

(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
4 juillet 2002 (04.07.2002)

PCT

(10) Numéro de publication internationale
WO 02/052515 A1

(51) Classification internationale des brevets⁷ : **G07F 7/10**

(21) Numéro de la demande internationale :
PCT/IB01/02603

(22) Date de dépôt international :
19 décembre 2001 (19.12.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
2000 2519/00 22 décembre 2000 (22.12.2000) 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) : **JAQUIER, Jean-Luc** [CH/CH]; Route de Corsy 35, CH-1093 La Con-
version (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, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK,
SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA,
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, CH, CY, DE, DK, ES, FI, FR, GB, GR,
IE, IT, LU, MC, NL, PT, SE, 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
- avant l'expiration du délai prévu pour la modification des
revendications, sera republiée si des modifications sont
reçues

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

(54) Title: MATCH CONTROL METHOD

(54) Titre : MÉTHODE DE CONTRÔLE D'APPARIEMENT

(57) Abstract: The invention aims at providing a method which guarantees encryption of data exchanged between a security module and a user unit through a matching key specific to the user unit/security module pair, while allowing the possibility to the security module to be matched with other units. Therefor, the invention provides a method which consists in: detection by the user unit whether the connected security module is matched therewith; if that is so, using a unique key specific to the user unit/security module pair to encrypt the exchanged data; otherwise, requesting from the management centre authorisation to be matched with said security module, the request being accompanied by identifiers of the user unit and of the security module; verification by the management centre the conformity of said matching and transmission of the result to the user unit; if authorisation is granted, establishing a unique key specific to the user unit/security module pair to encrypt the exchanged data.

(57) Abrégé : Le but de la présente invention est de proposer une méthode qui garantit l'encryptage des données échangées un module de sécurité et une unité d'utilisateur par une clé d'appariement propre au couple unité d'utilisateur / module de sécurité, en toutefois laissant la possibilité au module de sécurité d'être apparié avec d'autres unités d'utilisateur. Selon l'invention, ce but est atteint par une méthode consistant à :- détecter par l'unité d'utilisateur si le module de sécurité connecté lui est apparié, - dans l'affirmative, utiliser une clé unique propre au couple unité d'utilisateur / module de sécurité pour encrypter les données échangées, - dans la négative, requérir auprès du centre de gestion l'autorisation de s'apparier avec ce module de sécurité, requête accompagnée des identifiants de l'unité d'utilisateur et du module de sécurité, - vérifier par le centre de gestion la conformité de cet appariement et transmettre le résultat à l'unité de l'utilisateur, - si l'autorisation est donnée, établir une clé unique propre au couple unité d'utilisateur / module de sécurité pour encrypter les données échangées.

WO 02/052515 A1