AUTHENTICATION STANDARDS FOR THE USE OF ELECTRONIC SIGNATURES IN ELECTRONIC DOCUMENTS

JANUARY 8, 2008

Produced by the Electronic Signatures Work Group of the Standards Subcommittee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts

Roger Gates
Butler County Prosecutor's Office
Work Group Co-Lead

Milt Nuzum
Supreme Court of Ohio
Work Group Co-Lead
Standards Subcommittee Co-Chair

Hon. Gary Byers
Maumee Municipal Court
Standards Subcommittee Co-Chair

Hon. John Bessey
Franklin County Common Pleas Court
Chair, Advisory Committee on Technology and the Courts

Acknowledgements

These standards were produced through the work of the dedicated volunteer members of the Electronic Signatures Work Group of the Standards Subcommittee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts.

Roger Gates, Co-Lead
Butler County Prosecutor's Office

Milt Nuzum, Co-Lead
Supreme Court of Ohio

Jan Antonoplos
Delaware County Clerk of Courts

Alden Coleman
Cleveland Municipal Court

Annetta Fisher
East Cleveland Municipal Court

Jeffrey Fortkamp
Ohio Legal Assistance Foundation

Ajmeri Hoque
Franklin County Municipal Clerk of Court

Susan Horak
Franklin County Municipal Court

Tamiyka Koger
Franklin County Municipal Clerk of Court

Stephen Polinsky
Ohio Office of Information Technology

William Scherpenberg
Mason Municipal Court

Annette Wright
Montgomery County Domestic Relations Court

Robert Stuart, Director, Information Technology Division
Supreme Court of Ohio

This and all other standards developed by the Advisory Committee on Technology and the Courts are available online at the Supreme Court of Ohio website, www.supremecourtofohio.gov.

Introduction

Since the beginning of written language, individuals have affixed their signatures to writings with the intention of both establishing the source of the writing and memorializing their assent, or adoption, of its contents. According to Wikipedia,©

> The traditional function of a signature is evidential: it is to give evidence of:
>
> 1. the provenance of the document (identity)
> 2. the intention (will) of an individual with regard to that document
>
> For example, the role of a signature in many consumer contracts is not solely to provide evidence of the identity of the contracting party, but rather to additionally provide evidence of deliberation and informed consent. Signatures may be witnessed and recorded in the presence of a Notary Public to carry additional legal force. On legal documents, an illiterate signatory can make a "mark" (often an "X" but occasionally a personalized symbol), so long as the document is countersigned by a literate witness. . . .
>
> Some states' legal definition of a signature defines a signature to mean "any memorandum, mark, or sign made with intent to authenticate any instrument or writing, or the subscription of any person thereto." In the context of one particular statute, a signature doesn't have to be the popular notion of a written name, but may be other methods of authentication; the intent of any mark or memorandum makes a signature.

www.wikipedia.com.

Until relatively recent times, legal effect was generally given to documents only when they bore original signatures, or a seal of the signer. However, as advances in technology resulted in the ability to produce photographic images of documents and signatures, copies of original signatures began to be given legal effect. For example, Ohio Rules of Evidence, Rule 1003 now provides that "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."

Even though many statutes and rules require that a document be "signed" and that a "signature" be affixed to a document, Ohio has no statutory definition of either of those terms as applied to the judicial process. In the commercial context, Ohio Rev. Code §1301.01(MM) provides that a document may be "signed" by affixing "any symbol executed or adopted by a party with present intention to authenticate a writing." In essence, the affixing of a signature to a writing allows those persons who were not present at the making of the writing to be assured that the signer either originated the writing, or assented to its contents.

In 2000, Ohio Revised Code Chapter 1306 was enacted to authorize the use, by agreement, of electronic signatures to authenticate electronic records in electronic transactions. R.C. §304.02 provides that, prior to using electronic records and electronic signatures under R.C. Chapter 1306, a "county office" must "adopt, in writing, a security procedure for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record;" that statute further provides that "a security procedure includes, but is not limited to, a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures."

In the context of documents either filed with or generated by Ohio courts, and received by their clerks, the custom had, until recently, been that such documents were required to bear an original signature of the person who originated the document. R.C. §1306.22 states that no Ohio court is required to use or permit the use of electronic records and electronic signatures; however, the Supreme Court of Ohio is authorized to "adopt rules pertaining to the use of electronic records and electronic signatures." In 2001, Civil Rule 5(E)[1] was amended to provide:

> A court may provide, by local rules adopted pursuant to the Rules of Superintendence, for the filing of documents by electronic means. If the court adopts such local rules, they shall include all of the following:
>
> > (1) Any signature on electronically transmitted documents shall be considered that of the attorney or party it purports to be for all purposes. If it is established that the documents were transmitted without authority, the court shall order the filing stricken.
> >
> > (2) A provision shall specify the days and hours during which electronically transmitted documents will be received by the court, and a provision shall specify when documents received electronically will be considered to have been filed.
> >
> > (3) Any document filed electronically that requires a filing fee may be rejected by the clerk of court unless the filer has complied with the mechanism established by the court for the payment of filing fees.

The Staff Note for this amendment stated:

> The amendments to this rule were part of a group of amendments that were submitted by the Ohio Courts Digital Signatures Task Force to establish minimum standards for the use of information systems, electronic signatures, and electronic filing. The substantive amendment to this rule was the amendment of the second sentence and the addition of the last sentence of division (E), and the addition of divisions (E)(2) and (E)(3). Comparable amendments were made to Civil Rule 73 (for probate courts), Criminal Rule 12, Juvenile Rule 8, and Appellate Rule 13.
>
> As part of this electronic filing and signature project, the following rules were amended effective July 1, 2001: Civil Rules 5, 11, and 73; Criminal Rule 12; Juvenile Rule 8; and Appellate Rules 13 and 18. In addition, Rule 26 of the Rules of Superintendence for Courts of Ohio was amended and Rule of Superintendence 27 was added to complement the rules of procedure. Superintendence Rule 27 establishes a process by which minimum standards for information technology are promulgated, and requires that courts submit any local rule involving the use of information technology to a technology standards committee designated by the Supreme Court for approval.

Although no court is required to authorize the use of electronic signatures to authenticate electronic records, any court which elects to do so by local rule must comply with minimum standards promulgated under Sup. R. 27.

Description of Paradigm

There are generally three categories for the use of electronic signatures in electronic transactions in which a court, or more typically its clerk, may become involved.

> The first category involves transactions in which non-court personnel generate and send electronic records to the clerk. In these transactions, the electronic record is electronically signed by someone other than an employee of the court/clerk, and the

record is then transmitted to the clerk. In these transactions, the court must prescribe standards as to how the electronic signature is associated with the electronic record and security procedures to authenticate the source of the electronic signature.

The second category involves transactions in which court personnel including judges and magistrates electronically sign an electronic record, and the record is then sent to (filed with) the clerk. In these transactions, the court must prescribe standards as to how the electronic signature is associated with the electronic record. The court must also establish security procedures to authenticate the source of the electronic signature.

The third category involves transactions in which court personnel, typically the clerk but not including judges and magistrates, electronically sign an electronic record, and the record is then sent to recipients outside of the court. In these transactions, the court must prescribe standards as to how the electronic signature is associated with the electronic record and security procedures to authenticate the source of the electronic signature, so that the electronic signature and associated record will be accepted by the recipient.

Statement of Purpose and Intent

The purpose of this standard is to establish minimum authentication requirements for the use of electronic signatures in electronic records by the courts of Ohio. This standard prescribes minimum requirements for the creation of electronic signatures and for security procedures associated with the use of electronic signatures in electronic records.

The goal of the standard is to assure the authenticity of electronic signatures either received or generated by a court so that those who utilize electronic records in which an electronic signature is associated will have confidence that the signature is authentic; i.e., that the electronic signature associated with a court's electronic record will be as unassailable as the traditional pen on paper model or that the electronic signature is a reliable as an ink signature as a means to validate the signer's identity and intent. In order to assure public confidence in the use of technology applied to create electronic signatures in electronic records, it is necessary that courts follow these minimum standards. A court able to certify compliance with these minimum standards will be able to thwart third-party challenges to the validity of the electronic signature and save the time and effort of court personnel to defend the processes. Ultimately, compliance with these standards will allow the public to use electronic signatures in electronic records with assurance of the signature's validity.

This standard is meant to be used in conjunction with other standards promulgated under Sup. R. 27. Currently, various functions and subfunctions, in the Combined Case Management Systems Standard ("CCMS") require that the case management system (the "CMS") support the generation and/or distribution by the court of documents by electronic means. Also, the Electronic Filing Standards ("EFS") require that an electronic filing system must provide "authentication of filer identity in accordance with standards established by the ACTC." If a court chooses to adopt a local rule permitting the use of electronic signatures in practice before the court, then the local rule must, at a minimum, comply with this standard and with the requirements of the CCMS and the EFS which relate to the non-reputability and integrity of electronic signatures in electronic records.[2]

Statement of Applicability

This standard applies to the use of electronic signatures in electronic records which relate to "practice and procedure" in local courts; however, the standard is not applicable to the court's determination as to the admissibility of evidence. The standard is not intended to be applicable to the business of the court unrelated to the administration of justice in court cases; examples include the ordering of supplies, personnel policies, informational publications and informal communications generated by court personnel. This standard also is not intended to apply to electronic signature requirements of systems utilized by court personnel that are controlled by persons or entities outside of a court's system, for example, electronic banking.

Functional Standards for Authentication of Electronic Records

1. Definitions. For purposes of this standard, the following terms shall have the following meanings:

   a. "*Authentication*" - the process of assuring that an electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction.

   b. *"Digital Certificate"* - An attachment to an electronic message used for security purposes, which enables a user sending a message via an unsecured network, for example, the internet, to verify that the user is who he or she claims to be and that the electronic message has not been altered during the transmission.[3] Although there are a number of different processes by which a digital certificate may be created, certificate systems will typically "hash"[4] the certificate to validate that the certificate has not been altered.

   c. "*Electronic*" - relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. For the purposes of this standard, "electronic" is not meant to encompass activities involving facsimile transmission.

   d. "*Electronic record*" - a record created, generated, sent, communicated, received, or stored by electronic means.

   e. "*Electronic signature*" - an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.

   f. "*Electronic transaction*" - an action or set of actions occurring between two or more persons or entities relating to the conduct of governmental affairs by electronic means.

   g. "*PKI*" (public key infrastructure) – a digital certificate process which enables users of an unsecured network, for example, the internet, to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a certificate authority. PKI provides for the association of a digital certificate with the data to identify the source of the data along with directory services that can verify the validity and identity of the digital certificate.

   h. "*Record*" - information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

i. "*Security procedure*" - a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. "Security procedure" includes a procedure that requires the use of algorithms or other codes, identifying word or numbers, encryption, or callback or other acknowledgment procedures.

2. Legal force and effect. Electronic signatures used in electronic records under the auspices of a local rule adopted in accordance with Sup. R. 27 shall have the equivalent level of legal protection that is given to paper-based signatures.

3. Filing and Maintenance of Rules. Pursuant to Sup. R. 27, courts must submit and maintain their local rule pertaining to the use of electronic signatures in electronic records.

4. Required Elements for Local Rules. A local rule adopted under this standard shall ensure the authentication of any electronic signature employed in an electronic record. At a minimum, the local rule must:

a. Describe the categories of electronic records which may be exchanged in electronic transactions, involving the clerk of the court, in which an electronic signature is used.

b. Describe the format for an electronic signature which may be used in an electronic record to meet any of the signing requirements established by the Rules of Procedure promulgated by the Supreme Court pursuant to Art. IV, Sec. 5(B) of the Constitution of Ohio.

c. Describe the processes of authentication to be utilized in electronic transactions, involving the clerk of the court, in which an electronic signature is used.

d. Require that an electronic signature must be attached to or logically associated with the electronic record, and must be linked to the data in such a manner that any subsequent alteration to the electronic signature is detectable and will invalidate the electronic record.

e. Require that any electronic signature in an electronic record filed with the court in accordance with the court's local rule shall be presumed to be authentic. If it is established upon motion by the signer or the signer's personal representative that an electronic record was transmitted without authority or modified from what the signer adopted, the court may order the filing stricken.

f. Require that the electronic record in the court's case management or electronic filing system demonstrate that an electronic signature is associated with the electronic record and that any electronic or paper output from the case management or electronic filing system shall indicate that the record was signed electronically and identify by name the person who electronically signed the electronic record.[5]

5. Authentication Processes. For purposes of this standard, the process to ensure the authentication of an electronic signature in an electronic record shall, at a minimum, be of one of the following types:

a. *Type 1*: This process uses a signature pad or other similar device to associate with an electronic record a digital representation of a physical signature of the person signing the record. To authenticate the electronic signature on the electronic record, the signature shall be created in the presence of a deputy clerk other than the signer. Either the signer or the witness shall immediately submit the record to the e-filing or case management system.

b. *Type 2*: This process is used to authenticate an electronic signature on an electronic record by the sender logging-in to an application recognized by the court (i.e., a case management system, or an e-filing system/portal) which will receive the electronic record. The electronic record may be created from within the court's case management system (court user) or from an application outside of the court (non-court user). The login will involve a user name and password which are unique to the sender. The local court, or a vendor under a contract with the court, will maintain a secure register of the user name and password for each authorized user. The user name and/or password may be either created by the user, or assigned to the user by the administrator of the court application. The court must utilize secure password procedures.

c. *Type 3*: This process is used to authenticate an electronic signature on an electronic record by a two-step process. First, the sender must log in to the application as described above for the Type 2 process, plus the sender must additionally verify the transaction by either entry of a separate unique personal identifier (e.g., a personal identification number ["PIN"]) or the use of a physical identification device (e.g., smart card, biometric reader, etc.).

d. *Type 4*: This process is used by the clerk of the court to authenticate the electronic signature of the clerk in an e-mail which certifies that an electronic record attached to the e-mail is a true copy of a document on file with the clerk. Prior to transmitting the e-mail, the clerk must obtain a digital certificate from a certificate authority and must associate the digital certificate with the e-mail to authenticate the clerk's electronic signature. For this process, the digital certificate must use either PKI or a certificate system providing an equal or greater level of security.

e. *Type 5*: This process is used to authenticate electronic signatures on electronic records by complying with specific secure data transfer protocols (e.g., FTP, web services, etc.) negotiated by the clerk of the court with a trusted authority, such as a financial institution, large employer, or government agency (e.g. BMV, BCI&I, Ohio Courts Network, other courts, local law enforcement agencies, etc.).

6. <u>Minimum Authentication Requirements.</u> At a minimum, the following types of authentication shall be required for the different categories of electronic signatures in electronic records exchanged in electronic transactions involving the clerk of the court:

a. Electronic Records filed with the clerk of the court from outside of the court:

i.	Attorneys and other litigants	Type 2
ii.	Judges and magistrates	Type 3
iii.	Trusted authorities	Type 5

b. Electronic Records filed with the clerk of the court from inside of the court:

i.	Attorneys and litigants physically present at the court	Type 1 or 2
ii.	Judges and magistrates	Type 1 or 3
iii.	Other court personnel	Type 1 or 2

c. Electronic Records filed with the clerk and distributed, or made available, to persons/entities outside of the court:

i.	Certified copies of court filings	Type 4
ii.	Notices to attorneys or litigants	Type 2
iii.	Publicly-available copies (not certified) of court filings	no authentication
iv.	Transmission to a trusted authority,	Type 5

[1] Although the 2001 amendments of the rules of practice dealt only with electronic signatures on documents "filed with the court," a local rule of practice authorizing the use of electronic signatures by judges and judicial officers would not be "inconsistent with the rules promulgated by the Supreme Court." Article IV, Sec. 5(B), Constitution of Ohio provides that:

> The Supreme Court shall prescribe rules governing practice and procedure in all courts of the state, which rules shall not abridge, enlarge, or modify any substantive right. . . . Courts may adopt additional rules concerning local practice in their respective courts which are not inconsistent with the rules promulgated by the supreme court.

Article IV, Sec. 5(A), Constitution of Ohio provides that the supreme court shall have the power of superintendence over the courts of the state. Pursuant to this authority, the supreme court has adopted the rules of superintendence. Sup. R. 5(A)(1) provides that:

> Nothing in these rules prevents the adoption of any local rule of practice that promotes the use of any device or procedure to facilitate the expeditious disposition of cases. Local rules of practice shall not be inconsistent with rules promulgated by the Supreme Court.

However, Sup. R. 27(C) restricts the authority of a local court to adopt local rules of practice which relate to the use of information technology in the local court; the rule states:

> Before adopting any local rule of practice that relates to the use of information technology, a court shall submit a copy of the proposed local rule to the Supreme Court Advisory Committee on Technology and the Courts for review in accordance with the process established by the committee pursuant to division (B) of this rule. A local rule of practice that relates to the use of information technology shall be considered inconsistent with this rule and of no force and effect unless the committee determines that the local rule complies with the minimum, uniform standards adopted by the committee pursuant to division (B) of this rule.

Since any local rule of practice authorizing the use of electronic signatures in a local court relates to the use of information technology [see, Sup. R. 27(B)(1)(b)], any such rule will not be valid until the ACTC determines that the rule complies with minimum, uniform standards adopted by the ACTC concerning the use of electronic signatures.

Therefore, this standard deals not only with the use of electronic signatures on documents filed with the court by attorneys and litigants, but also with the use of electronic signatures by judges, magistrates and other court personnel.

[2] This standard is designed only to prescribe minimum requirements relating to the authentication of an electronic signature associated with an electronic record transmitted in an electronic transaction. The E-Filing Standard deals with issues regarding how an electronic transaction is processed by the clerk of a court. The Case Management Systems Standard relates to how the Court, and its Clerk, must deal with documents which have been either received, or generated, by the court. For this reason, this Authentication Standard for the Use of Electronic Signatures in Electronic Documents does not deal with minimum requirements as to protecting the integrity of electronic documents and the electronic signatures which are a part of those documents. The E-Filing Standard and the Case Management Standard should be consulted to determine the requirements for those functions. *See, e.g.*, Electronic Filing Standards, Policy Standard 1.1H and Functional Standard 3.6.

[3] A digital certificate is also sometimes also referred to as a "digital signature." In its November, 2004, "Electronic Signatures Report," the Court Technology Committee of the Ohio Judicial Conference stated:

> A digital signature is a special type of electronic signature that encrypts both the signature and the document. A digital signature employs "two different but mathematically related 'keys;' one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form." *Quoting from*, *Digital Signature Guidelines Tutorial*, American Bar

> Association Section of Science and Technology Information Security Committee, http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html. A digital signature is considered a very secure form of electronic signature. It is also the most costly.

This statement most likely described a digital signature/certificate using a PKI certificate process.

[4] A "hash" has been described as a digital fingerprint. Frequently, it is based upon a sum of the bits in a data set.

[5] In its November, 2004, "Electronic Signatures Report," the Court Technology Committee of the Ohio Judicial Conference stated in reference to the use of electronic signatures by judicial officers:

> Document acceptance: A certain amount of public and professional education will be necessary for acceptance of electronically signed documents. To facilitate such acceptance, we suggest electronically signed documents carry some notation that they have been electronically signed, such as "Electronically signed by Judge Jones."