



(12) **United States Patent**
Levine

(10) **Patent No.:** **US 6,393,566 B1**
(45) **Date of Patent:** **May 21, 2002**

(54) **TIME-STAMP SERVICE FOR THE NATIONAL INFORMATION NETWORK**

(75) Inventor: **Judah Levine**, Boulder, CO (US)

(73) Assignee: **National Institute of Standards and Technology**, Washington, DC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1192 days.

(21) Appl. No.: **08/508,747**

(22) Filed: **Jul. 28, 1995**

(51) **Int. Cl.**⁷ **H04L 9/30**; G06F 1/12

(52) **U.S. Cl.** **713/178**; 713/200; 713/400

(58) **Field of Search** 380/30; 713/176-179, 713/156, 400, 200

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,868,877 A	9/1989	Fischer	
5,001,752 A	3/1991	Fischer	
5,005,200 A	4/1991	Fischer	
5,022,080 A	6/1991	Durst et al.	
5,031,214 A	7/1991	Dziewit et al.	
5,136,646 A	8/1992	Haber et al.	
5,136,647 A	8/1992	Haber et al.	
5,163,091 A	11/1992	Graziano et al.	
5,189,700 A	2/1993	Blandford	
5,191,613 A	3/1993	Graziano et al.	
5,214,702 A	5/1993	Fischer	
5,367,573 A	11/1994	Quimby	
5,373,561 A	12/1994	Haber et al.	
5,497,422 A	* 3/1996	Tysen et al.	380/25

OTHER PUBLICATIONS

Lechter, "Doing Business on Internet: the Electronic Signature," Mar. 9, 1995.
Garfinckel, "Patented Secrecy," Forbes, Feb. 27, 1995, pp. 122-124.

Cipra, "Electronic Time-Stamping: The Notary Public Goes Digital," and "All the Hash That's Fit to Print;" Science, Jul. 9, 1993.

Anderson, "Foiling the Forgers ," Discover Magazine, 10-92.

Federal Information Processing Standards Publications 186, Digital Signature Standard (DSS), May 19, 1994.

Federal Information Processing Standards Publications 180, Secure Hash Standard, May 11, 1993.

* cited by examiner

Primary Examiner—Gilberto Barron, Jr.

(74) *Attorney, Agent, or Firm*—Charles E. Rohrer

(57) **ABSTRACT**

A system and method for time-stamping and signing a digital document by an authenticating party and returning the signed stamped document to the originator or his designated recipient. Messages may be received by a first "public" machine over a network, by fax, or through input mediums such as diskettes. The clock of the first machine is synchronized with Universal Coordinated Time (UTC) and can be checked for accuracy by anyone on the network. A second "private" machine, not connected to any network, receives the time-stamped message, applies a hashing procedure and provides a signature using a private key. The signed hashed time-stamped message is then returned. A verify procedure is made widely available to check the genuineness of a document by rehashing the document and applying a public key. The result should match the signed time-stamped message returned by the authenticating party.

12 Claims, 7 Drawing Sheets

