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

(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).

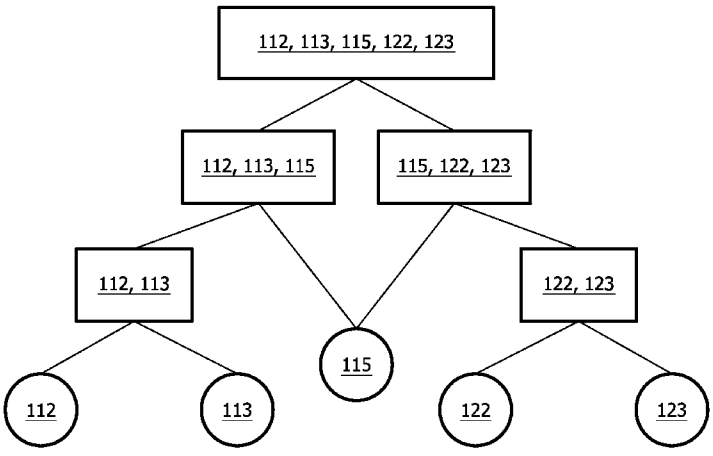
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, 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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
26 June 2008

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2007/053498

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	DE 198 47 941 A1 (DEUTSCHE TELEKOM AG [DE]) 13 April 2000 (2000-04-13) abstract page 3, line 12 - page 4, line 45 figures 1-5	1,2,8,9 3-7
Y	EP 1 505 594 A (SONY UK LTD [GB]) 9 February 2005 (2005-02-09) abstract paragraph [0029] - paragraph [0032] figures 5-8	3,5,6
Y	US 2006/015514 A1 (SUGA YUJI [JP]) 19 January 2006 (2006-01-19) abstract paragraph [0017] paragraph [0023]	4

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 April 2008	06/05/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dujardin, Corinne

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2007/053498

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/146015 A1 (CROSS DAVID B [US] ET AL) 29 July 2004 (2004-07-29) abstract paragraph [0006]	7

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2007/053498

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19847941 A1	13-04-2000	AT 247349 T	15-08-2003
		WO 0022775 A1	20-04-2000
		EP 1119942 A1	01-08-2001
		HU 0104054 A2	28-03-2002
		JP 2002527992 T	27-08-2002
EP 1505594 A	09-02-2005	CN 1581010 A	16-02-2005
		GB 2404486 A	02-02-2005
		JP 2005124146 A	12-05-2005
		US 2005025316 A1	03-02-2005
US 2006015514 A1	19-01-2006	JP 2006020292 A	19-01-2006
US 2004146015 A1	29-07-2004	US 2007088947 A1	19-04-2007