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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2008 (10.01.2008)

PCT

(10) International Publication Number
WO 2008/005789 A3

(51) International Patent Classification:
G06F 21/00 (2006.01) *H04L 9/08* (2006.01)
G06F 21/24 (2006.01)

(21) International Application Number:
PCT/US2007/072328

(22) International Filing Date: 28 June 2007 (28.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/428,367 30 June 2006 (30.06.2006) US

(71) Applicant *(for all designated States except US)*: **SCIENTIFIC-ATLANTA, INC.** [US/US]; 5030 Sugarloaf Parkway, Lawrenceville, GA 30044 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SCHLARB, John, M.** [US/US]; 4030 Boles Creek Drive, Duluth, GA 30096 (US). **BACON, Kinney, C.** [US/US]; 2820 Springtime Court, Lawrenceville, GA 30043 (US).

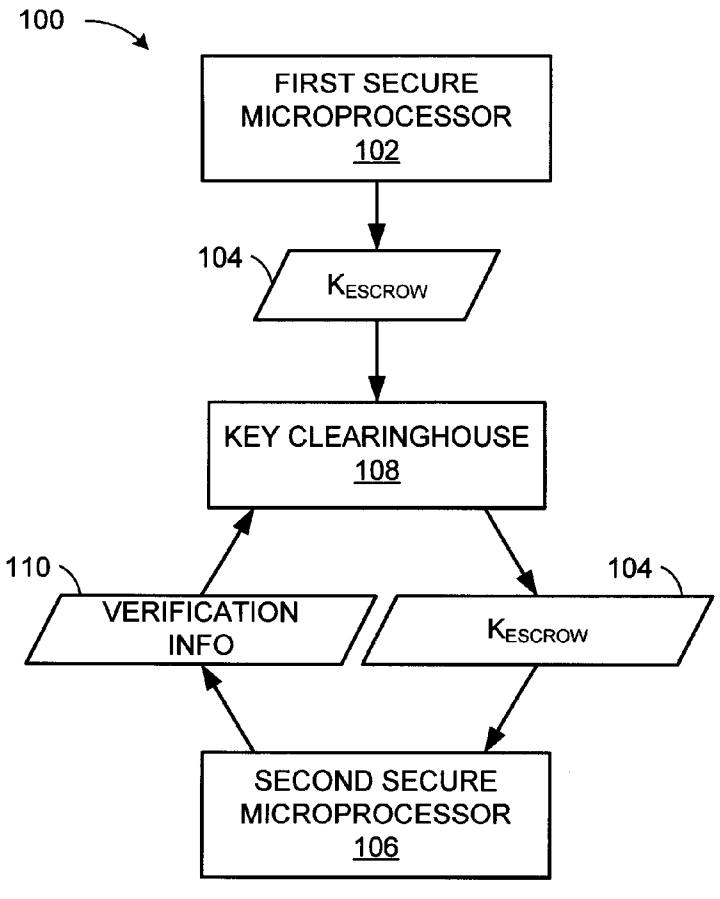
(74) Agents: **LAFFERTY, Wm., Brook** et al.; Scientific-Atlanta, Inc., Intellectual Property Dept., 5030 Sugarloaf Parkway, Lawrenceville, GA 30044 (US).

(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,

[Continued on next page]

(54) Title: SECURE ESCROW AND RECOVERY OF MEDIA DEVICE CONTENT KEYS



(57) Abstract: An embodiment of a method for secure escrow and recovery of media device content keys includes generating, with a first processor of a media device, an escrow key for encrypting a plurality of content keys, the content keys for encrypting instances of media content. The first processor of the media device encrypts the escrow key with a public key of a key clearinghouse. The escrow key, encrypted with the public key of the key clearinghouse, is stored in a storage location outside of the first processor of the media device.

WO 2008/005789 A3

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*

— *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:
17 April 2008

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/072328

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 G06F21/24 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)
G06F 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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 098 056 A (RUSNAK DAVID J [US] ET AL) 1 August 2000 (2000-08-01) column 4, line 54 - column 5, line 3 column 5, line 27 - column 6, line 53 figure 5	1-22
X	WO 01/18807 A (KONINKL PHILIPS ELECTRONICS NV [NL]) 15 March 2001 (2001-03-15) page 3, line 30 - page 4, line 5 page 4, line 15 - line 32 page 6, line 16 - line 25 figure 1	1,10,17

-/--

[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
13 February 2008	21/02/2008

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	Cartrysse, Kathy

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/072328

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MENEZES ET AL: "HANDBOOK OF APPLIED CRYPTOGRAPHY" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 567-570,546, XP002356115 ISBN: 0-8493-8523-7 paragraphs [13.5], [13.6] paragraph [13.3.1]	1-22
A	US 2003/161473 A1 (FRANSDONK ROBERT W [US]) 28 August 2003 (2003-08-28) paragraph [0231] - paragraph [0240] paragraph [0246] - paragraph [0249] figure 7	1-22

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/072328

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6098056 A	01-08-2000	NONE	
WO 0118807 A	15-03-2001	CN 1327586 A	19-12-2001
		EP 1145242 A2	17-10-2001
		JP 2003509881 T	11-03-2003
US 2003161473 A1	28-08-2003	NONE	