

# Electronic Signatures Report

## Court Technology Committee

### Ohio Judicial Conference

*Co-Chairs:*  
Guy C. Guckenberger  
Thomas Zachman

*OJC Staff:*  
Ulf Nilsson

November 2004

#### ~ Executive Summary ~

This report responds to the request of the Supreme Court of Ohio Advisory Committee on Technology & the Courts (ACTAC) for information on the use of electronic signatures. The report describes rule changes to allow courts to use electronic signatures. The report also suggests minimum security standards when electronic signatures are used.

#### **What is an Electronic Signature?**

An electronic signature is 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. For example, this definition can include one's name typed at the end an e-mail message, a scanned signature inserted into a document, and the standard webpage click through process, requiring, *e.g.*, a login and "I agree."

#### **Permitting Courts to Use Electronic Signatures**

Current court rules allow for the filing of documents with courts electronically, but do not allow courts to sign documents electronically. The committee recommends that court rules be changed to permit courts to sign documents electronically. We recommend this be done by defining "signature" to include an electronic signature, with the proviso that the use of electronic signatures in any court must be approved in advance by local court rule.

#### **Electronic Signature Security**

- 1) Ensuring the act of signing is genuine: The act of electronically signing a document should require an act only the signer can perform, as is the case with a conventional signature. The committee recommends that, at a minimum, the act of electronically signing a document should be a separately authorized act requiring at least a personal identification number (PIN) or a username and password.
- 2) Preserving the integrity of the document once it is signed: Once a document is electronically signed, it must be protected from change or destruction for it to be considered reliable. Standards for such protection are currently being formulated by the Electronic Filing Work Group of the Standards Subcommittee of the ACTAC. In the absence of statewide standards, existing computer networks and systems in most organizations can provide adequate protection for electronically signed documents, such as restricted access and archival routines.
- 3) 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."

# Electronic Signatures Report

## Court Technology Committee

### Ohio Judicial Conference

*Co-Chairs:*  
Guy C. Guckenberger  
Thomas Zachman

*OJC Staff:*  
Ulf Nilsson

November 2004

This report is in response to the request of the Supreme Court of Ohio Advisory Committee on Technology & the Courts for information on the use of electronic signatures by courts.<sup>1</sup> The report provides information on needed rule changes to allow courts to use electronic signatures. The report also makes suggestions for minimum-security standards when electronic signatures are used.

### What is an Electronic Signature?

An electronic signature is widely defined as follows:

‘Electronic signature’ means 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.<sup>2</sup>

Electronic signatures can take a variety of forms, some of which are decidedly simple and low tech. An electronic signature arguably includes the following, if intended to be a signing:<sup>3</sup>

- One's voice on an answering machine.
- One's name as part of an e-mail message, such as where a person types his/her name as part of an email purchase order, for himself or an employer.
- One's signature imbedded as an image in a document.<sup>4</sup>
- The firm name or letterhead on a facsimile, or the information printed across the top of the page that indicates the machine from which the facsimile was sent.

---

<sup>1</sup> Memo from Mary Beth Parisi to the OJC Technology Committee requesting help on electronic signature issues. In the memo Ms. Parisi stated the following:

We recommend before any official meetings are convened on this topic, a draft document should be pulled together that lists any new or additional functionality requirements, security requirements (authentication, non-repudiation, etc.), policy requirements and oversight recommendations (if any).

<sup>2</sup> R.C. 1306.01(H); Sup. R. 27(A)(2) incorporates R.C. 1306.01(H); 15 U.S.C. 7006(5), Electronic Signatures in Global and National Commerce (E-Sign) Act; & Section 2(8), Uniform Electronic Transactions Act (1999), National Conference of Commissioners on Uniform State Laws, 211 E. Ontario Street, Suite 1300, Chicago, Illinois 60611, <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.pdf>.

<sup>3</sup> See Comment 7 to section 2, and Comments 1, 3, 4 & 5 to section 9, Uniform Electronic Transactions Act (1999), National Conference of Commissioners on Uniform State Laws, 211 E. Ontario Street, Suite 1300, Chicago, Illinois 60611, <http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.pdf>.

<sup>4</sup> In some states that employ electronic filing, users sign a paper document, scan it, and e-file it. Users are required to retain the signed paper. Examples include California, Pennsylvania, & Texas.

- A person's computer, programmed to order goods upon receipt of inventory information within particular parameters, where the computer issues a purchase order that includes the person's name, or other identifying information, as part of the order.
- The standard webpage click through process, requiring, *e.g.*, a login and "I agree."
- A digital signature requiring PKI or other encryption technology.

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.”<sup>5</sup> A digital signature is considered a very secure form of electronic signature. It is also the most costly.

### **Permitting Courts to Use Electronic Signatures**

Current court rules allow for the filing of documents with courts electronically,<sup>6</sup> but do not allow courts to sign documents electronically. The committee has considered this issue and recommends that it be solved by providing a definition of signature in court rules that includes an electronic signature, as follows:

For all and any purposes under these rules, any signature or signing by any person includes an electronic signature, meaning 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 use of electronic signatures must be approved in advance by local court rule adopted in conformity with Sup. R. 27.

This definition would be incorporated into the following rules to be adopted or amended, as indicated:

Civil Rule 67: Signature (New Rule)

Criminal Rule 77: Signature (New Rule)

Juvenile Rule 5: Signature (New Rule)

Appellate Rule 31: Signature (New Rule)

Traffic Rule: 2. Definitions, (L) Signature (Addition to existing Rule)

Superintendence Rule 28: Signature (New Rule)

The committee recommends the suggested rule include the requirement that, “The use of electronic signatures must be approved in advance by local court rule adopted in conformity with

---

<sup>5</sup> 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>.

<sup>6</sup> See, *e.g.*, Civ.R. 5(E) and Crim.R. 12(B).

Sup. R. 27.” While Sup. R. 27 provides local rules on technology must be approved to ensure certain standards are met, it does not require a local rule be enacted. Absent a requirement that a local rule first be adopted, there is nothing to stop a court from using electronic signatures without adoption of a local rule or meeting minimum standards.

Perhaps Sup. R. 5(B) needs to be changed to require local courts to adopt rules governing electronic filing, electronic signatures and related matters. In the alternative, the same thing could be accomplished by the Supreme Court Advisory Committee on Technology and the Courts promulgating regulations under the authority of Sup. R. 27(B)(1).

### **Electronic Signature Security**

Three security issues are important: 1) ensuring the act of signing is genuine, 2) preserving the integrity of the document once it is signed, and 3) the acceptance of the document for what it is intended to be.

#### 1) Ensuring the Act of Signing is Genuine

Persons relying on an electronically signed document must be able to trust it has been authentically signed. The committee believes the act of electronically signing a document should require an act only the signer can perform, as is the case with a conventional signature. The committee recommends, at a minimum, the act of electronically signing a document be a separately authorized act requiring at least a personal identification number (PIN) or a username and password. Merely logging onto a computer or a network should not be sufficient.

A number of alternatives, of different costs<sup>7</sup> and complexities, would meet this minimum standard.

**Username/Password:** Requiring a unique PIN or username and password is inexpensive and relatively easy to integrate into existing processes.<sup>8</sup> The total cost may be as low as \$1 per registered user. Third party registration and validation of username/password information can cost up to \$75 per user.

**Smart Cards:** A credit card like device is used to authorize the signing of a document. The cost is approximately \$125 per card/reader. The cost of integrating smart cards into a process is higher than username/password/PIN systems, since the cards must be physically distributed and processes surrounding authentication may be more complicated.

---

<sup>7</sup> This cost information is very rough and should only be used to compare the options. Accurate cost information depends on a variety of factors, including what systems are already in place, features desired and competitive bidding.

<sup>8</sup> Username and password constitute a signature in Delaware, Montgomery County, PA, New York, US District Courts, Virginia, & Washington.

**Biometric Devices:** These devices read unique biometric information from a person, such as a fingerprint, to identify and authenticate an individual or an act. The devices cost from \$30 to \$150. If the process involves collecting and maintaining a registry of biometric information for reference, the devices can be more complex than smart cards.

**Signature Pads:** These are the pads we all have used in department stores to authorize a credit card charge. They cost \$100-600, depending on features. If the system collects reference signatures for comparison and authentication, the process can be complex.

**PKI Encryption (Digital Signature):** PKI technology provides a very secure method of signing documents and ensuring their integrity. Persons receiving the document can check through an independent source the authenticity of the signature and whether the document has been altered after it has been signed.<sup>9</sup> The cost to use PKI technology is \$75-125 per user, per year.<sup>10</sup>

**An Example:** The Cuyahoga County Common Pleas Court currently utilizes electronic signatures consistent with our recommendation. The judge must first sign onto his/her computer with a username and password, and then sign into case management software with another username and password. The case management system contains a template for journal entries. When the judge is ready to sign an entry, he or she is asked for a PIN number that has been assigned to the judge.<sup>11</sup> Entering the PIN number constitutes a separately authorized act that electronically signs the entry. An electronic image<sup>12</sup> of the judge's signature is then placed in the document.<sup>13</sup>

## 2) Preserving the Integrity of the Document Once it is Signed

Once a document is electronically signed, it also must be protected from change for it to be considered reliable. "Standards for Electronic Filing Processes" are currently being formulated by the Electronic Filing Work Group of the Standards Subcommittee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts. These standards include the measures necessary to preserve the integrity of electronically signed documents and are an essential accompaniment to electronic signature rules and standards.

For example, the standards being considered by the Electronic Filing Work Group include the following:

---

<sup>9</sup> Kansas law virtually requires PKI technology.

<sup>10</sup> Software programs such as MS Word XP and Adobe Acrobat Professional 6.0 include self-certification features that allow users to digitally sign a document created within the program. Unless there is third-party verification of the signature, however, the validity of the signature cannot be determined independently of the document. Once the document is self-certified, however, changes to the document can be detected.

<sup>11</sup> If necessary, multiple documents can be signed without repeated PIN entries.

<sup>12</sup> The image is a tiff image, similar to a photo of the signature. TIFF is an acronym for Tagged Image File Format.

<sup>13</sup> The tiff image is created from a signature pad. Each judge enters his or her signature once and then the signature file is stored in the system.

**[Policy] Standard 1.1H Integrity of Transmitted and Filed Documents and Data:** Courts will electronically maintain the integrity of transmitted documents and data, and documents and data contained in official court files.

. . . [C]ourts and private sector service providers supporting courts shall incorporate an electronic means for securing the integrity of all electronically filed documents. A simple “byte count” of a document will not suffice, however using an algorithm, software, or security permissions would ensure integrity of all official court records.

**Functional Standards:**

**Subfunction 3.6.3** With an electronic court record, the judicial officer official decision and action is recorded only within the electronic record. These standards do not explicitly call for a different method of authentication for judges than would be required of other filers. However, courts are cautioned that the burden is significant to provide strong safeguards to ensure that only judicial officers can authorize orders and official judicial actions, that any modifications are properly audited and tracked, and that both the public and litigants are confident of the technical integrity of judicial actions recorded electronically.

In the absence of statewide standards, electronically signed documents should be stored in a secure environment. This means access to electronic documents should be controlled and measures should be taken to ensure electronic documents cannot be altered or destroyed. Existing computer networks and systems in most organizations have features that can provide adequate protection for electronically signed documents. These features include restricted access and archival routines.

**An Example:** The Cuyahoga County Common Pleas Court utilizes a controlled and protected system. Once the judge signs an entry, the information is merged into a Word document. The Word document is protected by a “hash” algorithm to prevent unauthorized changes. Once every hour Word documents are printed to an image file and the Word documents are deleted. Once imaged, the documents are maintained in a secure case management system under the jurisdiction of the clerk.

3) Document Acceptance

As with any new process, a certain amount of public and professional education will be necessary for acceptance of electronically signed documents. The measures ensuring the integrity of electronic signatures and documents will have to be explained, as will ways to check the accuracy of documents. The availability of online resources will help greatly.

In some documents that are electronically signed, an image of the signature will be placed in the document and it will appear to have been signed. However, electronically signed documents do not necessarily have to display a signature or any indication that they have been

signed electronically. Many courts find it sufficient, for example, to allow the filing of documents through a username and password process without any signature being placed on the document.

Accordingly, it is suggested that an electronically signed document carry some notation that it has been electronically signed. For example, the following could be required, “Electronically signed by Judge Jones.” This would prompt confirmation of the signature if there is any doubt about its authenticity.

### **Other Issues**

The committee raised but did not address the following issues:

What about oath requirements and electronic signatures? Can electronic signatures be used where there is a requirement that a person appear before a judge?<sup>14</sup>

Can a document be electronically notarized?<sup>15</sup>

### **Conclusion**

This report has endeavored to provide helpful information on electronic signatures and the standards to be considered in the use of electronic signatures by courts. The report also suggests needed rule changes to allow courts to use electronic signatures. The Technology Committee hopes this report has been responsive to the information requested by the Supreme Court of Ohio Advisory Committee on Technology & the Courts. The Technology Committee is willing to continue to assist with electronic signature and other technology issues.

### **Acknowledgements**

This report is the result of the joint efforts of the members of the Court Technology Committee, co-chaired by Judges Guckenberger and Zachman. While Judge Guckenberger authored the report, Judge Zachman was primarily responsible for the suggested rule changes. Ulf Nilsson, OJC staff, was invaluable in helping to edit and rewrite the report. Judge Hoover helped collect information from other states and Judge Wise provided critical analysis. Judges Bessey and Nuzum are members of the committee, have participated in a number of our meetings concerning electronic signatures and provided valuable guidance.

---

<sup>14</sup> For example, Crim.R. 41(C) provides, “A warrant shall issue under this rule only on an affidavit or affidavits sworn to before a judge . . . .”

<sup>15</sup> Apparently the answer is yes, see The National Notary Association’s web site at <http://www.nationalnotary.org/about/index.cfm?Text=aboutPR&newsID=309> and The Model Notary Act, Article III, Electronic Notary. <http://www.nationalnotary.org/library/index.cfm?text=actionModel>.