Public Comments Regarding FIPS 186-1,
Digital Signature Standard (DSS)
[in response to a notice in the December 15, 1998 Federal Register
(Volume 63, Number 240; pages 69049-69051)]

From: tjcasar@its.cse.dnd.ca
To: fips186rsa@nist.gov
Cc: kodonaldson@its.cse.dnd.ca, alpoplove@its.cse.dnd.ca,
rjsmith@its.cse.dnd.ca, foti@csmes.ncsl.nist.gov
Subject: Comments on FIPS 186-1
Date: Thu, 21 Jan 1999 15:32:00 -0500
X-Mailer: Internet Mail Service (5.0.1460.8)

Dear Sir/Madam;

In response to your request for comments for the allowance of RSA signature technology within DSS, I applaud this recent initiative to include the RSA algorithm as defined in ANSI X9.31, as it already has widespread use within the cryptographic community.

Since ANSI has also just released X9.62, and the first phase of public comments for FIPS 186-1 has not yet been completed, I would like to propose that you consider the inclusion of Elliptic Curve digital signatures as defined by X9.62 as well. These type of algorithms are also being commonly used, particularly within devices constrained by speed and memory (i.e., smart cards). It would be a shame to ignore this recent ANSI development at this point, particularly since X9.31 and X9.62 have been released within a few weeks of each other.

Sincerely,
Tom Casar

Tom Casar, P.Eng.
Cryptographic Systems Evaluation Engineer
COMSEC Evaluation Unit
Information Protection Group
Communications Security Establishment
P.O. Box 9703, Terminal
719 Heron Rd.
Ottawa, ON, K1G 3Z4
Tel: (613) 991-7202
Fax: (613) 991-7251

From: john.purcell@gsa.gov
Date: 28 Jan 99 13:43:00 -0500
To: fips186rsa@nist.gov

Comments on FIPS 186-1 from Office of Governmentwide Security, Office of Information Security, GSA.

-- John Purcell

COMMENTS ON FIPS 186-1, DSS, AND REQUEST FOR COMMENTS

On behalf of Judith Spencer, Director, Governmentwide Security, Office of Information Security, GSA, I am replying to the Request for Comments with regard to FIPS 186-1.

This office is in favor of the approval for using the Rivest-Shamir-Adelman (RSA) digital signature technique, described by the X9.31 standard of the American National Standards Institute, along with the Digital Signature Algorithm (DSA) within the context of the Digital Signature Standard prescribed by FIPS 186-1. This office is aware of the commercial implementations of RSA in secure electronic commerce products, and agrees that the predominance of RSA in these products makes the RSA technique a logical addition to the standard. Adoption of RSA will add to the interoperability of these products.

This office also favors the approval of another digital signature technique, Elliptic Curve (ANSI Standard X9.62), for addition to the Digital Signature Standard. We feel the EC-DSA is also secure, and has a significant, growing market share of secure electronic commerce products. We recommend that the addition of these two digital signature techniques be combined in the approval within the FIPS 186-1.

Date: 08 Feb 1999 11:30:10 -0700
From: Mona M Sana <Mona.M.Sana@aexp.com>
To: FIPS186RSA <FIPS186RSA@nist.gov>
cc: Bonnie Howard <Bonnie.Howard@aexp.com>,
Alan J Zausner <Alan.J.Zausner@aexp.com>,
Glenn Weiner <Glenn.Weiner@aexp.com>
Subject: ECDSA should be included in the FIPS 186 upate

We support the NIST's decision to update FIPS 186 to include the RSA Digital Signature Standard (X9.31). But we feel that the update will not be complete until FIPS 186 is amended to include the newly passed Elliptic Curve Digital Signature Algorithm (ANSI -X9.62). The significant improvements in performance, size, and cost of ECC over RSA or DSA can have a marked effect on the Card industry and makes ECDSA's inclusion critical.

Regards,
Mona Sana (American Express Technologies)

From: Robert Zuccherato <robert.zuccherato@entrust.com>
To: "'FIPS186RSA@nist.gov'" <FIPS186RSA@nist.gov>
Subject: FIPS 186-1 Comments
Date: Tue, 16 Feb 1999 13:39:27 -0500
X-Mailer: Internet Mail Service (5.5.1960.3)

Below you will find Entrust's response to the Request For Comments on FIPS 186-1. A copy has also been sent by regular mail.

To: Director, Information Technology Laboratory

Entrust enthusiastically supports the inclusion of the RSA digital signature algorithm as an allowed alternative within FIPS 186-1 (Digital Signature Standard). In particular we welcome the recommendation that separate keys should be used for signatures and for confidentiality. This recognizes the fact that many users require recovery of confidentiality keys while still being able to support non-repudiation with signature keys. This is a positive step.

However, we are concerned about the requirement that the RSA algorithm must be implemented as specified in ANSI X9.31.

The ANSI X9.31 standard requires the use of "strong primes". These are primes, p, such that both p+1 and p-1 are divisible by large prime factors. At one time it was considered prudent to use primes of this form for computing an RSA modulus in order to prevent certain factoring attacks which took advantage of primes of this form (e.g. the Pollard p-1 and related special purpose attacks). However, most cryptographers today agree that the development of the number field sieve and the associated increase in RSA modulus size (to 1024, or even 2048 bits) has eliminated the need to use these special primes. Even "first party attacks" where a user purposely chooses a prime vulnerable to these attacks are not a concern because such primes are very rare, and thus any user that does have a modulus containing such a prime has, with overwhelming probability, generated that prime for malicious purposes. By mandating the use of these primes we are imposing an additional constraint on developers which is not required. We would recommend that this requirement be removed.

In addition, the X9.31 standard requires the use of an encoding method based on one included in the international standard ISO/IEC 9796. While we have no technical concerns with this particular technique, we would like to note that most North American implementations of RSA use the encoding method specified in RSA Laboratory's PKCS #1. Thus, most implementers will have to implement two different encoding methods and support both of them for a considerable amount of time. There are no known attacks on either the 9796 or the PKCS #1 method, so either choice would be acceptable. However, we believe that the PKCS #1 encoding method should at least be allowed by the DSS.

The X9.31 standard places a number of conditions on the private prime factors of the RSA modulus. This includes the use of "strong primes", conditions on the size of the primes, conditions on the distance between the primes, the method of generating the prime, etc. It is unclear at this time how one

would validate that a given implementation is actually generating primes that satisfy all of these conditions. For increased security, many implementations will not allow users direct access to their private keys, and thus direct examination of the primes may not be feasible. Even if direct access is obtained, some conditions, like the method used to generate the prime, may not be evident from examining the primes themselves. While there is presently research being conducted into zero knowledge techniques that will allow third parties to verify some or all of these conditions, we would recommend that NIST not require implementations to include these techniques within their RSA code. The techniques that are currently being proposed require a large number of rounds to complete and are quite complex to code. They would greatly increase not only the code size, but also the difficulty in producing a valid implementation.

Thank you for this opportunity to comment,

Dr. Robert Zuccherato
Cryptographic Specialist
Entrust Technologies

From: "Stapleton, Jeff" <jstapleton@kpmg.com>
To: FIPS186RSA@nist.gov
Cc: "Van Ranst Jr., Alfred F" <avanranst@kpmg.com>,
"Mannal, Robert H"
<rmannal@kpmg.com>
Subject: DSS/X9.31 Comments
Date: Mon, 8 Feb 1999 18:58:26 -0500
X-Mailer: Internet Mail Service (5.5.2448.0)

KPMG LLP per Jeff Stapleton, would like to submit the following comments:

1. As the editor for ANSI X9.31 (during my previous employment at Security Dynamics/RSA Laboratories), I would like to thank NIST for revising FIPS 186 and considering the detailed work that was accomplished by the X9F1 working group. In particular, I would like to express my appreciation to Bob Silverman (RSA Labs) for his mathematical expertise in developing the standard.

2. In parallel with the development of ANSI X9.31, the X9F1 working group was also developing ANSI X9.62 ECDSA. This standard is the DSS analogy using elliptic curve cryptography. The revision of FIPS 186 should also include ANSI X9.62, in addition to ANSI X9.31, for the following reason's;

2a. The ANSI X9.62 standard, approved in January 1999, underwent the same rigorous X9F1 working group review used for X9.31. In fact, due to the nature of the unfamiliar mathematics, the working group spent additional time on this standard.

2b. Several manufacturers are employing elliptic curve cryptography for low band width devices, most notably in the wireless industry, such as pagers and cell phones. This supports the government's COTS program.

2c. Several manufacturers are employing elliptic curve cryptography for low capacity devices, such as hand-held PDAs. This supports the government's COTS program.

3. The X9 Accredited Standards Committee, in conjunction with NIST and in the spirit of NVLAP, is developing the X9 Technical Guideline 19, which will address the conformance testing required by NIST.

From: Michael Crerar <mcrerar@dvnet.com>
To: "'FIPS186RSA@nist.gov'" <FIPS186RSA@nist.gov>
Subject: ECDSA and FIPS 186
Date: Tue, 2 Mar 1999 16:39:57 -0500
X-Mailer: Internet Mail Service (5.5.1960.3)

Dear Sirs:

Diversinet Corporation is a leading provider of digital certificate management tools and a developer of public-key infrastructure (PKI) products providing authentication and authorization platforms for cable, wireless and smart cards. Our head office is in Toronto, Canada with sales offices in San Jose, California and McLean, Virginia.

Regarding the proposed FIPS 186-1, Diversinet requests that NIST extend FIPS 186 to include the ability to conform to ANSI X9.62 ECDSA. We request this because:

(1) ECDSA is becoming more widely available in the marketplace. The FIPS Digital Signature Standard should endorse this recognized standard to ensure these commercial implementations provide a high level of security.

(2) ECDSA has advantages over other digital signature protocols in terms of key size, signature size and computational efficiency. It can be used to implement a secure authentication mechanism in less powerful devices such as smartcards, pagers and personal digital assistants.

(3) ECDSA is based on a different hard mathematical problem from other signature schemes, giving users a FIPS alternative in the event of a mathematical breakthrough in these other problems.

We thank you for your consideration of this matter.

Sincerely,

Michael Crerar
Diversinet Corporation

==========
Michael Crerar
Cryptographer, Diversinet Corp.

200 Yorkland Blvd.
Suite 605
Toronto, Canada
M2J 5C1

Phone: 416.756.2324 ext. 239
Fax: 416.756.7346
Toll Free: 800.357.7050
http://www.dvnet.com/

e-mail: mcrerar@dvnet.com

The Passport To Secure Commerce
==========

X-Lotus-FromDomain: CERTICOM
From: "William Lattin" <wlattin@certicom.com>
To: FIPS186RSA@nist.gov
Date: Wed, 3 Mar 1999 17:40:51 -0800
Subject: Request to include ECDSA in FIPS 186-1

Note to NIST: The original of this letter has been mailed by US mail.
Thank you again for your consideration. Bill Lattin, SECG Chair.

Information Technology Laboratory
ATTN: DSS/X9.31 Comments
National Institute of Standards and Technology
100 Bureau Drive Stop 8970
Gaithersburg, MD 20899-8970

1 March 1999

Subject: Request to include ECDSA in FIPS 186-1

Dear Sirs:

The Standards for Efficient Cryptography Group (SECG) is a multinational industry consortium committed to the development and use of Elliptic Curve Cryptography (ECC) for information security purposes in commercial and governmental applications.

Regarding the proposed FIPS 186-1, the SECG requests that NIST further extend FIPS 186 to include the ability to conform to ANSI X9.62 ECDSA, for the following reasons:

1. ECDSA is based on a different hard problem than RSA or DSA signatures. All three methods are recognized by ANSI X9 and are being recognized by ISO SC27, IEEE P1363, IETF, and other standards bodies. The FIPS Digital Signature Standard should encompass the same commercially-endorsed technology to ensure FIPS-conformant products will be able to use off-the-shelf technology.

2. X9.62 is the first digital signature standard to include specification of methods for domain parameter validation and public key validation - critical features for those users which wish additional assurance that:

(i) there was not a calculation error during key pair generation; and
(ii) no one was trying to use a false or spoofed set of domain parameters
or a false public key that would void all intended security.

3. ECDSA offers technical advantages in the areas of key size, certificate size, and performance over other digital signature methods. Its smaller data structures and calculation efficiencies enable it to be used in specific applications in which either RSA or DSS would be very difficult or expensive to

implement. As an example, the lowest cost smart cards (8-bit CPU and no cryptographic coprocessor) can be used to realize practical implementations of ECDSA, but not of RSA or DSA.

SECG DSS/X9.31 Comments

4. When the public key infrastructure model being used assumes that each user generates his or her own public/private key pair, choosing ECDSA means that more systems will be able to meet that assumption than if RSA and DSA are the only options.

5. ECDSA-enabled products and applications are currently available in the market. These include smart cards, hardware accelerators, certificate authorities, and EDI/financial applications. Elliptic Curve Cryptography is currently used in a number of commercial and government applications, including the US Postal Service IBIP program.

Members of the SECG include the following companies: 3Com, ABN-AMRO, American Express, Baltimore Technologies, Certicom, Deloitte & Touche, Diversinet, Ernst & Young, Fujitsu, Giesecke & Devrient, GlobeSet, GTE CyberTrust, Hewlett-Packard, Hitachi Ltd., Indicii Salus, Inter Clear Service Ltd., LPK Information Integrity Ltd., Motorola, NTT Electronics Corporation, Pitney Bowes, Rainbow Technologies, Thawte Consulting, Visa International and Xcert International. Additional information on the SECG may be found at our website, www.secg.org.

Should you wish any additional information, please feel free to contact the undersigned at 650/312-7991.

We thank you for your careful consideration of this matter.

Sincerely,

William L. Lattin
SECG Chair

From: dawn_adams@ott.lgs.ca
Date: Wed, 03 Mar 1999 11:06:33 -0500
Subject: The inclusion of ECDSA in FIPS 186-1
To: fips186rsa@nist.gov
X-Lotus-FromDomain: LGS

I have read the letter that was generated by the SECG advocating the inclusion of ECDSA in the FIPS 186-1 standard
and I agree with the statements provided by the standards group.

Dawn Adams
DOMUS ITSL

From: Dan Massey
To: "'FIPS186RSA@nist.gov'"
Subject: Including ECDSA in DSS - FIPS 186
Date: Thu, 4 Mar 1999 10:53:24 -0600
X-Mailer: Internet Mail Service (5.5.2232.9)

While adding ANSI 9.31 to DSS - FIPS 186 is valuable to some, the Digital Signature Standard should also include ECDSA (ANSI 9.62). As a developer of software for small devices I feel that ECDSA is necessary to complete DSS availability to the wide range of platforms, devices, and environments that exist today.

The banking community (through ANSI) and NIST itself (in the Minimum Interoperability Specification for PKI Components) agree that the three most important and prevalent digital signature algorithms in the industry today are: RSA, DSA, and ECDSA.

The size, performance and cost of elliptic curve cryptography makes the inclusion of ECDSA in the standard critical if Federal Agencies are going to enjoy the benefits of smart cards, iButtons, handheld devices, etc. From experience I know ECDSA smart cards can be as much as half the price of similar RSA or DSA cards and provide faster execution. We have also found the performance of RSA and DSA is poor on handheld systems when compared to ECDSA.

As a developer I would like to know that my software on limited devices will interoperate with DSS - FIPS 186 compliant systems.

-Dan Massey
dmassey@wholebrain.com

From: TomPLarson@aol.com
Date: Tue, 9 Mar 1999 22:50:19 EST
To: FIPS186RSA@nist.gov
Cc: lpretty@baltimoreinc.com
Subject: (no subject)
X-Mailer: AOL 4.0 for Windows 95 sub 13

Baltimore Inc. is an organization providing leading PKI products to the global market. We have developed our products to adhere to industry standards and have taken an algorithm independent approach.

Based on existing standards including ANSI, ISO and IEFT, we feel that RSA, DSA and ECDSA are mature and cryptographically secure algorithms. As a result, we support all three of these algorithms in our products.

We are pleased to hear that NIST is planning to include RSA (ANSI X9.31), in addition to DSA , in the FIPS 186. However, given the benefits of smaller key size and improved performance offered by ECDSA, we feel that FIPS 186 should also include ECDSA (ANSI X9.62).

Adding ECDSA to the standard will complete the full spectrum of platforms, devices, and environments that can be serviced by DSS compliant systems. The significant improvements in performance, size and cost of elliptic curve crypto over either RSA or DSA make ECDSA's inclusion in the standard critical if Federal Agencies are to take advantage of the most efficient and cost effective products on the market.

For example ECDSA is well suited to wireless and embedded systems and result in low cost smart cards with full strength signing cabability.

Regards,
Tom Larson
CEO, American Operations
Baltimore, Inc.
101 E. Park Blvd., Suite 600
Plano, TX 75074

X-Lotus-FromDomain: CERTICOM
From: "Jennifer Lombardi" <jlombard@certicom.com>
To: fips186rsa@nist.gov
cc: "Skip Hirsh" <shirsh@certicom.com>
Date: Wed, 10 Mar 1999 14:11:48 -0500
Subject: Certicom Comments of FIPS 186

Dear Sirs,

Certicom supports NIST's efforts to update FIPS 186.

We believe it is appropriate to include well-studied, commercially available signature methods in FIPS 186. This enables federal agencies to employ the method best suited to provide cost-effective security in their computing environments.

The addition of RSA to FIPS 186 is therefore a step in the right direction. However we strongly believe that FIPS 186 should additionally support ANSI X9.62 ECDSA as well as DSA and RSA.

ECDSA would represent a valuable addition to the DSS because:

- Elliptic curve cryptography offers efficiency advantages over other techniques. This means ECDSA is capable of reducing workload in servers and functioning on constrained devices like smart cards. ECDSA therefore represents the most cost-effective means to provide signature functionality in many environments.

- Addition of ECDSA would complete support in FIPS 186 for the three prevalent signature schemes today: DSA, ECDSA, and RSA. The importance of these three techniques is recognized worldwide - in particular by ANSI, ISO, and NIST (see for example NIST's Minimum Interoperability Specification for PKI Components).

- ECDSA supports additional security functionality compared to DSA and RSA like domain parameter validation and public key validation. These techniques may provide additional assurances desired by some users.

We therefore congratulate you on the improvements made to FIPS 186 so far but urge you to complete the improvements by adding support for ECDSA.

Best regards.

jkl per: Scott Vanstone
Certicom Corp.

From: "Sherry Shannon"
To:
Subject: Fw: comments
Date: Fri, 12 Mar 1999 19:11:01 -0500
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 4.72.2106.4
X-MimeOLE: Produced By Microsoft MimeOLE V4.72.2106.4

Please find attached my comments on this effort.

Sincerely,

Sherry Shannon
SVI Consulting Inc
10140 Pineview Trail
P. O. Box 490
Campbellville, ON L0P 1B0 CANADA
Tel: (905) 854-6363
Fax: (905) 854-6464
Email: <mailto:svi@idirect.com>svi@idirect.com

March 12, 1999

Information Technology Laboratory,
Attn: DSS/X9.31 Comments,
National Institute of Standards
and Technology,
100 Bureau Drive Stop 8970
Gaithersburg, MD 20899-8970

To Whom It May Concern:

I would like to comment on your current effort to update FIPS 186 to include ANSI X9.31. This effort is extremely valuable and commendable. However, it would seem to be more valuable if you would also include the recently approved ANSI X9.62 (ECDSA) in your update of FIPS 186.

Adding both RSA and ECDSA to FIPS 186 will provide the full spectrum of prevalent digital signature algorithms and provide cost effective solutions for the range of platforms from the desktop to PDAs to smart cards. This effort would also align with NIST's Minimum Interoperability Specification for PKI Components which specific these three digital signature algorithms - DSA, RSA and ECDSA and

I appreciate the opportunity to comment on this timely effort.

Sincerely,
Sherry E. Shannon
SVI Consulting Inc.

From: Burt Kaliski <burt@rsa.com>
To: "'fips186rsa@nist.gov'" <fips186rsa@nist.gov>
Subject: Comments on FIPS 186-1
Date: Fri, 12 Mar 1999 13:44:06 -0800
X-Mailer: Internet Mail Service (5.5.2232.9)

March 12, 1999

Information Technology Laboratory
ATTN: Review of FIPS 186-1
Bldg. 820, Room 562
National Institute of Standards and Technology
Gaithersburg, MD 20899

Ladies and Gentlemen:

As the division that coordinates standards development activities for both RSA Data Security, Inc. and its parent company Security Dynamics, RSA Laboratories has a strong interest in tracking security technology standards such as FIPS 186-1. RSA Laboratories appreciates NIST's support of this initiative and the opportunity to review and comment on FIPS 186-1.

NIST's recent announcement that it would extend Federal Information Processing Standard (FIPS) 186-1 to include both the Digital Signature Algorithm (DSA) and American National Standard X9.31 [1] is an important step forward in terms of government support for industry initiatives. Since the publication of FIPS 186 in 1994, many have viewed government and industry standards as being on separate tracks. NIST's adoption of ANSI X9.31 demonstrates its commitment to joining these tracks and enabling a secure information infrastructure spanning the public and private sectors.

Although the adoption of ANSI X9.31 is a significant milestone, RSA Laboratories respectfully observes that the proposed FIPS 186-1 does not recognize industry practice for the RSA algorithm, which is based on another standard, Public-Key Cryptography Standard (PKCS) #1 [2,3]. The PKCS #1 signature format (which is in both the current as well as previous versions of PKCS #1) is in many industry standards that have wide and emerging deployment, including the Secure Sockets Layer (SSL), its successor, Transport Layer Security (TLS) and S/MIME secure messaging. In addition, the recently published PKIX certificate profile [4], which is intended as the basis for many forthcoming Internet Engineering Task Force standards, lists DSA and PKCS #1 RSA as examples of supported signature algorithms, but not ANSI X9.31.

It is estimated that the number of copies of cryptography software worldwide that include the PKCS #1 RSA signature format is in the hundreds of millions. Federal agencies are making extensive use of such software, as incorporated into the products developed by RSA Data Security and its licensees. The PKCS #1 format, as implemented in products from such companies as Microsoft, Netscape, Oracle and many others, is being widely used in the Public-Key Infrastructure (PKI) pilot projects sponsored by

the Government Information Technology Services Board. By contrast, the ANSI X9.31 format does not have a significant base of implementations.

Although it is possible to distinguish between the ANSI X9.31 and PKCS #1 formats, it is not possible to convert a PKCS #1 signature to an ANSI X9.31 signature or vice versa. Thus, there is no way to make an existing PKCS #1-based product compatible with ANSI X9.31 or the proposed FIPS 186-1 without changing how the cryptography is implemented internally. To conform with FIPS 186-1, a vendor needs to reissue its products with the new signature format. For the standpoint of interoperability, this is not a desirable situation.

RSA Laboratories therefore recommends that NIST allow the PKCS #1 format as an alternative to the ANSI X9.31 format, at least for some transition period. While supporting two formats for RSA signatures may seem to make interoperability more complicated, the situation is no more difficult than what NIST already faces if it wishes to support three different kinds of signatures (DSA, elliptic curve and RSA). NIST has demonstrated its ability to manage multiple algorithm choices through the development of the interoperability profile for certificate authorities [5]. Under the multi-algorithm model, which is consistent with security architectures developed by industry, adding another format is not a significant complexity.

A transition from PKCS #1 to ANSI X9.31 signatures could parallel what NIST intends for DES and triple-DES, as described in the draft FIPS 46-3. In the draft, released last December, NIST establishes triple-DES as the FIPS encryption algorithm, recognizes the existing base of DES implementations, and allows that new implementations might operate in a compatibility mode that supports the existing base. For instance:

> Single DES (i.e., DEA) will be permitted for legacy systems only. New procurements to support legacy systems should, where, feasible, use Triple DES products running in the single DES configuration.

NIST could similarly allow that new digital signature implementations, after some transition period, would generate signatures in the ANSI X9.31 format but verify signatures in either format. During the transition period, implementations could generate and verify signatures in either format.

A transition between formats might also valuably be combined with industry changes in the area of hash functions. Currently, the MD5 hash function is often combined with RSA in PKCS #1 signatures, but industry is moving toward the SHA-1 hash function, which is specified in FIPS 180-1. As ANSI X9.31 is based on SHA-1 rather than MD5, moves toward SHA-1 and ANSI X9.31 could take place at the same time. The move toward SHA-1 brings a tangible benefit in terms of security, which provides added incentive for a change to support ANSI X9.31 as specified in FIPS 186-1. (Related to this, it is reasonable that NIST might allow the PKCS #1 format, but only with SHA-1, not MD5.)

RSA Laboratories again wishes to express its appreciation for the opportunity to comment on FIPS 186-1, and looks forward to continuing to work with NIST on the development on standards for security technology.

Sincerely,

Burton S. Kaliski Jr., Ph.D.
Chief Scientist and Director
RSA Laboratories

References

[1] American National Standard X9.31-1998: Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA). American Bankers Association, 1998.

[2] PKCS #1 v2.0: RSA Cryptography Standard. RSA Laboratories, October 1998. Available from http://www.rsa.com/rsalabs/pubs/PKCS/ <http://www.rsa.com/rsalabs/pubs/PKCS/> .

[3] B. Kaliski and J. Staddon PKCS #1: RSA Cryptography Specifications Version 2.0. IETF RFC 2437, October 1998.

[4] R. Housley, W. Ford, W. Polk and D. Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. IETF RFC 2459, January 1999.

[5] William E. Burr, Donna F. Dodson, Noel A. Nazario, and William T. Polk. NIST SPEC PUB 800-15: Minimum Interoperability Specification for PKI Components (MISPC), version 1. NIST, January 1998.

From: Murray Brown <mbrown@724.com>
To: "'FIPS186RSA@nist.gov'" <FIPS186RSA@nist.gov>
Subject: DSS/X9.31 Comments
Date: Thu, 11 Mar 1999 14:50:29 -0500
X-Mailer: Internet Mail Service (5.5.1960.3)

FIPS186RSA@nist.gov

Attn: DSS/X9.31 Comments
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive Stop 8970, Gaithersburg, MD
USA 20899-8970

Dear Sir/Madame,

The process that NIST is undertaking to extend the Digital Signature Standard (DSS - FIPS 186) to include ANSI 9.31 (the RSA signature standard) is very important and valuable to further the acceptance and adoption of standards-compliant digital signature technologies.

However, we believe that this standard will be incomplete if it does not also include ANSI 9.62 (ECDSA - Elliptic Curve Digital Signature Algorithm) for the following reasons:

- Adding ECDSA to the standard will complete the full spectrum of platforms, devices, and environments that can be serviced by DSS compliant systems. This is particularly important to 724 Solutions because of the number and variety of devices we need to support for our anytime, anywhere online banking and brokerage application.

- The banking community (through ANSI) and NIST itself (in the Minimum Interoperability Specification for PKI Components) agree that the three most important and prevalent digital signature algorithms in the industry today are: RSA, DSA, and ECDSA. Again, this is very important to 724 Solutions as we develop comprehensive electronic commerce solutions for our customers in the financial industry

- The significant improvements in performance, size and cost of elliptic curve cryptography over either RSA or DSA make ECDSA's inclusion in the standard critical if Federal Agencies are to take advantage of the most efficient and cost effective products on the market. For example, ECDSA smart cards can be as much as half the price of similar RSA or DSA cards and still execute faster. Wireless devices such as cellular telephones, pagers and personal digital assistants (PDAs) represent

a significant target market for our anywhere, anytime banking and brokerage application, as do smart-card enabled systems. Consequently, reducing the size and cost, while increasing the performance of cryptographic technology is essential to the user experience and the success of our application. ECDSA provides these advantages.

We urge you to include ECDSA (ANSI 9.62) in the FIPS-186 DSS standard.

Best regards,

Murray J. Brown
Sr. Security Architect, 724 Solutions Inc.
http://www.724.com

4201 North 24th Street, Suite 365
Phoenix, Arizona 85016-6268
(602) 957-9105
(602) 955-0749 FAX
www.ncpdp.org

January 18, 1999

Information Technology Laboratory
Attn: DSS/X9.31 Comments
National Institute of Standards and Technology
100 Bureau Drive Stop 8970
Gaithersburg, Maryland 20899-8970

Dear Director,

The purpose of this letter is to formally respond to the notice announcing approval of the Federal Information Processing Standard 186-1, Digital Signature Standard, and Request for Comments [Docket No. 981028268-8268-1] published in the Federal Register on December 15, 1998. The notice states that the Secretary of Commerce has approved an interim final standard, which will be known as Federal Information Processing Standard (FIPS) 186-1, Digital Signature Standard (DSS). This interim final standard allows for both the use of the Digital Signature Algorithm (DSA) and the American National Standards Institute X9.31 standard by federal organizations. The X9.31 standard describes the Rivest-Shamir-Adleman (RSA) digital signature technique.

The National Council for Prescription Drug Programs (NCPDP) is a non-profit ANSI-accredited Standards Development Organization in the pharmacy services sector of the health care industry. Our membership consists of over 1200 members who represent computer companies, drug manufacturers, pharmacy chains and independents, drug wholesalers, insurers, mail order prescription drug companies, pharmaceutical claims processors, physician services organizations, prescription drug providers, software vendors, telecommunication vendors, service organizations, government agencies and other parties interested in electronic standardization within the pharmacy services sector of the health care industry.

After reviewing the notice, NCPDP agrees with making the amendments to FIPS 186 by also including the use of RSA and elliptic curve. NCPDP will fully support this notice.

Thank you for the opportunity to officially respond to this notice. Please feel free to call me at 602-957-9105 ext. 108 if you have any questions.

Sincerely,

Lee Ann Stember
President

cc. Phillip Scott- NCPDP Chairman of the Board
Marla Brickley- NCPDP Chairman Elect
Margaret Weiker- NCPDP Standardization Co-Chair and Board of Trustee Member
Jason Moore- NCPDP Standardization Co-Chair and Board of Trustee Member
Bob Beckley- NCPDP Standardization Co-Chair
Dan Staniec- NCPDP Executive Vice President of External Affairs
David Goodspeed- NCPDP General Manager

381 Elden Street
Suite 1120
Herndon, VA 20170

February 10, 1999

Docket No. 981028268-8268-01

Information Technology Laboratory
Attn: DSS/X9.31 Comments
National Institute of Standards and Technology
100 Bureau Drive, Stop 8970
Gaithersburg, MD 20899-8970

Dear Sir or Madam:

SPYRUS applauds your efforts to include additional digital signature algorithms in the Digital Signature Standard Federal Information Processing Standard (FIPS PUB 186). We believe that the resulting standard should include DSA, RSA, and ECDSA. Each of these algorithms has benefits for Federal Government users.

Presently, DSA is the only digital signature algorithm included in FIPS PUB 186. However, the current specification limits the modulus size to 1024 bits. We believe that the updated FIPS PUB should support DSA modulus sizes up to 2048 bits.

The RSA digital signature algorithm has two specifications: ANSI X9.31 and PKCS#1. In both specifications, encrypting a message hash value with the signer's private key results in a digital signature. Unfortunately, the two specifications format the message hash differently. Consequently, digital signatures generated in accordance with these specifications are not interoperable. If the PKCS#1 formatting is not supported in updated FIPS PUB, then Federal Government users will require waivers to use several important applications, including SSL, S/MIME v2, and SET. We believe that the updated FIPS PUB should include PKCS#1 formatting. The X9.31 formatting can also be included if identified applications need it.

ANSI X9.62 specifies the ECDSA digital signature algorithm. Elliptic curves offer equivalent strength digital signatures with the advantages of smaller keys and reduced computational complexity. Therefore, we believe that the updated FIPS PUB should include ECDSA.

If you have any questions concerning these recommendations, please contact me at 703-707-0696.

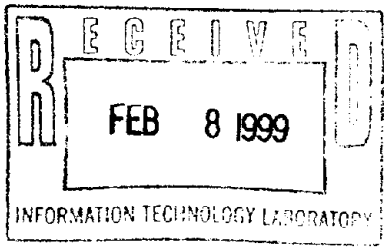
Sincerely,

Russell Housley
Chief Scientist

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 3, 1999

Shukri A. Wakid, Ph.D.
Director, Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8970
Gaithersburg, Maryland 20899-8970



Dear Dr. Wakid:

I am writing on behalf of the Federal Public Key Infrastructure Steering Committee regarding the notice announcing approval of the Federal Information Processing Standard (FIPS) 186-1, Digital Signature Standard (DSS), and Request for Comments [Docket No. 981028268-8268-01] published in the Federal Register on December 15, 1998. The notioe states that the Secretary of Commerce has approved an interim final standard, which will be known as FIPS 186-1, DSS. The interim final standard allows for the use of the Digital Signature Algorithm (DSA) and the American National Standards Institute X9.31 standard by Federal agencies. The X9.31 standard describes the Rivest-Shamir-Adleman (RSA) digital signature technique.

The Steering Committee strongly supports the proposed change for technical, policy and programmatic reasons. The RSA digital signature technique is well established in industry and in the technical community supporting applications requiring encryption, and we fully expect its use for digital signature purposes to be equally appropriate.

We also note that X9.62-1998, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), met final ANSI approval on January 7, 1999. The benefits of ECDSA are well known – faster processing speeds and smaller key lengths for equivalent cryptographic protection – so we also support NIST proceeding quickly with changes to FIPS 186 that would allow the use of this technology as well. To the extent that NIST believes it technically justified, we support amending FIPS 186 to allow ECDSA at the same time that FIPS 186 is finally amended to include RSA. This would save time and effort on the part of NIST, and get the technology into the hands of agencies more quickly.

We appreciate the opportunity to comment on NIST's efforts and look forward to further action on these matters. We also particularly appreciate the participation and invaluable contributions which NIST staff make to the activities of the Steering Committee, and look forward to their continued support.

Sincerely,

Richard A. Guida

Richard A. Guida, P.E.
Chair, Federal Public Key Infrastructure
Steering Committee