

02/12/02
2002073617

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



ACTION

(43) International Publication Date
3 January 2002 (03.01.2002)

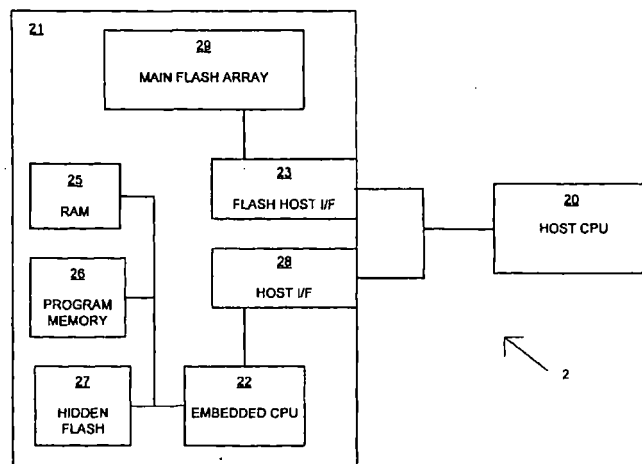
PCT

(10) International Publication Number
WO 02/001368 A3

- (51) International Patent Classification⁷: **G06F 12/14**, 1/00
- (21) International Application Number: PCT/US01/18756
- (22) International Filing Date: 7 June 2001 (07.06.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
09/604,377 27 June 2000 (27.06.2000) US
- (71) Applicant (for all designated States except US): **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **HASBUN, Robert** [US/US]; 2460 Mortara Circle, Placerville, CA 95667 (US). **VOGT, James** [US/US]; 4002 Tea Rose Court, El Dorado Hills, CA 95762 (US). **BRIZEK, John** [US/US]; 2029 Williamstown Road, Franklinville, NJ 08322 (US).
- (74) Agents: **MALLIE, Michael, J.**; Blakely Sokoloff Taylor & Zafman LLP, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 et al. (US).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- Published:
— with international search report
- (88) Date of publication of the international search report:
27 March 2003

[Continued on next page]

(54) Title: EMBEDDED SECURITY DEVICE WITHIN A NONVOLATILE MEMORY DEVICE



(57) Abstract: An improved security device to control access to restricted resources on an authorized basis. A security engine, such as a processor with associated security functions, is coupled between a first modifiable non-volatile memory, such as flash memory, and a first external interface, all on the same integrated circuit. The first memory contains secure data, and is controlled solely by the security engine, which also controls the first external interface and thereby prevents read or write access to the first memory by any external device. The integrated circuit also contains a second modifiable non-volatile memory, such as flash memory, that is coupled to a second external interface for read and write access by an external device. The second memory contains non-secure data, and is controlled through the second external interface by an external device. By isolating secure processing and storage from unsecure storage on the same integrated circuit, the security functions/data are protected from dedicated attack that could intercept or control transmissions between the two, while the benefits of placing all the functions on a single integrated circuit are achieved.

WO 02/001368 A3



162162

WO 02/001368 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.