



US006976172B2

(12) **United States Patent**
Girard

(10) **Patent No.:** **US 6,976,172 B2**
(45) **Date of Patent:** **Dec. 13, 2005**

- (54) **SYSTEM AND METHOD FOR PROTECTED MESSAGING**
- (75) Inventor: **Luke E. Girard**, Santa Clara, CA (US)
- (73) Assignee: **Intel Corporation**, Santa Clara, CA (US)
- (*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 185 days.

“Wired for Management Baseline”, Version 2.0 Release, Specification to help reduce Total Cost of Ownership for business computers, Dec. 18, 1998, Intel Corporation.

* cited by examiner

Primary Examiner—Khanh Dang
(74) *Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman LLP

- (21) Appl. No.: **09/752,882**
- (22) Filed: **Dec. 28, 2000**
- (65) **Prior Publication Data**
US 2004/0221168 A1 Nov. 4, 2004
- (51) **Int. Cl.⁷** **G06F 12/14**
- (52) **U.S. Cl.** **713/193; 713/200**
- (58) **Field of Search** 713/1, 2, 200, 713/202, 156, 187, 188, 189, 190, 193

(57) **ABSTRACT**

A system and method for protected messaging. The method comprises providing a first interface to a protected storage medium to enable a pre-operating system software program access to the protected storage medium. Similarly the method also comprises providing a second interface to the protected storage medium to enable an operating system present software program access to the protected storage medium. In one embodiment, the method comprises enabling a pre-operating system software program to pass information to and receive information from an operating system present software program or another pre-operating system software program by accessing a protected storage medium via the first interface. In another embodiment, the method comprises enabling an operating system present software program to pass information to and receive information from a pre-operating system software program or another operating system present software program by accessing the protected storage medium via the second interface. The method may be implemented on any personal computing device.

- (56) **References Cited**
U.S. PATENT DOCUMENTS
5,022,077 A * 6/1991 Bealkowski et al. 711/163
5,835,594 A * 11/1998 Albrecht et al. 713/187
5,844,986 A * 12/1998 Davis 713/187
6,138,239 A * 10/2000 Veil 713/200
6,327,660 B1 * 12/2001 Patel 713/193
6,546,489 B1 * 4/2003 Frank, Jr. et al. 713/187

OTHER PUBLICATIONS
Intel^R Protected Access Architecture, Application Interface Specification, Revision 0.9.5, Aug. 2000.
Trusted Computing Platform Alliance, Copyright 2000 Compaq Computer Corporation, HewlettPackard Company, IBM Corporation, Intel Corporation, Microsoft Corporation.

24 Claims, 2 Drawing Sheets

