PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: WO 98/26535

(43) International Publication Date: 18 June 1998 (18.06.98)

(21) International Application Number: PCT/US97/21968

(22) International Filing Date: 25 November 1997 (25.11.97)

(30) Priority Data:
08/764,154 12 December 1996 (12.12.96) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors: HERBERT, Howard, C.; 16817 South 1st Drive, Phoenix, AZ 85045 (US). DAVIS, Derek, L.; 4509 East Desert Trumpet Road, Phoenix, AZ 85044 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: CRYPTOGRAPHICALLY PROTECTED PAGING SUBSYSTEM

(57) Abstract

A physically secure environment (1) is coupled to an insecure environment (2). The device includes an integrity check engine (13), a flash memory (15), a processor (16), a random access memory (14), a random number generator (18), an encryption/decryption engine (12), a bus interface (19), an external storage unit (4), an internal bus (17), and an external bus (7). The integrity check engine (13) performs a one-way hash on paging data. The encryption/decryption engine (12) encrypts outgoing pages and decrypts incoming pages.

