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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 November 2006 (16.11.2006)

PCT

(10) International Publication Number
WO 2006/120302 A1

(51) International Patent Classification:
G07F 7/10 (2006.01) *H04L 9/00* (2006.01)
G06F 21/00 (2006.01) *G06K 19/07* (2006.01)

(21) International Application Number:
PCT/FI2006/050186

(22) International Filing Date: 11 May 2006 (11.05.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/128,676 13 May 2005 (13.05.2005) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **ASOKAN, Nadarajah** [CA/FI]; Ankkurinvarsi 6 K, FI-02320 Espoo (FI). **EKBERG, Jan-Erik** [FI/FI]; Seljatie 1 A 5, FI-00320 Helsinki (FI). **PAATERO, Lauri** [FI/FI]; Rikalantie 4, FI-00970 Helsinki (FI).

(74) Agent: **ESPATENT OY**; Tekniikantie 14, FI-02150 Espoo (FI).

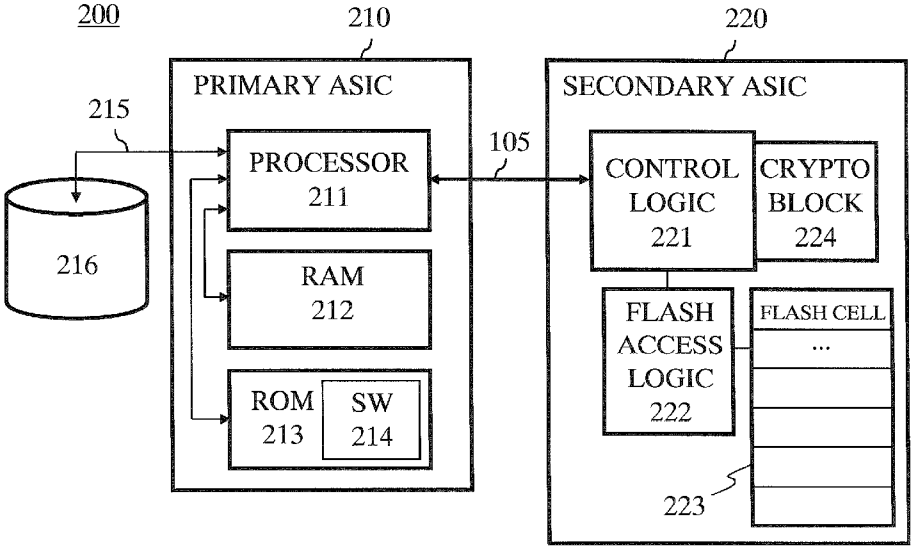
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

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.

(54) **Title:** IMPLEMENTATION OF AN INTEGRITY-PROTECTED SECURE STORAGE



(57) **Abstract:** An internal but not integrated security token is provided for a device which comprises a first integrated circuitry comprising a secure processor. The security token is provided by a second integrated circuitry separate from the first circuitry. The second integrated circuitry comprises a secure non-volatile storage. The secure processor communicates information to the second circuitry in a secure manner for the secure information to be securely stored in the secure non-volatile storage, and the second integrated circuitry communicates information stored in its secure non-volatile storage to the secure processor in a secure manner. Communications is secured by means of cryptography. The first integrated circuitry and the second integrated circuitry are internal parts of the device. An initialization method for distributing a secure key to be shared between the circuitries and to be used in cryptography is also disclosed.

WO 2006/120302 A1