PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 7/167, H04L 29/06 — A1

(11) International Publication Number: **WO 00/04718**

(43) International Publication Date: 27 January 2000 (27.01.00)

(21) International Application Number: PCT/IB99/01323

(22) International Filing Date: 14 July 1999 (14.07.99)

(30) Priority Data:

98401778.0	15 July 1998 (15.07.98)	EP
98401870.5	22 July 1998 (22.07.98)	EP

(71) Applicant *(for all designated States except US)*: CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André Citroën, F–75711 Paris Cedex 15 (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: DAUVOIS, Jean–Luc [FR/FR]; 19, rue Eugène Manuel, F–75116 Paris (FR). BENARDEAU, Christian [FR/FR]; 13, allée des Puisatiers, F–77600 Bussy Saint Georges (FR).

(74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Gray's Inn Road, London WC1X 8AL (GB).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(54) Title: METHOD AND APPARATUS FOR SECURE COMMUNICATION OF INFORMATION BETWEEN A PLURALITY OF DIGITAL AUDIOVISUAL DEVICES

(57) Abstract

The present invention relates to a method of providing secure communication of information between at least a first and second digital audiovisual device (30, 52) and characterised in that the first device (30) communicates to the second device (52) a certificate Ct(KpubT) comprising a transport public key KpubT encrypted by a management private key KpriMan, the second device (52) decrypting the certificate using an equivalent management public key KpubMan and thereafter using the transport public key KpubT to encrypt information sent to the first device, the first device using an equivalent private key KpriT to decrypt the information. The present invention is particularly applicable to a method of providing secure communication between a first and second decoder.

