ELECTRONIC RECORDS MANAGEMENT GUIDELINES

ELECTRONIC AND DIGITAL SIGNATURES

Summary

The advent of e-government is changing the way state agencies do business. As a result, electronic systems and processes are gaining in importance with traditional paper and ink. In a paper environment, a hand signature, also known as a "wet signature," authorizes and authenticates the content of a document. A signature provides a level of trustworthiness and accountability that aids the conduct of business. Up-to-date technologies and procedures must meet the demand for trustworthiness where hand signatures are not viable. Electronic signatures endeavor to create a level of confidence similar to traditionally formatted records.

Electronic signatures extend the function of handwritten signatures to electronic documents. Electronic signatures provide a way for two parties to conduct business confidently in an electronic environment. Signatures derive their primary importance from their legal and evidentiary value. These concerns must therefore drive the selection of signature technologies. Consequently, each agency will need to define its legal and evidentiary needs in relation to its business processes before choosing an electronic signature application.

Furthermore, the signature application must fit your technology architecture to create, preserve, and make available your records. Technical obstacles pose great challenges to the long term preservation of electronic signatures. Policy regarding the preservation of signatures should be adopted by each agency to ensure consistent practice across its organization.

Legal Framework

There are a number of statutes pertaining to government records which you need to understand because any document signed in the course of an official transaction becomes a government record. Among the most important are:

- South Carolina Public Records Act [PRA] (*Code of Laws of South Carolina, 1976*, Section 30-1-10 through 30-1-140, as amended) available at www.scstatehouse.org/code/t30c001.htm, which supports government accountability by mandating the use of retention schedules to manage records of South Carolina public entities. This law governs the management of all records created by agencies or entities supported in whole or in part by public funds in South Carolina. Section 30-1-70 establishes your responsibility to protect the records you create and to make them available for easy use. The act does not discriminate between media types. Therefore, records created or formatted electronically are covered under the act.
- South Carolina Uniform Electronic Transactions Act [UETA] (*Code of Laws of South Carolina, 1976*, Section 26-6-10 through 26-6-210). Enacted in 2004, UETA facilitates electronic commerce and electronic government services by legally placing electronic records and signatures on equal footing with their paper counterparts. UETA officially repeals the 1998 South Carolina Electronic Commerce Act (*Code of Laws of South Carolina, 1976*, Section 26-5-310 through 26-5-370). The purpose of UETA is to establish policy relating to the use of electronic communications and records in contractual transactions. This law does not require the use of electronic records and signatures but allows for them where agreed upon by all involved parties. While technology neutral, the law stipulates that all such records and signatures must remain trustworthy and accessible for later reference as required by law. Similarly, the federal Electronic Signatures in Global and National Commerce (E-Sign) Act [U.S. Public Law 106-229] encourages the use of electronic documents and signatures, although it goes further to provide some guidelines regarding standards and formats. For more information on UETA see Appendices A6 and A7 of the *Trustworthy Information Systems Handbook*.
- *The Health Insurance Portability & Accountability Act* of 1996 *[HIPAA]* (Public Law 104-191) establishes security and privacy standards for health information. The Act protects the

MORE →

confidentiality and integrity of "individually identifiable health information," past, present or future. HIPAA is also concerned with non-repudiation. Non-repudiation "provides assurance of the origin or delivery of data," so that the sender cannot deny sending a message and the receiver cannot deny receiving it. This prevents either party from modifying or breaking a legal relationship unilaterally. HIPAA holds that only a digital signature technology can currently provide that assurance. Visit the South Carolina HIPAA website at www.hipaa.state.sc.us/ for additional information.

Functions of Signatures

Signatures serve specific functions. The American Bar Association lists these as:

- ◆ *Evidence:* A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
- ◆ *Ceremony:* The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent inconsiderate engagements.
- ◆ *Approval:* In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it have legal effect.
- ◆ *Efficiency and logistics:* A signature on a written document often imparts a sense of clarity and finality to the transaction, and may lessen the subsequent need to inquire beyond the face of a document. Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

An electronic signature will have to fulfill some or all of these functions. You should determine which are pertinent to your business processes before selecting a particular electronic signature technology.

What is an Electronic Signature? How does it differ from a Digital Signature?

Legal and Technological Definitions

Because information technology communities often use the terms "electronic" and "digital" interchangeably, the distinction between an "electronic signature" and "digital signature" is not always clear. As a result, definitions of electronic and digital signature have varied from state to state. The Uniform Electronic Transactions Act, adopted by several states including South Carolina, defines an electronic signature as:

> An electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

The definition is not technology-specific and does not mandate the adoption of any particular hardware or software application. Any technology that could authenticate the signer and the signed document could generate a legally admissible electronic signature providing that the parties could demonstrate the trustworthiness of the process that created and preserved the records in question.

Digital signatures

A digital signature is a particular type of electronic signature that relies on a Public Key Infrastructure (PKI). UETA does not separately define digital signatures but permits their use under the broader definition of electronic signatures. A digital signature may offer the advantage of providing a unique identifier and linking the signature to the record. It can authenticate both the signer and the signed document, thus meeting legal requirements for admissibility and trustworthiness. PKI technology offers the additional advantages of adaptability to a wide range of applications and compatibility with basic office software.

Public Key Infrastructure

Public Key/Private Key technology

Digital signatures demand the use of a specific Public Key Infrastructure [PKI] technology. PKI systems depend on two different, yet mathematically related, prime numbers referred to as "keys" to authenticate the sender and guarantee the reliability of the document. The two keys are generated simultaneously and collectively; they are known as a "key pair." One key, the private key, is kept secret by the sender and used to create the signature. The other key, the public key, is made publicly available for the recipient to validate the signature. Once a message is signed using the private key, it can only be verified by the public key. Due to the large numbers used as keys, the potential for calculating a sender's private key from a public key is mathematically insignificant. A trusted third party, either a certification or registration authority, manages the keys and the key

MORE ➔

system, including the hardware, software, and associated procedures.

In practice, the digital signature is an outcome of a mathematical operation involving the content of the message and the signer's private key. A resulting digital signature might look like this:

```
256933ECA960A6B4 F46F1546B6D5F74B
C3570CD7DD981EA1
0B506B346FB159BE 6F7BAB26F6A8A143
000B4D0A944AE4D7
96C17A4587267B05 A991D76EDE989583
9E47C19054CDB818
5BD21EE36BAC9803 CB994483A1083AB5
896777AB26BE28631
1BF17D029332B6D5 2EE82CEB2FC554A8
BDE5874D82B20B9F
```

Once calculated, the signature is appended to the original message and both the message and the signature are sent to intended recipient(s). Because the digital signature is generated as a function of the key and the message's content, the signature serves two purposes. First, it authenticates the signer, since only the individual owner should have access to both the private key and the message. Secondly, it indicates the integrity of the message, since any alteration to the text would invalidate the signature. Since the signature is intrinsically linked to the content of the message and not the carrier or format, the signature will be compromised if the content is altered in any way from the original.

A digital signature is not an encryption technique that attempts to hide the content of a message. Although the technology used to create PKI-based digital signatures was originally developed for encryption, the use of a digital signature does not automatically encode a message's content. For that reason the use of a digital signature does not prevent the manipulation of a document's content. Instead, it is designed to authenticate a sender and provide a means to verify that the sender's message has not been altered after it was sent.

Certification Authority/Registration Authority

An agency using PKI for digital signatures must guarantee that a specific person actually owns a specific key and provide quick and easy access to public keys. Because it is completely impractical for each sender and each recipient of a message to work this out on a case-by-case basis, the use of PKI for digital signatures is dependent on Registration Authorities and Certification Authorities.

A Registration Authority is an independent, trusted third party that verifies the identity of applicants for public key certificates. A Certification Authority is an independent, trusted third party which issues and manages key pairs. To get a key pair, individuals must prove to a Certification Authority, or an independent Registration Authority, that they are who they claim to be. The Certification Authority then provides secure access to public keys that allow for the validation and verification of signatures. In addition, Certification Authorities develop policy, manage software and hardware configurations, renew and revoke certificates, and provide a directory of public keys.

Digital Certificate

Certification Authorities distribute keys as part of a digital certificate. Along with the key, a certificate identifies the subscriber, the issuing Certification Authority, limitations on certificate use such as the number of transactions allowed, and the expiration date of the keys. Expiration and revocation are necessary since the longer certificates are in use the greater the chance for corruption or unauthorized access.

Managing records created in a PKI

Administrative records not produced by the PKI system

When managing records created in a PKI environment, attention should be directed towards PKI-unique administrative records. These records are specific to the administrative functions related to planning, implementing, operating, auditing or monitoring, reorganizing, or terminating a PKI. They are generally appraised as temporary.

Operational records produced by the PKI system

Many of the records required to establish the validity of a certificate or the operational integrity of the PKI are created or received and maintained on an operational system, such as the system managed by a Certification Authority or Registration Authority. Operational systems maintain records for rapid access in the day-to-day activities of running a PKI, and potentially for a shorter time period than the authorized retention period of the documents they validate. An operational system may be the only official

MORE →

source of information about the PKI activities during part if not all of an authorized retention period; therefore, it contains the official copy of that information. Consequently, protecting the integrity of the records produced by an operational system is desirable. This may entail transferring the records to a recordkeeping system before they are changed or replaced. Because PKI operational records are inherently linked to documents validated by the PKI system, they do not generally constitute a unique body of records. Basic records management regulations, standards and best practices apply to both the documents validated by a PKI system and all related records created or received in a PKI environment.

Other Electronic Signature Technologies and Trustworthiness

UETA implicitly authorizes the use of more familiar technologies, such as faxes and imaging, and more exotic biometric ones, such as iris scans, for electronic signatures. In all cases, the key to demonstrating the trustworthiness of a record and its signature is by demonstrating the trustworthiness of the system that creates and manages the record. Therefore, sufficient and appropriate systems documentation is the only way to establish that the signature is authentic and reliable. For more information on building and managing system trustworthiness see the *Trustworthy Information Systems Handbook*.

Issues to Consider

No electronic signature technology by itself is sufficient to meet all your legal needs. The evidentiary value of your signed records will ultimately rely on your ability to produce legally admissible documentation of your recordkeeping system. In addition, you will, of course, have to produce the electronic records themselves. Merely preserving and providing access to electronic records presents daunting challenges. Adding electronic signatures to the equation can complicate the situation even further.

While every option has its own advantages and disadvantages, some issues remain constant:

- ◆ Hardware and software obsolescence make it difficult, if not impossible, to preserve and provide long-term or permanent access to both the digital signature and the electronic record. For example, if you are using different technologies to create and to sign a record, they might “age” at different rates. In a PKI system, the digital signature is a function of the content of the document. Due to this relationship, any migration or conversion of the document’s content for preservation will nullify the original digital signature and prevent its use as a means to ensure the authenticity and reliability of that document. Therefore, you will need to plan for technology obsolescence of both the record and the signature if preservation of electronic signatures is desirable.
- ◆ Plan to document your decisions and transactions. Understanding your legal needs and addressing them at the design phase of an application are important factors to making this work. Keeping documentation up-to-date is an on-going responsibility, which could be complicated if relying on a third party. For example, when using digital signatures make sure that your certificate authority is managing its records and documentation adequately.
- ◆ Make sure that the electronic signature technology is interoperable with your and your constituencies’ other software applications. Requiring complex or expensive solutions is probably not practical. It would be especially difficult to ask citizens to buy and maintain multiple signature technologies.
- ◆ Remember that the human side of the equation is critical: no technology will completely address your legal requirements. A digital signature is only as reliable as the certificate authority standing behind it as well as the ability of the users to protect personal certificate information from loss or inappropriate use.

Selecting the appropriate electronic signature technology means defining your most important criteria and then determining if your system and proposed application meet those criteria. The criteria should give priority to legal concerns, since signatures are primarily valuable for evidentiary purposes. Your assessment should also consider other factors, such as technology architectures, costs/benefits, your business practices, and all pertinent policies, hardware, software, controls, and audit procedures.

For a model of and methodology for system development and assessment, refer to the *Trustworthy Information Systems Handbook*. For a specific example of the criteria pertinent to a digital signature application, see the American Bar

MORE ➔

Association's *PKI Assessment Guidelines* (See the *Annotated List of Resources* at the end of these guidelines).

Suggestions for the use of electronic signature technology

- Clarify the reasons for using electronic signatures. What business functions will the technology support?
- Determine who will use and rely on the electronic signature.
- Consider how long the signatures and the records to which the electronic signatures are affixed need to be preserved. How will the signatures and records be preserved in a way that balances the ability to retrieve and read a record with the ability to verify its signature?
- Verify which state and federal statutes pertain to the functions and transactions that generate your signed records. What case law is available?
- Determine how the electronic signature technology fits into your overall technology architecture. What is the cost per transaction? What is the total cost of the technology?
- Consider what sort of electronic signature technologies your customers use. Will you have to share these records with any other organizations or agencies?
- Establish a methodology for documenting your information systems, policies, and practices.

Annotated List of Resources

Primary Resources

American Bar Association. *Digital Signature Guidelines Tutorial*. Washington, D.C.: American Bar Association, 1996.

www.abanet.org/scitech/ec/isc/dsg-tutorial.html

> *In 1996, the ABA's Section on Science and Technology produced the first legal overview of electronic and digital signatures, as well as related concerns. Although there have been many legal and technological developments in the years since, the site still contains fundamental information on signatures that is of value. The term "tutorial" is slightly misleading; this is basically a short essay, but it is the best introduction to signatures available. It has recently been complemented by the ABA's* PKI Assessment Guideline.

American Bar Association. *PKI Assessment Guidelines*. Washington, D.C.: American Bar Association, 2001.

www.abanet.org/scitech/ec/isc/pag/pag.html

> *The Information Security Committee of the Electronic Commerce Division of the ABA issued a draft version of its PKI Assessment Guidelines (PAG) in 2001. The PAG offers a practical guide for the evaluation and assessment of PKI systems and vendors. This is a very detailed document, almost four hundred pages long. It is available as a PDF file. As noted, it is currently a draft and will be updated in the future.*

Electronic and Digital Signature Resources

www.bmck.com/ecommerce/topic-esignatures.htm

> *Baker & McKenzie is a Chicago law firm that maintains a wide variety of resources on information technology and the law. This page is a lightly annotated list of links, regularly maintained by Thomas J. Smedinghoff. Because Baker & McKenzie has an international practice, there are some useful references to developments in other countries. As well, there are links to a number of articles written by Smedinghoff and other members of the firm.*

McBride Baker & Coles. *Legislative Analysis Database for E-Commerce and Digital Signatures*. Chicago, IL: McBride Baker & Coles, 2001.

www.mbc.com/ecommerce/legislative.asp

> *McBride Baker & Coles is a Chicago law firm with an interest in information technology and the law. The Legislative Analysis Database for E-Commerce and Digital Signatures is a set of tables that allow for the comparative analysis of practices in different states. These tables systematically list and distinguish enacted digital signature legislation and uniform laws. The firm's e-commerce site provides a variety of other tables for study of pertinent issues around the world.*

National Institute of Standards and Technology (NIST), U.S. Department of Commerce. *Cryptographic Toolkit: Digital Signatures*. Washington, D.C.: NIST, 2001.

http://csrc.nist.gov/encryption/tkdigsigs.html

> *NIST's web site provides access to three Federal Information Processing Standards (FIPS) for digital signature algorithms, along with a variety of other resources on cryptography.*

MORE →

Records Management Guidance for PKI-Unique Administrative Records. Washington DC: National Archives and Records Administration, 2005.

www.archives.gov/records_management/policy_and_guidance/managing_web_records_index.html

This document contains NARA's records management guidance for PKI-unique records created by federal agencies. It identifies records produced and managed by PKI operational systems and advises agencies on records management best practices. The guidance relies on agencies to determine specific retention periods for PKI-unique records. Non-unique PKI supporting records and non-administrative PKI transactional records are not covered. The guidance does not recommend or identify specific technology or products.

PKI Resources

www.pkiforum.org/resources.html

The PKI Forum is an international, non-profit alliance of vendors and users interested in PKI products and services. It maintains online an extensive list of resources, arranged by topic and country. There is information on certificate authorities, digital signature laws, security, policies, and vendors. Also available are a number of white papers on topics including interoperability. PKI Forum sponsors quarterly meetings. Memberships are required to gain all the advantages of the organization.

South Carolina Department of Archives and History. *Trustworthy Information Systems Handbook*. Version 1, July 2004.

www.state.sc.us/scdah/erg/tis.htm

This handbook provides an overview for all stakeholders involved in government electronic records management. Topics focus on accountability by developing systems that create reliable and authentic information and records. The handbook outlines the characteristics that define trustworthy information, offers a methodology for ensuring trustworthiness, and provides a series of worksheets and tools for evaluating and refining system design and documentation.

UETA Online

www.webcom.com/legaled/UETA/

This site is maintained by Carol A. Kunze, an attorney specializing in information technology. Kunze participated in the drafting sessions for UETA and the Uniform Computer Information Transactions Act (UCITA). The site includes background information on the development of UETA and its federal equivalent, the Electronic Signatures in Global and National Commerce Act (E-Sign). There are links to useful analyses of the acts and their applications.

Additional Resources

Commonwealth of Australia. *Gatekeeper*. Canberra, Australia: National Office for the Information Economy, 2000.

www.govonline.gov.au/projects/confidence/Securing/Gatekeeper.htm

Gatekeeper is the strategy Australia is using for the development of PKI in e-government. The site includes basic information on the use of PKI, FAQs, and criteria for accrediting certificate authorities. Since Australia has been an innovative force in the development of electronic records standards and e-government services, its electronic signature projects are generally worth analyzing. One aspect that is of special interest is the concern for interoperability across government.

HIPAAdvisory. *Standards for Security and Electronic Signatures*. Montgomery Village, MD: Phoenix Health Systems, 2001.

www.hipaadvisory.com/regs/securityandelectronicsign/electronicsignature.htm

HIPAA, the Health Insurance Portability and Accountability Act of 1996, has created a small industry of guidelines, consultancies, and web sites devoted to explaining how its mandates can be implemented. This site provides easy access to the rules created by the Department of Health and Human Services for "standards for the security of individual health information and electronic signature use by health plans, health care clearinghouses, and health care providers." Since so many important government functions are related to health care, HIPAA's requirements will probably heavily influence the development of standards and technology architectures for electronic signatures.

State of Washington. *Electronic Authentication*. Olympia, WA: Office of the Secretary of State, 2001.
www.secstate.wa.gov/ea

Washington's digital signature law was a model for a number of other states. The Secretary of State oversees the implementation of the law and particularly the regulation of certificate authorities. The web site includes useful information and resources on the workings of the law.