Electronic Signature Recordkeeping Guidelines

Summary

In a paper environment, a hand signature, also known as a “wet signature,” authorizes and authenticates the content of a document. Current technology 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. The electronic signature application selected must fit the agency’s technology architecture to create, preserve, and make available its records.

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.
- *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.

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?

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

Broadly, the Uniform Electronic Transactions Act (UETA) requires applications that use electronic signatures to 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 approved and recommended products. An agency should also consider long-term digital preservation as defined by the Kentucky Department for Libraries and Archives (KITS 4055).

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.

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.

Preserving permanent records with electronic signatures requires migration plans from one system to another (including the signature keys), especially if the records are transferred to the Kentucky Department for Libraries and Archives for long term preservation and appropriate access.

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.
- The Family Educational Rights and Privacy Act [FERPA] of 1974 "protects the privacy and confidentiality of personally identifiable information contained within student education records." In order to protect privacy and ensure confidentiality, a signed and dated written consent is required prior to the release of student information from either a parental guardian or an eligible student over the age of 18. Electronic signatures were specially recognized in 2004 as a method of authenticating both the source of the consent and the approval of the information of that consent.

Annotated List of Resources

American Bar Association. Digital Signature Guidelines Tutorial. Washington, D.C.: American Bar Association. https://scholarship.law.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1178&context=commlaw

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.

National Archives and Records Administration. ***Records Management Guidance for PKIUnique Administrative Records*****.** Washington DC: NARA, 2003.) https://www.archives.gov/files/records-mgmt/pdf/final-pki-guidance.pdf

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 186-5 - February 2023
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

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

FERPA Final Regulations Relating to Electronic Consent and Signature, U.S. Department of Education. **Federal Register -April 21, 2004**
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/042104a.pdf

This document finalizes the language regarding the use and benefits of electronic signatures in requests for records containing information on students.