Comptroller General
of the United States

Washington, D.C. 20548

Decision

Matter of: National Institute of Standards and Technology--Use of Electronic Data Interchange Technology to Create Valid Obligations

File: B-245714

Date: December 13, 1991

DIGEST

Contracts formed using Electronic Data Interchange technologies may constitute valid obligations of the government for purposes of 31 U.S.C. § 1501, so long as the technology used provides the same degree of assurance and certainty as traditional "paper and ink" methods of contract formation.

DECISION

By letter dated September 13, 1991, the Director, Computer Systems Laboratory, National Institute of Standards and Technology (NIST), asked whether federal agencies can use Electronic Data Interchange (EDI) technologies, such as message authentication codes and digital signatures, to create valid contractual obligations that can be recorded consistent with 31 U.S.C. § 1501. For the reasons stated below, we conclude that agencies can create valid obligations using properly secured EDI systems.

BACKGROUND

EDI is the electronic exchange of business information between parties, usually via a computer, using an agreed upon format. EDI is being used to transmit shipping notices, invoices, bid requests, bid quotes, and other messages. Electronic contracting is the use of EDI technologies to create contractual obligations. EDI allows the parties to examine the contract, usually on video monitors, but sometimes on paper facsimiles, store it electronically (for example, on magnetic tapes, on discs or in special memory chips), and recall it from storage to review it via electronic means. Using EDI technologies, it is possible for an agency to contract in a fraction of the time that traditional practices take.

As NIST pointed out in its request, the "paperless" nature of the technology has raised the question of whether electronic contracts constitute obligations which may be recorded against the government. NIST is in the process of developing standards

for electronic signatures to be used in various applications,[1] including the formation of contracts, but has been advised that section 1501 imposes a barrier to the use of electronic technologies by federal agencies in this regard.

DISCUSSION

Section 1501 establishes the criteria for recording obligations against the government. The statute provides, in pertinent part, as follows:

> "(a) An amount shall be recorded as an obligation of the United States Government only when supported by documentary evidence of--
>
> (1) a binding agreement between an agency and another person (including an agency) that is--
>
> (A) in writing, in a way and form, and for a purpose authorized by law. . . ."

31 U.S.C. § 1501(a)(1)(A).

Under this provision, two requirements must be satisfied: first, the agreement must bind both the agency and the party with whom the agency contracts; second, the agreement must be in writing.

Binding Agreement

The primary purpose of section 1501(a)(1) is "to require that there be an offer and an acceptance imposing liability on both parties." 39 Comp. Gen. 829, 831 (1960) (emphasis in original). Hence the government may record an obligation under section 1501 only upon evidence that both parties to the contract willfully express the intent to be bound. As explained below, EDI technology provides both the agency and the contractor the means to electronically "sign" a contract.

A signature traditionally has provided such evidence. See generally 65 Comp. Gen. 806, 810 (1986). Because of its uniqueness, the handwritten signature is probably the most universally accepted evidence of an agreement to be bound by the terms of a contract. See 65 Comp. Gen. at 810. Courts, however, have demonstrated a willingness to accept other

---

[1]The Congress has mandated that NIST (formerly the National Bureau of Standards) establish minimum acceptable practices for the security and privacy of sensitive information in federal computer systems. Computer Security Act of 1987, Pub. L. No. 100-235, § 2, 101 Stat. 1724 (1988).

notations, not necessarily written by hand. See, e.g., Ohl & Co. v. Smith Iron Works, 288 U.S. 170, 176 (1932) (initials); Zacharie v. Franklin, 37 U.S. (12 Pet.) 151, 161-62 (1838) (a mark); Benedict v. Lebowitz, 346 F.2d 120 (2nd Cir. 1965) (typed name); Tabas v. Emergency Fleet Corporation, 9 F.2d 648, 649 (E.D. Penn. 1926) (typed, printed or stamped signatures); Berryman v. Childs, 98 Neb. 450, 153 N.W. 486, 488 (1915) (a real estate brokerage used personalized listing contracts which had the names of its brokers printed on the bottom of the contract in the space where a handwritten signature usually appears).

As early as 1951, we recognized that a signature does not have to be handwritten and that "any symbol adopted as one's signature when affixed with his knowledge and consent is a binding and legal signature." B-104590, Sept. 12, 1951. Under this theory, we approved the use of various signature machines ranging from rubber stamps to electronic encryption machines ranging from rubber stamps to electronic encryption devices. See 33 Comp. Gen. 297 (1954); B-216035, Sept. 20, 1984. For example, we held that a certifying officer may adopt and use an electronic symbol generated by an electronic encryption device to sign vouchers certifying payments. B-216035, supra. The electronic symbol proposed for use by certifying officers, we concluded, embodied all of the attributes of a valid, acceptable signature: it was unique to the certifying officer, capable of verification, and under his sole control such that one might presume from its use that the certifying officer, just as if he had written his name in his own hand, intended to be bound.

EDI technology offers other evidence of an intent to be bound with the same attributes as a handwritten signature. We conclude that EDI systems using message authentication codes which follow NIST's Computer Data Authentication Standard (Federal Information Processing Standard (FIPS) 113)[2] or digital signatures following NIST's Digital Signature Standard, as currently proposed, can produce a for of evidence that is acceptable under section 1501.

---

[2]FIPS 113 adopts American National Standards Institute (ANSI) standard X9.9 for message authentication. It outlines the criteria for the cryptographic authentication of electronically transmitted data and for the detection of inadvertent and/or intentional modifications of the data. By adopting the ANSI standard, FIPS 113 encourages private sector applications of cryptographic authentication; the same standard is being adopted by many financial institutions for authenticating financial transactions.

Both the message authentication code and the digital signature are designed to ensure the authenticity of the data transmitted. They consist of a series of characters that are cryptographically linked to the message being transmitted and correspond to no other message. There are various ways in which a message authentication code or digital signature might be generated. For example, either could be generated when the sender inserts something known as a "smart card"[3] into a system and inputs the data he wants to transmit. Encoded on a circuit chip located on the smart card is the sender's private key. The sender's private key is a sequence of numbers or characters which identifies the sender, and is constant regardless of the transmission. The message authentication code and the digital signature are functions of the sender's private key and the data just loaded into the system. The two differ primarily in the cryptographic methodology used in their generation and verification.

After loading his data into the system, the sender notifies the system that he wants to "sign" his transmission. Systems using message authentication codes send a copy of the data tot he chip on the smart card; the chip then generates the message authentication code by applying a mathematical procedure known as a cryptographic algorithm. Systems using digital signatures will send a condensed version of the data to the smart card, which generates the digital signature by applying another algorithm, as identified in NIST's proposed standard. The card returns the just-generated message authentication code or digital signature to the system, which will transmit it and the data to the recipient.

Under either approach, when an offeror or a contracting officer notifies the system that he wants to "sign" a contract for being transmitted, he is initiating the procedure for generating a message authentication code or digital signature with the intention of binding his company or agency, respectively, to the terms of the contract.[4] The code or digital signature evidences that intention, as would a handwritten or other form of signature. Both, generated using the sender's private key, are unique to the sender; and, the sender controls access to and use of his "smart card," where his key is stored.

---

[3]A smart card is the size of a credit card. It contains one or more integrated circuit chips which function as a computer.

[4]NIST officials advise us that technology using message advise us that technology using message authentication codes and digital signatures will be available to both contractors and contracting officers for use in government contracting.

They are also verifiable. When the recipient receives the contract, either on his computer monitor or in paper facsimile, it will carry, depending on which approach is used, a notation which constitutes the message authentication code or the digital signature of the sender, necessary information to validate the code or the signature and, usually, the sender's name. The recipient can confirm the authenticity of the contract by entering the data that he just received and asking his system to verify the code or the digital signature. The system will then use the information provided by the sender and either verify or reject it.[5] Both approaches use a key to verify the message just received; however, the digital signature requires application of a different key from that used to verify a message authentication code. The change of any data included in the message as transmitted will result in an unpredictable change to the message authentication code or the digital signature. Therefore, when they are verified, the recipient is virtually certain to detect any alteration.

Writing

To constitute a valid obligation under section 1501(a)(1)(A), a contract must be supported by documentary evidence "in writing." As NIST pointed out, some have questioned whether EDI, because of the paperless nature of the technology, fulfills this requirement. We conclude that it does.

Prior to the enactment of section 1501, originally section 1311 of the Supplemental Appropriations Act of 1955,[6] there was no "clean cut definition of obligations." H.R. Rep. No. 2266, 83rd Cong., 2d Sess. 50 (1954). Some agencies had recorded questionable obligations, including obligations based on oral contracts, in order to avoid withdrawal and reversion of appropriated funds. See 51 Comp. Gen. 631, 633 (1972). Section 1501 was enacted not to restrict agencies to paper and ink in the formation of contracts, but because, as one court noted, "Congress was concerned that the executive might avoid spending restrictions by asserting oral contracts." United States v. American Renaissance Lines, 494 F.2d 1059, 1062 (D.C. Cir. 1974) cert. denied, 419 U.S. 1020 (1974). The purpose of section 1501 was to require that agencies submit evidence that affords a high degree of certainty and lessens the possibility of abuse. See H.R. Rep. No. 2266 at 50.

---

[5]For the sake of simplicity, this example does not describe the complicated system of controls used to ensure that (1) no human knows the sender's private key and (2) the information received from the sender for validating the message authentication code or digital signature is correct and accurate.

[6]Pub. L. No. 663, 68 Stat. 800, 830 (1954).

While "paper and ink" offers a substantial degree of integrity, it is not the only such evidence. Some courts, applying commercial law (and the Uniform Commercial Code in particular), have recognized audio tape recordings, for example, as sufficient to create contracts. See, e.g., Ellis Canning Company v. Bernstein, 348 F. Supp. 1212 (D. Colo. 1972). The court, citing a Colorado statute, stated that the tape recording of the terms of a contract is acceptable because it is a "reduction to tangible form."[7] Id. at 1228. In a subsequent case, a federal Court of Appeals held that an audio tape recording of an agreement between the Gainesville City Commission and a real estate developer was sufficient to bind the Commission. Londono v. City of Gainesville, 768 F.2d 1223 (11th Cir. 1985). The court held that the tape recording constituted a "signed writing." Id. at 1228.

In our opinion, EDI technology, which allows the contract terms to be examined in human readable form, as on a monitor, stored on electronic media, recalled from storage and reviewed in human readable form, has an integrity that is greater than an audio tape recording and equal to that of a paper and ink contract. Just as with paper and ink, EDI technology provides a recitation of the precise terms of the contract and avoids the risk of error inherent in oral testimony which is based on human memory.[8] Indeed, courts under an implied-in-fact contract theory, have enforced contracts on far less documentation than would be available for electronic contracts. See Clark v. United States, 95 U.S. 539 (1877). See also Narva Harris Construction Corp. v. United States, 574 F.2d 508 (Ct. Cl. 1978).

---

[7]Other courts, interpreting the laws of other states, have held that a tape recording is not acceptable. See Sonders v. Roosevelt, 102 A.D.2d 701, 476 N.Y.S.2d 331 (1984); Roos v. Aloi, 127 Misc.2d 864, 487 N.Y.S.2d 637 (N.Y. Sup. Ct. 1985).

[8]Of course, just as with any contract or other official document, an agency must take appropriate steps to ensure the security of the document, for example, to prevent fraudulent modification of the terms. Agencies should refer to NIST standards in this regard. See, e.g., FIPS 113 (regarding message authentication codes). In addition, agencies should refer to the GSA regulations regarding the maintenance of electronic records, see 41 C.F.R. § 201-45.2, and to the Federal Rules of Evidence with regard to managing electronic records to ensure admissibility, see generally Department of Justice Report, "Admissibility of Electronically Filed Federal Records as Evidence," Systems Policy Staff, Justice Management Division (October 1990).

For the purpose of interpreting federal statutes, "writing" is defined to include "printing and typewriting and reproductions of visual symbols by photographing, multigraphing, mimeographing, manifolding, or otherwise." 1 U.S.C. § 1 (emphasis added). Although the terms of contracts formed using EDI are stored in a different manner than those of paper and ink contracts, they ultimately take the form of visual symbols. We believe that it is sensible to interpret federal law in a manner to accommodate technological advancements unless the law by its own terms expressly precludes such an interpretation, or sound policy reasons exist to do otherwise. It is evident that EDI technology had not been conceived nor, probably, was even anticipated at the times section 1501 and the statutory definition of "writing" were enacted. Nevertheless, we conclude that, given the legislative history of section 1501 and the expansive definition of writing, section 1501 and 1 U.S.C. § 1 encompass EDI technology.

Accordingly, agencies may create valid obligations using EDI systems which meet NIST standards for security and privacy.

Comptroller General
of the United States