



Understanding Electronic Signatures

A Discussion of Electronic Signatures, the E-Sign Act, and the Admissibility of Electronic Signatures in the Law

Presented by RealLegal, the Applications Division of Law.com

"Our Age of Anxiety is, in great part, the result of trying to do today's jobs with yesterday's tools." - Marshall McLuhan¹

The introduction of technology into the legal world has created the need to develop a body of law to promote its growth. Important to this growth is the concept of open standards, allowing all actors to compete on the same plane. Specifically, the standards relating to business created by a computer and transacted over fiber optic connections are expected to remain neutral, allowing time to choose the most reliable and efficient system. As with the dawn of any new era of technology, negotiating legislation through the considerations each actor deems important creates an environment of rapidly changing standards.

The purpose of this document is to assist the reader in understanding both electronic and digital signatures and how RealLegal's technology fits within these

¹ Paul Levinson, "Digital McLuhan: A Guide to the Information Millennium."

definitions. In addition, this paper will offer a detailed explanation regarding the usage and admissibility of electronic signatures in the law, with specific attention to how the electronic signature technology created by RealLegal complies with the rules for admissibility.

Electronic Signatures vs. Digital Signatures

It is important to recognize the difference between “electronic signatures” and “digital signatures.” A clear understanding of the different definitions is important in both the legal and technological arena. In fact, a number of state statutes provide specific definitions for each term.² What follows is a brief definition of each expression, an analysis of their differences, an explanation as to why and how realLegal’s electronic transcript signature service falls within the “digital signature” spectrum, and a discussion of how issues of security are addressed by the varying technologies.

Electronic Signature

The phrase “electronic signature” is the umbrella term to describe any type of digital marking used by a party to be bound or to authenticate a record.³ It is a very broad term, and could include markings as diverse as digitized images of paper signatures, typed notations such as “/s/ John Smith” at the bottom of an electronic document, or even addressing notations, such as electronic mail headers or footers.⁴ It is considered the digital equivalent of the traditional “X” used to sign a contract or document.

² See www.mbc.com

³ Enterprise Solutions: Legal Requirements. (See <http://www.cic.com/enterprise/legal/>).

⁴ Digital Signature Guidelines Tutorial, American bar Association, (See <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>).

“Electronic signature” implementations may offer no greater security than that of a password. Further, “electronic signatures” have no way of verifying whether a document has been altered since the time that it was signed. In other words, “electronic signature” technology does not provide any kind of signer or document authentication.

Digital Signature

“Digital signatures” are a specific type of “electronic signature.” A “digital signature” is legally more acceptable than other types of “electronic signatures,” as it offers both signer and document authentication. Signer authentication is the capability to identify the person who digitally signed the document. Document authentication ensures that the document or transaction (or the signature) cannot be easily altered.⁵ The process of creating a digital signature and verifying it accomplishes the essential effects that a handwritten signature does today for many legal purposes⁶:

- **Signer authentication:** If a public and private key is associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key, such as by divulging it or losing the media or device in which it is contained.
- **Message authentication:** The digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals any tampering, since the comparison of the hash results (one made at signing and the other made at verifying) shows whether the message is the same as when signed.
- **Non-Repudiation:** Creating a digital signature requires the signer to use the signer’s private key. This act can alert the signer to the fact that they are consummating a transaction with legal consequences.
- **Integrity:** The process of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer’s. Compared to paper methods, such as checking signature cards, digital signatures yield a high degree of assurance without adding greatly to the resources required for processing.

⁵ *Id.*

⁶ *Id.*

RealLegal's Electronic Signature Service

A RealLegal electronic signature embodies a triumvirate of the court reporter's identity, industry-leading digital notarization, and electronic file fingerprinting which combine to provide a unique electronic signature for each transcript.⁷ This process is similar to the "digital signature" process in style and manner. As a result, there is a strong presumption of both secure and reliable results. The following is a detailed explanation outlining exactly how this process occurs:

- **First**, the 'Sign' button is pressed for a selected transcript in RealLegal's E-Transcript Manager. This results in the creation of a unique document fingerprint. After this point, any tampering with the original file will result in fingerprint invalidation.
- **Second**, E-Transcript Manager prompts the reporter for confidential username, password, and delegate information, and optionally the name of the intended transcript recipient. An Internet connection is established and the reporter is authenticated with the National Digital Transcript Certification Authority (NDTCA) database, the standards body for electronic transcript signatures.
- **Third**, RealLegal creates a master fingerprint by combining the transcript fingerprint with the court reporter's authenticated system identity. A digital notarization process occurs by including a witnessed timestamp of the master fingerprint to ensure that the signing event is "widely witnessed" as taking place at that moment in time, on that specific information.
- **Fourth**, the time-stamped master fingerprint, reporter identification information, and attorney details (if any) are sent to the secure RealLegal signature server. Combining the time-stamped master fingerprint, recipient name, transcript title, transcript tracking number, and the date and time creates an encrypted electronic bundle.
- **Fifth**, the bundle is stored in the RealLegal signature database that is returned as an electronic transcript signature certificate and attached to the original E-Transcript.

⁷ See www.realLegal.com for more information.

Security and RealLegal's Technology

Security is always a concern with any electronic signature technology. A digital signature is considered superior to a handwritten signature in that it attests to the contents of a message as well as to the identity of the signer. As long as a secure hash function [an algorithm that creates a digital representation or "fingerprint"] is used, there is almost no chance of taking someone's signature from one document and attaching it to another, or of altering a signed message in any way. The slightest change in a signed document will cause the signature verification process to fail, alerting the recipient to the alteration.⁸

This methodology is utilized in RealLegal's signature technology. Communication with the RealLegal Electronic Transcript Signature service is conducted through fully redundant, secure Internet servers. Furthermore, the tool used to verify the electronic transcript signature is contained in a publicly available Class 3 Verisign certificate, which provides third-party assurance for additional protection.

Sending the transcript is secure, as E-Transcript uses digital fingerprints to represent the transcript documents. In fact, the actual transcript never leaves the court reporter's desktop. Verifying the transcript by validating the signature certificate is done through E-Transcript. The RealLegal electronic transcript signature database will compare the fingerprint, the timestamp and the reporter's identity within the signature to ensure an exact match, thus preventing alteration of the document or signature.

⁸ Pam Roberts, "Electronic/Digital Signature Position Paper." (See <http://www.state.tn.us/finance/oir/prd/edsignat.html>)

Are Electronic Signatures Valid?

The validity of electronic signatures in the legal arena is best understood by understanding the technology as it is defined and interpreted in three specific areas: the legislative history of electronic signatures (legislative history refers to the documentation that describes the intent of lawmakers when creating electronic signature rules and legislation); state and federal solutions created by the courts to address electronic signatures and technology; and the precedent set by the trial court judge in the case management order for a case.

LEGISLATIVE HISTORY

Each individual state in the U.S. has considered the ramifications of electronic commerce and electronic signatures, and has either passed or is introducing electronic signature legislation. Although each state is in agreement regarding the need to create laws that give an electronic signature the same validity as the traditional pen and ink signature, the states are conflicted in the type of technology that they choose to embrace. Most States have adopted requirements that are either described as the Public Key / Private Key, Asymmetric Cryptology, or the Five-Point Definition technologies.⁹ Early efforts were made by certain states to lend security to electronic commercial transactions. Utah, California and Illinois were among the front-runners in providing state solutions. The first piece of digital signature legislation was the Utah Digital Signature Act, passed in 1995.¹⁰ The Act attached a presumption of validity to digital signatures. The meaning of "digital signature" was very limited, as it only applied to signatures created using a

⁹ For Specific State information see the McBride, Baker and Coles website at <http://www.mbc.com/>.

¹⁰ www.le.state.ut.us/~code/title46/46_03.htm.

specific technology and not to electronic signatures generally.¹¹ In California, digital signature legislation known as Assembly Bill 1577 was passed in 1995.¹² The legislation only applied to transactions conducted with public entities, but was expansive in that it did not prescribe the use of a certain type of technology.¹³ The Illinois Electronic Commerce Security Act took effect in 1998.¹⁴ This legislation distinguished electronic signatures of varying degrees of security and correspondingly applied presumptions of validity at each level.¹⁵

No matter the type of technology embraced, the laws passed by the different states recognized the growing dependency on electronic transactions. Merely identifying the need to fully utilize the potential of the Internet was an important first step in establishing the framework for future Federal legislation.

However, the fact that each state independently formulated requirements for electronic signatures created the need for standardization. Subsequent legislation suggested by the National Conference of Commissioners on Uniform State Laws and enacted by the United States Congress changed the scope, applicability and function of these individual state laws.

Emerging Common Ground: Enactment of the Uniform Electronic Transactions Act

The purpose of the National Conference of Commissioners on Uniform State Laws in fashioning the Uniform Electronic Transactions Act (UETA) was to furnish

¹¹ Karl D. Belgum and Thelen Reid & Priest, LLP, *Legal Issues in Contracting on the Internet* (visited September 13, 2000) <http://library.findlaw.com/scripts/getfile.pl?file=/thelen/trp000045.html>.

¹² www.mbc.com/ecommerce/legis/california.html#CA_REGS

¹³ Karl D. Belgum and Thelen Reid & Priest, LLP, *Legal Issues in Contracting on the Internet* (visited September 13, 2000) <http://library.findlaw.com/scripts/getfile.pl?file=/thelen/trp000045.html>

¹⁴ www.mbc.com/ecommerce/legis/illinois.html#IL_ECSCA.

¹⁵ Karl D. Belgum and Thelen Reid & Priest, LLP, *Legal Issues in Contracting on the Internet* (visited September 13, 2000) <http://library.findlaw.com/scripts/getfile.pl?file=/thelen/trp000045.html>.

States with uniform rules governing electronic commerce transactions. The primary objective of UETA is to provide electronic transactions with the same legal effect as transactions memorialized on paper without changing any applicable substantive laws.¹⁶

UETA sets forth three fundamental goals:

1. A record or signature will not be denied legal effect and enforceability solely because an electronic record was used in its formation
2. An electronic record will satisfy any law that requires a writing.
3. Any signature requirement in the law will be met if there is an electronic signature.¹⁷

The drafters sought to eliminate barriers to electronic commerce with the adoption of the standard-free UETA. Requirements for electronic records, transactions, and signatures are virtually the same as the requirements for the paper counterparts. An important consideration (one which is concurrent with business dealings in general) is that both parties must assent to conducting business electronically. Basic rules of contract law (i.e. desire to contract, offer and acceptance, etc.) continue to apply as they have applied traditionally. Electronic signatures are not required nor are parties prohibited from transacting business by more traditional means.¹⁸

Federal Preemption: Enactment of the Electronic Signatures in National and Global Commerce Act (E-Sign)

UETA was in the process of being adopted by many states when on June 30, 2000, President Clinton signed the Electronic Signatures in National and Global

¹⁶ National Conference of Commissioners on Uniform State Laws – Introductions and Adoptions of Uniform acts http://www.nccusl.org/uniformact_summaries/uniformacts-s-ueta.htm

¹⁷ *Id.*

¹⁸ *Id.*

Commerce Act (E-Sign). The enactment of E-Sign had broad reaching ramifications, as it preempted state laws governing electronic transaction requirements. As required by E-Sign, each state must operate under neutral standards when transacting business electronically. E-Sign recognizes that UETA, when enacted in its pure form, provides this neutral standard. E-Sign prohibits a jurisdiction from rejecting an electronic record on the basis of conflicting requirements between two jurisdictions.

An Important Exclusion: The Relationship of E-Sign and UETA to Court Documents

The drafters of E-Sign excluded certain types of electronic transactions from coverage. Important to the legal industry is the exclusion described in the “Specific Exceptions,” Section 103 of the Federal Act:

- (b) *ADDITIONAL EXCEPTIONS. – The provisions of section 101 shall not apply to-*
 - (1) *Court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings.*¹⁹

Congress made specific overtures to exclude court documents from the Act, affording each court the choice to formulate and adopt their own electronic signature standard. 20

COURT SOLUTIONS

Both E-Sign and UETA share a common purpose: to ease the way for electronic commerce by giving legal validity to electronic transactions. The current trend towards electronic filing (e-filing) that is occurring within both the state and federal court systems provides a clear example of the acceptance of electronic technology and signatures.

With the advent of e-filing, courts needed to address the issue of the false filing or signing of pleadings and documents electronically. In the traditional paper method of

¹⁹ Electronic Signatures in Global and National Commerce Act § 103(b)(1).

filing, a witness or notary may be required to validate a person's identity or signature. However, verification using that method is not a deterrent for someone who chooses to misrepresent his/her identity. Very seldom is the identity of the signer or the signature questioned or even noticed in non-verified paper filings. The issues of identity and signature verification have been addressed by all of the current e-filing projects across the country. Most systems require the attorney to submit an application to utilize an e-filing site, and upon approval, a user name and password is provided to the applicant. The enactment of local court rules or an adaptation of Rule 11 of the Rules of Civil Procedure has largely regulated the appropriate submission and signing of documents.²¹ The courts have been satisfied with this method of identity and signature verification.²² It should be noted that this method of signing and verification is significantly less detailed or secure than the current method utilized by RealLegal's Electronic Signature Technology²³. In Federal Court, rules mandate that every brief, motion, or other documents are signed by the attorney of record. In response to the growing trend toward electronic signatures in Federal Court, the 10th Circuit Court of Appeals adopted Rule 46.5, which provides that "an electronic signature is an original signature."²⁴

CASE MANAGEMENT

Finally, one can look to individual trial judges to provide guidelines regarding the validity of electronic signatures in the courtroom. In order to combat inefficiencies in the paper process, judges often issue case management orders to allow for the use of

²⁰ Patricia Brumfield Fry, "A Preliminary Analysis of Federal and State Electronic Commerce Laws" (see <http://www.uetaonline.com/docs/pfry700.html>).

²¹ See, for examples, Colorado Local Rule 121, Section 1-26; C.R.C.P. Rule 11.

²² Premiere issue of the E-Filing Report: November/December 2000; Vol. 1, No. 1.

²³ For a more detailed look at e-filing as it pertains to the state and federal courts, more information can be found at www.courts.net/efiling.htm

electronic filing in a particular case or project. Such a case management order establishes the conditions and requirements for filing documents electronically and becomes the "law of the case." Currently, many electronic filing projects are controlled by the case management order signed by the Judge, authorizing the use of electronic filing and specifying the rules and technology that will apply to each project. Electronic signature signing of documents and pleadings are usually specified in each management order, and follow traditional e-filing guidelines.

Conclusion

It is not possible to cover every aspect of electronic signatures in a short summary. This paper merely highlights some essential aspects of the different types of technology, the changes in both state and national legislation, and the acceptance of electronic signatures in the court setting. More information, including the status of state and federal initiatives on electronic signatures, may be found at RealLegal's website, <http://www.reallegal.com/esig.asp>. The electronic signature technology utilized by RealLegal is secure, cost efficient and easy to use, and is in compliance with E-Sign, UETA and current court rules and procedures. In summary, it is important to stress that the usage of electronic signatures in the law is continuing to expand and is being afforded the same legal effect as the traditional signatures that are memorialized on paper.