

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

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



162162

(43) Date de la publication internationale
18 juillet 2002 (18.07.2002)

PCT

(10) Numéro de publication internationale
WO 02/056592 A1

(51) Classification internationale des brevets⁷ :

H04N 7/167

(21) Numéro de la demande internationale :

PCT/IB02/00106

(22) Date de dépôt international :

15 janvier 2002 (15.01.2002)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

01/0061

16 janvier 2001 (16.01.2001) CII

(71) Déposant (pour tous les États désignés sauf US) : NA-
GRACARD S.A. [CH/CH]; Route de Genève 22, CH-1033
Cheseaux-sur-Lausanne (CH).

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : NICOLAS,
Christophe [CH/CH]; Rue de Lausanne 59, CH-1028
Préverenges (CH).

(74) Mandataire : LEMAN CONSULTING S.A.; 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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI,
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, 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, 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
— entièrement sous forme électronique (sauf la présente page
de couverture) et disponible sur demande auprès du Bureau
international

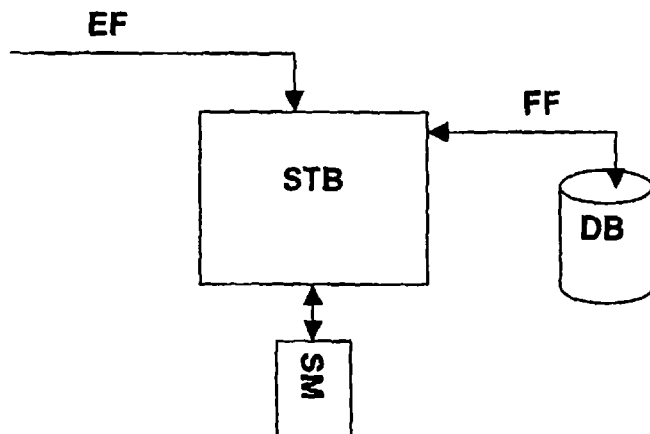
En ce qui concerne les codes à deux lettres et autres abrégia-
tions, se référer aux "Notes explicatives relatives aux codes et
abréviations" figurant au début de chaque numéro ordinaire de
la Gazette du PCT.

(54) Title: METHOD FOR STORING ENCRYPTED DATA

(54) Titre : METHODE POUR STOCKER DES DONNEES ENCRYPTEES



G00002



(57) Abstract: The invention concerns a method for pre-
venting decryption of a file of keys of a set of data stored
on a storage unit (DB) of a decoder (STB), the latter com-
prising a security module (SM), which may enable nu-
merous malevolent users to take advantage of said prod-
uct illegally. Said method consists in retrieving from a
flow of encrypted data the data to be sent to the storage
unit (DB) and in re-encrypting the data before trans-
ferring them into the storage unit (DB) with at least a unique
key (K1, K2).

(57) Abrégé : Le but de la présente invention est de
proposer une méthode pour empêcher que le décryptage
d'un fichier de clés d'un ensemble de données stocké
sur une unité de stockage (DB) d'un décodeur (STB),
ce dernier comprenant un module de sécurité (SM),
permette à de nombreux utilisateurs malveillants de

bénéficier de ce produit illicitement. Cette méthode consiste donc à extraire d'un flux de données encryptées les données à envoyer
vers l'unité de stockage (DB) et à re-encrypter les données avant leurs transferts dans l'unité de stockage (DB) par au moins une
clé (K1, K2) unique.

WO 02/056592 A1