

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
25 septembre 2003 (25.09.2003)

PCT

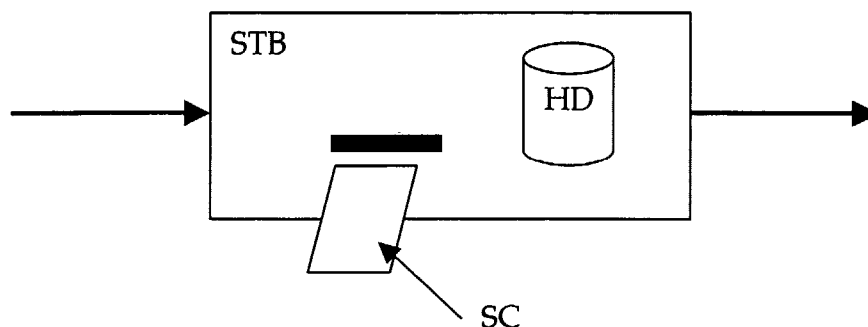
(10) Numéro de publication internationale
WO 03/079683 A2

- (51) Classification internationale des brevets⁷ : **H04N 5/913**
- (21) Numéro de la demande internationale : **PCT/IB03/00916**
- (22) Date de dépôt international : 13 mars 2003 (13.03.2003)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
0456/02 15 mars 2002 (15.03.2002) CH
- (71) Déposant (pour tous les États désignés sauf US) :
NAGRAVISION SA [CH/CH]; Route de Genève 22,
CH-1033 Cheseaux-sur-Lausanne (CH).
- (72) Inventeurs; et
(75) Inventeurs/Déposants (pour US seulement) : **LE BUHAN, Corinne** [CH/CH]; Route des Vérollys 89,
CH-1619 Les Paccots (CH). **BERTHOLET, Patrick**
[CH/CH]; Avenue de Rosemont 1, CH-1006 Lausanne
(CH). **SASSELLI, Marco** [CH/CH]; Chemin des Roches
20, CH-1803 Chardonne (CH).
- (74) Mandataire : **LEMAN CONSULTING SA**; Route de
Clémenty 62, CH-1260 Nyon (CH).
- (81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, 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, MA, MD, MG, MK, MN, MW, MX,
MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE,

[Suite sur la page suivante]

(54) Title: SECURE METHOD OF STORING ENCRYPTED DATA ON A PERSONAL DIGITAL RECORDER

(54) Titre : METHODE DE STOCKAGE SECURISE DE DONNEES ENCRYPTEES SUR UN ENREGISTREUR NUMERIQUE PERSONNEL



(57) Abstract: The invention relates to a method of storing an event encrypted by control words (CW) on a decoder (STB). The inventive method guarantees access to the aforementioned event at all times, even if certain system keys have changed for security reasons. For this purpose, the invention relates to a method of storing an event encrypted by control words (CW) in a receiving and decryption unit which is connected to a security unit (SC), said control words (CW) and the necessary rights being contained in control messages (ECM, EMM) encrypted by system keys (TK, RK). The invention is characterised in that it consists in: storing the encrypted event and the control messages (ECM) on the storage unit, and also storing the system keys (SK), which are encrypted by a pre-defined local key that is stored in the security unit (SC), on said storage unit.

(57) Abrégé : Le but de la présente invention est de proposer une méthode de stockage sur un décodeur (STB) d'un événement encrypté par des mots de contrôle (CW) qui garantisse l'accès à cet événement à n'importe quel moment, même si certaines clés du système ont changé pour des raisons de sécurité. Ce but est atteint par une méthode de stockage d'un événement encrypté par des mots de contrôle (CW) dans une unité de réception et de décryptage connectée à une unité de sécurité (SC), ces mots de contrôle (CW) et les droits nécessaires étant contenus dans des messages de gestion (ECM, EMM) encrypté par des clés systèmes (TK, RK), caractérisée en ce qu'elle consiste à stocker l'événement encrypté ainsi que les messages de contrôle (ECM) sur l'unité de stockage, et à stocker sur l'unité de stockage les clés système encryptées (SK) par une clé locale prédéfinie stockée dans l'unité de sécurité (SC).



WO 03/079683 A2



SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

- (84) **États désignés (régional)** : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (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), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.