ELECTRONIC RECORDS MANAGEMENT GUIDELINES

ELECTRONIC SIGNATURES

Summary

The advent of e-government and e-services is changing the way state agencies and local government offices 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 the same level of confidence associated with handwritten signatures.

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

Furthermore, the electronic signature application selected must fit the agency's technology architecture to create, preserve, and make available its 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 the organization.

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. Agencies should determine which are pertinent to their business processes before selecting a particular electronic signature technology.

What is an Electronic Signature?

The Uniform Electronic Transactions Act [UETA] (*Code of Laws of South Carolina*, 1976, Section 26-6-10 through 26-6-210 http://www.scstatehouse.net/code/t26c006.doc), 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.

MORE →

South Carolina Standards for Electronic Signatures

In February 2007, the South Carolina State Budget and Control Board through its Architecture Oversight Committee (AOC) approved the *SC Standards for Electronic Signatures*.
http://cio.sc.gov/NR/rdonlyres/A825AF86-8FDA-4A63-8A02-8907639020EC/0/scrUETASCStandardsforElectronicSignatures.pdf

These standards, promulgated to comply with the UETA, are applicable to all state government entities including agencies, boards, commissions, colleges and universities. Local governments may, at their discretion, consent to be governed by these standards.

All programs implemented by state government entities which utilize electronic signatures shall meet the following conditions:

- **Use of signature unique to the signer:** The electronic signature must uniquely identify the signer, and must be under reasonable control of the signer. That is, it must be unlikely that any other unauthorized entity provided the signature.
- **Agreement by the parties:** A party signs a document in order to convey a mutually understood message to another party, such as authorship, receipt, or approval of the document. In the case of an electronic signature, both the signer and the intended recipient of the signed document must agree that the electronic sound, symbol, or action will be accepted as serving as a signature for the electronic document or record.
- **Intent to sign:** The application of the electronic signature to the electronic record must be a deliberate act. It cannot be implied or inferred.
- **Association of the signature with the signed record:** The electronic signature must be physically or logically associated with the electronic record that is signed, and that association must persist for as long as the signature is in effect, which may be the life of the record.

The degree to which each of the above conditions is met is dependent on several factors normally associated with security concerns:

- **Authentication:** the ability to prove that the actual signer is the intended signer
- **Non-Repudiation:** the inability of the signer to deny the signature
- **Integrity:** the assurance that neither the record nor the signature has been altered since the moment of signing.

For additional detail on the standards and assistance with implementation, refer to the *South Carolina Electronic Signatures Analysis and Implementation Guide*.
http://cio.sc.gov/NR/rdonlyres/9F3BA2ED-7A88-4EE4-A090-93BB482B1502/0/scrUETASCAnalysisandImplementationGuideforElecSignatures.pdf

Types of Electronic Signature Technologies

There are a number of currently available electronic signature technologies that are capable of meeting state standards. Examples include PIN/password, physical token, digitized signature, biometric signature, and digital signature. For complete descriptions and specific examples of state government applications using these technologies, refer to Sections 10 and 11 of the *South Carolina Electronic Signatures Analysis and Implementation Guide*.
http://cio.sc.gov/NR/rdonlyres/9F3BA2ED-7A88-4EE4-A090-93BB482B1502/0/scrUETASCAnalysisandImplementationGuideforElecSignatures.pdf

Regardless of the technology chosen, the key to demonstrating the trustworthiness of a record and its signature is by demonstrating and documenting the trustworthiness of the system that creates and manages the record and signature. 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*.
http://arm.scdah.sc.gov/erp/tishandbook.htm

Issues to Consider

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

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

MORE →

- Hardware and software obsolescence make it difficult, if not impossible, to preserve and provide long-term or permanent access to both the electronic signature and the associated electronic record. For example, if an agency is using different technologies to create and to sign a record, those technologies might "age" at different rates. In a digital signature (PKI) system, the 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, agencies will need to plan for technology obsolescence of both the record and the signature if long-term preservation of electronic signatures is desirable.
- Agencies should plan to document their decisions and transactions. Understanding 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 agencies should make sure that the certificate authority is managing its records and documentation adequately.
- Agencies should make sure that the electronic signature technology is interoperable with their and their 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.
- Agencies should assess risks associated with the use of electronic signature technology and develop a well-documented risk management plan based upon the risks identified. Information on the issues to be considered in assessing and managing risks can be found in Section 4 of the South Carolina Electronic Signatures Analysis and Implementation Guide. http://cio.sc.gov/NR/rdonlyres/9F3BA2ED-7A88-4EE4-A090-93BB482B1502/0/scrUETASCAnalysisandImplementationGuideforElecSignatures.pdf
- The human side of the equation is critical: no technology will completely address your legal requirements. For example, 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 the most important criteria and then determining if the system and proposed application meet those criteria. The criteria should give priority to legal concerns, since signatures are primarily valuable for evidentiary purposes. A selection decision should also reflect consideration of other factors, such as technology architectures, costs/benefits, agency business practices, and all pertinent policies, hardware, software, controls, and audit procedures.

Guidance with selecting and implementing the appropriate electronic signature technology can be found in the *South Carolina Electronic Signatures Analysis and Implementation Guide*.
http://cio.sc.gov/NR/rdonlyres/9F3BA2ED-7A88-4EE4-A090-93BB482B1502/0/scrUETASCAnalysisandImplementationGuideforElecSignatures.pdf
A model of and methodology for information system development and assessment can be found in the *Trustworthy Information Systems Handbook*.
http://arm.scdah.sc.gov/erp/tishandbook.htm
A specific example of the criteria pertinent to a digital signature application can be found in the American Bar Association's *PKI Assessment Guidelines*.
www.abanet.org/scitech/ec/isc/pag/pag.html)

Suggestions for the use of electronic signature technology

All agencies should:

- Clarify the reasons for using electronic signatures and determine what business functions the technology will 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 and how the signatures and records will 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 the signed records and determine what case law is available.
- Determine how the electronic signature technology fits into the overall technology architecture, what is the cost per transaction, and what is the total cost of the technology.

MORE →

- Consider what sort of electronic signature technologies customers use and if records will have to be shared with any other organizations or agencies.
- Establish a methodology for documenting information systems, policies, and practices.

Legal Framework

There are a number of statutes pertaining to government records which agencies 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.net/code/t30c001.doc. The PRA 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 agency responsibility to protect records 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) available at http://www.scstatehouse.net/code/t26c006.doc. The UETA facilitates electronic commerce and electronic government services by legally placing electronic records and signatures on equal footing with their paper counterparts. 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. More information on UETA can be found in Appendices A6 and A7 of the *Trustworthy Information Systems Handbook*. http://arm.scdah.sc.gov/erp/tishandbook.htm
- *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 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.

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.*

MORE →

South Carolina Enterprise Architecture. *Uniform Electronic Transactions Act, SC Standards for Electronic Records*, February 28, 2007.

http://cio.sc.gov/NR/rdonlyres/A825AF86-8FDA-4A63-8A02-8907639020EC/0/scrUETASCStandardsforElectronicSignatures.pdf

The standards promulgated in this document were created in an effort to comply with the purpose and intent of the Uniform Electronic Transactions Act (UETA — S.C. Code Ann. 26-6-10 et seq.). South Carolina Code Section 26-6-190 of UETA, *entitled* Development of standards and procedures; service of process.

South Carolina Architecture Oversight Committee UETA Task Force. *South Carolina Electronic Signatures Analysis and Implementation Guide*, March 28,2007.

http://cio.sc.gov/NR/rdonlyres/9F3BA2ED-7A88-4EE4-A090-93BB482B1502/0/scrUETASCAnalysisandImplementationGuideforElecSignatures.pdf

Proposed by the UETA Task Force to the South Carolina Architecture Oversight Committee, this document expands upon the four factors comprising the SC Standards for Electronic Signatures and explores some of the implementation considerations in each of the four areas. The document also provides descriptions of various electronic signature technologies and examples of state agency applications using those technologies.

Electronic and Digital Signature Resources

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

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.

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

www.archives.gov/records-mgmt/policy/pki.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/

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 2, March 2007.

http://arm.scdah.sc.gov/erp/tishandbook.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.

MORE →

Additional Resources

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

www.agimo.gov.au/infrastructure/gatekeeper

> *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.*

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.*