US005604803A

United States Patent [19]

Aziz

[11] Patent Number: 5,604,803

[45] Date of Patent: Feb. 18, 1997

[54] **METHOD AND APPARATUS FOR SECURE REMOTE AUTHENTICATION IN A PUBLIC NETWORK**

[75] Inventor: **Ashar Aziz**, Fremont, Calif.

[73] Assignee: **Sun Microsystems, Inc.**, Mountain View, Calif.

[21] Appl. No.: **253,802**

[22] Filed: **Jun. 3, 1994**

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/25**; 380/21

[58] **Field of Search** 380/4, 21, 25, 380/49, 50; 340/825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,193,131	3/1980	Lennon et al.	380/25
4,349,695	9/1982	Morgan et al.	380/25
4,736,423	4/1988	Matyas	380/25
4,817,140	3/1989	Chandra et al.	380/25

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

2168831 11/1984 United Kingdom .

OTHER PUBLICATIONS

Whitfield Diffie, "The First Ten Years of Public–Key Cryptography", (Proceedings of the IEEE, vol. 76, No. 5, May 1988).

Paul Fahn, "Answers to Frequently Asked Questions About Today's Cryptography", (RSA Laboratories, 1992).

"Part I: Message Encryption and Authentication Procedures", (Privacy Enhancement for Internet Electronic Mail, J. Linn (Network Working Group).

"Part II: Certificate–Based Key Management", (Privacy Enhancement for Internet Electronic Mail, S. Kent (Network Working Group).

"Part III: Algorithms, Modes, and Identifiers", (Privacy Enhancement for Internet Electronic Mail), D. Balenson (Network Working Group).

"Part IV: Key Certification and Related Services" (Privacy Enhancement for Internet Electronic Mail), B. Kaliski (Network Working Group).

Whitfield Diffie, Paul C. Van Oorschoot and Michael J. Weiner, "Authentication and Authenticated Key Exchanges" (Designs, Codes and Cryptography, 2–107–125 (1992), Kluwer Academic Publishers).

"The MD5 Message–Digest Algorithm", MIT Laboratory for Computer Science and RSA Data Security, Inc. (1992) R. Rivest (Network Working Group).

RSA Data Security, Inc. Technology Bulletin.

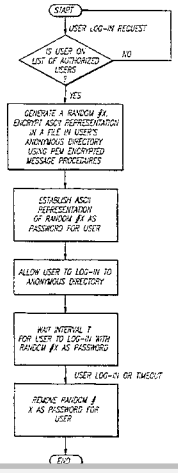
Primary Examiner—Salvatore Cangialosi

Attorney, Agent, or Firm—Irell & Manella LLP

[57] **ABSTRACT**

A client workstation provides a login address as an anonymous ftp (file transfer protocol) request, and a password as a user's e-mail address. A destination server compares the user's e-mail address provided as a password to a list of authorized users' addresses. If the user's e-mail address is located on the list of authorized users' addresses maintained by the destination server, the destination server generates a random number (X), and encrypts the random number in an ASCII representation using encryption techniques provided by the Internet Privacy Enhanced Mail (PEM) procedures. The encrypted random number is stored in a file as the user's anonymous directory. The server further establishes the encrypted random number as one-time password for the user. The client workstation initiates an ftp request to obtain the encrypted PEM random number as a file transfer (ftp) request from the destination server. The destination server then sends the PEM encrypted password random number, as an ftp file, over the Internet to the client workstation. The client workstation decrypts the PEM encrypted file utilizing the user's private RSA key, in accordance with established PEM decryption techniques. The client workstation then provides the destination server with the decrypted random number password, which is sent in the clear over the Internet, to login to the destination server. Upon receipt of the decrypted random number password, the destination server permits the user to login to the anonymous directory, thereby completing the user authentication procedure and accomplishing login.

20 Claims, 4 Drawing Sheets



U.S. PATENT DOCUMENTS

5,056,140	10/1991	Kimbell	380/25
5,109,413	4/1992	Comerford et al.	380/4
5,136,642	8/1992	Kawamura et al.	380/21
5,323,146	7/1994	Glaschick	340/825.34
5,323,465	6/1994	Avarne	380/25

FIG. 1

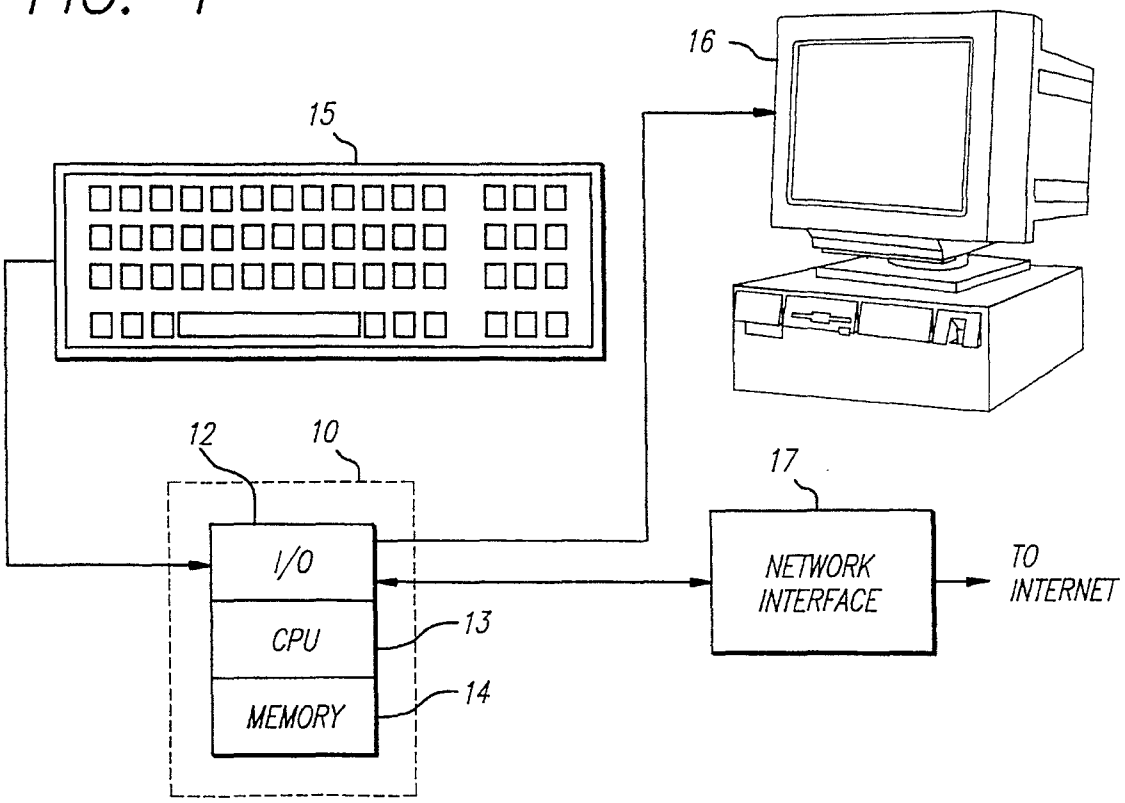


FIG. 2

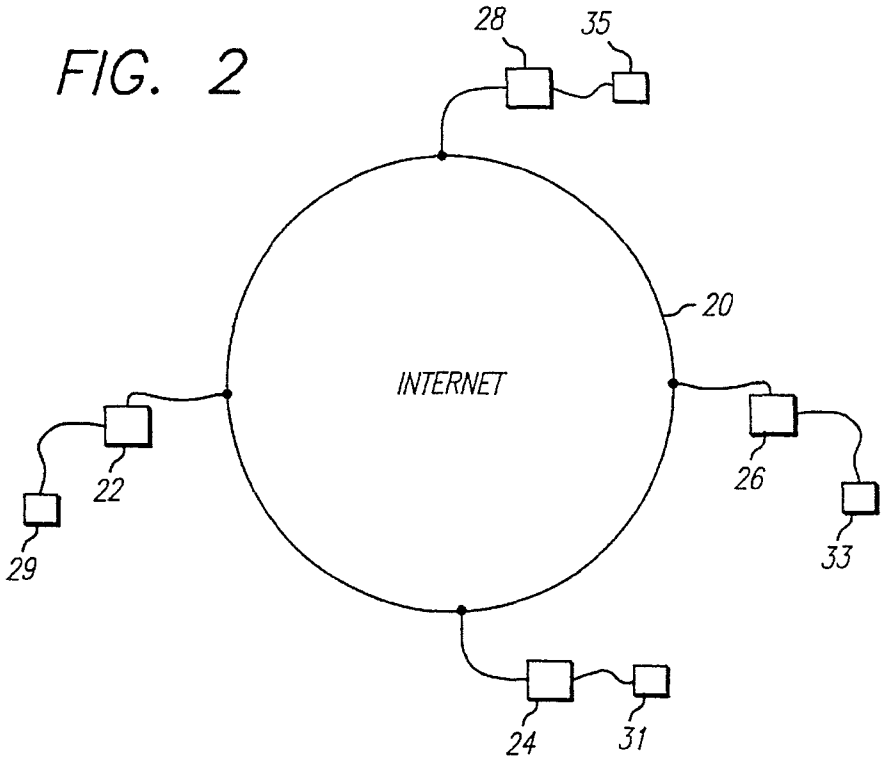


FIG. 3

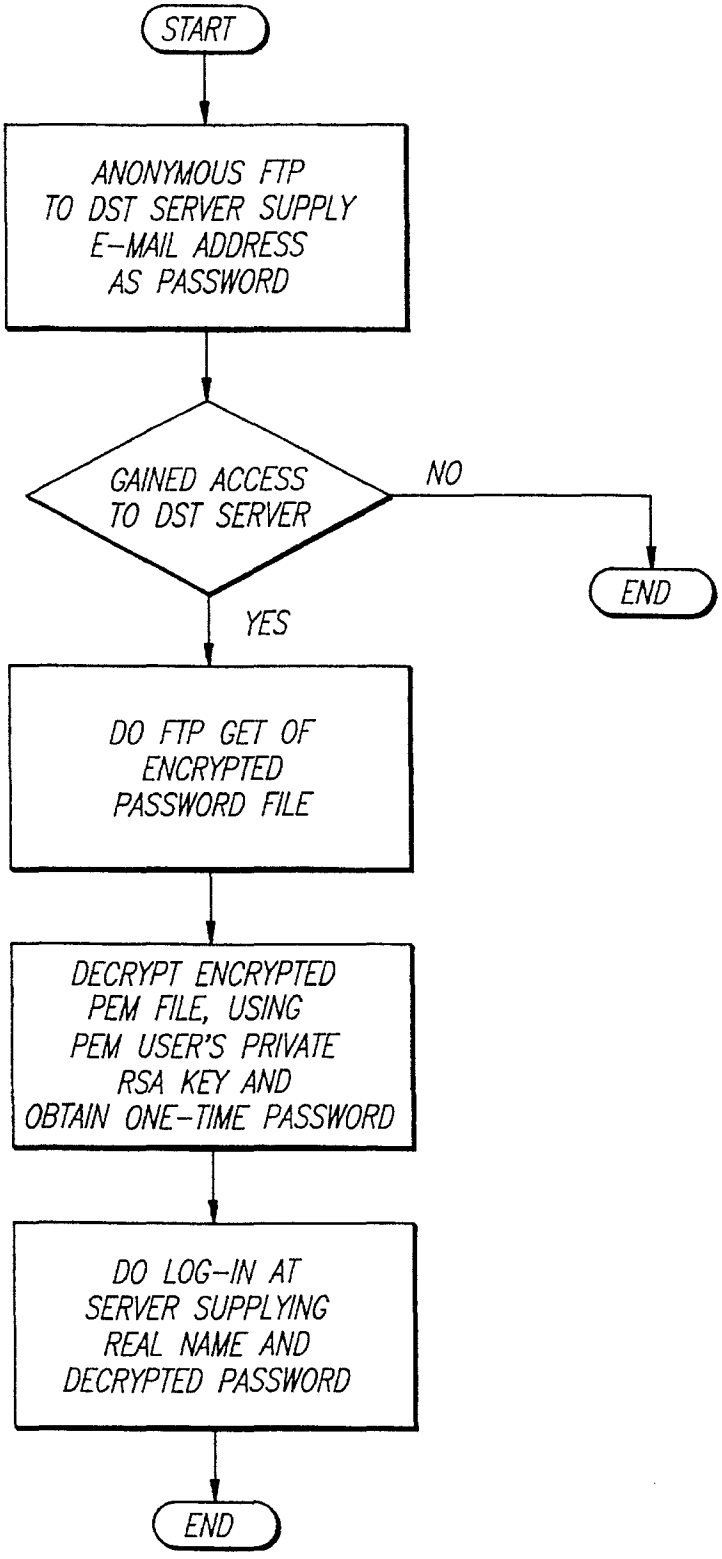
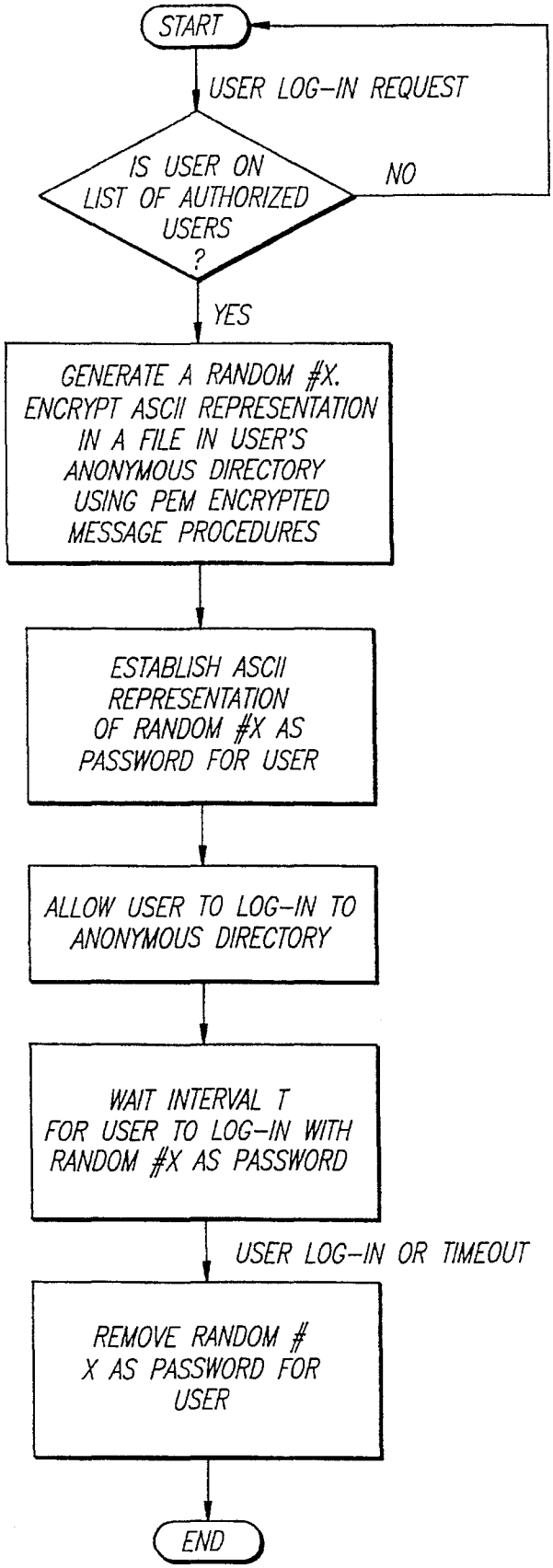


FIG. 4



DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.