Digital Security Signed, Sealed, Delivered

The handwritten signature at the end of a letter or contract stands as a simple and reasonably reliable means of authenticating the document. But when a document exists only in electronic form, anyone can affix an identifying string of electronic characters, or alter the text itself, without leaving a trace of forgery.

Over the last decade or so, computer scientists and cryptographers have developed a variety of ingenious schemes, known as digital signatures, to guarantee that an electronic document is genuine. Now the National Institute of Standards and Technology (NIST) in Gaithersburg, Md., has issued a proposal for a digital signature standard, which allows recipients of electronically transmitted information to verify the sender's identity and the data's integrity. The announcement appears in the Aug. 30 FEDERAL REGISTER.

"The fact that the government has finally come forth with a proposed standard is very important," says Stephen T. Walker, president of Trusted Information Systems, Inc., in Glenwood, Md. "It's too bad that it's taken so long. There's a whole lot of areas where digital signatures are crucial."

The proposed standard specifies a particular mathematical procedure for creating and verifying a digital signature. Although it would apply only to unclassified information in federal government computer systems, it would likely have a considerable influence on other computer users as well. Many companies, for example, have been reluctant to select a particular digital signature scheme for their electronic transmissions without some assurance that the chosen method will be widely used and that it harbors no weaknesses that could be exploited by an unscrupulous party bent on fraud.

"The existence of a standard should make vendors more willing to offer [a digital signature scheme] and people more willing to use it," says Joan Feigenbaum of AT&T Bell Laboratories in Murray Hill, N.J.

But controversy surrounds NIST's choice of an unfamiliar mathematical algorithm as the federal standard for generating and verifying a digital signature. "If no one challenges what they've done, we'll be stuck with a weakened standard," says Jim Bidzos, president of RSA Data Security, Inc., in Redwood City, Calif., which produces equipment and software based on a rival, proprietary digital signature and encryption method known as RSA.

The proposed NIST algorithm, like most digital signature methods, relies on a concept known as public-key cryptography. Such schemes use two mathematically related "keys" – one for encrypting a message as a scrambled string of bits, and a complementary key for unscrambling the encoded message.

Because one key can't easily be derived from the other, a user can keep one key secret, using it to create a digital signature, and make public the other key so that anyone can verify – but not forge – that signature. The same procedure can be applied to a sample of bits from the text itself, which acts as a kind of fingerprint to allow detection of surreptitious alterations in an electronically transmitted or stored document.

The RSA method is the most widely used and best-known method for producing such keys for both encrypting messages and creating digital signatures. Its security depends on the computational difficulty of factoring a large number to find the two prime numbers that were multiplied together to generate the original number. In contrast, the proposed NIST method relies for its security on the difficulty of computing what are called discrete logarithms.

At a congressional hearing in June, NIST Deputy Director Raymond G. Kammer described the criteria used to select the proposed standard. "Our efforts in this area have been slow, difficult and complex," he testified. "We evaluated a number of alternative digital signature techniques and considered a variety of factors in this review." Those factors included the degree of security provided, the ease of implementation in both hardware and software, the ease of export from the United States, the applicability of patents, and the level of efficiency for generating and verifying signatures.

Guided by these criteria and assisted by representatives from the National Security Agency, NIST officials rejected the RSA method, which is protected by a number of patents in the United States, and developed an alternative approach that, according to government lawyers, isn't covered by existing patents. The future of the proposed standard now depends on how well it survives a concerted mathematical attack regarding its security, and on the resolution of any conflicting patent claims that may arise.

"Should there be some kind of weakness, [NIST] is putting its method into the public record in order to enable people to try to uncover that weakness," says computer scientist Michael O. Rabin of Harvard University. "If the system passes the mathematical test, then it would certainly be a possible way of doing digital signatures." – *I. Peterson*

Milking engineered 'pharm animals'

In the first steps toward populating a biotechnological barnyard, research teams in the United States and Scotland report that genetically engineered goats and sheep can secrete medically useful quantities of drugs in their milk. And according to scientists in the Netherlands, cows may become the next four-legged drug factories down on the pharm.

All three groups, who describe their work in the September BIO/TECHNOLOGY, say the new findings illustrate the potential of harnessing transgenic livestock to produce drugs more rapidly, more cheaply and in greater quantities than the standard "bioreactor" approach, in which vats of gene-altered bacteria or culture dishes of animal cells churn out genetically engineered drugs.

"Commercialization of this technology will permit further development of complicated proteins that are currently difficult and expensive to produce with bacteria or mammalian cells," says Henri A. Termeer, chairman of Genzyme Corp. in Cambridge, Mass.

"Our success with transgenic goats demonstrates the feasibility of producing commercially viable pharmaceuticals from livestock," adds Karl M. Ebert of Tufts University School of Veterinary Medicine in North Grafton, Mass., who coordinated the goat experiments in collaboration with Genzyme.

Genzyme

The milk of this transgenic nanny contains the clot-dissolving drug TPA.

The Tufts-Genzyme study yielded two goats – one male, one female – carrying human genes for an enzyme called tissue plasminogen activator (TPA). Many countries, including the United States, have approved TPA for dissolving blood clots in cases of myocardial infarction, the primary cause of heart attacks.

Ebert and his collaborators produced the transgenic goats by surgically remov-