

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
22 July 2004 (22.07.2004)

PCT

(10) International Publication Number
WO 2004/060042 A3

(51) International Patent Classification⁷: **H04L 9/00**,
H04N 7/167

(21) International Application Number:
PCT/US2003/041296

(22) International Filing Date:
29 December 2003 (29.12.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/334,606 30 December 2002 (30.12.2002) US

(71) Applicant: **GENERAL INSTRUMENT CORPORATION** [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

(72) Inventors: **PETERKA, Petr**; 5126 Caminito Vista Lujó, San Diego, CA 92130 (US). **MEDVINSKY, Alexander**; 8873 Hampe Court, San Diego, CA 92129 (US).

(74) Agents: **SILVERIO, John** et al.; Motorola, Inc., 101 Tournament Drive, Horsham, PA 19044 (US).

(81) Designated States (*national*): 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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

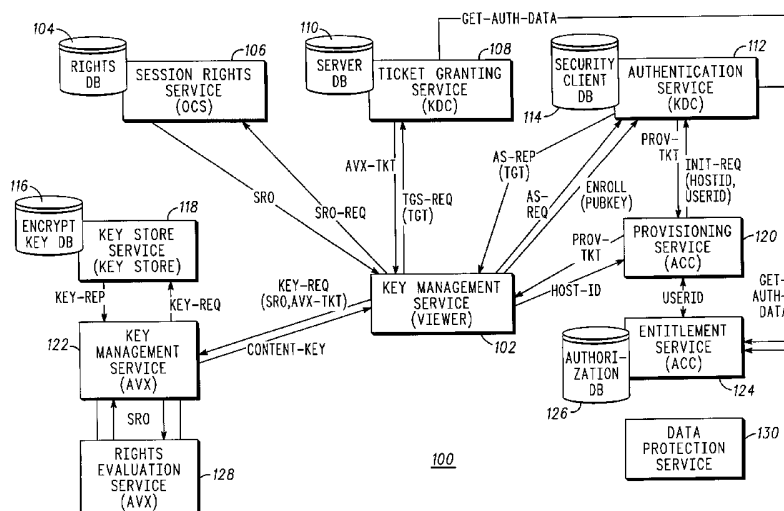
(84) Designated States (*regional*): ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF,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

Published:
— with international search report

(88) Date of publication of the international search report:
6 January 2005

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 FOR DIGITAL RIGHTS MANAGEMENT USING DISTRIBUTED PROVISIONING AND AUTHENTICATION



(57) Abstract: A digital rights management system (DRM) (100) for restricting and permitting content access in a digital content distribution network such as a network used to deliver television programming. The DRM uses distributed authentication and provisioning so that the potentially many different entities involved in the content distribution network can have localized management control. Distributed authentication can use single or multiple instances of authentication services. A ticket granting service (TGS) (108) is used to allow clients to request services. In one approach, multiple authentication services use a common key that is known to the TGS (108). In another approach, unique keys are provided to each authentication service and these keys are communicated to the TGS.

WO 2004/060042 A3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/41296

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00; H04N 7/167

US CL : 713/155; 380/227

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)

U.S. : 713/155; 380/227

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	MENEZES et al. Handbook of Applied Cryptography, Washington, D.C.: CRC Press, 1997, ISBN 0-8493-8523-7, pages 500 to 502 and pages 570 to 572.	1-16
Y	US 2001/0035814 A1 (UCHIDA, KAORU) 01 November 2001 (01.11.2001), paragraph 77	1-16
Y	US 6,073,242 A (HARDY et al.) 06 June 2000 (06.06.2000) col 3, ln 23 - col 6 ln 44	1-16

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 08 September 2004 (08.09.2004)	Date of mailing of the international search report 15 SEP 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Andrew Caldwell Telephone No. (571) 272-3578