Appendix C: Evolution of the Digital Signature Standard

C

INTRODUCTION

A digital signature (see box 4-4, "What Are Digital Signatures?") is used to authenticate the origin of a message or other information (i.e., establish the identity of the signer) and to check the integrity of the information (i.e., confirm that it has not been altered after it has been signed). Digital signatures are important to electronic commerce because of their role in substantiating electronic contracts, purchase orders, and the like. (See chapter 3 for discussion of electronic contracts and signatures, nonrepudiation services, and so forth.) The most efficient digital signature systems are based on public-key cryptography.

On May 19, 1994, the National Institute of Standards and Technology (NIST) announced that the Digital Signature Standard (DSS) was finalized as Federal Information Processing Standard (FIPS) 186.[1] Federal standards activities related to public-key cryptography and digital signatures had been proceeding intermittently at NIST for over 12 years. Some of the delay was due to national security concerns regarding the uncontrolled spreading of cryptographic capabilities, both domestically and internationally. The most recent delay has been due to patent-licensing complications and the government's desire to provide a royalty-free FIPS.

The algorithm specified in the DSS is called the Digital Signature Algorithm (DSA). The DSA uses a private key to form the digital signature and the corresponding public key to verify the signature. However, unlike encryption, the signature operation is not reversible. The DSA does not do

[1] NIST, "Digital Signature Standard (DSS)," FIPS PUB 186 (Gaithersburg, MD: U.S. Department of Commerce, May 19, 1994 (advance copy)). See also *Federal Register,* vol. 59, May 19, 1994, pp. 26208-11 for the Department of Commerce announcement "Approval of Federal information Processing Standard (FIPS) 186, Digital Signature Standard (DSS)."

NIST proposed the revised draft DSS in February 1993; NIST had announced the original version of the proposed DSS in August 1991. The finalized DSS has a larger maximum modulus size (up to 1,024 bits). The 1991 version of the proposed standard had a fixed modulus of 512 bits. Increasing the number of bits in the modulus increases strength, analogous to increasing the key size.

public-key encryption,[2] and the DSS does not provide capabilities for key distribution or key exchange.[3]

There is at present no progress toward a federal standard for public-key encryption, per se, and it appears unlikely that one will be promulgated.[4] Work had been proposed for a new key-management standard, but as of June 1994, NIST was not pursuing a new FIPS for key management or key exchanges The combination of the DSS and a key-management standard would meet user needs for digital signatures and secure key exchange, without providing a public-key encryption standard, per se.[6] The implementation of the Escrowed Encryption Standard (EES) algorithm that is used in data communications—in the Capstone chip-also contains a public-key Key Exchange Algorithm (KEA).[7] However, this KEA is not part of any FIPS.[8] Therefore, individuals and organizations that do not use the Capstone chip (or the TESSERA card, which contains a Capstone chip) will still need to select a secure form of key distribution.[9]

The National Bureau of Standards (NBS, now NIST) published a "Solicitation for Public Key Cryptographic Algorithms" in the *Federal Register* on June 30, 1982. According to the results of a classified investigation by the General Accounting Office (GAO), NIST abandoned this standards activity at the request of the National Security Agency (NSA). According to GAO:

> RSA Data Security, Inc., was willing to negotiate the rights to use RSA [named for the inventors of the algorithm, Drs. Ronald Rivest, Adi Shamir, and Leonard Adleman]—the most widely accepted public-key algorithm-as a federal standard, according to a NIST representative. NSA and NIST met several times to discuss NSA concerns regarding the 1982 solicitation. However, NIST terminated the public-key cryptographic project because of an NSA request, according to a 1987 NIST memo-

Z The DSS does not specify an encryption algorithm; encryption is a "two-way" function that is reversible, via decryption. The DSS specifies a "one-way" function. The DSS signature is generated from a shorter, "digest" of the message using a private key, but the operation is not reversible. Instead, the DSS signature is verified using the corresponding public key and mathematical operations on the signature and message digest that are different from decryption. Burton Kaliski, Jr., Chief Scientist, RSA Data Security, Inc., personal communication, May 4, 1994.

[3] According to F. Lynn McNulty, Associate Director for Computer Security, NIST, the rationale for adopting the technique used in the DSS was that, "We wanted a technology that did signatures-and nothing else-very well." (Response to a question from Chairman Rick Boucher in testimony before the Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994.)

[4] See U.S. Genera] Accounting Office, *Communications Privacy: Federal Policy and Actions, GAO/OS l-94-2* (Washington, DC: U.S. Government Printing Office, November 1993), pp. 19-20.

[5] F. Lynn McNulty, Associate Director for Computer Security, NIST, personal communication, May 25, 1994.

There is a 1992 FIPS on key management that uses the Data Encryption Standard (DES) in point-to-point environments where the parties share a key-encrypting key that is used to distribute other keys. NIST, "Key Management Using ANSI X9. 17," FIPS PUB 17 I (Gaithersburg, MD: U.S. Department of Commerce, Apr. 27, 1992). This FIPS specifies a particular selectionof options for federal agency use from the ANSI X9. 17-1985 standard for "Financial Institution Key Management (Wholesale)."

[6] But the ElGamal algorithm upon which the DSS is based does provide for public-key encryption. Stephen T. Kent, Chief Scientist, Bolt Beranek and Newman, Inc., personal communication, May 9, 1994.

[7] The Capstone chip is used for data communications and contains the EES algorithm (called SKIPJACK), as well as digital signature and key exchange functions. (The Clipper chip is used in telephone systems and has just the EES algorithm.) TESSERA is a PCMCIA card with ii Capstone chip inside. It includes additional features and is being used in the Defense Message System. Clinton Brooks, Special Assistant to the Director, National Security Agency, personal communication, May 25, 1994.

[8] Miles Smid, Manager, Security Technology Group, NIST, personal communication, May 20, 1994.

[9] One public-key algorithm that can be used for key distribution is the "RSA" algorithm; the RSA algorithm can encrypt. (The RSA system was proposed in 1978 by Rivest, Shamir, and Adleman.) The Diffie-Hellman algorithm is another method that can be used for key generation and exchange, but does not encrypt. The public-key concept was first published by Whitfield Diffie and Martin Hellman in "New Directions in Cryptography," *IEEE Transaction on Information Theory, vol. IT-22, No. 6,* November 1976, pp. 644-654. Diffie and Hell man also described how such a system could be used for key distribution and to "sign" individual messages.

randum. The 1982 NIST solicitation was the last formal opportunity provided for industry, academia, and others to offer public-key algorithms for a federal standard and to participate in the development of a federal public-key standard that could support key management/exchange. [10]

CHOICE OF A SIGNATURE TECHNIQUE FOR THE STANDARD

In May 1989, NIST again initiated discussions with NSA about promulgating a public-key standard that could be used for both signatures and key exchange. These NIST/NSA discussions were conducted through the Technical Working Group (TWG) mechanism specified in the memorandum of understanding between the agencies, which had been signed several weeks earlier (see chapter 4). According to NIST memoranda, the NIST members of the TWG had planned to select a public-key algorithm that could do both signatures and key exchange. This plan was terminated in favor of a technique developed by NSA that only did signatures. [11] A patent application for the DSS technique was filed in July 1991; patent number 5,231,668 was awarded to David Kravitz in July 1993. The patent specification describes the signature method as a variant of the ElGamal signature scheme based on discrete logarithms. [12] The invention, developed under NSA funding, was assigned to the United States of America, as represented by the Secretary of Commerce.

According to GAO, the NIST members of the working group had wanted an unclassified algorithm that could be made public, could be implemented in hardware and software, and could be used for both digital signatures and key management. [13] NIST and NSA members of the Technical Working Group met frequently to discuss candidate algorithms; according to GAO, the NIST members preferred the RSA algorithm because it could perform both functions (i.e., sign and encrypt), but NSA preferred its own algorithm that could sign but not encrypt.

At the time these Technical Working Group discussions were taking place, many in the private sector expected that NIST would release a public-key standard—probably based on the RSA algorithm—as early as 1990. Major computer and software vendors were reportedly hoping for a federal public-key and signature standard based on the RSA technique because it was already in-

[10] General Accounting Office, op. cit., footnote 4, p. 20.

[11] General Accounting Office, op. cit., footnote 4, pp. 20-2 I; and the series of NIST/NSA Technical Winking Group minutes from May 1989 to August 1991, published in "Selected NIST/NSA Documents Concerning the Development of the Digital Signature Standard Released in *Computer Professionals for Social Responsibility v. National Institute of Standards and Technology*, Civil Action No. 92-0972," Computer Professionals for Social Responsibility, *The Third Cryptography and Privacy Conference Source Book*, June 1993 (see Note in footnote 14 below). See also D.K. Branstad and M.E. Smid, "Integrity and Security Standards Based on Cryptography, "*Computers & Security, vol. 1, 1982,* pp. 255-260; Richard A. Danca, "Torricelli Charges NIST with Foot-Dragging on Security," *Federal Computer Week,* Oct. 8, 1990, p. 9; and Michael Alexander, "Data Security Plan Bashed," *Computerworld*, July 1, 1991, p. 1

[12] See: U.S Patent 5,23 1,668 (Digital Signature Algorithm; David W. Kravitz), "Background of the Invention." See also Taher ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory, vol.* IT-31, No. 4, July 1985.

[13] See Genera] Accounting Office, 0p. cit., footnote 4, pp. 20-21.

[14] Ibid GAO based this conclusion on NIST memoranda. See also NIST memoranda obtained through Freedom of Information Act (FOIA) litigation and published as "Selected NIST/NSA Documents," op. cit., footnote 11. (Note: According to NSA officials, the FOIA'd materials are not a true picture of all the different levels of discussion that took place during this period, when NIST management and NSA were in agreement regarding the development of a signature standard. Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.)

eluded in their products, and they hoped they would not have to support both a federal standard *and* a de facto industry standard (RSA).[15] NIST's announcement that it would instead propose a different technology as the standard was greeted with severe industry criticisms and industry announcements of plans to jointly affirm RSA as the de facto industry signature standard. [16]

NIST proposed the original version of the DSS (with the NSA algorithm anda512-bit modulus) in the *Federal Register* in August 1991.[17] NIST's August 1991 request for comments generated a number of severe criticisms during the initial comment period and afterward. Criticisms focused on both the choice of signature method[18] itself and the process by which it was selected, especially NSA's role. Countering allegations that NSA had dictated the choice of standard, F. Lynn McNulty (Associate Director for Computer Security, NIST) stated that:

> NIST made the final choice. We obtained technical assistance from NSA, and we received technical inputs from others as well, but [NIST] made the final choice.[19]

McNulty also pointed to the fact that NSA had approved the DSS for use with some classified data as proof of its soundness.

In early 1992, the Computer System Security and Privacy Advisory Board (CSSPAB) advised NIST to delay a decision on adopting a signature standard pending a broad national review on the uses of cryptography.[20] Noting the significant public policy issues raised during review of the proposed signature standard, the CSSPAB unanimously approved a resolution to the effect that: "a national level public review of the positive and negative implications of the widespread use of public and secret key cryptography is required" in order to produce a "national policy concerning the use of cryptography in unclassified/sensitive government [sic] and the private sector" by June 1993.[21] The CSSPAB also approved (but not unanimously) a resolution that the Secretary of

[15] Industry supporters of a federal signature standard based on RSA included Digital Equipment Corp., Lotus Development Corp., Motorola, Inc., Novell, Inc., and, of course, RSA Data Security, Inc. Ellen Messmer. "NIST To Announce Public Key Encryption Standard," *Network World,* July 23, 1990, p. 7; and G. Pascal Zachary, "U.S. Agency Stands in Way of Computer-Security Tool," *The Wall Street Journal*, July 9, 1990.

[16] Critics claimed the technique was t(M) slow for commercial use and did not offer adequate protection. At least six major computer vendors (Novell, Inc., Lotus Development Cm-p., Digital Equipment Corp., Sun Microsystems, Inc., Apple Computer, Inc., and Microsoft Corp.) had endorsed or were expected to endorse RSA's signature system. Michael Alexander, "Encryption Pact in Works," *Computerworld*, Apr. 15, 1991; and Michael Alexander, "Data Security Plan Bashed," *Computerworld*, July 1, 1991, p. 1. (Note: The original technique was refined to offer more security by increasing the maximum size of the modulus.)

[17] *Federal Register*, Aug. 30, 1991, pp. 42980-82, NIST's announcement of the proposed standard stated the intention Of making the DSS technique available worldwide on a royalty-free basis in the public interest. N] ST stated the opinion that no other patents would apply to the DSS technique.

[18] The final DSS technique specified in the standard is stronger than the one originally proposed; in response to public comment, the maxirnum modulus size was increased.

[19] Richard A. Danca, "NIST Signature Standard Whips Up Storm of Controversy from Industry," *Federal Computer Week*, Sept. 2, 1991. p. 3.

[20] Minutes of the Mar. 17-18, 1992 meeting Of the CSSPAB (available from NIST). See also Darryl K. Taft, "Board Finds NIST's DSS Unacceptable," *Government Computer News, Dec. 23,* 1991, pp. 1,56; and Kevin Power, "Security Board Calls for Delay on Digital Signature," *Government Computer News,* Mar. 30, 1992, p. 114. In the public comments, negative responses outnumbered endorsements of the DSS by 90 to 13 (Power, ibid.).

[21] CSSPAB Resolution No. 1 of Mar. 18, 1992. The CSSPAB endorsed the National Research Council's study of national cryptography policy that was chartered in Public Law 103- I 60 as the study that "best accomplishes" the board's "repeated calls" (in Resolution No. 1 and subsequently) for a national review. CSSPAB Resolution 93-7, Dec. 8-9, 1993.

Commerce should only consider approval of the proposed DSS upon conclusion of the national review,[22] and unanimously approved another resolution that the board defer making a recommendation on approval of the proposed DSS pending progress on the national review.[23]

Criticism of the 1991 version of the proposed DSS—targeted at technology and process-continued to mount. At hearings held by the House Subcommittee on Economic and Commercial Law in May 1992, GAO testified that the DSS (at that time, with a 512-bit modulus) offered such weak protection that it raised questions as to whether "any practical purpose would be served" by requiring federal agencies to use it, especially since the private sector would continue to use the more effective commercial products on the market. Other questions and concerns were targeted more generally at U.S. cryptography policies and the extent to which NIST "had the clout" to resist pressure from NSA and the Federal Bureau of Investigation, or "had the upper hand" in negotiations and standards-setting procedures. The Computer Professionals for Social Responsibility (CPSR) noted that NIST was required by the Computer Security Act to develop "cost-effective" methods to safeguard information. Because the chosen DSS technique did not provide confidentiality, CPSR questioned the extent to which NSA's interest in signals intelligence dictated the choice of technology.[24]

During this period, NIST continued to work on a revised version of the DSS, strengthening it by increasing the maximum size of the modulus (up to 1,024 bits). Ways were found to implement the algorithm more efficiently.[25] A companion *hashing (i.e.,* condensing) standard was issued; hashing is used to create the condensed *message digest* that is signed.[26] NIST also formed an interagency group to study how to implement DSS, and contracted with MITRE[27] to study alternatives for automated management of public keys used for signatures.[28] The revised draft DSS **was** issued **in** February 1993 as FIPS Publication XX.

While NIST pursued the Digital Signature Standard, Computer Professionals for Social Responsibility sought to obtain NIST memoranda documenting the NIST/NSA Technical Working Group discussions related to the DSS and the aborted federal public-key standard. CPSR charged that the DSS was purposely designed to minimize privacy protection (i.e., encryption capabilities) and that the actions of NIST and NSA's had contravened the Computer Security Act of 1987. CPSR based these charges on documents re-

[22] CSSPAB Resolution No. 2 of Mar. 18,1992.

[23] CSSPAB Resolution No.3 of Mar. 18, 1992.

[24] See Kevin Power, "DSS Security Weak, GAO Official Testifies," *Government Computer News,* May 1 I, 1992, pp. 1, 80. The hearings were held on May 8, 1992. (Note: Discussion of strength and efficiency is in the context of the original (1991) proposal, witha512-bit modulus.)

[25] See E.F. Brickell et al., "Fast Exponentiation with Precomputation" *Advances in Cryptology—Eurocrypt '92,* R.A. Rueppel (cd.) (New York, NY: Springer-Verlag, 1992), pp. 200-207.

[26] NIST, *'Secure Hash Standard," FIPS PUB 180, (Gaithersburg, MD: U.S. Department of Commerce, May 11, 1993). The Secure Hash Algorithm specified in the hash standard may be implemented in hardware, software, and/or firmware. It is subject to Department of Commerce export controls. (See also Ellen Messmer, "NIST Stumbles on Proposal for Public-Key Encryption," *Network World,* July 27, 1992, pp. 1,42 -43.)

In April 1994, NIST announced a technical correction to the Secure Hash Standard. NSA had developed the mathematical formula (hat underlies the hash standard; NSA researchers subsequent y discovered a "minor flaw" during their continuing evaluation process. (NIST media advisory, Apr. 22, 1994.) According to NIST, the hash standard, "while still very strong, was not as robust as we had originally intended" and was being corrected. Raymond Kammer, Deputy Director, NIST, Testimony Before the Senate Committee on the Judiciary, May 3, 1994, p. 1 I.

[27] MITRE Corp., "public Key Infrastructure Study (Final Repro)," April 1994. (Available from NIST.)

[28] The final DSS notes that: "A means of associating public and private key pairs to the corresponding users is required...[A] certifying authority could sign credentials containing a user's public key and identity to form a certificate. Systems for certifying credentials and distributing certificates are beyond the scope of this standard. NIST intends to publish separate document(s) on certifying credentials and distributing certificates."' NIST, FIPS PUB 186, op. cit., footnote 1, p. 6.

ceived from NIST after litigation under the Freedom of Information Act,[29] and asked the House Judiciary Committee to investigate.[30]

As part of the Defense Authorization Bill for FY 1994, the Committees on Armed Services, Intelligence, Commerce, and the Judiciary have asked the National Research Council to undertake a classified, two-year study of national policy with respect to the use and regulation of cryptography.[31] The study is expected to be completed in summer 1996 and has been endorsed by the CSSPAB as best accomplishing its repeated calls for a broad national review of cryptography.[32]

PATENT PROBLEMS FOR THE DSS

Patents had always been a concern in developing any federal public-key or signature standard. One reason NIST gave for not selecting the RSA system as a standard was the desire to issue a royalty-free FIPS. A royalty-free standard would also be attractive to commercial users and the international business community. An approach using RSA technology would have required patent licenses. When the inventors of the RSA, Ronald Rivest, Adi Shamir, and Leonard Adleman, formed RSA Data Security, Inc. in 1982, they obtained an exclusive license for their invention[33] from the Massachusetts Institute of Technology (MIT), which had been assigned rights to the invention.

Other patents potentially applied to signature systems in general. In the early 1980s, several pioneer patents in public-key cryptography had been issued to Whitfield Diffie, Martin Hellman, Stephen Pohlig, and Ralph Merkle, all then at Stanford University. Although the government has rights in these inventions and in RSA, because they had been developed with federal funding, royalties for commercial users would have to be negotiated if a federal standard infringed these patents.[34] Another patent that was claimed by the grantee to apply to the DSS technique had been issued to Claus Schnorr in 1991, and the government did not have rights in this invention .[35]

Stanford and MIT granted Public Key Partners (PKP) exclusive sublicensing rights to the four Stanford patents and the RSA patent. PKP also holds exclusive sublicensing rights to the Schnorr patent.[36] It is a private partnership of organizations (including RSA Data Security, Inc.) that develops and markets public-key technology, In an attempt to minimize certain royalties from use of the DSS, NIST proposed to grant PKP an exclusive license to the government's patent on the technique used in the DSS. What was proposed was a cross-license that would resolve patent disputes with PKP, without lengthy and costly litigation to determine which patents (if any) were infringed by DSS. PKP would make practice of the DSS technique royalty-free for personal, noncommercial, and U.S. federal, state, and local government uses. Only parties that enjoyed commercial benefit from making or selling products

[29] NIST memoranda published as. "Selected NIST/NSA Documents," op. cit., footnote l I. (See Note in footnote 14 above.)

[30] Richard A. Danca, "CPSR Charges N] ST, NSA with Violating Security Act," *Federal Computer Week,* Aug. 24, 1992, pp. 20, 34.

[31] Announcement from (he Computer Science and Telecommunication Board, National Research Council, Dec. 7, 1993.

[32] CSSPAB Resolution 93-7, Dec. 8-9, 1993.

[33] U.S. Patent 4,405,829 (Cryptographic Communication System and Method; Ronald Rivest, Adi Shamir, and Lenard Adleman, 1983).

[34] U.S. patents 4,200,770 (Cryptographic Apparatus and Method; Martin Hellman, Whitfield Diffie, and Ralph Merkle, 1980); 4,218,582 (Public Key Cryptographic Apparatus and Method; Martin Hellman and Ralph Merkle, 1980); 4,424,414 (Exponentiation Cryptographic Apparatus and Method; Hellman and Pohlig, 1984); and 4,309,569 (Method of Providing Digital Signatures; Merkle, 1982) are all assigned to Stanford University.

Stanford considers that the -582 patent covers any public key system in any implementation (including RSA); variations of the -582 patent have been issued in I I other countries. Robert B. Fougner, Director of Licensing, Public Key Partners, letter to OTA, Nov. 4, 1993.

[35] Patent 4995,082 (Claus p. Schnorr; Method for Identifying Subscribers and for Generating and Verifying Electronic Signatures in a Data Exchange System, 1991). The patent was applied for in February 1990.

[36] Fougner, op. cit., footnote 34.

incorporating the DSS technique, or from providing certification services, would be required to pay royalties according to a set schedule of fees.[37]

The government announced that it had waived notice of availability of the DSS invention for licensing because expeditious granting of the license to PKP would "best serve the interest of the federal government and the public."[38] The arrangement would allow PKP to collect royalties on the DSS for the remainder of the government 17-year patent term (i.e., until 2010); most of the patents administered by PKP would expire long before that. However, the Schnorr patent had an almost equivalent term remaining (until 2008); so the arrangement was seen as an equitable tradeoff that would avoid Litigation.[39]

Some saw the PKP licensing arrangement as lowering the final barrier to adoption of DSS.[40] However, others-including the CSSPAB—questioned the true cost[41] of the DSS to private-sector users under this arrangement:

> The board is concerned that:
>
> 1. the original goal that the Digital Signature Standard would be available to the public on a royalty-free basis has been lost; and
> 2. the economic consequences for the country have not been addressed in arriving at the Digital Signature Algorithm exclusive licensing arrangement with Public Key Partners, Inc.[42]

Ultimately, patent discussions had to be reopened, after a majority of potential users objected to the original terms and the Clinton Administration concluded that a royalty-free digital signature technique was necessary to promote its widespread use. NIST resumed discussions in early 1994, with the goal of issuing a federal signature standard "that is free of patent impediments and provides for an interoperability and a uniform level of security."[43]

ISSUANCE OF THE DIGITAL SIGNATURE STANDARD

In May 1994, the Secretary of Commerce approved the DSS as FIPS 186, effective December 1, 1994. It will be reviewed every five years in order to assess its adequacy. According to FIPS Publication 186, the DSS technique is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and origin authentication. The DSS can be implemented in hardware, software, and/or firmware and is to be subject to Commerce Department export controls. NIST is developing a validation program to test implementations of DSS for conformance to the standard. The DSS technique is available for voluntary private or commercial use.[44]

[37] *Federal Register*, June 8 1993, pp. 32105-06, "Notice of Prospective Grant of Exclusive Patent License." This includes an appendix from Robert Fougner stating PKP's intentions m licensing the DSS technology. The PKP licenses would include key management for the EES at no additional fee. Also, PKP would allow a three-year moratorium on collecting fees from commercial signature certification services. Thereafter, all commercial services that "certify a signatures authenticity for a fee" would pay a royalty to PKP (ibid., p. 32106).

[38] Ibid.

[39] OTA staff interview with Michael Rubin, Deputy Chief Counsel, NIST, Jan. 13, 1994.

[40] See Kevin Power, "With Patent Dispute Finally Over, Feds Can Use Digital Signatures," *Government Computer News*, June 21, 1993, pp. 1,86.

[41] See Kevin Power, '"Board Questions True Cost of DSS Standard," *Government Computer News*, Aug. 16, 1993, pp. 1, 107. Digital signatures (hence, the DSS) will be widely used in health care, electronic commerce, and other applications (see chapter 3).

[42] CSSPAB Resolution No. 93.4, July 30, 199.3. This was not unanimously adopted.

[43] *Federal Register*, May 19, 1994, op. cit., footnote 1, p. 26209.

[44] NIST FIPS PUB 186, op. cit., footnote 1, pp. 2.3, The DSS applies to all federal departments and agencies for use in protecting unclassified information that is not subject to the Warner Amendment (i.e., 10 USC sec.2315 and 44 USC sec. 3502(2)). It "shall he used in designing or implementing public-key based signature systems which federal departments and agencies operate or which are operated for them under contract." (I bid., p. 2).

The Federal Register announcement stated that NIST had “considered all the issues raised in the public comments and believes that it has addressed them.”[45] Among the criticisms and NIST responses noted were:

- criticisms that the Digital Signature Algorithm specified in the DSS does not provide for secret key distributions. NIST’s response is that the DSA is not intended for that purpose.
- criticisms that the DSA is incomplete because no hash algorithm is specified. NIST’s response is that, since the proposed DSS was announced, a Secure Hash Standard has been approved as FIPS 180.
- criticisms that the DSA is not compatible with international standards. NIST’s response is that is has proposed that the DSA be an alternative signature standard within the appropriate international standard (IS 9796).
- criticisms that DSA is not secure. NIST’s response is that no cryptographic shortcuts have been discovered, and that the proposed standard has been revised to provide a larger modulus size.
- criticisms that DSA is not efficient. NIST’s response is that it believes the efficiency of the DSA is adequate for most applications.
- criticisms that the DSA may infringe on other patents. NIST’s response is that it has addressed the possible patent infringement claims and has concluded that there are no valid claims.[46]

According to FIPS Publication 186, the Digital Signature Algorithm specified in the standard provides the capability to generate and verify signatures. A private key is used to generate a digital signature. A hash function (see FIPS Publication 180) is used in the signature generation process to obtain a condensed version, called a *message digest,* of the data that are to be signed. The message digest is input to the DSA to generate the digital signature. Signature verification makes use of the same hash function and a public key that corresponds to, but is different than, the private key used to generate the signature. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. The security of the DSS system depends on maintaining the secrecy of users’ private keys.[47]

In practice, a digital signature system requires a means for associating pairs of public and private keys with the corresponding users. There must also be a way to bind a user’s identity and his or her public key. This binding could be done by a mutually trusted third party, such as a certifying authority. The certifying authority could form a “certificate” by signing credentials containing a user’s identity and public key. According to FIPS Publication 186, systems for certifying credentials and distributing certificates are beyond the scope of the DSS, but NIST intends to publish separate documents on certifying credentials and distributing certificates.[48]

Although the DSS has been approved as a Federal Information Processing Standard, issues concerning the DSS have not all been resolved, particularly with respect to patent-infringement claims (see above) and the possibility of litigation.[49] As this report was completed, whether or not Public Key Partners would file suit was “still a pending question.” [50]

[45] *Federal Register,* May *19, 1994, op.* cit., footnote 1, p. 262@.

[46] Ibid.

[47] NIST, FIPS PUB 186, op. cit., footnote 1, pp. 1-3.

[48] Ibid., p. 6.

[49] See John Markoff, “U.S. Adopts a Disputed Coding Standard,” *The New York Times,* May 23, 1994, pp. D1, D8.

[50] Robert B. Fougner, Director of Licensing, Public Key Partners, Inc., personal communication, June 24, 1994.