

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
4 January 2007 (04.01.2007)

PCT

(10) International Publication Number  
**WO 2007/000711 A3**

(51) International Patent Classification:

*G11B 20/00* (2006.01) *H04L 9/32* (2006.01)  
*G06F 21/00* (2006.01)

(21) International Application Number:

PCT/IB2006/052082

(22) International Filing Date: 26 June 2006 (26.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

05105834.5 29 June 2005 (29.06.2005) EP

(71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **STARING, Antonius, A., M.** [NL/NL]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agents: **MAK, Theodorus, N.** et al.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(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, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, 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, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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).

Declaration under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

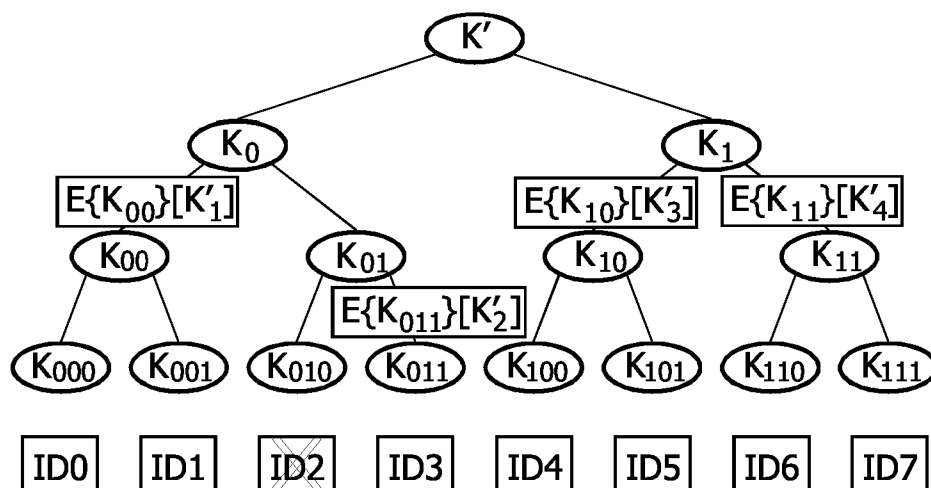
— with international search report

(88) Date of publication of the international search report:

5 July 2007

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: SYSTEM AND METHOD FOR A KEY BLOCK BASED AUTHENTICATION



(57) Abstract: The present invention relates to a system (70, 80) and a method for a key- block based authentication comprising a plurality of drive units (3) comprising a plurality of subsets, wherein a drive unit (3) has a set of node keys (KMd) and an identifier (IDd) indicating the subsets said drive unit (3) is part of and wherein an application unit (1) has a key block (AKB). In order to allow identification of a hacked drive unit (3) in order to revoke the hacked drive unit (3) from said key block based authentication, wherein said systems is to a large extent compatible with existing systems and methods for a key block based authentication, it is proposed that said keyblock (AKB) comprises a plurality of pairs of authorization and authentication keys (KAX, KR authx), wherein each pair of keys is associated with one of said subsets.