiation:** "Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents."

PKI is the only mature technology currently available to meet the HIPAA requirement for digital signature.



---

The required technical security measures to protect data that is transmitted over a communications network include message integrity measures, message authentication measures, and either access controls or encryption. While PKI is not the only technology that can provide these protections, it is clearly the easiest to implement, and, because it is based on open standards, free of interoperability issues caused by proprietary technology.

If the network is open (e.g., the Internet), encryption is required in addition to an entity authentication scheme that **irrefutably** identifies authorized users and programs. Because technology to impersonate other users is common on the Internet, irrefutable identification requires more than a username and password. PKI, perhaps in combination with smart cards, or in the roaming PKI environment, provides that irrefutable identity.

Smart cards—digitally encoded identification cards—may be part of the overall solution. These cards can contain the user’s digital certificate, and when used with a PIN (just like an ATM card) they provide strong evidence of the user’s identity. Another method for ensuring this identity is biometric identification, which uses some measurement of the user’s body, such as a thumb or fingerprint as identification. The ComTrust™ PKI solution offers another option—Roaming PKI. The technology allows users to authenticate with two servers, each of which provides a portion of the user’s key. Using this technology, users can log on securely, but do so at locations without the dedicated hardware required for the other options.

PKI’s great advantage over other technologies (where those exist) is not enough to make it the right HIPAA answer for everybody. Certainly when used properly, PKI is a convenient way to provide security and authentication and should be considered as one important weapon in the HIPAA arsenal.

### **Who should consider PKI right now?**

Every healthcare organization should consider PKI as part of a total solution for protecting their electronic data. PKI will be of immediate interest to five groups:

- Organizations with substantial security needs. A PKI solution provides the high level of security desired for extremely sensitive situations, such as addiction treatment facilities.
- Large, forward-looking organizations that see the need for PKI in the future, and want to get started now.
- Organizations that can realize cost savings today by replacing traditional dedicated lines with Internet connectivity. This is ideal for the hospital with multiple clinics, or the multi-hospital group. HIPAA standards for open network communications require the level of protection PKI can easily provide.



- 
- Organizations that plan to implement electronic signatures, perhaps as part of an electronic medical records project. PKI represents the only real open solution for this group.
  - Medical software vendors. These groups will have at least two critical uses for the technology:
    - Connecting with customers' networks for off-site support. PKI encryption and identity verification will be valuable for identity assurances to users, as well as allowing use of the Internet to provide this support at a substantial cost-savings over dial-up service.
    - Integrating the technology into products as part of their HIPAA compliance and Internet migration strategies

*For more information about PKI and ComTrust™, please see our Web page [www.comtrust.com](http://www.comtrust.com), or call us at (248) 226-4005.*