Electronic Signatures, Digital Signatures, and Digital Certificates

Save to myBoK

by Julie Welch, RHIA (formerly RRA)

Electronic Signatures

The Department of Health and Human Services (HHS) published a proposed rule for electronic signatures (45 CFR Part 142, Security and Electronic Signature Standards) in the August 12, 1998, *Federal Register*. Its comment period ended October 13, 1998. When finalized, the standards will specifically apply to the electronic signature transactions that are defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Every indication is that a final rule will not be published in the *Federal Register* until the end of 1999. The effective date of the final rule will be 60 days after the final rule is published in the *Federal Register*. However, HHS will not enforce the rule until two years after the rule officially becomes a standard (three years for small health plans). The proposed rule specifies that an electronic signature must accomplish the following:

- identify the signatory individual
- assure the integrity of a document's content
- provide for nonrepudiation -- strong and substantial evidence that will make it difficult for the signer to claim that the electronic representation is not valid

The proposed rule defines an electronic signature as the attribute affixed to an electronic document to bind it to a particular entity (the signer of the document). In addition, an electronic signature secures the user authentication at the time the signature is generated. It creates the logical manifestation (or display) of the signature (including the possibility for multiple parties to sign a document and have the order of application recognized and proven). It supplies additional information such as time stamp and signature purposes specific to that user and ensures the integrity of the signed document to enable transportability of data, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document confirms the integrity of the document and associated attributes. It also authenticates the identity of the signer. The proposed rule states that currently, the only technically mature electronic signature meeting the above criteria is the cryptographically based digital signature.[1]

The American Society for Testing and Materials (ASTM) has also published standards for electronic signatures:

- E1762-95 Standard Guide for Electronic Authentication of Health Care Information
- PS100-97 Provisional Standard Specification for Authentication of Health Care Information

A description of the ASTM standards and information on how to obtain copies is available at http://www.astm.org.

Both the proposed HIPAA standards and the ASTM standards require the aforementioned features. Authentication is needed to ensure that persons performing the transaction are who they claim to be. Data integrity is necessary to ensure that information has not been altered since the data was signed. Nonrepudiation is mandatory to prevent a signer or sender of a document from denying the origination, submission, delivery, or integrity of its contents. It is important to note that HHS does not advocate or reference specific technology in its proposed standard for electronic signatures.

Digital Signatures

A digital signature is an enciphered algorithm that utilizes an asymmetric key unique to the signer. The sender and receiver both have hashing algorithms that are exactly the same on each end of the transaction. Digital signatures differ from electronic signatures that authenticate documents in that they use actual handwritten signatures via pen-pad applications, while electronic signatures are based on the entry of a unique personal identification number (PIN), biometric technologies, or electronic identification. When sending a digitally signed document, the sender sends the hashed document and the receiver compares the hashes. If they are the same, the receiver knows who sent it. In a secure system, before you digitally sign a document, you should have had to sign on or enter a PIN to obtain access to the methodology for signing the document. Digital signatures are usually data items that indicate that a document has been authenticated from within the application. The main difference between an electronic signature and a digitally signed document is that senders cannot repudiate or deny that they authenticated or sent that document.

A digital signature authenticates the identity of the signer of a document because the sender's key is the only one that can create the signature. It can also be used to ensure that no changes were made to the original content of the message or document that was signed. Any alterations to the document after it is signed would invalidate the signature. Additional benefits to the use of a digital signature include the following:

- easily transported
- cannot be easily repudiated
- cannot be imitated by someone else
- can be automatically time stamped

Digital Certificates

A digital certificate is an electronic credential issued and digitally signed by a certificate authority that establishes the signer's credentials when completing transactions via the Internet. A digital certificate contains the digital signature of the certificate-issuing authority -- enabling anyone to verify the certificate's validity. Certificate authorities control public key infrastructures. The digital certificate represents the certification of an individual, business, or organizational public key (used for encrypting and decrypting messages and digital signatures). Public key encryption involves encrypting messages with one key (the public key) that can only be decrypted with a second key (the private key) and vice versa. Each key unlocks the encryption that the other key creates. For security purposes, the private key is never revealed to unauthorized users. Only the public key is widely known.

To certify a public key, the prospective subscriber requesting the certificate must register his public key with a certificate authority. Once the request is approved by the certificate authority, a certificate is generated and issued to the subscriber. A basic digital certificate includes:

- the certificate holder's identity
- the certificate's serial number
- the digital certificate's expiration dates
- a copy of the certificate holder's public key
- the identity of the certificate authority and its digital signature to affirm the digital certificate was issued by a valid agency

Once a digital certificate is properly stored on a computer, one can send and receive secure e-mail with it or attach a signature that proves who sent the e-mail. Digital certificates are necessary to verify the authenticity, roles, privileges, and limitations of the private key holder of that certificate. This verification is necessary for secure communications. Digital certificates can be used for electronic commerce (E-commerce), which consists of any automated business transactions through paperless mechanisms. For example, United Parcel Service (UPS) has launched UPS Document Exchange, a service designed to offer

secure electronic delivery of documents over the Internet. The service uses two layers of encryption and digital certificates to provide secure transmission, delivery confirmation, tracking, and insurance. Companies can also utilize digital certificates to control access to their corporate intranets.

(For more information on this topic see "HIPAA, Security, and Electronic Signature: A Closer Look" on page 26 of the March 1999 issue of the *Journal of AHIMA*.)

Notes

1. Department of Health and Human Services. "Security and Electronic Signature Standards; Proposed Rule." *Federal Register* 63, no. 155 (August 12, 1998): 43243-43280.

References

Cole-Gomolski, Barb. "Need to Send Secure Documents Via the Internet? See UPS." *Computerworld* 32, no. 10 (1998): 6.

Crowe, Elizabeth P. "Internet Basics: Certifiable." *Chicago Computer Currents* 5, no. 9 (1997): page 35.

Krishna, Arvind. "Protect Yourself -- Public Key Infrastructure and Digital Signatures Play a Critical Role in Secure Internet Commerce." *Inform* 12, no. 10 (1998): 26-29.

McLendon, Kelly. "Encrypted Signatures: Electronic vs. Digital." *Advance for Health Information Professionals* 8, no.19 (1998): 22-26.

"Raising the Standard for Electronic Signatures." *Medical Records Briefing* 13, no. 10 (1998): 7.

"What Is...A Digital Signature?" Available online at http://www.whatis.com.

***Julie J. Welch**, RRA, is an HIM practice manager at AHIMA.*

Article citation:
Welch, Julie J. "Electronic Signatures, Digital Signatures, and Digital Certificates." *Journal of AHIMA* 70, no.3 (1999): 14-15.
