

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 March 2008 (06.03.2008)

PCT

(10) International Publication Number
WO 2008/026184 A3

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:

PCT/IB2007/053498

(22) International Filing Date: 30 August 2007 (30.08.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
06119878.4 31 August 2006 (31.08.2006) EP

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

(72) Inventors; and

(75) Inventors/Applicants (for US only): **ZYCH, Anna, K.** [PL/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL). **DOUMEN, Jeroen, M.** [NL/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL). **JONKER, Willem** [NL/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL). **HARTEL, Pieter, H.** [NL/NL]; University of Twente, PO Box 217, NL-7500 AE Enschede (NL). **PETKOVIC, Milan** [RS/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL).

(74) Agents: **GROENENDAAL, Antonius, W., M.** et al.; High Tech Campus Building 44, NL-5656 AE Eindhoven (NL).

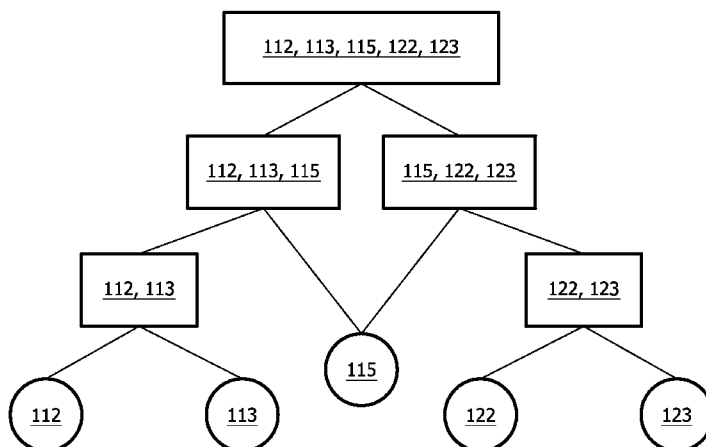
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, 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, MT, 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

[Continued on next page]

(54) Title: METHOD OF KEY MANAGEMENT



(57) Abstract: A method of key management for group-based controlled access to encrypted data, in which a decryption key for the encrypted data can be obtained by a party if the party is a member of at least one group which is authorized to access the data, the groups being organized in a hierarchical tree in which each non-leaf node represents a group and each leaf node represents a member of all groups represented by nodes hierarchically superior to the leaf node in question, characterized in that the leaf nodes are each assigned a respective arbitrarily chosen private key and corresponding public key, in that the private key associated with a particular non-leaf node is obtained by executing a key agreement protocol using a private key associated with a first child of the particular non-leaf node and a public key associated with a second child of the particular non-leaf node, and in that the private key for a group associated with a particular node is obtained by recursively obtaining the group private keys of the nodes on a path from the leaf node corresponding to the party in question and the node corresponding to the authorized group.

WO 2008/026184 A3

