US006968459B1

(12) **United States Patent**
Morgan et al.

(10) **Patent No.: US 6,968,459 B1**
(45) **Date of Patent: Nov. 22, 2005**

(54) **COMPUTING ENVIRONMENT HAVING SECURE STORAGE DEVICE**

(75) Inventors: **Jeffrey A. Morgan**, Afton, MN (US); **C. Thomas Jennings**, Woodbury, MN (US); **Larold L. Olson**, Lindstrom, MN (US); **Luiz S. Pires**, St. Paul, MN (US); **Daniel P. Stubbs**, Marine on St. Croix, MN (US)

(73) Assignee: **Imation Corp.**, Oakdale, MN (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/464,347**

(22) Filed: **Dec. 15, 1999**

(51) **Int. Cl.**[7] **G06F 12/14**; G06F 12/16; H04L 9/00

(52) **U.S. Cl.** **713/189**; 713/164; 713/165

(58) **Field of Search** 713/164, 165

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,412,718	A	5/1995	Narasimhalu et al.	
5,475,839	A *	12/1995	Watson et al.	713/2
5,887,131	A *	3/1999	Angelo	713/202
6,067,622	A *	5/2000	Moore	713/200
2002/0124176	A1 *	9/2002	Epstein	713/186

FOREIGN PATENT DOCUMENTS

EP	0 706 174 A1	4/1996

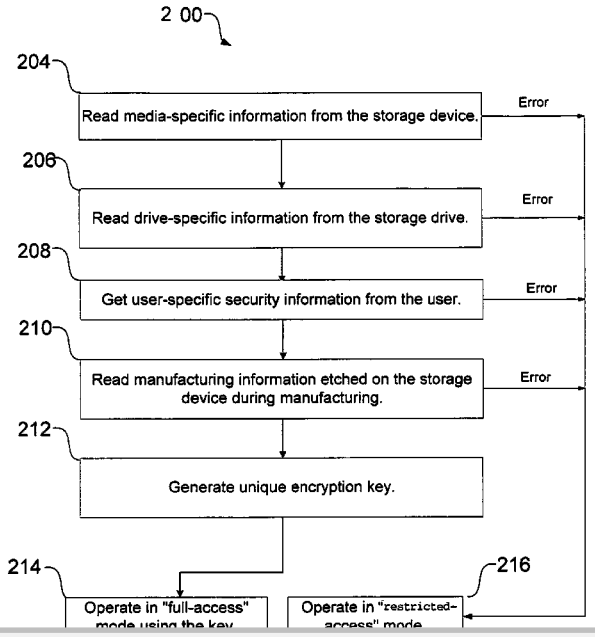
* cited by examiner

Primary Examiner—Matthew Smithers
(74) *Attorney, Agent, or Firm*—Eric D. Levinson

(57) **ABSTRACT**

A secure computing environment in which a computer automatically operates in a full-access data storage mode when it detects the presence of a secure removable storage device. In full-access mode all data written to removable storage device is encrypted with a cryptographic key and the user is given access to sensitive if authorized. Otherwise, the computer operates in a restricted-access mode in which the user is unable to write to the removable storage device and is unable to access sensitive data. The invention detects security information on the data storage device and generates a cryptographic key from the security information. The security information can be a function of the unique format characteristics of the underlying storage medium, a unique identifier retrieved from an electronic circuit embedded within the removable storage device or a serial number etched on the storage device during manufacturing. In addition, drive-specific information and even user-specific information can also be used to generate the cryptographic key, thereby creating a highly secure computing environment. When the computer operates in a full-access mode, all data written to the storage device is encrypted and the user is able access to sensitive data within the organization. When security information is not present on the removable storage device the computer automatically operates in a restricted-access mode in which the user does not have access to sensitive data and data cannot be written to the removable storage device.

50 Claims, 5 Drawing Sheets



DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

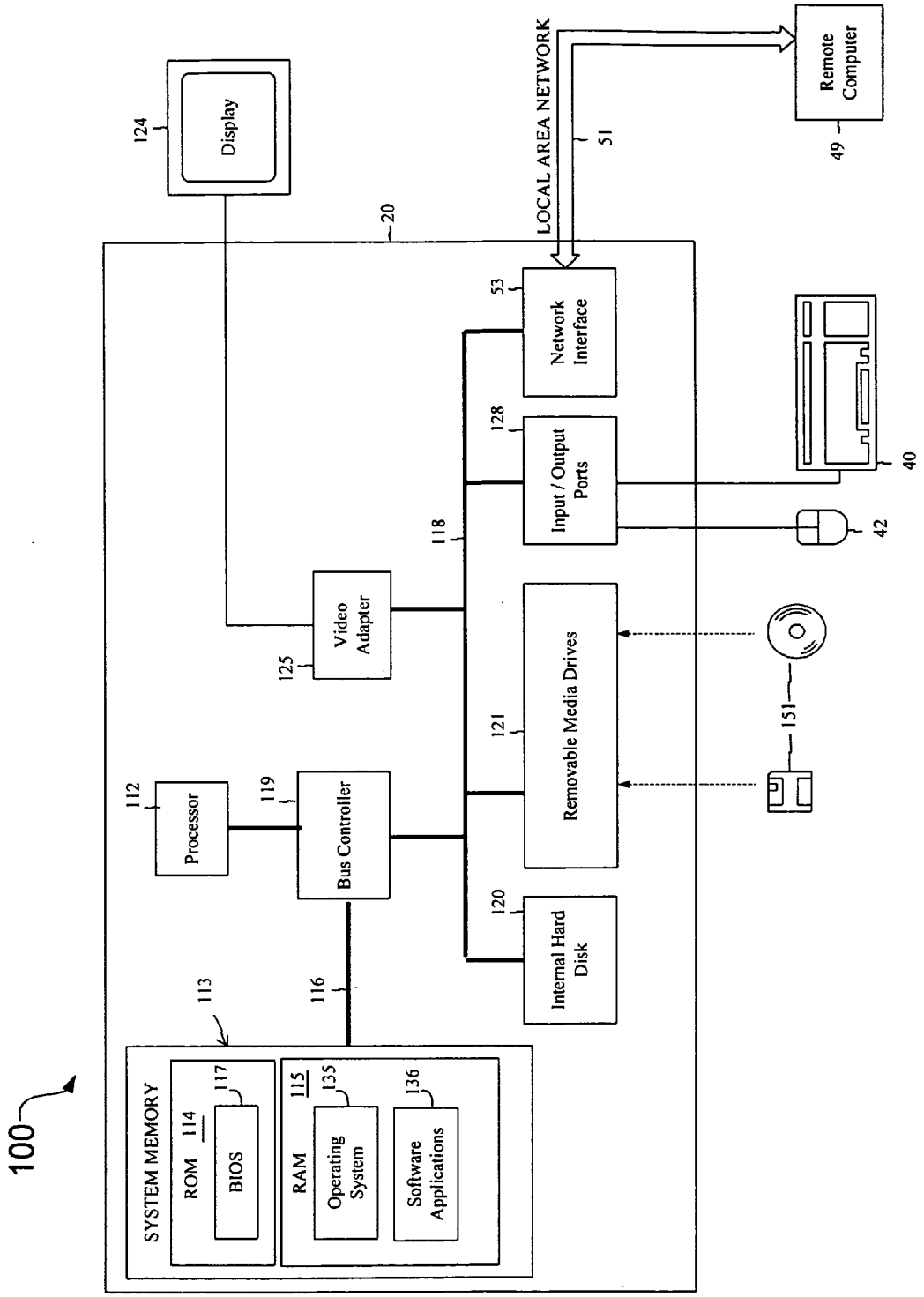


FIG. 1

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

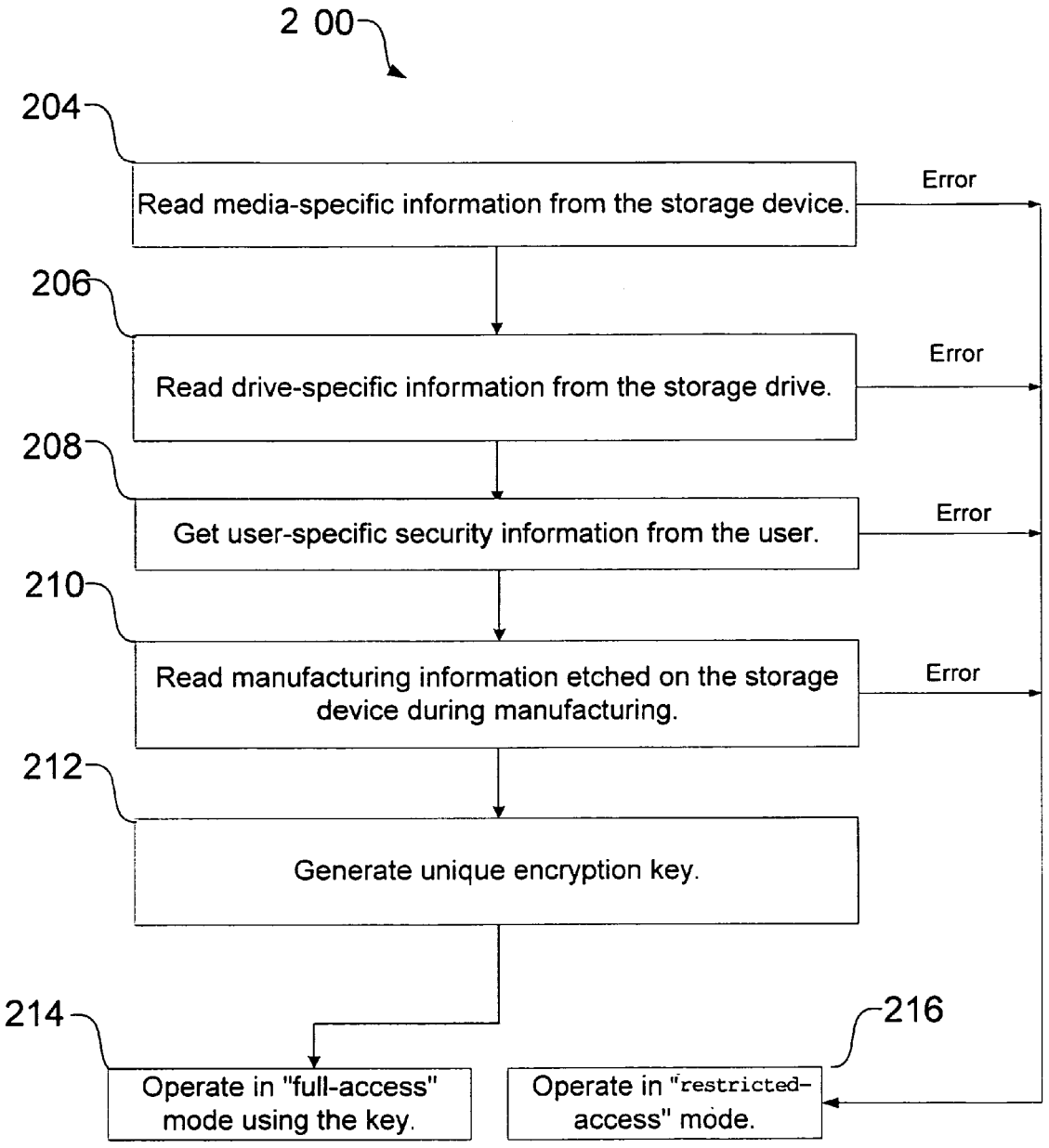


FIG. 2

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

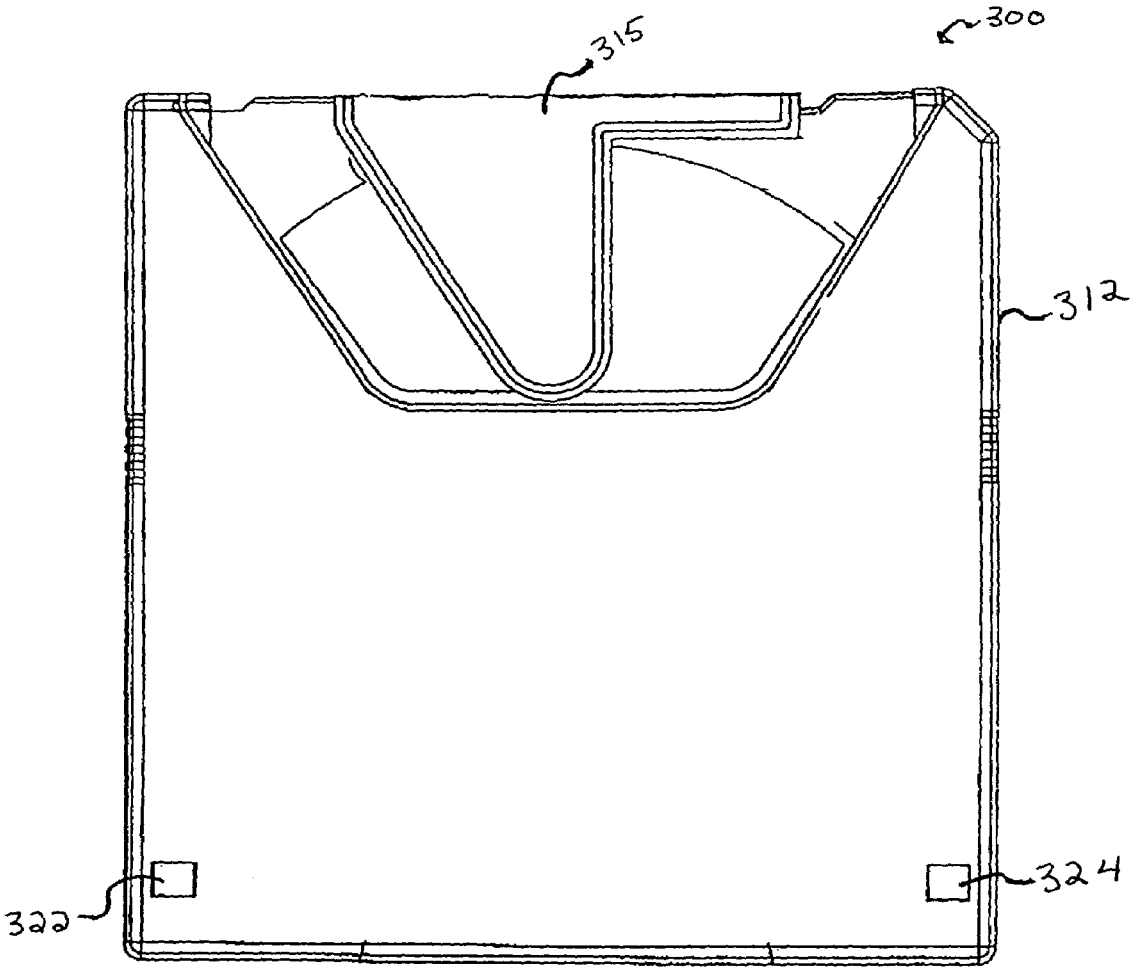


Figure 3A

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

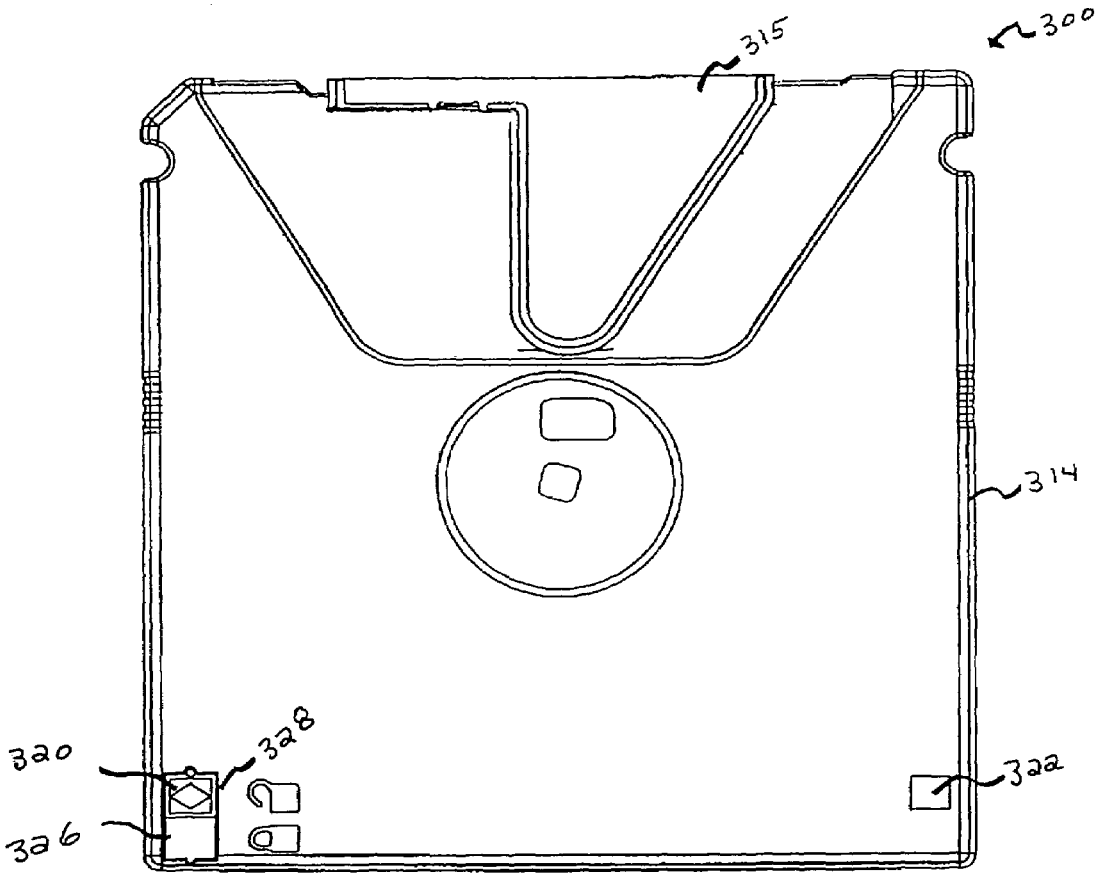


Figure 3B

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

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.