



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04N 5/913		(11) International Publication Number: WO 99/41907
A1		(43) International Publication Date: 19 August 1999 (19.08.99)
(21) International Application Number: PCT/IB99/00303		(81) Designated States: 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, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, 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).
(22) International Filing Date: 11 February 1999 (11.02.99)		
(30) Priority Data: 98400344.2 13 February 1998 (13.02.98) HP 98401513.1 18 June 1998 (18.06.98) 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): MAILLARD, Michel [FR/FR]; 42, avenue du Maréchal Leclerc, F-28130 Maintenon (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 Grays Inn Road, London WC1X 8AL (GB).		

Published

With international search report.

(54) Title: METHOD AND APPARATUS FOR RECORDING OF ENCRYPTED DIGITAL DATA

(57) Abstract

A method of recording transmitted digital data in which transmitted digital information CW (96) is encrypted (97) using a recording encryption key E(NE) (98) and the resulting encrypted ECM message (99) stored on recording support medium. An equivalent of the recording encryption key E(NE) (100) is further encrypted by a recording transport key RT(A) (102) to form an EMM message (103) stored on the support medium together with the encrypted ECM message (99). In one embodiment, the recording transport key may be generated and managed by a central authorising unit. Alternatively, the recording transport key may be generated and managed within the decoder and recorder configuration of the user, for example, by generating the key at the recorder and communicating a version to the decoder for safekeeping.

