

AAAS

Janet Raloff and Richard Lipkin report from Atlanta at the American Association for the Advancement of Science annual meeting

A digital notary

In an increasingly paperless society, information often exists only in the digital netherworld of electronic files. As such, documenting records has become a dicey affair.

For instance, during the 1991 Senate confirmation hearings of Clarence Thomas as a justice of the U.S. Supreme Court, telephone logs arose as evidence. When Thereza Imanishi-Kari's laboratory came under investigation for scientific fraud, the authenticity of notebook entries became relevant. On Wall Street in 1992, officers of a computer corporation came under fire for allegedly backdating financial records.

How does one prove that no one has tampered with or altered computer files needed to confirm legal facts?

To solve this problem, Stuart Haber and W. Scott Stornetta, both at Bellcore in Morristown, N.J., and Surety Technologies in Chatham, N.J., have created a "digital notary system."

Haber describes the system as "a publicly verifiable insurance policy," which proves that a computer record "existed in a specific form at a specific time" and that the file "has not been altered."

When linked to an individual's or company's computer system, the digital notary certifies files by producing a coded fingerprint of a document, using a mathematical process called one-way hashing. The process distills the document down to a short, unique string of characters. Changing even one letter or number in the notarized document would create a totally different coded string.

The fingerprint itself contains no data from the document. Rather, it functions as a code that can be used to reconstruct and authenticate a file, Haber says. Every time a document gets certified, the system generates a so-called electronic time stamp. The stamp becomes part of a collective file whose code is publicly logged on the Internet and published weekly in the New York Times.

"Publishing the code in a public place guarantees that it existed in a particular form at a particular time," Haber says. "There's no way to falsify it."