Electronic Signature Recordkeeping Guidelines

Summary

E-government and e-services change the way state and local government agencies conduct business. In a paper environment, a hand signature, also known as a "wet signature," authorizes and authenticates the content of a document. Up-to-date technologies and procedures must meet the demand for trustworthiness and accountability when replacing hand signatures with electronic 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. Government agencies will need to define legal and evidentiary needs in relation to business processes (such as authorization of an action or authentication of a document) before choosing an electronic signature application.

The electronic signature application selected must fit the agency's technology architecture to create, preserve, and make available its records. Policies for preserving signatures adopted by each agency will 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 record 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.
- C*eremony:* 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.

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

What is an Electronic Signature?

The Uniform Electronic Transactions Act [UETA] (*Kentucky Revised Statutes* KRS 369.102 (8)), 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 (PKI, pin/password, biometric identification, physical token etc.) 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. The purpose of the signature can vary from authorizing approval in a workflow to signing a legal contract.

Kentucky Standards for Electronic Signatures

Electronic Signatures

Broadly, the UETA requires applications that use electronic signatures 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 an 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 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.

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 state government agencies, the Enterprise Information Technology (IT) Architecture Standard, 2370 Electronic Commerce-Electronic Signature, identifies 3 approved and recommended products.

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. Sufficient and appropriate systems documentation is key in establishing that the signature is authentic and reliable.

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

- Agencies should plan to document their decisions and transactions. Understand and address legal needs during the design phase of an application and keep documentation up-to-date. (This 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 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.
- 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 using a system and application that 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 pertinent policies, hardware, software, controls, and audit procedures.

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. Determine 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. (See Enterprise Information Technology (IT) Architecture Standard, 4055 **"**Preservation of Long-term Records" for an explanation of the issues in maintaining records over time)
- 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, the cost per transaction, and the cost of the technology.
- 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

Pertinent laws include:

- Kentucky Public Records law (KRS 171.410-171.740). The law supports government accountability by mandating the use of retention schedules to manage Kentucky public records. This law governs the management of all records created by agencies or entities supported in whole or in part by public funds in Kentucky. It also establishes agency responsibility to protect records and to make them available for easy use. The act does not discriminate between media types. Records created or formatted electronically are covered under the act.
- Kentucky Uniform Electronic Transactions Act [UETA] (KRS 369.101-369.120.) 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, and provides some guidelines for standards and formats.
- *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

American Bar Association. *Digital Signature Guidelines Tutorial*. Washington, D.C.: American Bar Association. www.abanet.org/scitech/ec/isc/dsg-tutorial.html

To explain the value of digital signatures in legal applications, this tutorial begins with an overview of the legal significance of signatures. It outlines basics of digital signature technology, and examines how, with some legal and institutional infrastructure, digital signature technology can be applied as a robust computer-based alternative to traditional signatures.

Australia, Commonwealth of. *National e-Authentication Framework.* Canberra, Australia: National Office for the Information Economy, Dec. 2008. http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html

To manage some of the risks associated with online transactions, the Australian Government developed the National e-Authentication Framework (NeAF). The NeAF encompasses the electronic authentication (e-authentication) of the identity of individuals and businesses dealing with the government, on one side of the transaction, as well as the authentication of government websites on the other side.

Illinois. *Digital Signature Project*. http://www.illinois.gov/pki/

The State of Illinois Digital Signature Project is an integral part of the State's e-government infrastructure, from providing digital certificates as a standard means of authenticating and simplifying access for citizens, to signing electronic documents, to application development benefits for state agencies, integrating applications that cross the current boundaries between local, state, and federal government.

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

National Institute of Standards and Technology (NIST), U.S. Department of Commerce. **Federal Information Processing Standards Publication 186-3 - June 2009** http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

NIST's web site provides access to the latest Federal Information Processing Standards (FIPS) for digital signature algorithms.

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

Washington's digital signature law served as 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.