US005402490A

United States Patent [19]

Mihm, Jr.

[11] Patent Number: 5,402,490

[45] Date of Patent: Mar. 28, 1995

[54] **PROCESS FOR IMPROVING PUBLIC KEY AUTHENTICATION**

[75] Inventor: **Thomas J. Mihm, Jr.**, Mesa, Ariz.

[73] Assignee: **Motorola, Inc.**, Schaumburg, Ill.

[21] Appl. No.: **937,772**

[22] Filed: **Sep. 1, 1992**

[51] **Int. Cl.**[6] **H04L 9/08**

[52] **U.S. Cl.** **380/21**; 380/25; 380/30

[58] **Field of Search** 380/21, 23–25, 380/30, 52; 340/825.34

[56] **References Cited**

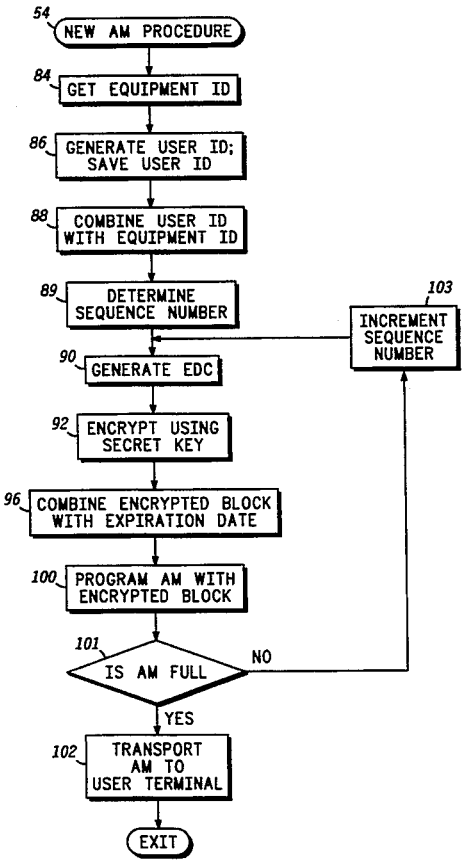
U.S. PATENT DOCUMENTS

3,665,162	5/1972	Yamamoto et al.	380/23
4,423,287	12/1983	Zeidler	380/23
4,438,824	3/1984	Mueller-Schloer	380/25
4,691,350	9/1987	Kleijne et al.	380/52
4,956,863	9/1990	Goss	380/30
5,012,514	4/1991	Renton	380/52
5,029,207	7/1991	Gammie	380/23
5,033,084	7/1991	Beecher	380/25
5,036,461	7/1991	Elliot et al.	340/825.34
5,077,790	12/1991	D'Amico et al.	380/23
5,093,860	3/1992	Steinbrenner et al.	380/21
5,161,189	11/1992	Bray et al.	380/21
5,185,795	2/1993	Bright	380/25
5,189,700	2/1993	Blandford	380/23

Primary Examiner—Salvatore Cangialosi

Attorney, Agent, or Firm—Robert M. Handy; Gregory J. Gorrie

[57] **ABSTRACT**

An environment which includes a communications network, user terminals, and an authentication center provides communication services only to legitimate subscribers. The authentication center receives an equipment ID for each terminal, generates a series of sequence numbers and uses a secret key to encrypt the sequence numbers and the equipment ID with a user ID and an error detection code to form an encrypted block. This block is programmed into an authentication module and sent to the subscriber for installation in the subscriber's terminal. The authentication center sends a public key to network authentication nodes. When the subscriber operates the terminal to gain access to the network, a log-on message, which includes the encrypted block and an unencrypted version of the equipment ID, is sent to an authentication node. The node decrypts the encrypted block and evaluates the IDs and sequence number to determine whether to grant access to services.

32 Claims, 8 Drawing Sheets