PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32, H04N 7/167

A1

(11) International Publication Number: **WO 99/49614**

(43) International Publication Date: 30 September 1999 (30.09.99)

(21) International Application Number: PCT/IB99/00621

(22) International Filing Date: 25 March 1999 (25.03.99)

(30) Priority Data:
98400686.6 25 March 1998 (25.03.98) EP

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

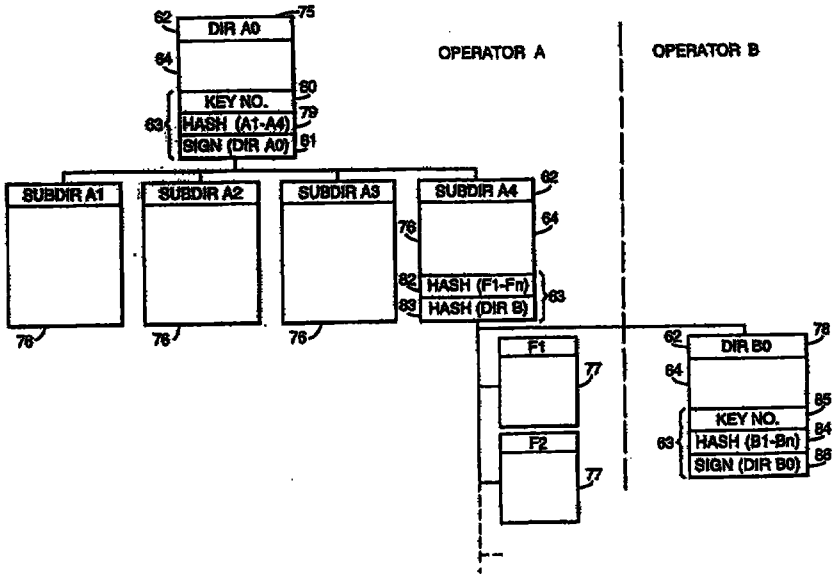
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BEUQUE, Jean–Bernard, Gérard, Maurice [FR/FR]; 132, rue Victor Hugo, F–92270 Bois–Colombes (FR).

(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: AUTHENTIFICATION OF DATA IN A DIGITAL TRANSMISSION SYSTEM



(57) Abstract

A method of authentification of data sent in a digital transmission characterised by the organisation and authentification of the data prior to transmission into a hierarchy of at least one root directory unit (75), subdirectory unit (76) and file unit (77), data in a file (77) being acted upon by an authentification algorithm and an associated file authentification value (82) stored in the referring subdirectory unit (77), this file authentification value (82) being in turn acted upon by an authentification algorithm and an associated subdirectory authentification value (79) stored in the referring root directory. Other aspects of the invention relate to the authentification of a second root directory (78) by generation of a second authentification value (83) and the authentification of data before encapsulation in tables or sections of a transport stream.