

Electronic Signatures: What are they anyhow?

Houston Putnam Lowry, Esq.

Brown & Welsh, P.C.¹

May 8, 2001 – CT Bar Association Young Lawyers

- I. What is an Electronic Signature?
 - A. General rule from the Uniform Commercial Code §1-201(39) is: "signed" includes any symbol executed or adopted by a party with present intention to authenticate a writing. A writing is further defined in §1-201(46) as including printing, typewriting or any other intentional reduction to tangible form.
 - B. Therefore, the definition of an electronic signature is rather broad.
 - C. The key issue is intent, which must be determined from the entire circumstances surrounding the signature. A signature performs one or more of the following functions, depending on the context:
 1. Identify a person.
 2. To provide certainty as to the personal involvement of that person in the act of signing.
 3. To associate a person with the contents of a document (such as agreeing to the terms of the document, etc.).
 - D. The current trend is towards technology neutrality in Electronic Signatures. In determining what is a reasonable signature under the circumstances, . The court should consider the following factors when evaluating any signature, (which come from the 1996 UNCITRAL Model Law commentary):
 1. the sophistication of the equipment used by each of the parties;
 2. the nature of their trade activity;
 3. the frequency at which commercial transactions take place between the parties;
 4. the kind and size of the transaction;
 5. the function of signature requirements in a given statutory and regulatory environment;
 6. the capability of communication systems;
 7. compliance with authentication procedures set forth by intermediaries;

¹ Meriden Executive Park, 530 Preston Avenue, Second Floor, Meriden, Connecticut; Telephone (203) 235-1651; Fax: (203) 235-9600; <http://www.BrownWelsh.com>; email: HPLowry@BrownWelsh.com.

8. the range of authentication procedures made available by any intermediary;
 9. compliance with trade customs and practice;
 10. the existence of insurance coverage mechanisms against unauthorized messages;
 11. the importance and the value of the information contained in the data message;
 12. the availability of alternative methods of identification and the cost of implementation;
 13. the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and
 14. any other relevant factor.
- E. For example, a four digit personal identification number is a signature (although you may never have thought about this).

II. What is a Digital Signature?

- A. Digital Signatures are a subset of Electronic Signatures. While all Digital Signatures are Electronic Signatures, not all Electronic Signatures are Digital Signatures.
- B. Public key cryptography (sometimes called asymmetrical key cryptography) is used to create Digital Signatures. The process is mathematically similar to the process of encryption.
1. The public key can be freely distributed and is used to test the validity of the signature.
 2. The private key must be kept secret and is used to make the signature.
 3. The reliability of the signature is determined, in part, by the length of the key. Most browsers use 56 bit² or 128 bit keys.
- C. The process is based upon the mathematical fact is presently impossible to determine the very large prime numbers that make up a single large product (the factoring problem). If this mathematical puzzle is solved, the present day Digital Signature will be about as effective as typing your name in ASCII. The process depends on the implementation of this “one way” mathematical function.

² The length of the key originally set for the Data Encryption Standard (DES).

- D. While the mathematical process is the same, different software vendors implement it differently. The implementation may affect the likelihood an unsophisticated party will accept the signature.
 - 1. Pretty Good Privacy (see attached examples).
 - 2. Adobe Acrobat 5.0 (see attached examples).
- E. The important feature is the length of the key.
 - 1. For a long time, 56 bit keys were the largest that could be handled by software that was exported (otherwise the software was a munition). Keys of this length were first used with the Data Encryption standard established by the United States government.
 - 2. Browsers came in “strong” encryption domestic versions using 128 bit keys. They could not be exported.
 - 3. I use a 4,096 bit key with Pretty Good Privacy, which is about 8,000 time harder to break than a 128 bit key.³

III. Why do we worry about it? The forgery and privacy concerns.

- A. What are electronic signatures used for?
 - 1. Sending email.
 - 2. Connecting/authenticating with servers.
 - 3. Buying and selling goods.
 - 4. Buying and selling stocks.
 - 5. Authorizing electronic transfers of money.
- B. Examples where the system failed:
 - A. January 9, 2001 CNN report on Egghead.com computer penetration.
 - B. December 15, 2000 CNN report on copying of hospital patient files.
 - C. December 13, 2001 CNN report on a hacker stealing 55,000 credit card numbers.
 - D. November 15, 2000 CNN report of release of mortgage information.
 - E. November 9, 2000 CNN report of release of bank information.

³ But remember computing power doubles every 18 months, as a general rule.