

(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
30 octobre 2003 (30.10.2003)

PCT

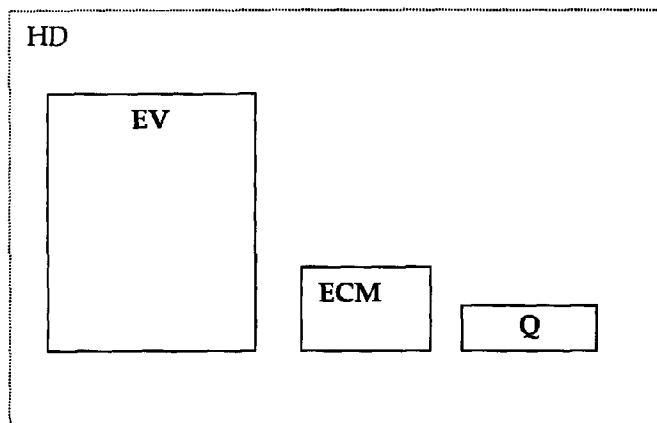
(10) Numéro de publication internationale
WO 03/090465 A1

- (51) Classification internationale des brevets⁷ :
H04N 7/167, 5/00
- (21) Numéro de la demande internationale :
PCT/IB03/01514
- (22) Date de dépôt international : 15 avril 2003 (15.04.2003)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
0664/02 19 avril 2002 (19.04.2002) CH
- (71) Déposant (pour tous les États désignés sauf US) : NA-
GRAVISION SA [CH/CH]; 22, route de Genève, CH-1033
Cheseaux-sur-Lausanne (CH).
- (72) Inventeur; et
(75) Inventeur/Déposant (pour US seulement) : SASSELLI,
Marco [CH/CH]; 20, chemin des Roches, CH-1803
Chardonne (CH).
- (74) Mandataire : ROULET, Pierre; Leman Consulting SA,
62, route de Clémenty, 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,
SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD FOR MANAGING THE RIGHTS OF AN ENCRYPTED CONTENT STORED ON A PERSONAL DIGI-
TAL RECORDER

(54) Titre : METHODE DE GESTION DES DROITS D'UN CONTENU ENCRYPTÉ ET STOCKÉ SUR UN ENREGISTREUR
NUMÉRIQUE PERSONNEL



(57) Abstract: The aim of the invention is to provide a method for storing an event which is encrypted by control words (CW) guaranteeing access to said event at any moment, even if certain modifications occur in the designation of the identifiers of said events between the moment of storage and the moment of visualization. This is achieved by means of a method for storing such an event in a receiving and decrypting unit (STB) connected to a security unit (SC), said control words (CW) and the required rights being contained in control messages (ECM). The inventive method is characterized in that it comprises the following steps: the encrypted event is stored, along with the control messages (ECM), on the storage unit; the control messages (ECM) are transmitted to the

security unit (SC); verification occurs as to whether the access rights to said event are contained in the security unit (SC), if this is the case, a receipt (Q) is provided for all or part of the control message (ECM) by means of a secret key (K) which is contained in the security unit (SC) and is proper to each security unit; said receipt (Q) is stored on the storage unit.

(57) Abrégé : Le but de la présente invention est de proposer une méthode de stockage 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 modifications dans la désignation des identifiants de ces événements sont intervenues entre le moment du stockage et le moment de la visualisation. Ce but est atteint par une méthode de stockage d'un tel événement dans une unité de réception et de décryptage (STB) connectée à une unité de sécurité (SC), ces mots de contrôle (CW) et les droits nécessaires étant contenus dans des messages de contrôle (ECM), caractérisée en ce qu'elle comprend les étapes suivantes: -à stocker l'événement encrypté ainsi que les messages de contrôle (ECM) sur l'unité de stockage, -à transmettre à l'unité de sécurité (SC) les messages de contrôle (ECM), -à vérifier si les droits d'accès à cet événement sont contenus dans l'unité de sécurité (SC), -dans l'affirmative, à déterminer une quittance (Q) sur tout ou partie du message de contrôle (ECM) grâce à une clé secrète (K) contenue dans l'unité de sécurité (SC) et propre à chaque unité de sécurité, -à stocker cette quittance (Q) sur l'unité de stockage.

WO 03/090465 A1



(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 :

— avec rapport de recherche internationale

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.