(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
20 mars 2003 (20.03.2003)

PCT

(10) Numéro de publication internationale
WO 03/024092 A1

(51) Classification internationale des brevets[7] : H04N 5/00, 7/24

(21) Numéro de la demande internationale :
PCT/IB02/03739

(22) Date de dépôt international :
10 septembre 2002 (10.09.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1682/01 12 septembre 2001 (12.09.2001) 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) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **ROBERT, Arnaud** [CA/CH]; Dufourstrasse 22, CH-3005 Berne (CH).

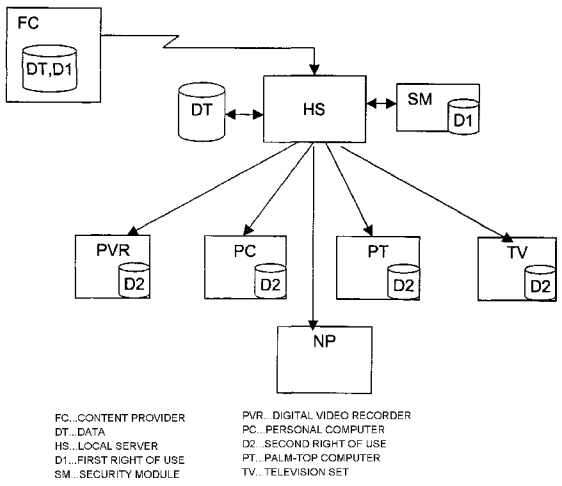
(74) Mandataire : **LEMAN CONSULTING SA**; Route de Clémenty 62, CH-1260 Nyon (CH).

(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,

[Suite sur la page suivante]

(54) Title: METHOD FOR DATA BROADCAST BETWEEN A LOCAL SERVER AND LOCAL PERIPHERALS

(54) Titre : MÉTHODE DE DIFFUSION DE DONNÉES ENTRE UN SERVEUR LOCAL ET DES PÉRIPHÉRIQUES LOCAUX



(57) **Abstract:** The invention aims at providing domestic broadcasting of conditional access encrypted data without limitation concerning the type of terminal used while guaranteeing that said broadcast will not exceed said limit. This is achieved by a method for encrypted data broadcasting between a local server connected to one or more local peripherals, said local server comprising security means responsible for acquiring a first right of use of said data, characterized in that it consists in: transmitting the encrypted data from the local server to a peripheral; extracting from the first right a second right corresponding to the part required for decrypting the data in the peripherals; encrypting by the security module the second right with a matching key particular to the couple formed by the local server security module and the peripheral security module; transmitting said encrypted second right to the local peripheral; decrypting with the matching key the second right with the peripheral security means; decrypting by the peripheral the data encrypted with the second right.

(57) **Abrégé :** Le but de la présente invention est de permettre la diffusion domestique de données encryptées à accès conditionnel sans limitation au type de terminal utilisé tout en garantissant que cette diffusion ne pourra aller au-delà de cette limite.Ce but est atteint

[Suite sur la page suivante]

WO 03/024092 A1

LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, 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, IE, IT, LU, MC, NL, PT, SE, 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.

par une méthode de diffusion de données encryptées entre un serveur local connecté à un ou des périphériques locaux, ce serveur local comprenant des moyens de sécurité en charge d'acquérir un premier droit d'utilisation de ces données, caractérisée en ce quelle consiste à: - transmettre les données encryptées du serveur local vers un périphérique,- extraire du premier droit un second droit correspondant à la partie nécessaire au décryptage des données dans les périphériques,- encrypter par le module de sécurité le second droit par une clé d'appariement propre au couple formé par le module de sécurité du serveur local et le module de sécurité du périphérique,- transmettre ce second droit encrypté au périphérique local,- décrypter à l'aide de la clé d'appariement le second droit par les moyens de sécurité du périphérique,- décrypter par le périphérique les données encryptées par le second droit.