IN THE

SUPREME COURT OF ILLINOIS

In re: Electronic Signature Standards	)	M.R. 18368

ORDER

Effective immediately, in the exercise of the Court's general administrative and supervisory authority over all courts, and consistent with the Electronic Commerce Security Act (5 ILCS 175/1-101 et seq.), the Supreme Court of Illinois hereby approves the attached "Electronic Signature Standards" to ensure that courts in Illinois seeking to utilize electronic signatures in their jurisdiction do so according to these standards. The Administrative Director of the Illinois Courts has authority to amend the "Electronic Signature Standards" as is necessary and appropriate.

FURTHER, IT IS ORDERED that any court currently operating an electronic signature program under an approved pilot program or pursuant to the Electronic Filing Standards and Principles may continue operations as authorized and shall make diligent efforts to conform with the "Electronic Signature Standards" to the extent that such standards conflict with current operations under an existing electronic signature program.

Order Entered by the Court.

SUPREME COURT OF ILLINOIS

ELECTRONIC SIGNATURE STANDARDS

1. **Purpose:**
   The purpose of this standard is to guide courts in the use and retention of electronic records which are authenticated using electronic and digital signatures and to aid in the development of procedures around use. This standard includes the adoption of Illinois' Electronic Commerce Security Act (5 ILCS 175/1 et seq.), effective July 1, 1999 which promotes the use of electronically signed documents and e-Commerce.

2. **Directives for the use of Electronic and Digital Signatures**
   A court's electronic and digital signature software applications must provide secure signature application methods. Users and those officials' assigned electronic signatures must be given the ability to test the application of their signatures using the secure method in place. Verification mechanisms and retention procedures must be tested to provide verification of the document to the signature that is applied and its ability to be retained in a stand-alone manner.

   The court must determine when an electronic or digital signature is required. For example, determination is necessary if a filer is allowed to use an electronic signature to submit an electronically filed document or if the court requires a digital signature. Similarly, the court must determine if a judge or court official is required to digitally sign a document or if an electronic signature is allowed. Unless a court has deemed the electronic court record to be the official record, a process for digitizing wet-signature process documents must be available.

   The electronic and digital signatures implemented by a court must comply with the practices defined in the Electronic Commerce and Security Act.

3. **Definitions**

   (a) "Conventional Filing" means a physical, non-electronic presentation of a document to the clerk for filing in a judicial proceeding. It includes documents filed by facsimile or by e-mail.

   (b) "Court User" means a person employed in any capacity by a judicial or non-judicial member of the judicial branch of Illinois who has been authorized by law, rule or custom to apply his or her electronic signature to a document for filing in a judicial proceeding in accordance with this policy.

(c) **"Electronic Record or Document"** means a record or document generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another.

(d) **"Electronic Signature"** As defined in the Electronic Commerce and Security Act (5 ILCS 175/5-105).

(e) **"Digital Signature"** As defined in the Electronic Commerce and Security Act (5 ILCS 175/5-105

(f) **"Legal User"** means a person who participates in the judicial process, such as an attorney, a self-represented litigant, or other person external to the judicial branch, who in accordance with law and practice may apply his or her electronic or digital signature through an external application that is not directly controlled by this policy.

(g) **"Electronically Signed Document"** means a document containing an electronic or digital signature.

(h) **"Official Court Record"** is any document, information or other item that is collected, received, or maintained by a clerk of the circuit court in connection with a judicial proceeding and is maintained pursuant to the Supreme Court's *General Administrative Order on Recordkeeping in the Circuit Courts.*

4. Minimum Technical Requirements

(a) System Security

The system and methods used shall ensure that a complete, reliable backup of each electronically signed document is retained in the format in which the signed document was generated, sent or received, or in a format that accurately represents the information contained in the document when it was signed. The clerk shall have a disaster recovery plan that includes procedures to restore operations within a reasonable period of time after any interruption in service.

(b) Authentication

The system and methods shall ensure user authentication through the use of industry standard technologies, which includes encrypting passwords, minimum password requirements, and minimum network security protocols. For example, users may be authenticated via three general methods, based upon information the user knows (password, pin), something the user has (security token, fob, or ID card), and something the user is (fingerprint, biometrics, signature). The generation of digital signatures is to include key pairs and be issued by a certificate authority as defined in the Electronic Commerce and Security Act.

Each court shall develop a procedure for the assignment of digital signatures to officials which ensures verification of each person being assigned a digital signature and allows for the encrypted exchange of digital signatures across public networks using, at minimum, AES 256-bit encryption. A court's procedures shall ensure a protocol for the revocation of authority to electronically or digitally sign documents. Each signature shall use secure and encrypted passwords, or other technology of the same or greater strength, to authenticate the use of the electronic signature.

i. The storage, retention and exchange of electronic signature images and digital signatures must be treated as confidential and protected by internal system security measures. The signing solution provider should keep a complete audit trail of access and assignment of signatures.

ii. If external exchanges over public networks of signature images are used, a secure TLS/SSL connection must be used. All signature images being externally exchanged must be minimally encrypted between the web-browser and web-server using AES 256-bit encryption or storage. The decryption keys shall not be available to any user or operator and only the owner shall have the ability to decrypt and then apply the signature.

(c) Verification Process / Authenticity of Electronically Signed Documents

In "e-record" courts which have eliminated the paper file, the court must provide a process for verifying the integrity and authenticity of an electronically signed document, that it has not been changed or altered, either intentionally or unintentionally, after the document was incorporated into the official court record. Successful transference of electronic documents from one destination to another must not affect the authenticity of, or the ability to authenticate, an electronically signed document.

(d) Durability of the Electronic Signature

The systems and methods employed cannot permit the signature verification process to erode over time. Acts of viewing, printing, copying, downloading or transmitting an electronically signed document must not affect the integrity of the document or of the signature. The clerk and the case management system vendor must assure that the format of the signature is constantly maintained in the most current and accessible format.

(e) Accessibility of Verification Process

Nothing in the electronic or digital signature process shall restrict or inhibit any person from applying the verification process against an electronically signed document. When required as noted above, the verification process must be available and accessible to any person, at any time, and must not require interaction with

specialized software or any specialized software environment to perform the verification.

5. General Provisions

(a) Electronically filed documents that require an original signature when conventionally filed shall bear a facsimile or typographical signature of the attorney or self-represented party authorizing such filing, (e.g. "/s/ Adam Attorney"), and shall be deemed to have been signed in-person by the individual identified.

(b) Electronically filed documents entered under a court user's logon ID and password shall be deemed entered by the holder of that logon ID.

(c) Electronically filed documents through a legal user's logon ID is deemed to have been personally signed by the holder of that logon ID.

(d) Electronically filed documents containing signatures of a third party shall bear that person's facsimile or typographical signature. The attorney or party electronically filing any document which includes the signature of a person neither a party to the case nor registered for electronic filing must retain the original document for one year after the date of final judgment in the proceeding, and shall make the original available for inspection by the court and other parties upon five business days notice.

(e) Where a Clerk of the Circuit Court is required to endorse a document, the electronic or digital representation of the clerk's name shall be deemed to be the clerk's signature on an electronic document.

(f) An electronic or digital signature is considered to be the original signature upon the court record or document for all purposes allowed under Supreme Court Rule or statute.

Statutes: 5 ILCS 175/1 *et seq.* – Electronic Commerce Security Act.
http://www.ilga.gov/legislation/ilcs5.asp?ActID=89&ChapterID=2