Comments on the proposed FIPS for Key Exchange and Agreement:
(All of the following were received by e-mail. Comments received in
hardcopy format are not included here.)

==

Date: Wed, 28 May 97 18:11:39 EDT
From: "Douglas A. Gwyn (IST)" <gwyn@ARL.MIL>
To: keyex@nist.gov
Subject: Re: NIST to Consider Revised Digital Signature Standard for Fede

Any system incorporating "key recovery" facilities is insufficiently
secure. The idea that somehow government has a "right" to monitor
other people's conversations is the antithesis of the principles on
which this nation was founded, and supporters of mandatory key
recovery should be ashamed of themselves.

===========

From: Burt Kaliski <burt@RSA.COM>
To: "'keyex@nist.gov'" <keyex@nist.gov>
Subject: Comments on key exchange/agreement FIPS
Date: Mon, 16 Jun 1997 07:18:46 -0700

June 16, 1997

Director, Information Technology Laboratory
Key Agreement/Exchange FIPS
A231 Technology Building
NIST
Gaithersburg, Md. 20899-0001
<keyex@nist.gov>

Dear Director:

Responding to the recent announcement by NIST of its intention to develop a FIPS for key exchange/agreement, the IEEE P1363 working group, "Standard for Public-Key Cryptography," would like to convey its support of this effort and offer its assistance.

The IEEE P1363 project, now in its fourth year, is developing a comprehensive standard for public-key cryptography, including techniques from the three major families -- discrete logarithms (of which the existing Digital Signature Standard is an example), elliptic curves, and integer factorization (including RSA). The standard also covers the three major categories of public-key techniques: key agreement, digital signatures, and public-key encryption. Substantial consensus among industry participants in the U.S. and abroad has already been achieved through the development process, making the IEEE P1363 working drafts a helpful reference for the development of the FIPS.

The IEEE P1363 effort is closely coordinated with the ANSI X9F1 standards, which are also helpful references.

Balloting of the IEEE P1363 standard is currently planned for early 1998. Further information is available on the IEEE P1363 Web page, http://stdsbbs.ieee.org/groups/1363.

IEEE P1363 applauds NIST's efforts to develop a FIPS for key exchange/agreement, and will be happy to assist in this effort, by contributing the IEEE P1363 working drafts as input to the development process, by reviewing the FIPS, or by other means. Please let me know if you have any questions.

Sincerely,

Burt Kaliski
Chair, IEEE P1363

===========

Return-receipt-to: blake.greenlee@internetmci.com
Date: Fri, 01 Aug 1997 08:18:16 -0400
From: "M. Blake Greenlee" <blake.greenlee@internetmci.com>
Subject: Comments on proposed changes to FIPS 186
To: "'KEYEX@NIST.GOV'" <KEYEX@nist.gov>
X-MIME-Autoconverted: from quoted-printable to 8bit by email.nist.gov id IAA05069

Dear Sirs:

I believe that FIPS 186 should be revised to include ANSI standard key agreement and key transport standards by reference.

I am particularly concerned that elliptic curve cryptographic techniques be included. This can easily be done be allowing adoption by reference to ANSI X9.63. Where NIST may desire to particularize what it wishes to have the Federal Government use, that may be done easily by reference to the appropriate sections in the Standard.

As a note, the X9 program of work on public key infrastructure standards in X9F1 is/has developed a family of standards. Four of these will directly address key management:

1. X9.42, Management of Symmetric Algorithm Keys Using Diffie-Hellman (in ballot).
2. X9.44, Management of Symmetric Algorithm Keys Using Reversible Public Key Cryptography (in preparation; includes RSA)
3. X9.63, Key Agreement and Key Management Using Elliptic Curve-based cryptography (in preparation)
4. X9.43, Key Archiving and Retrieval (not applicable to FIPS 186)

The changes to FIPS 186 should allow a variety of competitive techniques either in the public domain (like Diffie Hellman) or for a nominal license fee. No technology should be included where licenses are not available on a non-discriminatory basis to implement the technology in embodiments of the licensee's own choosing.

I note that a major factor in the costs of using cryptography is the "overhead." Quoting from the Foreword to ANSI X9.62,

"The primary advantage of elliptic curve systems is their apparent high cryptographic strength relative to key size. The attractiveness of elliptic curve cryptosystems may increase relative to other public-key cryptosystems as computing power improvements warrant a general increase in key size. The shorter key sizes may result in significantly shorter certificates and system parameters. These potential advantages manifest themselves in many ways, including storage efficiencies, bandwidth savings and computational efficiencies. The computational efficiencies may lead in turn to higher speeds, power efficiency, code size reductions or a combination thereof.

These potential efficiencies are particularly beneficial in applications such as:
? high volume transaction systems,
? wireless communications,
? hand-held computing (e.g., personal digital assistants),

? broadcast communications
? smart cards
where bandwidth, processing capacity, power availability or storage are constrained."

Because of costs, efficiencies and security, I believe that it is in the best interests of the US Government and the citizens that it serves to include elliptic curve key agreement and key management techniques in FIPS 186.

M. Blake Greenlee
M. Blake Greenlee Associates

=============

Date: Fri, 01 Aug 1997 08:51:00 -0400
From: Paul Raines <Paul.Raines@ny.frb.org>
Subject: Comments on FIPS Federal Register Announcements
To: fips186@nist.gov, keyex@nist.gov

I am writing in response to your Federal Register announcement dtd 5/13/97 which requests comments on NIST's proposed upgrades to the FIPS 186 standard and developing a new FIPS standard for public key based cryptographic key agreement and exchange.

I believe it is critical that NIST include in its standards support for both RSA and Elliptic Curve Cryptography. The former cryptographic algorithm has gained widespread industry acceptance and is close to becoming a de facto standard. The latter algorithm has very obvious technical advantages. Namely, the encryption processes are done much faster and the smaller key size is ideal for limited bandwidth applications (e.g. smart cards). It is currently being considered as a standard by IEEE. For these reasons, I believe NIST should include these algorithms in any future standards and do so in a way that would be royalty-free to the public.

For key exchange mechanisms, I believe NIST should examine both the RSA and Diffie-Hellman methods of exchanging the session encryption key. For the actual session key algorithm, I feel NIST should give strong consideration to triple DES as a follow-on to single DES.

If you have any questions about anything I have written or need to contact me, my phone number is 212-720-7657.

Sincerely,

Paul Raines
Vice President
Electronic Security
Federal Reserve Bank of New York

=============

X-Sender: sergio@exchsvr1.entegrity.com
Date: Thu, 07 Aug 1997 17:48:48 +0200
To: KEYEX@nist.gov
From: Sergio Faissol <sergio@entegrity.com>
Subject: RFC for Key Agreement and Exchange
Cc: john@entegrity.com, dave@entegrity.com

To: Director, Information Technology Laboratory, NIST

Entegrity Solutions Corporation is a software company providing a comprehensive framework of products and services utilizing strong public key encryption and digital certificate technology to integrate security into the global enterprise.

We believe that the new FIPS for Key Agreement and Exchange should include standards for the use of all major techniques mentioned in your RFC, especially the new Elliptic Curve Cryptosystems. In our view, this technology has the highest strength-per-bit of any public-key cryptographic technique available today. We are planning to use this technology in products targeting several environments, including smart cards, authentication products, and electronic commerce related applications.

Open competition of several strong cryptographic algorithms is critical to perpetuating a competitive market in these technologies. ECC appears to be among the most competitive of these technologies and should be included. We further advocate that any truly secure data system will require the use of hardware based cryptography. In order to meet this requirement in a cost-effective way we need to be able to provide hardware solutions that are fast, small and inexpensive. It has been demonstrated in prototype environments that ECC can provide significant advantages in this area.

Regards,

Sergio Faissol
V.P. Worldwide Product Development
Entegrity Solutions Corp.
2077 Gateway Pl, Suite 200
San Jose, CA 95110 USA
Voice: +1 (408) 487-8600 x112
FAX: +1 (408) 487-8610
E-mail: sergio@entegrity.com
http://www.entegrity.com

===========

From: john.purcell@gsa.gov
Date: 11 Aug 97 12:36:00 (-0400)
Subject: Comments on FR Vol. 62, No. 92 (Digital Signature Standard)
To: fips186@nist.gov, judith.spencer@gsa.gov, stanley.choffrey@gsa.gov

Attached herewith are the comments of the Center for Governmentwide Security on the Federal Register notice (Vol. 62, No. 92), regarding the Digital Signature Standard. The format is Microsoft Word.

-- John Purcell
for Judith A. Spencer
Director, Center for Governmentwide Security

COMMENTS IN RESPONSE TO NOTICES IN FEDERAL REGISTER VOL. 62, NO. 92, ANNOUNCING PLANS TO DEVELOP A FEDERAL INFORMATION PROCESSING STANDARD FOR PUBLIC-KEY BASED CRYPTOGRAPHIC KEY AGREEMENT AND EXCHANGE -- RIN 0693-ZA10

AND

ANNOUNCING PLANS TO REVISE FEDERAL INFORMATION PROCESSING STANDARD 186, DIGITAL SIGNATURE STANDARD -- RIN 0693-2A11

The two notices are so closely related in the development of the Federal Security Infrastructure by this office, that we are combining our comments on the two notices.

In our development effort, we are using vendor products which comply with Federal Information Processing Standard 186, (and other FIPS) with regard to the Digital Signature Standard, the Digital Signature Algorithm, the Secure Hash Algorithm, and the Data Encryption Standard. In doing so, we are relying on the minimum standards for security as published by the National Institute of Standards and Technology, Department of Commerce, pursuant to the Computer Security Act of 1987.

At this time, we see no reason to change our approach, even if the FIPS 186 is modifired to incorporate other algorithms.

We do wish to comment on the special needs for security in systems which are intended to transfer funds. We point out that these systems may require security algorithms stronger than those systems which only convey normal message traffic. Of course, information that is particularly sensitive may require the same security level as is needed by systems that convey funds.

We are aware that the customer community is already using algorithms other than those specified in the FIPS. Since interoperability of the algorithms is essential for the usability of the cryptographic products, we are especially concerned that an immediate, high-level effort be mounted to ensure this interoperability.

Thank you for the opportunity to comment.

===========

To: Keyex@nist.gov
Date: Mon, 11 Aug 1997 12:47:25 -0400
Subject: Key Agreement/Exchange FIPS

>From Dr. Scott Vanstone

(See attached file: KeyAgreement.doc)

August 11, 1997

Director, Information Technology Laboratory
Attn: Key Agreement/Exchange FIPS

Certicom supports NIST"s initiative to develop a FIPS which addresses the key agreement and key exchange issue. Currently the IEEE P1363 and ANSIX9.63 draft standards have incorporated key exchange techniques (in fact, X9.63 addresses only this issue). As is well known, key agreement and key exchange are crucial components in any secure data exchange. Efficient techniques to perform this task are needed and they must perform well even on the most constrained platforms. In order to meet the demands of the wireless, smart card and various other environments Certicom encourages NIST to adopt elliptic curve technology as the underlying algebraic structure for the protocols. Furthermore, Certicom encourages NIST to adopt similar protocols for key agreement as currently being drafted for ANSI X9.63. In particular, the one and two pass versions of the MQV provides a fully authenticated Diffie-Hellman key agreement with a minimum of bandwidth overhead. This protocol when performed in the elliptic curve setting is ideally suited to many constrained environments which would have a difficult time supporting any other key agreement protocol.

Certicom has filed for patent protection on the MQV protocol. Certicom's licensing policy is public knowledge and MQV has been made available to ANSI X9.63 on a royalty free basis provided it is used for financial applications. As for the unified model for Diffie-Hellman, this protocol was proposed and is being supported by IBM. Certicom has no knowledge of the patent status of this protocol with respect to IBM or any other organization.

Dr. Scott Vanstone
Certicom Corp.
Chief Cryptographer

===========

Date: Mon, 11 Aug 1997 14:46:12 -0400
From: Thierry Moreau <"Thierry Moreau"@hawksbill.nist.gov>
Reply-To: Thierry.Moreau@connotech.com
Organization: CONNOTECH Experts-conseils Inc./Montreal/Quebec/Canada
To: KEYEX@nist.gov
Subject: Comment on key exchange

ATTN: Director, Information Technology Laboratory,
Subject: Key Agreement/Exchange FIPS

Dear Sirs,

please find enclosed a comment on "Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange".

The attachement is formatted using the HTML format. If this format creates difficulties with processing of the comment, please indicate your choice for alternate format, among 1) WordPerfect 6.x, 2) Word for Windows, 3) plain ASCII, and I will be glad to re-submit the attachment accordingly.

[ASCII included for this file - NIST]

Yours Truly,

Thierry Moreau

Probabilistic Encryption Key Exchange

(Comment on Plans to Develop a FIP Standard for Public-Key Based Cryptographic Key Agreement and Exchange)

August 11th, 1997

by Thierry Moreau,
CONNOTECH Experts-conseils Inc.

Introduction

Probabilistic Encryption Key Exchange (PEKE) [1] was invented as a secret key establishment method to be plug-in compatible, protocol-wise, with the Diffie-Hellman key exchange [2]. In fact, PEKE happens to be applicable in other circumstances as well.

In this document, we first present a taxonomy of secret key exchange mechanisms, in order to position PEKE in relation with other schemes. Then, we present the security foundation of PEKE, which is shared with Annex A of ISO /IEC 9796 when the public exponent is 2 [3] [4].

Last, we mention the patent pending rights that CONNOTECH Experts-conseils has over the PEKE cryptosystem in Canada.

A taxonomy of secret key establishment protocols

Secret key establishment protocols may be classified according to a number of criteria, derived from application requirements or implementation issues. In all cases, a fresh secret key is established from pre-existing conditions.

Type of key established by the scheme under consideration

The secret key established may be used as a short term session key between two entities directly linked in a protocol exchange, or as a longer term key used e.g. in a store and forward system.

Originally, PEKE was disclosed for session key establishment with direct protocol involvement of both entities. But closer examination of the PEKE two-message protocol reveals that the first message may be generated and/or sent on behalf of the "initiating entity" instead of by the initiating entity, with only a slight decrease in security (specifically, the essential protection against chosen ciphertext attack remains when PEKE is used in a store-and-forward scheme). So, PEKE can be used in store-and-forward applications.

Number-theoretic public parameters

In discrete logarithm systems, the number-theoretic public parameters are generally common to a group of entities and subject to complete public scrutiny. In this case, the private component of a private/public key pair is just a secret random number (as in the Lein Harn's authentication improvement of the Diffie-Hellman scheme, see [5]). In the case of one-way trapdoor cryptosystems, the number-theoretic public parameter is specific to one entity. The issues of trust in the implementation of the number-theoretic parameter selection vary accordingly.

PEKE falls in the latter category, where a number-theoretic private/public key pair is associated with one of the two entities participating in the secret key exchange.

Authentication capabilities

In a secret key exchange protocol, one party may or may not get cryptographic assurance that the remote party is one which knows the private counterpart of a public key used in the computations. This authentication capability is independent in each direction of the secret key establishment protocol. The "certification" of the public key is an important related issue.

PEKE offers a one-way authentication capability.

Local secure computing facilities

We can distinguish the following computing facilities as being critical for some secret key establishment schemes, but not always trivially procured:

* a secure memory for storing a long-term secret,

* a truly random source for locally generating random secret values,

* sufficient processing power for 1) a small number of multiply-reduce cycles, 2) a full modular exponentiation (that is a much larger number of multiply-reduce cycles), 3) the computation of the modular inverse, and 4) the capability to pre-compute a number of intermediate results in advance of subsequent instances of the secret key exchange protocol.

For instance, the Diffie-Hellman cryptosystem requires a truly random source and sufficient processing power for a full modular exponentiation, and may benefit from the capability to pre-compute intermediate results. Any entity which is authenticated in a key exchange protocol requires a secure memory for storing a long term secret. Whenever a secure memory is available, a truly random source may be provided by a cryptographic-strength pseudo-random number generator of which the internal state is kept in the secure memory.

The PEKE cryptosystem has un-balanced requirements. The low-processing end of the transaction requires a truly random source and sufficient processing power for a small number of multiply-reduce cycles. The higher processing end of the transaction requires a secure memory, and sufficient processing power for a full modular exponentiation. The random source used by the higher processing end need not be of cryptographic strength.

Resistance to failure of random source

There are various attack scenarios that can exploit weaknesses in a random source used in secret key establishment protocol. For instance, a vulnerability to replay attacks may occur if an adversary is able to force a constant output from a random source. Another worrisome weakness is a too small set of possible outcomes of the random source process. Any secret key establishment protocol that is to ensure uniqueness of the generated secret key requires at least two messages.

An instance of the PEKE secret key establishment protocol may encompass one or two message transmissions. When two message transmissions are used, uniqueness of the generated secret key is ensured. In addition, a failure of one party's random source is not noticeable by a third party who oversees the protocol exchange. This last property occurs in a single direction, that is when the random source failure occurs in the low-processing end of the transaction (recall that PEKE has unbalanced processing requirements).

Accomodation of key escrow schemes

Ideally, the "granularity" of key escrow mechanisms associated with a secret key exchange scheme should reflect the balance of conflicting interests of the parties involved. Actually, the foremost secret key exchange schemes are at the two opposite ends of the granularity scale (unless modified for key escrow purposes): the Diffie-Hellman scheme has the smallest granularity (each generated secret key must be individually escrowed), and the one-way trapdoor cryptosystems has the coarsest granularity (the entity's private key being escrowed, all secret-keys generated with the corresponding public key can be recovered at once).

PEKE is like one-way trapdoor cryptosystems with respect of accomodation of key escrow schemes.

Security foundation of PEKE

The PEKE security foundation is the "x^2 mod N" one-way trapdoor function where N is the product of two prime numbers "congruent to 3 modulo 4". The first author to suggest the use of this particular formulation is Hugh C. Williams [6]. But this is now usually referred to as the Rabin public key cryptosystem (used for both encryption and digital signatures) [7]. Blum Blum and Shub independently published a pioneer article on the mathematical properties of this "x² mod N" primitive [8], and Blum and Goldwasser documented an efficient probabilistic encryption scheme from this work [9].

The security foundation of the "x^2 mod N" one-way trapdoor function is used by an international standard on digital signatures, [3] [4].

There are two difficulties with the application of the "x^2 mod N" primitive to practical cryptographic schemes. One is the threat of chosen ciphertext attack, where the possessor of the private key is repeatedly probed with ciphertext to decrypt and returns (part of) the corresponding cleartext. While the RSA primitive so far has resisted public cryptanalysis attempts with respect to the chosen ciphertext attack, the "x^2 mod N" primitive is known to be vulnerable to it. The other difficulty is the fact that the "x^2 mod N" function is a 4:1 mapping that creates ambiguity.

In practical proposals, the chosen ciphertext attack is prevented by introducing redundancy in the input (cleartext) to the "x^2 mod N" function, and mandating the possessor of the private key to hide any cleartext devoid of the redundancy (e.g. [10], page 9, lines 16-28). PEKE works according to this principle.

Resolving the 4:1 ambiguity in the "x^2 mod N" function is more an operational concern than a security issue, and diverse solutions has been proposed (e.g. [11], [12], [13]).

Patent Issues

A patent application has been filed in Canada for PEKE [14]. This patent application has been laid open to the public on September 23, 1995. No patent application had been filed outside of Canada for PEKE by or on behalf of the inventor or assignee in the Canadian patent application.

For more information

On-line Internet documentation http://www.connotech.com/pekemap.htm

Electronic mail: info@connotech.com

CONNOTECH Experts-conseils Inc.
9130 Place de Montgolfier
Montreal, Quebec, Canada, H2M 2A1
Tel.: +1-514-385-5691 Fax: +1-514-385-5900

References

----

[1] Moreau, Thierry, Probabilistic Encryption Key Exchange, Electronics Letters, Vol. 31, number 25, 7th December 1995, pp 2166-2168

[2] Diffie, Bailey Whitfield, Hellman, Martin E., New Directions in Cryptography, IEEE Transactions in Information Theory, vol IT-22, 1976, pp 644-654

[3] ISO/IEC 9796:1991, Information Technology - Security Techniques - Digital Signature Scheme Giving Message Recovery

[4] Guillou, Louis Claude, Quisquater, Jean-Jacques, Walker, Mike, Landrock, Peter, and Shaer, Caroline, Precautions taken against various potential attacks in ISO/IEC DIS 9796 'Digital signature scheme giving message recovery', Advances in Cryptology, Eurocrypt'90, Lecture Notes In Computer Science no. 473, pp 465-473

[5] Harn, Lein, Digital signature for Diffie-Hellman keys without using a one-way function, Electronics Letters, 16th January 1997, Vol 33, No 2, pp125-126

[6] Williams, Hugh C., A Modification of RSA Public-Key Encryption, IEEE Transactions on Information Theory, Vol IT-26, no. 6, November 1980, pp 726-729

[7] Rabin, M.O., Digital Signatures and Public Key Functions as Intractable as Factorization, MIT Laboratory for computer science, TR 212, January 1979, pp 1-16

[8] Blum, Leonore, Blum, Manuel, and Shub, M., A Simple Unpredictable Pseudo-random Number Generator, SIAM Journal of Computing, vol. 15, no. 2, May 1986, pp 364-383

[9] Blum, Manuel, and Goldwasser, Shafi, An Efficient Probabilistic Public-key Encryption Scheme which Hides All Partial Information, In Advances in Cryptology: Proceedings of Crypto'84, Springer-Verlag, 1985, pp 289-299

[10] USA patent document 5,406,628, Beller, Michael J., Yacobi, Yacov, Public Key Authentication and Key Agreement for Low-cost Terminals, April 11, 1995 (application number 101,437, August 2, 1993)

[11] Lieberherr, Karl, Uniform Complexity and Digital Signatures, Theoretical Computer Science, Vol. 16 (1981), pp 99-110

[12] Harn, Lein, and Kiesler, T., Improved Rabin's Scheme with High Efficiency, Electronics Letters, Vol. 25, no. 11, May 25th, 1989, pp 726-728 (see also erratum published in Electronics Letters, Vol. 25, no. 15, page 1016)

[13] Shimada, M., Another Practical Public-Key Cryptosystem, Electronic Letters, Vol. 28, no. 23, November 5th, 1992, pp 2146

[14] Moreau, Thierry, Apparatus and Method for Cryptographic System Users to Obtain a Jointly Determined, Secret, Shared, and Unique Bit String, Canadian patent application number 2,156,780, filed on August 23, 1995, laid-open to the public on September 23, 1995, CONNOTECH Experts-conseils Inc., Montréal, Canada

----

[CONNOTECH home page: http://www.connotech.com/ | about us | web editorial policy | e-mail to: info@connotech.com]

CONNOTECH Experts-conseils Inc.
9130 Place de Montgolfier
Montreal, Quebec, Canada, H2M 2A1
Tel.: +1-514-385-5691 Fax: +1-514-385-5900

=============

Date: Mon, 11 Aug 1997 15:35:44 -0400
From: Mike <John.Michael.Williams@Computer.org>
X-Mailer: Mozilla 2.01KIT (Win16; U)
MIME-Version: 1.0
To: keyex@nist.gov
CC: John.Michael.Williams@Computer.org
Subject: Include Elliptic Curve Cryptography
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset=us-ascii
X-UIDL: a5373e36914f373dd8adad5268bbbf3a

As a consultant in information security, I strongly recommend the NIST be inclusive in its consideration of Key Agreement/Exchange standards, and in particular, the ANSI X9 ECC standards.

John Michael Williams
6210 Leeke Forest Court
Bethesda MD 20817

===========

X-Sender: lee.k.stanton@postoffice.worldnet.att.net
Date: Mon, 11 Aug 1997 15:45:05 -0400
To: KEYEX@nist.gov
From: Lee Stanton <lee.k.stanton@worldnet.att.net>
Subject: Key Agreement/Exchange FIPS
Cc: cgriffis@v-one.com, cbrook@v-one.com, KNewcomer@v-one.com

Director, Information Technology Laboratory
National Institute of Standards, & Technology
Gaithersburg, MD 20899

V-ONE Corporation, a vendor of data security products that provide security solutions to both private industry and government users, both in the US and abroad, respectfully offers these comments on the proposed Key Agreement/Exchange Standard.

V-ONE's products primarily support communications security, particularly Internet/Intranet TCP/IP protocols. As markets develop for additional product areas, we expect to offer solutions in the areas of Electronic Commerce document and messaging security as well. V-ONE is a member of the National Computer Security Association Cryptographic Products Consortium with particular interest in the Virtual Private Networks area.

Key Agreement is an area that may not be ready for standardization. Many techniques for key exchange are still being tested and evaluated. New methods are being invented and old ways have become suspect. Diffie-Hellman, for example, has been subject to "man in the middle" attacks that may or may not jeopardize the reliability of the algorithm. Since patent protection for the algorithm is just running out, it becomes freely available, and thus very attractive for implementation.

V-ONE uses a proprietary approach that provides equally reliable results at very low overhead while simultaneously offering strong user authentication. Thus, the key agreement technology is only part of the protocol of establishing a connection. V-ONE would like the option of employing the best possible solution for the application at hand. Elliptic Curve and RSA techniques are clearly desirable alternatives, but a standard may not be helpful in selecting the best solution for a particular application. If a standard is necessary for PK based key agreement, it should certainly allow the three alternative systems, but hopefully would also allow alternative mechanisms as they become available and qualified.

Since key agreement is between two parties on a dynamic basis and does not need to necessarily be compatible between multiple other parties, it seems that the need for a standard in this area is unnecessary.

A number of other areas in the security technology area may be more needful of standards, such as the quality or entropy in random number generation or the quality of random numbers and primes. Measures of quality are completely lacking. Perhaps efforts could be redirected into this badly needed tecnology.

Lee K. Stanton, Consultant
V-ONE Corporation
20250 Century Boulevard, Suite 300
Germantown, MD 20874
(301) 515-5200
(301) 515-5280 (FAX)

===========

From: Burt Kaliski <burt@RSA.COM>
To: "'keyex@nist.gov'" <keyex@nist.gov>
Subject: Comments on key exchange/agreement FIPS
Date: Mon, 11 Aug 1997 13:19:45 -0700

August 11, 1997

Director, Information Technology Laboratory
Key Agreement/Exchange FIPS
A231 Technology Building
NIST
Gaithersburg, Md. 20899-0001
<keyex@nist.gov>

Dear Director:

RSA Laboratories is pleased to note NIST's announcement that it is planning to develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange. This announcement is very timely, and we would like to offer some comments in support of the effort.

(These comments reflect the position of RSA Laboratories and RSA Data Security, of which RSA Laboratories is a division; they are independent of those the author submitted earlier this summer as chair of IEEE P1363.)

NIST's plan to develop a FIPS for key agreement and exchange is an important step in promoting information security in industry and government alike. The intention expressed in the announcement to offer government users a choice between techniques such as RSA, Diffie-Hellman, and elliptic-curve algorithms provides a degree of flexibility that will encourage further implementation of security techniques, making security the central issue, not just the choice of algorithm.

There are a great number of choices to be made in the process, however, especially as there many different key agreement and exchange algorithms, and presumably the FIPS cannot specify every one of them. Moreover, each key agreement and exchange algorithm has many implementation options. The challenge to NIST, then, is to determine which choices to support.

A number of choices remain to be made:

* Which key agreement/exchange primitives (i.e., which underlying mathematical operations)? There are the RSA primitive, the Diffie-Hellman primitive, and the elliptic curve analog of Diffie-Hellman, as well as the new MQV primitives, among others.

* Which choices of arithmetic? RSA and Diffie-Hellman are both based on modular arithmetic. Elliptic-curve key agreement algorithms can be based either on modular arithmetic alone, or a combination of modular arithmetic and arithmetic over a characteristic-2 finite field. Within the choice of characteristic-2 arithmetic, there is a further issue of finite field representation (polynomial vs. normal basis).

* Which key sizes? For many reasons a range of key sizes is useful to have in a standard. Related to this, the size of the subgroup in which operations are performed (akin to the size of the prime q in DSA) may need to be defined for the Diffie-Hellman and elliptic curve algorithms.

The question of elliptic-curve key sizes is a particularly interesting one, given their promise of shorter key sizes and what some consider to be a relatively small level of experience in the open research community with elliptic curve cryptanalysis. We would be interested on NIST's process of developing confidence here, as with the other algorithms.

* Which auxiliary functions? Key agreement algorithms often involve an additional step of processing an agreed-upon secret numeric value to derive a key, and likewise key transport algorithms based on public-key encryption may involve some "encoding" of the key into a numeric value prior to encryption. Key derivation functions and encoding techniques are thus also choices that need to be made.

The fact that there are many choices to be made should not be viewed as an obstacle to standardization, but rather as an opportunity for an optimal outcome. NIST need not be limited to a few candidate algorithms, but rather has great flexibility. Each choice has its own benefits, and NIST can make choices that best reflect the needs of both commerce and government.

NIST's choices are important, as they lend an endorsement to technology on a global scale, not just for the U.S. government. We encourage NIST to consider the options broadly and conservatively.

Some other comments:

1. Regarding the issue of encryption capability mentioned in the request for comments:

> Any algorithms proposed for digital signature must be able
> to be implemented such that they do not support encryption unless keys
> used for encryption are distinct from those used for signature and are
> recoverable.

Typical approaches for digital signatures have this property when the digital signature algorithm is implemented with a required hash-function step. While it is true that some digital signature primitives alone may provide encryption capability (including DSA variants and their elliptic curve analogues as well as RSA), any such primitive can be combined with a hash function to eliminate unintended use as an encryption function.

2. Regarding patents:

>   Comments are particularly sought with respect to the RSA, Diffie-
>Hellman, and elliptic curve techniques. In addition, parties believing
>their patents or other intellectual property pertain to any of these
>three techniques are asked to comment and provide specifics of the
>nature of their claims.

RSA Data Security is exclusive licensee of U.S. Patent No. 4,405,829, which covers digital signatures based on the RSA algorithm. A sample open patent license is available from RSA Data Security. RSA Data Security supports the ANSI patent license policy.

RSA Laboratories looks forward to further participation in the development and review of the proposed FIPS. Thank you for this opportunity to comment.

Sincerely,

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

20 Crosby Drive
Bedford, MA 01730
(617) 687-7057
(617) 687-7019 (fax)
burt@rsa.com

===========

From: William_Binzel@mastercard.com
X-Authentication-Warning: pur1: Host mcnpur41.mastercard.com claimed
to be mastercard.com
X-Lotus-FromDomain: MASTERCARD
To: keyex@nist.gov
Date: Mon, 11 Aug 1997 18:53:41 -0400
Subject: FIPS - Public Key Agreement and Exchange -- Comments

Subject: Announcing Plans to Develop a Federal Information Processing
Standard for Public-Key Based Cryptographic Key Agreement and Exchange

Solicited Comments:

MasterCard International supports the development of a Federal Information Processing Standard for public-key key agreement and exchange. A FIPS in this discipline may assist in the adoption of public-key based systems in a wider range of existing and new applications and may result in some federal agencies migrating to advanced public-key based systems.

MasterCard supports the inclusion in the FIPS of protocols that are covered in the drafts of X9.63 and X9.44 developed within the ANSI ASC X9F1 working group.

MasterCard appreciates the opportunity to comment on this announcement. If you have any questions about these comments or MasterCard International's support of this effort, please feel free to contact me.

Sincerely,

William P. Binzel
Vice President
Government Relations
MasterCard International

===========

X-Sender: dpj@world.std.com
Date: Mon, 11 Aug 1997 22:56:18 -0400
To: KEYEX@nist.gov
From: David Jablon <dpj@world.std.com>
Subject: Comments on RFC: Key Agreement/Exchange FIPS
Cc: David Jablon <dpj@world.std.com>, Miles Smid <smid@st1.ncsl.nist.gov>

Director, Information Technology Laboratory
ATTN: Key Agreement/Exchange FIPS
Technology Building, Room A231
National Institute of Standards and Technology
Gaithersburg, MD 20899

Comments on RFC: Key Agreement/Exchange FIPS

Prepared by:

David P. Jablon <dpj@world.std.com>
Integrity Sciences, Inc. <http://world.std.com/~dpj/>
August 11, 1997

Introduction

For the past 20 years, many public-key techniques have been developed to provide a diverse set of benefits for secure computing systems. As NIST develops a FIPS for Public-Key Based Cryptographic Key Agreement and Exchange, we urge you to consider the widest range of techniques that leverage public-key functions for secure key agreement. The many aspects of human/computer interaction demand a variety of approaches, and public-key techniques are crucial for solving many of these problems. This memo focuses on a specific class of these public key agreement techniques that use standard public key agreement functions to protect low-entropy shared secrets in the process of authentication.

This response has been created by Integrity Sciences, a consulting firm and developer of computer security technology. Some specific methods in the class of methods described in this memo have been developed by our company, and we are working to encourage the widespread application of this entire class of important techniques within the industry.

The problem

Several long-standing difficult problems in computer security are related to addressing limitations of human behavior, and in particular, the problem of how to safely and reliably identify and authenticate a live human presence with an electronic mechanism. One important element in authentication is "something you know", which is typically represented by a PIN, password, or passphrase. For simplicity, we refer to this element as a "password". The password element has a chronic problem: It is often difficult to guarantee that the chosen word, phrase, or number has sufficient entropy to resist brute-force attack, especially when the password is used as a cryptographic key.

Public-key based solutions

A class of public-key exchange techniques has been developed over the past seven years to directly address this limitation of memorized passwords. These methods use public key techniques to remotely prove knowledge of a potentially small secret password, without revealing that secret to any party. A crucial difference between these techniques and classical techniques for password verification is that with these new techniques, even small elements are not exposed to brute-force attacks on the network messages. These methods are preferable to earlier alternatives since they do not use the password as an encryption key, at least not where there is any verifiable plaintext which could permit a dictionary attack. Another distinction is that these methods do not even require a deployed public-key infrastructure or certificate hierarchy.

There are at least two basic forms of these password-authenticated public-key exchange methods. In a basic form, a common shared secret is used on both sides of the connection. In an extended form, one party holds a verifier for the secret, which is constructed as a one-way function of the secret. In extended methods, this verifier is exactly analogous to a public-key, with one important exception: Distribution of this verifier should be restricted to limit the exposure of the verifier to brute-force attack. This is required if one wants to fully protect a password of low or uncertain entropy. Despite this limitation, many of the remaining benefits of the public-key exchange process remain intact.

Typical methods

Several methods in this general class have been developed. The first methods developed included the EKE protocols [BM92], and the "secret public key" protocols [Gong93, Gong95]. More recent work has analyzed and refined these methods [STW95, Pat97], and created several alternative methods including SPEKE [Jab96] and OKE [Luc97]. The class of extended methods includes at least A-EKE [BM94], B-SPEKE [Jab97], and SRP-2 [Wu97].

The P1363 effort

At least one of these methods has been submitted to the IEEE P1363 committee and is under review for inclusion in this standard [P1363] for public-key methods. Integrity Sciences has participated in the P1363 effort to insure that these methods and the closely related Diffie-Hellman key agreement methods are standardized in an appropriate manner, and are safe against a variety of cryptanalytic attacks. In particular, the subgroup confinement problem of Diffie-Hellman is relevant to some of these methods, and the safeguards in P1363 are specifically designed to prevent this problem.

Convergence with classical public-key exchange

With a suitably large and random password, certain extended password-authenticated key exchange protocols provide the exact same benefits as a dual Diffie-Hellman key agreement, with some extra added protection. In the primary D-H exchange, the password serves as a long-term private key for authentication, the verifier serves as the corresponding long-term public key, and the secondary D-H exchange uses ephemeral keys to guarantee perfect forward secrecy. Special modifications are incorporated to give additional protection to the long-term private key, just in case the entropy of this key is smaller than expected. This optimization makes the method superior in all cases to an ordinary dual D-H exchange. In particular the B-SPEKE method is a form of dual Diffie-Hellman exchange, and is one that is specifically designed to permit elliptic curve implementations.

Patents

As a class, many (but not all) of these methods appear covered by patents for the DH-EKE and A-EKE methods. It is possible that other still-pending patents will eventually cover some of the other alternatives. In any case, there appears to be no single patent holder with a monopoly position in these methods, so there is assurance that the competitive situation will be considerably more open than past experience with the original public-key patents might lead us to believe.

I encourage NIST to consider the use of patented techniques, with a reasonable license policy, to be acceptable, especially in the situations where two unrelated patent licensors can provide functionally equivalent methods.

Conclusion

These methods are very important since many of the classical approaches to password authentication have failed to address the problems of passwords with insufficient or indeterminate randomness. This particularly human problem remains, despite many years of attempting to educate and therefore improve human behavior. It is well-accepted that multi-factor authentication is important for strong security, and that these factors should remain as independent as possible for maximum security. Password-based key agreement methods are important for providing an independent factor in multi-factor systems. As passwords remain one of the essential ingredients in personal authentication, we believe it is essential to include the important class of password-based public-key agreement techniques within the FIPS on Public Key Agreement and Exchange.

References

[BM92] S. M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", Proceedings of the I.E.E.E. Symposium on Research in Security and Privacy, Oakland, May 1992.

[BM94] S. M. Bellovin and M. Merritt, "Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise", AT&T Bell Laboratories (c. 1994).

[GLNS93] L. Gong, M. Lomas, R. Needham, & J. Saltzer,

"Protecting Poorly Chosen Secrets from Guessing Attacks",
I.E.E.E. Journal on Selected Areas in Communications,
Vol. 11, No. 5, June 1993, pp. 648-656.

[Jab96] D. Jablon, "Strong Password-Only Authenticated Key
Exchange", Computer Communication Review, vol. 26, no. 5,
pp. 5-26, October 1996.

[Jab97] D. Jablon, "Extended Password Methods Immune to Dictionary
Attack", Proceedings of the WETICE '97 Enterprise Security Workshop,
Cambridge, MA, June 18-20, 1997. Also at <http://world.std.com/~dpj/>

[Luc97] S. Lucks, "Open Key Exchange: How to Defeat Dictionary
Attacks Without Encrypting Public Keys", Proceedings of the
Security Protocol Workshop '97, Springer-Verlag, April 7-9,
1997.

[Pat97] S. Patel, "Number Theoretic Attacks on Secure Password
Schemes", Proceedings of the 1997 IEEE Symposium on Security
and Privacy, May 5-7, 1997.

[P1363] IEEE P1363 working group, "IEEE P1363 Working Draft --
Standards for Public-key Cryptography", This document is
currently available at: <http://stdsbbs.ieee.org/1363>

[STW95] M. Steiner, G. Tsudik, and M. Waidner, "Refinement and
Extension of Encrypted Key Exchange", Operating Systems Review,
vol. 29, Iss. 3, pp. 22-30 (July 1995).

[Wu97] Tom Wu, "The Secure Remote Password Protocol",
Stanford University, July 21, 1997. Pending publication,
this is available at <http://srp.stanford.edu>

===========

From: Scott Schnell <schnell@RSA.COM>
To: "'keyex@nist.gov'" <keyex@nist.gov>
Subject: Additional RSA comments on Key Agreement / Exchange FIPS
Date: Mon, 11 Aug 1997 20:27:20 -0700

August 11, 1997

Director, Information Technology Laboratory
Key Agreement/Exchange FIPS
A231 Technology Building
NIST
Gaithersburg, Md. 20899-0001
<keyex@nist.gov>

Dear Director:

We at RSA Data Security, a major supplier of cryptographic security products and toolkits, are pleased by the announcement that NIST is planning to develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange. RSA encourages this effort and believes that the government and commercial use of cryptography will be enhanced by this initiative.

By authoring a FIPS that includes industry standards such as RSA and Diffie-Hellman, NIST will both provide flexibility in algorithm choice and accelerate the use of commercially successful products employing public key techniques in both the commercial and government sectors. However, the inclusion of several different key agreement and exchange schemes will require specific implementation options and algorithm choices that NIST will need to determine and define. As the industry leader in cryptographic security technology and software toolkits, we urge you to factor in the following items in your decision-making process.

Firstly, we are encouraged that the RSA algorithm is being considered for inclusion in this new FIPS. Its status as the de facto algorithm of choice in practically every security standard for commercial use of cryptography today has given us and others a substantial history and confidence in RSA and commercially applied key lengths as a basis for sound policy.

Secondly, the recommendation of RSA is that the current limited expertise and understanding of elliptic curve cryptosystems (ECC) represents a significant risk for today's data security applications. In protecting valuable data with cryptography, we are relying on the proven strength of a mathematical technique. In industry and cryptographic academia, the trust in this strength is typically earned over years of intensive study. Surprises can never wholly be ruled out, and only by studying a problem closely from many different perspectives can we hope that unforeseen advances are less likely. Our input to the FIPS process is that this immaturity in the state of ECC science warrants substantial caution in including this technology in a FIPS, as it will likely prompt short term deployment. If included, it should be on an exploratory basis. Many of the world's top cryptographers and cryptanalysts share this view, and we present excerpts of their comments below for your review.

Lastly, considerable work remains to fully understand the appropriate choices to be made between the variants of ECC technology. We have observed that the success or failure of a variety of standards over the years has often revolved around both selecting theoretically and empirically proven technologies, and also in implementing these in an "industry standard" way such that each implementation is compliant with others. It is RSA's view that elliptic curve cryptosystem variants are not well or broadly understood, that several of these incorporate vastly different options and implementation choices, and that incompatibility risks warrant further study prior to choices being made on a national or worldwide scale.

Sincerely,

Scott T. Schnell
Vice President of Marketing
RSA Data Security Inc.

Comments from noted cryptographers and cryptanalysts:

"It is true that 160-bit elliptic curve cryptosystems may offer some advantages compared to 1024-bit RSA: smaller keys, less communication, storage, and faster computation. But if I would have to make a choice today between the two, purely based on perceived security, I would opt for 1024-bit RSA. The elliptic curve discrete logarithm problem has been around for a relatively short amount of time. In my opinion only relatively few people have looked at it. Therefore, we cannot yet feel sufficiently confident, where it should be noted that even marginal progress could have very damaging consequences for the security of 160-bit elliptic curve cryptosystems. Thus, right now I think it would not be prudent to switch from 1024-bit RSA to 160-bit elliptic curve cryptosystems."

Dr. Arjen K. Lenstra
VP, Emerging Technologies, Corporate Technology Office
Citibank, N.A.

"Major systems must be based on security technology that meets performance and functionality needs, while leaving little to chance in how well the technology is understood and trusted. The RSA public key cryptosystem meets these needs elegantly, providing superior performance in the most often used scenarios like signature verification, and by being supported by a robust body of research and cryptanalytic results. Elliptic curve technology is interesting, perhaps a little newer than factoring or discrete logs, but needs more study and analysis before it is mature."

Dr. Taher ElGamal
Chief Scientist
Netscape Communications Corp.

"The discrete logarithm problem for elliptic curves is something that is fairly new. Very little research has been done on this problem. There is one specific result by Menezes and Vanstone, STOC 91. It gives a subexponential algorithm for discrete logarithms in supersingular elliptic curves. This suggests that the general problem is of a similar nature as the discrete log modulo primes p (i.e. in the multiplicative group mod p) and the problem of factoring integers. However we do not know subexponential algorithms for all elliptic curves. In the cases we know subexponential algorithms, they are somewhat less efficient than those for factoring integers.

"From what we know now, it looks as if the discrete logarithm problem for elliptic curves is somewhat harder than the discrete logarithm modulo primes p which itself looks a bit harder than factoring integers. But it is unreasonable to assume that it has straight exponential complexity.

"A very particular case are elliptic curves in fields of powers of 2. They have been proposed since there the arithmetic is quite efficient. This particular choice seems to be risky. There are only a few fields that can be used. If the discrete logarithm problem collapses for these particular fields it nearly collapses for all elliptic curves of this type."

Dr. Claus P. Schnorr
Professor of Mathematics and Computer Science
University of Frankfurt a.M.

"Elliptic curves show promise as an alternative basis on which to implement public-key cryptography. They are a plausible "back-up" to RSA in case should someone discover a fast integer factorization algorithm. And in some applications their apparent ability to utilize smaller public keys might be of interest.

"But the security of cryptosystems based on elliptic curves is not well understood, due in large part to the abstruse nature of elliptic curves. Few cryptographers understand elliptic curves, so there is not the same widespread understanding and consensus concerning the security of elliptic curves that RSA enjoys. Over time, this may change, but for now trying to get an evaluation of the security of an elliptic-curve cryptosystem is a bit like trying to get an evaluation of some recently discovered Chaldean poetry. Until elliptic curves have been further studied and evaluated, I would advise against fielding any large-scale applications based on them.

"In the end, time will tell how well they stand up to attack."

Dr. Ronald L. Rivest
Founder
RSA Data Security

"It is correct that I am suspicious of elliptic curve cryptosystems. I have never heard an argument which persuaded me that there were reasons in principle for believing that the discrete logarithm problem on elliptic curves is strictly exponential. I suspect that the lack of a sub-exponential algorithm is merely a matter of neglect and that intense scrutiny - which a commercial implementation of an elliptic curve cryptosystem might engender - could readily change the situation. I am fortified in this opinion by the fact that the Jacobians of hyperelliptic curves (elliptic curves are a special case of hyperelliptic curves) were also suggested for cryptography and their presumed complexity was based on the same arguments used for elliptic curves. Nonetheless Ming-Deh Huang, Jonathan DeMarrais and I [1] were able to show that for `high genus' hyperelliptic curves a subexponential algorithm does exist. I believe that it would be imprudent to base the security of a cryptosystem on the assumption that an exponential time algorithm is required for the elliptic curve problem."

[1] Leonard M. Adleman, Jonathan DeMarrais and Ming-Deh Huang ``A subexponential algorithm for discrete logarithms in the rational subgroup of the Jacobian of a hyperelliptic curve over a finite field''. Proceedings of the 1994 Algorithmic Number Theory Symposium Eds. L.M. Adleman and M-D. Huang. Springer-Verlag Lecture Notes In Computer Science, 877: 28-40. 1994.

Dr. Leonard M. Adleman
Henry Salvatori Professor of Computer Science
University of Southern California

"The public-key cryptosystem of choice for a Public-Key Infrastructure (PKI) is RSA because of its very fast digital signature verification and public-key encryption operations. The competitors to RSA are systems based on the discrete logarithm problem, such as DSA, Diffie-Hellman, and the elliptic curve variants of DSA and Diffie-Hellman. These schemes are competitive with RSA on speed of digital signature generation and private-key decryption, but are up to two orders of magnitude slower at digital signature verification and public-key encryption.

"The importance of the speed of signature verification and public-key encryption can be seen from the way that cryptography is used in a PKI. Consider the example of secure email. An email is signed just once, but that signature must be verified by each recipient. Certificates and revocation lists are signed once by a Certification Authority (CA), but are typically verified many thousands of times. A full-scale PKI will have multiple cross-certified CAs requiring end user software to verify multiple certificates and revocation lists to complete a single transaction. When encrypting email, the symmetric key used to encrypt the email contents must be individually encrypted for each recipient so that many public-key encryptions must be performed to send a single email. These operations are quite fast when using RSA, but are much slower when using DSA, Diffie-Hellman, or their elliptic curve variants.

"The main advantage that elliptic curve cryptography has over other public-key algorithms is that its digital signatures and encrypted symmetric keys are shorter. This is not important for most applications on PCs, but there are other applications where this can be important. Elliptic curve operations can also be implemented fairly compactly in custom silicon.

"Public-Key Infrastructures should be flexible enough to handle the full range of popular public-key algorithms available. Currently, RSA is the most widely used, and this is likely to continue to be the case due to its advantages of fast digital signature verification and fast public-key encryption."

Dr. Michael J. Wiener
Senior Cryptologist
Entrust Technologies

"Recent work carried out at Royal Holloway, University of London indicates that with current technology, and anticipated technology advances, RSA at 706 bits may be required by 2006 to resist attack.

"While one can never rule out the possibility of a mathematical breakthrough, and hence should support the concept of 'algorithm agility', the analysis referenced above suggests, and I believe, that 1024 bit RSA will continue to be considered secure for many years to come."

Dr. Henry Beker
Chairman and Chief Executive
Zergo, plc

===========

X-Sender: jim.brandt@postoffice.worldnet.att.net
Date: Tue, 12 Aug 1997 15:58:08 -0400
To: FIPS186@nist.gov, KEYEX@nist.gov
From: James Brandt <jim.brandt@postoffice.worldnet.att.net>
Subject: NIST Response
Cc: npiazzola@verisiggn.com, jbrandt@verisign.com

Director, Information Technology Laboratory
ATTN: Planned Revision to FIPS 186
Technology Building, Room A231
National Institute of Standards and Technology
Gaithersburg, MD 20899

VeriSign supports the Government's initiatives to revise the Federal Information Processing Standard (FIPS) 186 Digital Signature Standard, and to develop a new FIPS for Public-Key Based Cryptographic Key Agreement and Exchange. In particular, we support the recommendation to incorporate the RSA algorithm within the revised/new FIPS in order to faciltate a more rapid expansion and use of available secure electronic commerce and communications technology by Federal departments and agencies.

As you are already aware, the RSA technology has been adopted as the de facto industry standard with over 80 million products shipped worldwide. These products provide industry, government, and private citizens the ability to securely and reliably conduct business, government, and personal transactions on the Internet easily, efficiently, and at low cost. Although there are many useful applications that have already been pioneered using the RSA security technology, secure web browsing (SSL 2/3) and secure mail (S/MIME) are probably the two most important that could have significant near-term benefit, particularly within government.

VeriSign has worked extensively with Netscape, Microsoft and other leading electronic commerce vendors to seamlessly integrate their secure browser and mail applications with VeriSign's public key infrastructure (PKI) for ubiquitous certificate management and directory services. These commercial security applications, in conjunction with VeriSign's PKI, use the RSA digital signature and key exchange algorithms to provide the security services of authentication, data integrity, non-repudiation, and privacy. The current FIPS 186 compliant DSS algorithm has not been adopted on nearly as wide a scale as has the RSA technology. Failure of wide spread DSS support within commercial security applications has also inhibited the support of DSS by commercial PKI service providers. As a result, most government agencies are left with the unpleasant alternatives to either develop their own custom application and PKI support infrastructure, skirt the FIPS by declaring their project as "pilot" or file a formal waiver in order to take advantage of RSA based commercial security products and PKI services, or delay/postpone implementation. All of these alternatives result in unnecessary cost, inefficiencies, and schedule delay to important re-engineering initiatives that could substantially reduce the cost and improve productivity in the way government agencies operate internally, interact together and with their industry partners, and provide service to the public.

VeriSign agrees with the government that the privacy of a User's signature key should always be maintained and not be divulged to a third party. We further agree there are legitimate business and public safety concerns that justify the use of techniques to support the recovery of encrypted data when access to the User's private encryption key is neither possible or practical. However, these two requirements do not necessarily result in the need to mandate two distinct public/private key pairs (and digital certificates), one for signature and the other for key exchange. A single public/private key pair (and digital certificate) should be permitted at all times, even when "key recovery" is a requirement, since most techniques provide for recovery of the session key without requiring access to the private key used for both signature and key exchange functions.

We appreciate the opportunity to comment on the government's proposed strategy to expand the existing FIPS. We fully concur that the RSA algorithm should be included in a revised FIPS 186 and also be included in a new FIPS for key agreement and exchange, and believe it should be quickly adopted. In so doing, we believe many Federal agencies and departments will be enabled to move forward to implement important re-engineering initiatives that have the potential to significantly reduce the cost of government operations while at the same time improve the efficiency and robustness of its services.

/s/

Nicholas Piazzola
V.P. Federal Markets
VeriSign, Inc