# DIGITAL SIGNATURE STANDARD

We can do better!

Stephen T. Walker
President
Trusted Information Systems, Inc.

July 28, 1993

The National Institute of Standards and Technology (NIST) recently announced its intention to grant Public Key Partners (PKP) an exclusive license to NIST's pending patent for the Digital Signature Algorithm (DSA), stating that this action "will best serve the interests of the Federal Government and the public." While this may be a "good" deal for the Government's own use of the Digital Signature Standard (DSS)[1], it leaves the public in much worse shape for a much longer time than if NIST did nothing. History is full of examples where, if what is thought to be best for the Government is not also clearly best for the public, the Government also loses. This will be yet another example if something is not done very soon. But there are alternatives that open a wide range of possibilities, some not very far from where we wanted to be in the first place with DSS.

This paper explores the background of the present NIST proposal and how we got here. It then analyzes the public key patent situation and provides a high level economic analysis of the impact that the NIST decision will have, followed by a discussion of several alternatives. Finally, it recommends a course of action which seems to serve the interests of the Federal Government and the public much better than the present proposal.

These comments are my own personal opinions and should not be construed as necessarily representing the views of any organization with which I am affiliated.

## Background

In August 1991, after years of urging by Congress and industry, NIST, with the behind-the-scenes help of the National Security Agency (NSA), announced the Digital Signature Standard, which adopts the Digital Signature Algorithm as a proposed Federal Information Processing Standard (FIPS). Most advocates actually wanted a Federal standard for public key encryption that would include both signature and confidentiality capabilities. The

[1] The Digital Signature Algorithm is the algorithm that NIST has chosen to be the Digital Signature Standard. For clarity throughout this document, the term DSS will be used to refer to both the standard and the algorithm.

Rivest/Shamir/Adleman (RSA) algorithm is the obvious choice and is already widely used in the U.S. and around the world. Nonetheless, the Government chose an algorithm which is useful only for signatures and appears to have no plans to choose a public key algorithm for encryption.

DSS is based on a variant of the ElGamal signature algorithm. The Government filed a patent application for DSS in July 1991. Dr. Ray Kammer, then Deputy Director of NIST, testified on June 27, 1991, to the House Subcommittee on Technology and Competitiveness that "the digital signature technique is expected to be available on a royalty-free basis in the public interest world-wide." Several months prior to this, Prof. Dr. C. P. Schnorr of Germany obtained a U.S. patent for his digital signature algorithm. In October 1991, Dr. Schnorr notified NIST of his belief that DSS infringed his patent rights.

The ability to digitally sign information in electronic form is a fundamental capability of great importance to the future of all forms of Electronic Commerce (EC). Some means of verifying the identity of the sender and integrity of the message is essential for the widespread success of EC. Since EC will soon encompass all forms of communications devices including telephones, personal computers, and televisions, a universal, freely available means for digitally signing electronic messages is essential for U.S. industry.

If DSS could provide a royalty free signing capability, many people would view this as an advantage which might outweigh the serious disadvantage of its being incompatible with the widely available, proprietary RSA algorithm which is subject to royalty payments for the next seven (7) years in the U.S.

After the August 1991 announcement, much debate over the technical strengths and weaknesses of DSS ensued, and the Government initiated efforts to resolve the potential patent issues that had arisen over the relationship of DSS to the Schnorr patent and others held by PKP (see The Patent Situation section below). Minor changes to the key length resulted from the first comment period on the proposed standard, and then a long period of silence set in. During 1992, both the Government and PKP pursued the rights to the Schnorr patent and eventually PKP succeeded in licensing those rights.

Then in the June 8, 1993 Federal Register[2], NIST announced its intention to grant an exclusive license to PKP for the NIST DSS patent. In an Appendix to this notice, PKP stated "It is PKP's intent to make practice of the DSA royalty free for personal, non-commercial, and U.S. Federal, state and local government use." Commercial use of DSS would be subject to royalty payments to PKP throughout the life of the Government DSS patent, a period of seventeen (17) years after the patent is awarded (as of this writing, the DSS patent has yet to be awarded).

The Government has not publicly stated all of the reasons why it believes granting PKP this exclusive license is in its and the public's best interests. It is not a far-reaching speculation that this action was viewed by the Government's lawyers as necessary to prevent PKP from charging the Government a royalty for use of DSS based on its infringement of the PKP-owned Schnorr patent. Despite the fact that the Government has royalty free rights to the PKP patents, it does not have rights to the Schnorr patent.

All of this seems most unfortunate for the commercial development of EC. Suddenly the only significant argument for many in the private sector in favor of DSS, the fact that it was to be free for all uses to all users, is gone. Without that positive benefit, there no longer appears to be any advantage to DSS, and the negative factor, its incompatibility with RSA (now even more widely used), looms all the more heavily. Much of industry will continue to use RSA irrespective of the Government's position on DSS, so those who must interact with both industry and the Government will be forced to use both algorithms, each with its own royalty payment. The difficulties of validating digital signatures based on two incompatible algorithms have been described in detail at the February 1993 NIST-sponsored Federal Digital Signature Applications Symposium.

The Government has always maintained that DSS is not covered by earlier patents. However, to avoid lengthy patent disputes and to get its proposed algorithm approved quickly, the Government has, unfortunately, lost sight of one of its original objectives. The Government has protected its own direct interests by getting royalty free use of its own algorithm, but at an enormous price to the American public. Does the Government have the right to propose a Federal standard that goes directly against a well established industry trend (the use of RSA)

---

[2] The announcement was signed by the Acting Director of NIST on June 2, 1993, the first of three days of public hearings on the Government's policies on cryptography by the Computer System Security and Privacy Advisory Board (CSSPAB), a Congressionally chartered Board charged with advising the Executive and Legislative Branches on technical matters relating to computer security. Had the Government thought to have this major development in the long struggle to get a digital signature FIPS revealed to the public for criticism or endorsement, they would have had the perfect audience and opportunity. Unfortunately, those in charge decided to keep the announcement under wraps until four days after the meeting, missing an excellent opportunity to explain the circumstances behind their decision.

and that will result in U.S. commercial interests having to pay substantially greater royalty fees? Can a FIPS be promulgated without an analysis of the impact it will have on the public? The answers appear to be yes, but there are alternatives that should be considered first.

## The Patent Situation

To understand these alternatives, we must first understand some basic facts about the public key patent situation.

In the early 1980s, four patents covering various forms of public key cryptography were granted. They are, in order of date of patent award:

(1) Patent #: 4,200,770 — Issued on: April 29, 1980; Expires on: April 29, 1997

Diffie/Hellman - Cryptographic Apparatus and Method
(the "Diffie-Hellman" key exchange, covering both the secure generation and the secure exchange of the key)

(2) Patent #: 4,218,582 — Issued on: August 19, 1980; Expires on: August 19, 1997

Hellman/Merkle - Public Key Cryptographic Apparatus
(general concepts of secure communications using public key cryptography and general concepts of digital signature; specific public key "knapsack" systems for secure communications)

(3) Patent #: 4,405,829 — Issued on: September 20, 1983; Expires on: September 20, 2000

Rivest/Shamir/Adleman - Cryptographic Communications System and Method
(cryptographic communications systems employing the "RSA" algorithm)

(4) Patent #: 4,424,414 — Issued on: January 3, 1984; Expires on: January 3, 2001

Hellman/Pohlig - Exponentiation Cryptographic Apparatus and Method
(variant of Diffie-Hellman for secure exchange of messages)

In the late 1980s, the owners/licensees of these patents banded together to form Public Key Partners.

Because the research that developed these algorithms was sponsored by the U.S. Government, the Government has royalty free access to these technologies.

In 1985, ElGamal published a paper on a digital signature technique but did not seek a patent. In August 1989, Schnorr published a paper on this subject and in 1991 received a U.S. patent:

| | | |
|---|---|---|
| Patent #: 4,995,082 | Issued on: | February 19, 1991 |
| | Expires on: | February 19, 2008 |

Schnorr - Method for Identifying Subscribers and for Generating and Verifying Electronic Signatures in Data Exchange Systems
(data exchange system working with processor chip cards to perform identification and electronic signature generation/verification procedures)

The U.S. Government does not have royalty free access to the Schnorr patent.

After NIST announced the proposed DSS in August 1991, Schnorr informed NIST of his belief that DSS infringed on his patent. Sometime later, PKP obtained a license for the Schnorr patent, giving them a virtual monopoly in public key technology patents in the U.S.

Economic Impact of NIST's June 8 Announcement

I recently asked NIST if the Government had analyzed the economic impact on the Government or the public of granting an exclusive license to PKP for DSS. I was told that no such analysis had been done.

The following high level analysis offers some very approximate estimates of what it might cost if DSS, licensed as proposed by NIST, were fully accepted by industry and became widely used. We acknowledge that these estimates could be off by as much as a factor of five (5) or more either way, nonetheless they tell a compelling story.

In its July 26, 1993 issue, *Business Week* discussed home shopping networks which will involve the use of televisions, telephones, and personal computers. The article describes recent conglomerates that will reach "more than 60 million viewers, or two thirds of all television households."

If digital signature standards were routinely available today, they would be highly useful in confirming the identity of the purchaser and the authenticity of the purchase request.

The cost of a DSS royalty per the NIST announcement "will be no more then 2 1/2% for hardware products and 5% for software, with the royalty rate further reduced to 1% on any portion of the product price exceeding $1000."

The analysis below focuses on the potential home shopping market for the Digital Signature Standard involving televisions, telephones, and personal computers. It assumes conservative numbers of devices, periods of use, and royalties to derive potential royalty figures.

Assuming: 60 million televisions used in home retail
that need to be replaced every five (5) years and
a royalty of $2.50 per television
(5% of the $50 price for the signature software),

during the seventeen (17) years that the public will have to pay royalties to PKP for DSS, the cost will be approximately $500 million.
(60 million * 17 years/5 years * $2.50)

Assuming: 150 million telephones, only 20% involved in home retailing
that need to be replaced every five (5) years and
a royalty of $2.50 per telephone,

the royalty cost will be approximately $250 million.
(150 million * 20% * 17 years/5 years * $2.50)
If one includes growth from new phone markets, this number could easily grow to $750 million.

Assuming: 40 million personal computers and workstations
that need to be replaced every five (5) years and
a royalty of $5.00 per computer,

the royalty cost will be approximately $680 million
(40 million * 17 years/5 years * $5.00)

Approximate total royalty payment over seventeen (17) years is $2 billion.

These are rough estimates for one business segment. They do not take into account business use for banking, financial, or dozens of other commercial uses. If one chooses to scale these down by five (5) to be even more conservative, the $2 billion royalty bill drops just below $400 million. Others may want to raise the estimate by five (5) because of growth in a rapidly emerging industry, raising it to over $10 billion.

These are of course hypothetical scenarios that assume DSS is widely endorsed by industry and becomes a commercial standard.

No matter how one looks at this deal, it's a very good thing the Government got use of the DSS for free, because the public certainly will pay a fortune for it.

Alternatives?

The Government appears to have been operating under the premise that DSS, as currently defined, is its only possible way to proceed. The close relationship of DSS to the Schnorr patent makes it subject to infringement charges from PKP. This unfortunate relationship seems to have forced the Government to their June 8 "give away" of DSS as "best serving the Federal Government and the public."

However, we should recognize that within four (4) years, the Hellman/Merkle patent, which is the principal broadly based public key signature patent, expires. At that time, one could implement an ElGamal-based algorithm which did not use the techniques of the Schnorr patent and is therefore royalty free from then on. The Schnorr techniques involve efficiency enhancements for ElGamal, but even if this new approach were not as efficient as the present DSS, the removal of patent issues and royalty payments would make up for a lot of inefficiency.

The above alternative suggests doing nothing for four (4) years except defining a new signature algorithm (which may take that long anyway). Of course, we could take this path immediately and agree to pay PKP royalties for the new algorithm until the Hellman/Merkle patent expires. The Government would not be subject to these royalties since it has a free license to the technology anyway. Commercial users and developers would be much less unhappy to pay royalties for a few years rather than for seventeen (17). NIST scientists could start immediately to identify an ElGamal-based algorithm that is not subject to Schnorr patent restrictions. There are indications in the highly censored minutes to the NIST-NSA Technical Working Group that there were at least three (3) other algorithms being considered before the present DSS candidate was chosen, so perhaps we already have a head start on this process.

Realizing that this alternative algorithm approach could reduce PKP's potential royalty period for DSS from seventeen (17) years to four (4) years opens other alternatives that include paying PKP a reasonable sum based on estimates of DSS royalties for this limited period, to allow royalty free use of the present DSS for all users forever. Faced with the alternative of the extremely high royalty payments discussed above, it is likely that a Government/industry consortium could be formed to raise the funds to eliminate the four (4) year wait and the need to switch to a new algorithm.

Of course, such a Government/industry consortium could also decide to apply pressure on PKP to grant, as IBM did with the Data Encryption Standard algorithm, royalty free use for the public for all time. PKP could continue to collect royalties on all its other algorithms but, in return for the Government's (and, therefore, the public's) having paid for the research that led to those patents in the first place, PKP should make DSS available for all royalty free.

There are those who claim the whole DSS exercise has been forced upon us because some in Government do not want to see RSA become a widely used "standard." Those individuals must recognize that the present plan is working directly against their desires. The RSA patents expire in seven (7) years, while the NIST plan forces a seventeen year (17) royalty period. Industry will choose the shorter period, and DSS will be relegated to Government special purchase efforts. Indeed, after the RSA patent expires, it will be impossible for the Government to get DSS from any commercial source. Thus, by the very terms of the June 8 announcement, RSA will become the de facto standard for digital signature that these individuals want to prevent.

Reflecting on this range of alternatives, it quickly becomes apparent that the June 8 approach advocated by the Government is just about the worst approach one could devise. (Please do not try to find a worse one!)

## A Suggested Plan of Action

We strongly suggest that the Government back up from its headlong plunge toward indenturing the U.S. public for a much needed Digital Signature Standard. There are alternatives, if we are willing to wait a few years, that will reduce a high royalty payment bill to zero. There are approaches to analyzing this situation that allow continuing with DSS at a greatly reduced cost to the American public, perhaps even reducing it to zero. Any of these approaches will yield a more economically viable and more generally available solution which serves the interests of the Federal Government and the public far better than the present plan.

Even if none of these alternatives are pursued, this analysis shows that everyone, including the Government, will be better off if NIST just dropped DSS, including the plan announced on June 8, 1993, and did nothing else.

Please, NIST, reconsider your options before it's too late!