

# Digital Signatures and Authentication

## Definition

Historically, the legal concept of a signature is very broad and can be defined as any mark that is made with the intention of authenticating a marked document or record. Signatures serve to give evidence or authenticate a record by identifying the signer with the signed record. In some contexts, a signature records the signer's approval or authorization of the signed record and the signer's intention to give it legal effect. A signature also has some ceremonial significance, and can impart a sense of clarity and finality to a record or transaction. For purposes of evidence, a signature must provide for: (1) Signer authentication: i.e., the signature must indicate who signed a record and should be difficult for another person to (re)produce without authorization, and (2) Record authentication: i.e., the signature should identify what is signed, making it difficult or impractical to falsify without detection. Formal requirements for legal transactions, including the need for signatures, vary in different legal settings. In some settings, these requirements still involve documenting a transaction on paper with penned signatures. (Such requirements remain codified in specific laws, rules and regulations.) However, traditional methods of authentication are undergoing major changes today. For many reasons, computer-based transactions and information can achieve far more than their paper counterparts, including the level of security and authentication possible. Digital signatures are such an example. (American Bar Association, Digital Signature Guidelines, <http://www.abanet.org>.)

## Standards

For purposes of this discussion, an examination of the issues and standards involved with electronic representation of traditional authentication, such as an electronic image of a handwritten signature, has not been included.

## Digital Signature Standard (DSS)

Digital signatures represent a specific technology used to authenticate electronic messages, records, or transactions by confirming the identity of the signing/sending party and the integrity of the data/information received. Digital signatures are created and verified by cryptography which is the process of applying a mathematical algorithm to transform information into seemingly unintelligible forms and back again. Digital signatures use "public key cryptography," which employs an algorithm that uses two different but mathematically related keys -- one "private key" for creating and encrypting a digital signature; and another "public key" for verifying the digital signature and returning the information to its original form. Digital signature technology involves the use of "hash functions" which are the mathematical algorithms applied in the creation and verification of digital signatures.

The National Institute of Standards and Technology (NIST) has issued Federal Information Processing Standard (FIPS) 186, Digital Signature Standard (DSS), on May, 1994. The DSS defines a public key cryptographic system for generating and verifying digital signatures. The private key is randomly generated. Using this key and a mathematical process defined in the standard, the public key is generated. The DSS is used with FIPS 180, Secure Hash Standard (SHS), to generate and verify digital signatures. The DSS specifies a Digital Signature Algorithm (DSA) for use in computing and verifying digital signatures. The DSA could be employed in a variety of business applications requiring a replacement of handwritten signatures.

Information on FIPS 186, Digital Signature Standard, is available from: Computer Systems Laboratory, Room B64, Technology Building, National Institute of Standards and Technology, Gaithersburg, MD 20899-9001. Telephone: (301) 975-2816. Fax: (301) 948-1784. E-mail: [dward@enh.nist.gov](mailto:dward@enh.nist.gov).

## Professional Association Guidelines

*Digital Signature Guidelines*, Information Security Committee, Science and Technology Section, American Bar Association, 1996. These Guidelines explain digital signature technology in simple terms and examine how this technology can be applied as a computer based alternative to traditional signatures. The Guidelines are designed to assist anyone involved in on line transactions that need to be secure and authentically signed. (<http://www.abanet.org/home.html>)

### Public-Key Cryptography Standards (PKCS)

"RSA Laboratories' Public-Key Cryptography Standards (PKCS), the informal intervendor standard was developed in 1991 by RSA Laboratories with representatives of Apple, Digital, Lotus, Microsoft, MIT, Northern Telecom, Novell and Sun. Since its publication in June 1991, PKCS has become a part of several standards and products, including Internet Privacy-Enhanced Mail, the NIST/OSI Implementers' Workshop, BLOC F3 Forms Automation, Apple's PowerTalk, Shana Informed, and Fischer International's Workflow 2000. These standards cover RSA encryption, Diffie-Hellman key agreement, password-based encryption, extended-certificate syntax, cryptographic message syntax, private-key information syntax, and certification request syntax, as well as selected attributes." (<http://www.rsa.com/rsalabs/pubs/PKCS/>)

### Secure Electronic Transaction (SET)

"Secure Electronic Transaction (SET) is a technical specification for securing payment card transactions over open networks such as the Internet. SET was developed by Visa and MasterCard, with participation from several technology companies, including Microsoft, IBM, Netscape, SAIC, GTE, Terisa Systems and VeriSign. SET will be based on specially developed encryption technology from RSA Data Security."

(<http://www.visa.com/cgi-bin/vee/sf/set/faq.html>) "SET, which includes digital certificates - a way of verifying the actual cardholder is making the purchase - will provide financial institutions, merchants, and vendors with a new and secure way of getting the most from the emerging electronic commerce marketplace."

(<http://www.visa.com:80/cgi-bin/vee/sf/standard.html>)

## Best Practices

### Digital Signature

Like a hand written signature in a printed document, a digital signature can be used to identify and authenticate the originator of an electronic document. A digital signature is an unforgeable piece of data, which asserts that a certain person either wrote or otherwise agreed to the electronic document to which the digital signature is attached. The recipient of a digitally signed electronic document can verify both that this document came from the person whose digital signature is attached and that this document is not altered after it is signed.

### Pretty Good Privacy (PGP)

Sending e-mail message over the Internet is more like sending a paper mail on postcard than on a sealed envelope. Everybody who has the authority to get into the mail passageway can easily read or even alter the mail. Pretty Good Privacy (PGP), created by Philip Zimmermann, is software that allows the sender of an electronic mail to encrypt and digitally sign the e-mail message or files using the sender's private key. Only the designated e-mail recipient can use the sender's public key to decrypt this e-mail message or files. While the recipient decrypting the e-mail message or files, the sender authenticates himself/herself to the recipient that the sender is the person who he/she claimed he/she is and the e-mail message or files are not altered after the sender signed the e-mail message or files. Once a digital signature is created, it is impossible for anyone to modify either the message or the signature without being detected by PGP.

Each PGP user must initially generate a pair of complementary keys: a public key and a secret key. Public key and private key are generated at the same time and each key unlocks the code that the other key makes. Public key is publicly distributed to whoever wants to send e-mail message to the person who distributed the public key. Only the person who distributed the public key knows the secret key and it should be guarded carefully.

### Policies

On June 11, 1996, Governor's Task Force on Information Resource Management (now known as 'The Office for Technology') released 'Technology Policy 96-14 New York State Use of Electronic Mail.' The purpose of this policy is to promote the use of e-mail as an efficient communication and data gathering tool, and to ensure that State agencies have the information necessary to use e-mail to their best advantage in supporting agency business. It states general policies and security issues about using e-mail communications.