Order Code RS20344
Updated January 19, 2001

CRS Report for Congress

Electronic Signatures: Technology Developments and Legislative Issues

Richard M. Nunno
Analyst in Information Technologies
Resources, Science, and Industry Division

Summary

Electronic signatures, a means of verifying the identity of the user of a computer system to control access or authorize a transaction, are increasingly being used in electronic commerce. Several technologies can be used to produce electronic signatures, the most prominent being digital signatures, which use cryptographic techniques to provide data integrity and nonrepudiation. Legislation enacted in the 106th Congress enables the legal recognition of electronic signatures in interstate commerce. Other legislation introduced but not enacted was intended to promote federal agency use of electronic signatures to enable electronic filing of information.

Definitions and Technologies Used for Electronic Signatures. Electronic signatures are methods used to provide *electronic authentication*, a process of verifying the identity of users of a computer (either a stand-alone mainframe or a network or Internet-based system) in order to control access or authorize transactions. In many states and industry sectors, electronic signatures attached to *electronic records* (documents created, stored, generated, received, or communicated by electronic means) are legally recognized in the same manner as handwritten signatures on paper. Electronic signatures are used to establish identity in electronic commerce, and to control access to facilities or systems. Electronic signatures are either being implemented or planned for medical and financial records, and various government transactions. The following technologies are forms of electronic signatures at various levels (and are used in combination to provide added security):

- **password or personal identification number (PIN)**—a set of numbers or characters shared only by the system and the user, and usually encrypted if the authentication occurs over an open network (i.e., a network to which the public has access);
- **smart card**—a plastic card similar to a credit card, except that it contains a microprocessor (a "chip") that can generate, store, and process data, and can be programmed to be activated only when the user enters a PIN or other identifier. Together with a reader device, smart cards are

used for telephone calling, electronic cash payments, access to ATMs, and to store medical or financial data for individuals, and provide greater security than a PIN, because the user must have both the card and the PIN;

- **biometrics**—technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements to authenticate their identity. Biometric devices consist of a reader or sensor, software that converts the received information into digital form (i.e., a series of binary digits or bits), and if the data are analyzed, a database to store an individual's known biometric data with the entered biometric data;
- **digitized signature**—(a form of biometric) a graphical image of a hand-written signature, usually entered using a special digital pen and pad input device. The input signature is automatically compared with a stored copy of the digitized signature of the user, and authenticated if the two signatures meet specifications for similarity;
- **digital signature**—an electronic signature that is produced on a message using a key (a very large binary number) that is known only by the signer, and a signature algorithm (a mathematical formula) that is publicly known. The digital signature is unique to each message and key combination. It can be used to verify the identity of the signer and to provide *data integrity* (authentication that nothing in the data has been altered since the message was signed). It can also be used to prove to a third party that the signature was in fact signed by the signatory (known as *nonrepudiation*).

While PINs and biometrics are used for access control to information or capabilities on a smart card (which may include other PINs, biometric information, keys, or certificates), only digital signatures (and other cryptographic processes) can provide data integrity and nonrepudiation. Digital signatures use a system called *public key cryptography*,[1] that uses two keys: a private key (held only by the sender of transmitted data) used in conjunction with a signature algorithm to sign the data, and a public key (often made public in an on-line directory) used by the receiver of the data with the algorithm to verify the signature received (see box for a typical step-by-step procedure for creating and using digital signatures in an Internet application).

Process for Using a Digital Signature for Secure Internet Transmissions:

1. The sender's public key and proof of identity are given to a *certification authority* (a trusted third party, such as a government agency or an established company).
2. The certification authority creates a digital signature certificate (an electronic file containing the sender's name and public key).
3. When the sender creates an email message, special software is used to compute a *hash* (a mathematical summary) of the message.
4. The hash and the sender's private key are used by the signature algorithm to produce the digital signature.
5. The message and digital signature are transmitted.
6. The receiver obtains the digital signature certificate, either from the sender along with the message, from the certification authority, or from a directory of certificates.
7. The receiver processes the digital signature using the public key of the certification authority, and computes a hash on the content of the certificate. If the two results match, the receiver knows that the message is valid.

[1] Public key systems are also called *asymmetric* systems.

As a result of the growth of electronic commerce, a *public key infrastructure* (PKI) is being planned, consisting of several competing certification authorities from which users can choose, to meet a range of computer security needs. The Administration is working with the private sector to develop a PKI for electronic data exchanges within and among federal agencies, vendors, state and local governments, and citizens.[2] Many federal agencies are conducting research and development on and procurement of electronic signature technologies to enhance security and efficiency. Digital signatures are often confused with the software that is used for *encryption* (a process of scrambling the bits according to a secret algorithm) of the content of messages and data. Indeed, the cryptographic technology they use is very similar. Unless encryption is used in conjunction with digital signatures, however, anyone who intercepts the electronic file can read the content of the message or data. Only encryption products (whether software or hardware) can provide *confidentiality* (preventing transmitted data from being monitored by unwanted parties). Furthermore, the U.S. export restrictions for strong encryption products do not apply for digital signatures (for further discussion, see CRS Issue Brief IB96039, *Encryption Technology: Congressional Issues*).

Congressional Interest in Electronic Signatures. The main congressional interests in electronic signatures focus on enabling electronic signatures to carry legal weight in place of written signatures, removing the inconsistencies among state policies that some fear may deter the growth of electronic commerce, and establishing requirements for government use of electronic signatures to enable electronic filing of information. Neither law enforcement nor national security organizations oppose these objectives, and many business associations would like a national electronic signatures standard to be established to enhance electronic commerce. State legislatures have been active in electronic signature issues for several years. All states except for Arkansas, South Carolina, and South Dakota, have considered or enacted some form of electronic authentication law (although some state legislation does not distinguish between electronic and digital signatures). Currently, 36 states have introduced or are considering 76 electronic signature initiatives. Twenty-six states have enacted one or more of these initiatives into law. In the area of digital signatures or PKI technologies, 20 states have introduced or considered 36 different initiatives or regulations, with 13 states adopting some form into law. Seven states are examining laws that address both digital and electronic signatures (see the Internet Law and Policy Forum [http://www.ilpf.org/]). Three models for electronic signatures have developed at the state level: the "Utah" or "prescriptive" model with a specific public key infrastructure scheme including state-licensed certification authorities; the "California" or "criteria-based" model that requires electronic signatures to satisfy certain criteria of reliability and security; and the "Massachusetts" or "signature enabling" model that adopts no specific technological approach or criteria, but recognizes electronic signatures and documents in a manner parallel to traditional signatures. The first two models have been criticized for failing to be *technology neutral*, i.e., favoring digital signatures over competing electronic signature technologies. Some of the proposed state laws are general, applying to a wide range of government or private sector activities, while others are more narrowly cast. One controversial aspect of the debate over electronic signatures is whether there should be a single federal law in place of the various state laws. Many in industry believe that the lack

---

[2] See report at [http://gits.gov] first released September 1998 by the Vice President's Government Information Technology Services Board, a collaborative effort by government and industry.

of national rules governing the use of electronic signatures is one of the barriers to the growth of electronic commerce. Others, however, are concerned that some national rules might interfere with state or international laws.

The Government Paperwork Elimination Act. Enacted at the end of the 105th Congress as part of the Omnibus Appropriations Act (S. 2107, P.L. 105-277), this measure directed the Office of Management and Budget (OMB) to establish procedures for executive branch agencies to accept electronic submissions using electronic signatures, and required agencies to accept those electronic submissions except where found to be impractical or inappropriate. By October 2003, executive branch agencies must provide for the option of electronic maintenance, submission, or disclosure of information as a substitute for paper. The Act gives full legal effect to electronic records produced and, information collected from an executive agency using electronic signature services may only be used or disclosed by those using the information for business or government practices. These provisions do not apply to the Department of Treasury, if they conflict with internal revenue laws or codes. On March 5, 1999, OMB proposed procedures to implement the Act, outlining actions for specific federal agencies, much of which had already been underway. No industry group responded negatively to the proposal. Some privacy advocacy groups were concerned that OMB plans might create a reliance on "identity-based" authentication techniques (i.e., using personal information to establish one's identity) that could lead to larger storehouses of information collected by the government and its contractors. In April 2000, OMB issued procedures and guidance to federal agencies to permit private employers to electronically file their employee forms with executive agencies. OMB, together with the National Telecommunications and Information Administration, is conducting an study of the use of electronic signatures, including its impact on paperwork reduction, electronic commerce, individual privacy, and the security and authenticity of electronic transactions, and will report to Congress on these issues.

Federal Use of Commercial Standards. To foster government use of electronic signatures, the National Institute of Standards and Technology (NIST) adopting commercial standards. In December 1998, in response to the National Technology Transfer Act of 1995 (P.L. 104-113) and direction from OMB (Circular A-119, February 10, 1998), NIST approved an interim Federal Information Processing Standard (FIPS) to allow federal agencies to use the RSA digital signature standard (the de facto commercial standard developed by RSA Data Security, a cryptography company). Prior to that time the only such standard adopted by the federal government was the Digital Signature Algorithm (DSA), developed by the federal government for electronic data transfers between federal agencies. DSA, however, does not support confidentiality, unlike RSA and other private sector digital signature standards. The RSA standard was approved by the Secretary of Commerce in January 2000, which is expected to increase its use by firms that conduct business with the federal government. NIST is also reviewing a third digital signature standard, called Elliptic Curve Cryptography (ECC). Adopting a third standard would likely produce a more competitive market for digital signature software, and an increase in its use in both government and industry.

Legislation in the 106th Congress. Several bills were introduced in the 106th Congress regarding electronic signatures. The Millennium Digital Commerce Act (S. 761,

Abraham, and its companion, H.R. 1320, Eshoo, both introduced March 25, 1999)[3] and the Electronic Signatures in Global and National Commerce Act (H.R. 1714, Bliley, introduced May 6, 1999) were intended to permit and encourage the continued expansion of interstate electronic commerce through the operation of free market forces. Each of these bills provided for the legal recognition of electronic signatures and records, preempting state electronic signatures laws until the states enact uniform standards.[4] H.R. 1714 was more explicit than S.761 in directing the Department of Commerce (DOC) to report to Congress on the impediments to foreign acceptance of electronic signatures and records, and to promote their use in interstate and foreign commerce. A state law would supersede this legislation only if it specifies alternative procedures for the use of electronic signatures, and is enacted within two years of enactment of this bill. H.R. 1714 also gives legal recognition to electronic securities trading, notwithstanding state laws, and authorize the Securities and Exchange Commission to prescribe implementing regulations. The bill does not apply to certain proceedings, such as wills, trusts, adoption, or divorce documents. The House Commerce Committee approved H.R. 1714 (amended) July 13 (H.Rept. 106-341, Part 1, September 27); the bill was then approved by the House Judiciary Committee (H.Rept. 106-341 Part II, October 15), and passed the House (amended) November 9, 1999.

Unlike H.R. 1714, S. 761 was limited to commercial transactions between private parties that affect interstate commerce, and allowed parties to a transaction to determine the technologies and business methods to be used in the execution of an electronic contract. S. 761 established principles for the U.S. government to follow in international negotiations regarding the use of electronic signatures to facilitate electronic commerce, and directed DOC and OMB to report on federal laws and regulations that might pose barriers to electronic commerce. S. 761 was approved by the Senate Commerce Committee July 30 (S.Rept. 106-131) and passed the Senate November 19, 1999. Business and industry groups supported both H.R. 1714 and S. 761. Some states have endorsed one or the other bill. On August 4, 1999, OMB issued a Statement of Administration Policy (SAP) supporting the passage of S. 761. On November 8, OMB issued an SAP opposing passage of H.R. 1714, stating that it unnecessarily deprives consumers of protections under current law, deprives regulators of the ability to ensure that electronic disclosures and notices under existing statutes will be made in a meaningful way, and preempts state laws too broadly. Many consumer and privacy advocacy groups and individuals opposed one or both bills, arguing that some of their provisions may be overly broad or undefined and might create disadvantages for consumers who do not have updated computers or access to the Internet. Some also criticized the legislation as being unnecessary, since the states are already working toward enacting electronic signature statutes. Others, however, argued that companies are not offering many new electronic services out of fear that electronic transactions would not be legally recognized without national legislation. House-Senate negotiations on this legislation continued for several months, and the conference (H.Rept. 106-661) was filed on June 8. The conference report passed the House on June 14 (426-4) and the Senate on June 16 (87-0), and was signed

---

[3] No further action was taken on H.R. 1320 after committee referral.

[4] In July 1999, the National Conference of Commissioners on Uniform State Laws approved a model state law, called the Uniform Electronic Transactions Act, that adapts existing commercial law to govern electronic commerce. To take legal effect, the model will have to be adopted separately by each state legislature, which could take several years for some states.

into law (P.L. 106-229) by the President (using a smart card) on June 30, 2000. Other bills introduced in the 106th Congress (but not enacted) with electronic signature provisions include:

- Paperwork Elimination Act of 1999 (H.R. 439, intr. February 2, 1999) intended to minimize federal paperwork demands on small businesses, educational and nonprofit institutions, federal contractors, state and local governments, and others through sponsorship and use of electronic signatures and records. Bill adds to provisions of the Government Paperwork Elimination Act by directing OMB to report on progress of federal agencies in promoting use of electronic signatures and records by businesses and individuals, without hindering use of paper-based transactions (passed House without committee referral, February 9; received in Senate Committee on Governmental Affairs February 22);
- Digital Signature Act (H.R. 1572, Gordon, intr. April 27, 1999) would require NIST to adopt guidelines and standards for use of digital (and electronic) signatures by federal agencies, evaluate commercial products and certificate authority services, and release to the public a list of those meeting federal standards. It would establish a national policy panel to study the use of digital signatures in private sector electronic transactions (referred to the House Committee on Science);
- Internet Growth and Development Act of 1999 (H.R. 1685, Boucher, intr. May 5, 1999) contains a provision to provide for the recognition of electronic signatures for the conduct of interstate and foreign commerce (referred to Committees on Commerce and Judiciary);
- Computer Security Enhancement Act of 1999 (H.R. 2413, Sensenbrenner, intr. July 1, 1999) contains a provision (adapted from H.R. 1572) directing NIST to develop electronic authentication (i.e., electronic signature) infrastructure guidelines and standards for use by federal agencies to effectively utilize electronic authentication technologies in a manner that is sufficiently secure and interoperable to meet the needs of those agencies and their transaction partners (referred to Committee on Science, marked-up by Subcommittee on Technology); and
- Electronic Securities Transactions Act (S. 921, Abraham, introduced April 29, 1999) would facilitate and promote electronic commerce in securities transactions involving broker-dealers, transfer agents and investment advisers (referred to Committee on Banking). This bill is equivalent to the section of H.R. 1714 addressing electronic securities trading, but was introduced separately for jurisdictional purposes.

Privacy. Privacy is a major concern associated with the widespread use of electronic signatures. If electronic signatures are stolen or sold by unauthorized persons, the use of fraudulent copies could not only thwart the goals of providing reliable authentication, data integrity, and nonrepudiation, but also potentially lead to legal problems for individuals who become victims of identity theft. The continued growth of electronic commerce is a shared goal by nearly all interested parties. At issue, however, is balancing that goal with appropriate limits on the scope of a national law governing and encouraging the acceptance of electronic signatures and records in government and the private sector.