

Electronic Signatures

1. The Electronic Signatures in Global and National Commerce Act, 15 USC Sec. 7001, P. L. 106-229, hereinafter “the Act”, provides at Section 101, that a signature, contract or other record relating to interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because it is in electronic form. The Act further provides that a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation. Oral communications, or a recording of an oral communication, however, do not qualify as an electronic record under the Act. The Act became effective on 1 October 2000.
2. The Act also provides that if there is a requirement that a contract or other record to a transaction be retained, that requirement is met by retaining an electronic record of the information, provided it accurately reflects the information set forth in the contract or other record and remains accessible to all persons who are entitled to access in a form that is capable of being accurately reproduced.
3. An electronic signature is defined at 15 USC Sec. 7006 as “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.” An electronic record is defined as “a contract or other record created, generated, sent, communicated, received, or stored by electronic means.”
4. There are several specific exceptions to the use of electronic records and electronic signatures at 15 USC Sec. 7003 - Specific Exceptions. One of the listed exceptions, which may be of particular interest to the legal community, is:
 - (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;
5. Under the Government Paperwork Elimination Act (GPEA), part of P.L. 105-277, included in H.R 4328, the Omnibus Consolidated and Emergency Supplemental Appropriation Act for FY 1999, the Office of Management and Budget (OMB) is charged with development of a policy for Executive agencies to follow in using and accepting electronic documents and signatures. The GPEA provides that in developing procedures for the use of electronic signatures, OMB is to give due consideration to maintaining compatibility with standards and technology for electronic signatures generally used in commerce and industry and by state governments. OMB is not to inappropriately favor one industry or technology, is to ensure that electronic signatures are as

reliable as is appropriate for the purpose in question and that electronic record keeping systems reliably preserve the information submitted.

OMB Guidance

6. On 5 March 1999, OMB issued proposed guidance for implementation of the GPEA. In the proposed guidance, OMB emphasized the need for security and privacy protection in the use of electronic signatures. Before selecting the type of electronic signature to be used and accepted, Government agencies must perform a risk assessment of the electronic signature alternatives and they must maintain appropriate confidentiality and security in accordance with OMB Circular A-130, Appendices I and III. According to OMB, the goal of information security is to protect the integrity of electronic records and transactions.

7. There are several methods of authenticating electronic signatures discussed by OMB in its guidance. Some methods are non-cryptographic such as the “shared secrets” method using personal ID number and passwords; smart cards; digitized signatures and biometric means of identification such as fingerprints or retinal patterns and voice recognition. There are also methods using cryptographic control such as symmetric (or shared private key) cryptography, or asymmetric (public key/private key) cryptography, which are used to produce digital signatures.

8. In using electronic signatures it is important that clear procedures be established so that all parties know what the obligations, risks and consequences are. According to OMB, digitized (not digital) signatures, Personal Identification Numbers (PINs) and biometric identifiers do not directly bind a company or individual to the content of a document. For them to do so, they must be used in conjunction with some other mechanism.

Non-cryptographic Methods of Authenticating Identity

9. The “shared secrets” system provides for a user accessing an agency’s electronic application to enter a “shared secret” such as a password or PIN. The system checks the password or PIN to authenticate the user. If this process is done over an open network, such as the internet, it is necessary that the shared secret be encrypted.

10. A smart card is a plastic card that contains an embedded chip that can generate, store, and/or process data. A user inserts the card into a card reader device attached to a microcomputer or network input device. In the computer, information from the chip is read by security software only when the user enters a PIN, password or biometric identifier. This method provides greater security than use of a PIN alone as the user must have physical possession of the smart card and knowledge of the PIN.

11. Digitized signatures are graphical images of handwritten signatures. Some applications require a user to create a hand-written signature using a special computer input device, such as a

digital pen and pad. The digitized representation of the entered signature is compared with a stored copy of the graphical image of the handwritten signature.

12. Biometrics are unique physical characteristics that can be converted into digital form and then be interpreted by a computer such as voice patterns, fingerprints and the blood vessel patterns present on the retina of one or both eyes. In this method, the physical characteristic is measured, converted into digital form, and then compared with a copy of that characteristic stored in the computer and then authenticated beforehand as belonging to a particular person. This method provides a high level of authentication but as with all shared secrets, if the digital form is compromised, impersonation becomes a serious risk. Thus, this information should not be sent over open networks unless it is encrypted.

Cryptographic Control

13. In a shared private key approach, the user signs a document and verifies the signature using a single key that is not publicly known. The key must be transferred to the recipient of the message. This, however, could undermine confidence in the authentication of the user's identity because the private key is shared between sender and recipient and is no longer unique to one person.

14. Digital signatures are created when the owner of a private signing key uses that key to create a unique mark (called a "signed hash") on an electronic document or file. The recipient employs the owner's public key to validate the authenticity of the attached private key. This process also verifies that the document was not altered. If the private key has been properly protected from compromise or loss, the signature is unique to the individual who owns it, that is, the owner is bound by their signature. A potential problem with this approach is that the private key owner could feign loss to repudiate a transaction. This concern can be mitigated by encoding the private key onto a smart card or an equivalent device, and by using a biometric mechanism (rather than a PIN or password) as the shared secret between the user and the smart card for unlocking the private key to effect a signature.

15. To produce a digital signature, a user has his or her computer generate two mathematically linked keys – a private signing key that is kept private, and a public validation key that is available to the public. The private key cannot be deduced from the public key. In practice, the public key is made part of a "digital certificate," which is a specialized electronic document digitally signed by the issuer of the certificate, binding the identity of the individual to his or her private key in an unalterable fashion.

Agency Implementation of Electronic Signatures

16. In its proposed guidance, OMB advises that, in implementing the use of electronic signatures, Agencies develop a well-documented and established mechanism and procedure to ensure that transactions between the Government and outside contractors are legally binding. The

integrity of even the most secure digital signature rests, however, on the continuing confidentiality of the private key. If a contractor were later charged with a crime or a breach of the terms and conditions of a contract based on an electronically signed document, the contractor would have every incentive to show a lack of control over (or loss of) the private key or PIN. Indeed, if a contractor plans to commit fraud, the contractor may intentionally compromise the secrecy of the key or PIN, so that the Government would later be unable to link the contractor to the electronic transaction.

17. Transactions which appear to be at high risk for fraud, e.g. one-time high-value transactions with contractors not previously known to an agency, may require extra safeguards or may not be appropriate for electronic transactions. One way to mitigate this risk is to require that private keys be encoded on hardware tokens, making possession of the token a critical requirement. Another way to guard against fraud is to include other identifying data in the transaction that links the key or PIN to the individual, preferably something not readily available to others.

Department of Defense (DoD) Guidance

18. On 13 December 1999, the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence issued "X.509 Certificate Policy for the Department of Defense." DoD is developing a Key Management Infrastructure (KMI) to provide engineered solutions for security of networked computer-based systems. Part of this KMI is a Public-Key Infrastructure (PKI) consisting of products and services that provide and manage X.509 certificates for public-key cryptography. These certificates identify the individual named in the certificates and bind that person to a particular public/private key pair. The DoD Certificate Policy was issued to provide a unified certification policy for DoD but does not define how the components of DoD are to implement PKI. The intent of the policy is to identify the minimum requirements and procedures that are necessary to support trust in the PKI and to minimize imposition of specific implementation requirements on DoD components. The policy statement defines the creation and management of Version 3 X.509 public-key certificates for use in applications requiring communication between networked computer-based systems. Such applications include contract formation signatures. According to the DoD policy the PKI must support five primary security services: access control, confidentiality, integrity, authentication and technical non-repudiation. The PKI supports these security services by providing Identification and Authentication (I&A), integrity and technical non-repudiation through digital signatures, and confidentiality through key exchange.

19. By memorandum dated 12 August 2000, the DoD Chief Information Officer in the Office of the Assistant Secretary of Defense, issued a memorandum to update DoD policies for the development and implementation of a Department-wide PKI. DoD intends to develop a common, integrated, interoperable DoD PKI to enable security services at multiple levels of assurance. To this end, the memorandum sets forth various dates for the implementation of the use of electronic signatures. For example, the memorandum provides that all electronic mail, as distinct from organizational messaging, sent within DoD will be digitally signed by October 2002.

As part of this plan, PKI certificates will be issued to all active duty military personnel and civilian employees. A PKI certificate is defined as “(a) digital representation of information that binds the user’s identification with the user’s public key in a trusted manner.” The memorandum also states that it is DoD policy that:

Secure interoperability between DoD and its vendors and contractors will be accomplished using External Certificate Authorities (ECAs). ECAs will operate under a process that delivers the level of assurances that is required to meet business and legal requirements. Operating requirements for ECAs will be approved by the DoD Chief Information Officer, in coordination with the DoD Comptroller and the DoD General Counsel. In Interim ECA (IECA) capability is currently available. Requirements for interoperable PKI-enabled services with industry partners shall be met via certificates generated from IECA or ECA.

An ECA is defined as “(a)n agent that is trusted and authorized to create, sign, and issue certificates to approved vendors and contractors for the purpose of enabling secure interoperability with DoD entities.”

20. In discussing this issue with the Office of the General Counsel of DoD, Mr. James Scuro of the CECOM Legal Office spoke with Mr. Douglas Larsen, Deputy General Counsel for Acquisition and Logistics, and Ms. Shauna Russell of his office. Mr. Scuro was advised that the General Counsel’s Office’s position is that electronic signatures should not be used for legally binding documents, such as contracts, until a DoD-wide system is established to ensure that a contractor cannot subsequently repudiate an electronic signature used to execute a contract or other legally binding document. The Office of the General Counsel’s concern is similar to that set forth in the OMB guidance regarding repudiation of contracts by a contractor if electronic signatures are used. Electronic signatures, however, may be used for non-binding documents using the PKI method.

Proposed FAR Revisions

21. On 1 November 2000, the General Services Administration, National Aeronautics and Space Administration and the DoD published a proposed rule in the Federal Register, Vol. 65, No. 212, to amend the Federal Acquisition Regulation (FAR) to authorize the use of electronic signatures. The proposed rule, which has not as of this date been approved, provides for the following amendments to the FAR:

- a. FAR Section 2.101- Definitions, to be amended to incorporate the following definitions:

Electronic commerce means business transactions accomplished by electronic bulletin boards, purchase cards, electronic funds transfer, or electronic data interchange.

* * * *

In writing or written means any expression of information in words, numbers, or other symbols, including electronic expressions, that can be read, reproduced, and stored.

* * * *

Signature or signed means the discrete, verifiable symbol of an individual that, when attached to or logically associated with a written contract or other record with the knowledge and consent of the individual, indicates a present intention to authenticate the contract or other record. This includes an electronic signature made by electronic sound, symbols, or process.

b. FAR Section 4.502 – Policy, to be amended to include the following:

(d) As required by the Government Paperwork Elimination Act (GPEA) (Title XVII of Division C of Public Law 105-277), by October 21, 2003, agencies must allow individuals or entities the option to submit information or transact with the agency electronically when practicable. The GPEA requirement includes execution of contracts and associated records using electronic signatures of the offeror or contractor and the agency.

22. According to Ms. Shauna Russell of the Office of the General Counsel of DoD, the proposed FAR revisions are based on using electronic signatures in accordance with the guidance set forth in the Assistant Secretary of Defense and Intelligence’s memorandum dated 13 December 1999, as updated by the 12 August memorandum by the DoD Chief Information Officer.

SUMMARY

23. Pursuant to 15 USC Sec. 7003, electronic signatures cannot be used for court orders, notices or official court documents, including briefs and pleadings. The Office of the General Counsel for DoD has taken the position that electronic signatures cannot be used to execute legally binding documents such as a contract until a system is established to ensure that a contractor cannot subsequently repudiate an electronic signature. For non-legally binding documents, electronic signatures can be used in accordance with the PKI guidance provided in the 13 December 1999 memorandum by the Assistant Secretary of Defense, Command, Control, Communications and Intelligence.

24. The Point of Contact for this subject in the CECOM Legal Office is Mr. James Scuro, (732) 532-9801; DSN 992-9801.

KATHRYN T. H. SZYMANSKI
Chief Counsel

Source Materials:

1. 15 USC 7001 etc. seq., Electronic Signatures in Global and National Commerce Act (2000).
2. 40 USC 3504(a)(vi), Government Paperwork Elimination Act, amended by Pub. L. 105-277 (1998).
3. Office of Management and Budget Circular A-130, Appendices I and III.
4. Management of Federal Information Resources, 64 Fed. Reg. 43, 10896 (1999).
5. X.509 Certificate Policy for the United States Department of Defense, issued by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (1999).
6. Memorandum from Department of Defense Chief Information Officer, Office of the Assistant Secretary of Defense to Secretaries of the Military Departments; Chairman of the Joint Chiefs of Staff; Under Secretaries of Defense; Director, Defense Research and Engineering; Assistant Secretaries of Defense; General Counsel of the Department of Defense; Director, Operational Test and Evaluation; Assistants to the Secretary of Defense; Director, Administration and Management and Directors of the Defense Agencies, Subject: Department of Defense (DOD) Public Key Infrastructure (PKI) (August 12, 2000).
7. Federal Acquisition Regulation; Electronic Signatures, 65 Fed. Reg. 212, 65698 (2000).